



UNIVERSITÀ DI PISA

Facoltà di Scienze Matematiche, Fisiche e Naturali
Dipartimento di Matematica “Leonida Tonelli”
Corso di Laurea in Matematica

La teoria di Picard-Vessiot

**Una introduzione con applicazione alle
equazioni differenziali Fuchsiane**

Candidato
Mattia Puddu

Relatore
Prof. Paolo Acquistapace

A.A. 2017/2018

Introduzione	Pagina III
---------------------	-------------------

Capitolo 1

Nozioni preliminari	Pagina 1
----------------------------	-----------------

1.1 Prodotto tensoriale	1
1.1.1 Prodotto tensoriale di moduli	1
1.1.2 Prodotto tensoriale di algebre	3
1.2 Localizzazione	4
1.3 Algebra differenziale	6
1.3.1 Derivazioni	6
1.3.2 Anelli e campi differenziali	9
1.3.3 Operatori differenziali	11

Capitolo 2

Estensioni di Picard-Vessiot	Pagina 13
-------------------------------------	------------------

2.1 Definizioni	13
2.2 Il Wronskiano	14
2.3 Esistenza di un'estensione di Picard-Vessiot	18
2.4 Unicità di un'estensione di Picard-Vessiot	19

Capitolo 3

Il gruppo di Galois differenziale	Pagina 23
--	------------------

3.1 Richiami di teoria di Galois	23
3.2 Il gruppo di Galois differenziale	25
3.2.1 Un'ulteriore caratterizzazione delle estensioni di Picard-Vessiot	27
3.2.2 Esempi	28
3.3 Estensioni particolari	32
3.4 Gruppi algebrici	34
3.5 La corrispondenza di Galois	37

Capitolo 4

Equazioni differenziali Fuchsiane **Pagina 41**

4.1 Definizioni e prime proprietà 41

4.2 Soluzioni formali ed equazione indiciale 43

 4.2.1 Soluzioni nell'intorno di un punto regolare 45

 4.2.2 Soluzioni nell'intorno di un punto singolare regolare 47

4.3 Monodromia 51

4.4 L'equazione ipergeometrica di Gauss 53

4.5 Alcuni risultati sul gruppo di Galois differenziale 57

4.6 Estensioni di Liouville 59

Bibliografia **Pagina 62**

Indice analitico **Pagina 64**

Introduzione

Nei primi anni del diciannovesimo secolo, il matematico francese Évariste Galois (1811-1832) mise in luce alcune relazioni tra le radici di un polinomio $p(x) \in \mathbb{Q}[x]$ irriducibile, il suo campo di spezzamento e il gruppo degli automorfismi di quest'ultimo che lasciano fissi gli elementi di \mathbb{Q} (noto oggi come gruppo di Galois dell'estensione), enunciando e dimostrando il teorema di corrispondenza di Galois e gettando così le basi della sua teoria. La teoria di Galois produsse conseguenze importanti, come la non esistenza di una formula generale per il calcolo delle radici di un polinomio $p(x) \in \mathbb{Q}[x]$ di grado superiore al quarto, in cui compaiano solo le operazioni elementari e l'estrazione di radice; lo stesso Galois provò che l'esistenza di una tale formula per un dato polinomio è vincolata alla risolubilità del corrispondente gruppo di Galois, ovvero all'esistenza di una serie normale abeliana per tale gruppo.

Qualche decennio più avanti, il matematico norvegese Sophus Lie (1842-1899) tentò di sviluppare una teoria analoga a quella di Galois, ma avente come oggetto le equazioni differenziali. I matematici francesi Émile Picard (1856-1941) ed Ernest Vessiot (1865-1952) raccolsero l'eredità di Galois e Lie e svilupparono una teoria avente molte similitudini con la teoria di Galois classica. Anche le conseguenze furono simili: i due, dopo aver introdotto il gruppo di Galois differenziale associato a un'equazione differenziale ordinaria lineare omogenea, dimostrarono che quest'ultima è risolubile per quadrature se e solo se il suo gruppo di Galois differenziale è risolubile.

La teoria di Picard e Vessiot fu infine rivisitata dal matematico americano Ellis Kolchin (1916-1991), che mediante la sua teoria sui gruppi algebrici la formalizzò e la estese, dimostrando l'analogo del teorema di corrispondenza di Galois e che il gruppo di Galois differenziale è un gruppo algebrico lineare.

Teoria di Galois classica	Teoria di Picard-Vessiot
Polinomio	Operatori differenziali lineari
Radici di un polinomio	Soluzioni di un'equazione differenziale
Campo di spezzamento	Estensione di Picard-Vessiot
Gruppo di Galois	Gruppo di Galois differenziale
Gruppo di Galois risolubile	Gruppo di Galois risolubile

Figura 1: Similitudini tra la teoria di Galois classica e la teoria di Picard-Vessiot

Come forse si può intuire da questa breve introduzione storica, la teoria di Picard-Vessiot abbraccia molti settori della matematica, come l'algebra, l'analisi e anche la geometria algebrica: è pertanto molto difficile riuscire ad avere una sua visione esaustiva senza scavare a fondo in ognuno di questi settori. Lo scopo di questa tesi è presentare la teoria, dimostrando alcuni fra i suoi principali risultati e vedendo una sua applicazione alle equazioni differenziali Fuchsiane.

Nel capitolo 1 richiameremo alcuni strumenti ed alcune nozioni che ci saranno utili nel seguito: introdurremo le strutture algebriche di prodotto tensoriale e di localizzazione con le loro principali proprietà, e le nozioni di base dell'algebra differenziale.

Nel capitolo 2 definiremo le estensioni di Picard-Vessiot, e mediante alcuni strumenti, come il Wronskiano, analizzeremo le proprietà richieste nella definizione. Infine, affronteremo il problema dell'esistenza e dell'unicità di tali estensioni: dimostreremo che le estensioni di Picard-Vessiot esistono, e sono uniche a meno di isomorfismo.

Nel capitolo 3 richiameremo i principali risultati della teoria di Galois classica e vedremo più da vicino il suo legame con la teoria di Picard-Vessiot. In particolare, dopo aver studiato diversi esempi e introdotto i gruppi algebrici, enunceremo i teoremi di Kolchin: il primo di questi teoremi caratterizza i gruppi di Galois differenziali, mentre il secondo è l'analogo del teorema fondamentale della teoria di Galois classica. Di quest'ultimo teorema dimostreremo la corrispondenza di Galois fra i sottocampi di un'estensione di Picard-Vessiot e i sottogruppi chiusi (rispetto a una topologia opportuna) del gruppo di Galois differenziale corrispondente.

Nel capitolo 4 vedremo un'applicazione della teoria di Picard-Vessiot alle equazioni differenziali Fuchsiane. Vedremo il problema dell'esistenza locale di soluzioni e vedremo come le soluzioni si raccordano, introducendo il gruppo di monodromia. Infine, dopo un primo studio dell'equazione ipergeometrica di Gauss, a cui sono riconducibili diverse equazioni aventi una discreta importanza, come l'equazione di Schrödinger e l'equazione di Bessel, presenteremo alcuni risultati che caratterizzano un certo tipo di soluzioni di un'equazione Fuchsiana in termini del suo gruppo di Galois differenziale.

*"... E dirò sempre le stesse cose
viste sotto mille angoli diversi..."*

*"... Io invece sono stato
in piedi tutta notte
per trovarle ad una ad una
le mie risposte esatte..."*

*"... Eccomi qua
sono venuto a vedere
lo strano effetto che fa..."*

CAPITOLO 1

Nozioni preliminari

Introduzione

Richiamiamo alcuni degli strumenti necessari per poter sviluppare la teoria di Picard-Vessiot. Dopo aver introdotto le strutture algebriche di prodotto tensoriale e di localizzazione, che ci serviranno per provare l'esistenza e l'unicità delle estensioni di Picard-Vessiot nel secondo capitolo, descriviamo i principali oggetti dell'algebra differenziale: in particolare, presentiamo il concetto di derivazione, di campo differenziale e di operatore differenziale.

1.1. Prodotto tensoriale

1.1.1. Prodotto tensoriale di moduli

Sia \mathcal{R} un anello commutativo con unità, e siano \mathcal{M}, \mathcal{N} due \mathcal{R} -moduli.

Teorema 1.1. (Esistenza e unicità del prodotto tensoriale) *Esistono un \mathcal{R} -modulo \mathcal{T} e una mappa \mathcal{R} -bilineare $\phi : \mathcal{M} \times \mathcal{N} \rightarrow \mathcal{T}$ che verificano la seguente proprietà:*

- Per ogni \mathcal{R} -modulo \mathcal{P} e per ogni mappa \mathcal{R} -bilineare $\psi : \mathcal{M} \times \mathcal{N} \rightarrow \mathcal{P}$ esiste un'unica mappa $\psi' : \mathcal{T} \rightarrow \mathcal{P}$ tale che il diagramma seguente è commutativo:

$$\begin{array}{ccc} \mathcal{M} \times \mathcal{N} & \xrightarrow{\psi} & \mathcal{P} \\ \phi \downarrow & \circlearrowright & \nearrow \psi' \\ \mathcal{T} & & \end{array}$$

Figura 1.1:
Costruzione del prodotto tensoriale

Inoltre, \mathcal{T} e ϕ sono univocamente determinati a meno di isomorfismo.

Dimostrazione

Dividiamo la dimostrazione in due parti:

Unicità Supponiamo che sia \mathcal{T}_1 e $\phi_1 : \mathcal{M} \times \mathcal{N} \rightarrow \mathcal{T}_1$, sia \mathcal{T}_2 e $\phi_2 : \mathcal{M} \times \mathcal{N} \rightarrow \mathcal{T}_2$ verifichino la proprietà. Allora esistono e sono uniche due mappe $\phi'_1 : \mathcal{T}_2 \rightarrow \mathcal{T}_1$, $\phi'_2 : \mathcal{T}_1 \rightarrow \mathcal{T}_2$ tali che i seguenti diagrammi sono commutativi:

$$\begin{array}{ccc}
 \mathcal{M} \times \mathcal{N} & \xrightarrow{\phi_2} & \mathcal{T}_2 \\
 \phi_1 \downarrow & \circlearrowright & \nearrow \phi'_2 \\
 \mathcal{T}_1 & &
 \end{array}
 \qquad
 \begin{array}{ccc}
 \mathcal{M} \times \mathcal{N} & \xrightarrow{\phi_1} & \mathcal{T}_1 \\
 \phi_2 \downarrow & \circlearrowright & \nearrow \phi'_1 \\
 \mathcal{T}_2 & &
 \end{array}$$

$$\phi_2 = \phi'_2 \circ \phi_1 \qquad \phi_1 = \phi'_1 \circ \phi_2$$

Dunque

$$\phi_2 = \phi'_2 \circ \phi'_1 \circ \phi_2 \Rightarrow \phi'_2 \circ \phi'_1 = \text{Id}_{\mathcal{T}_2},$$

e allo stesso tempo

$$\phi_1 = \phi'_1 \circ \phi'_2 \circ \phi_1 \Rightarrow \phi'_1 \circ \phi'_2 = \text{Id}_{\mathcal{T}_1}.$$

Pertanto, le mappe ϕ'_2 e ϕ'_1 sono una l'inversa dell'altra, cioè ϕ'_1 è un isomorfismo.

Esistenza Sia \mathcal{A} l' \mathcal{R} -modulo libero generato da $\mathcal{M} \times \mathcal{N}$ ¹, e sia $\iota : \mathcal{M} \times \mathcal{N} \rightarrow \mathcal{A}$ l'immersione naturale di $\mathcal{M} \times \mathcal{N}$ in \mathcal{A} : nel seguito, denoteremo con $m \odot n$ l'elemento $\iota(m, n)$ per ogni $m \in \mathcal{M}$, $n \in \mathcal{N}$. Sia poi \mathcal{B} il sottomodulo di \mathcal{A} generato, al variare di $a \in \mathcal{R}$ e di $x, x' \in \mathcal{M}$, $y, y' \in \mathcal{N}$, dagli elementi della forma

$$\begin{aligned}
 &(x + x') \odot y - x \odot y - x' \odot y, \\
 &x \odot (y + y') - x \odot y - x \odot y', \\
 &(ax) \odot y - a(x \odot y), \\
 &x \odot (ay) - a(x \odot y).
 \end{aligned}$$

Consideriamo il quoziente $\mathcal{T} = \mathcal{A}/\mathcal{B}$, e la mappa $\phi = \pi \circ \iota$, dove abbiamo denotato con $\pi : \mathcal{A} \rightarrow \mathcal{T}$ la mappa di proiezione al quoziente: nel seguito, denoteremo con $m \otimes n$ l'elemento $\phi(m, n)$ per ogni $m \in \mathcal{M}$, $n \in \mathcal{N}$. Osserviamo che ϕ è \mathcal{R} -bilineare e che $\phi(\mathcal{M} \times \mathcal{N}) = \{m \otimes n : m \in \mathcal{M}, n \in \mathcal{N}\}$ genera \mathcal{T} .

Proviamo che \mathcal{T} e ϕ verificano la proprietà richiesta: se $\psi : \mathcal{M} \times \mathcal{N} \rightarrow \mathcal{P}$ è una mappa \mathcal{R} -bilineare, osserviamo che può essere estesa, per linearità, a un omomorfismo di \mathcal{R} -moduli $\psi' : \mathcal{A} \rightarrow \mathcal{P}$, che si annulla sull'insieme di generatori di \mathcal{B} con cui è stato definito, e quindi su tutto \mathcal{B} . Per il primo teorema di omomorfismo è ben definita una mappa $\bar{\psi} : \mathcal{T} \rightarrow \mathcal{P}$ tale che $\bar{\psi}(x \otimes y) = \psi(x, y)$. Infine, osserviamo che tale mappa è univocamente determinata da questa condizione.

□

Chiameremo \mathcal{T} il *prodotto tensoriale* di \mathcal{M} e \mathcal{N} , e lo denoteremo con $\mathcal{M} \otimes_{\mathcal{R}} \mathcal{N}$, o più semplicemente con $\mathcal{M} \otimes \mathcal{N}$, se non c'è ambiguità. La proprietà nell'enunciato del teorema precedente è nota come la *proprietà universale del prodotto tensoriale*.

¹ $\mathcal{A} = \mathcal{R}^{(\mathcal{M} \times \mathcal{N})}$. Gli elementi di \mathcal{A} sono, al variare di $\alpha_1, \dots, \alpha_N \in \mathcal{R}$ e $(m_1, n_1), \dots, (m_N, n_N) \in \mathcal{M} \times \mathcal{N}$, dati da

$$\sum_{k=1}^N \alpha_k (m_k, n_k).$$

I *tensori* sono gli elementi del prodotto tensoriale: quelli non nulli della forma $x \otimes y$ si diranno tensori di rango 1. Per questi ultimi abbiamo delle semplici regole di calcolo: per ogni $a \in \mathcal{R}$, $m, m' \in \mathcal{M}$ e $n, n' \in \mathcal{N}$,

$$\begin{aligned} 0 \otimes n &= m \otimes 0 = 0 \otimes 0, \\ (m + m') \otimes n &= m \otimes n + m' \otimes n, \\ m \otimes (n + n') &= m \otimes n + m \otimes n', \\ (am) \otimes n &= m \otimes (an) = a(m \otimes n). \end{aligned}$$

Non è detto che tutti i tensori siano di rango 1, ma ogni tensore si può scrivere come combinazione lineare di questi ultimi: per il principio di induzione, per ogni tensore non nullo esiste il più piccolo intero positivo $r \in \mathbb{N}$ tale che quest'ultimo si possa scrivere come somma di r tensori di rango 1: diremo che r è il rango di tale tensore.

Esempio 1.1. *Il prodotto tensoriale $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ è nullo se m, n sono coprimi: infatti, in tal caso, esistono $a, b \in \mathbb{Z}$ tali che $am + bn = 1$. Preso un generico tensore di rango 1, si ha*

$$x \otimes y = (am + bn)x \otimes y = a(mx) \otimes y + bx \otimes (ny) = a0 \otimes y + bx \otimes 0 = 0.$$

Più in generale, si dimostra allo stesso modo l'esistenza del prodotto tensoriale di un numero qualsiasi (ma finito) di \mathcal{R} -moduli. Si può inoltre dimostrare che, ad esempio nel caso di tre \mathcal{R} -moduli $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3$, il prodotto tensoriale è associativo, nel senso che esiste un isomorfismo $\psi : (\mathcal{M}_1 \otimes \mathcal{M}_2) \otimes \mathcal{M}_3 \rightarrow \mathcal{M}_1 \otimes (\mathcal{M}_2 \otimes \mathcal{M}_3)$ (a tal proposito, si veda ad esempio [AM69]).

1.1.2. Prodotto tensoriale di algebre

Siano \mathcal{R}, \mathcal{S} due anelli commutativi con unità, e sia $\phi : \mathcal{R} \rightarrow \mathcal{S}$ un omomorfismo: possiamo dotare \mathcal{S} della struttura di \mathcal{R} -modulo con il prodotto

$$\begin{aligned} \mathcal{R} \times \mathcal{S} &\rightarrow \mathcal{S} \\ (x, y) &\mapsto \phi(x)y. \end{aligned}$$

In questo modo, \mathcal{S} possiede allo stesso tempo la struttura di anello e di \mathcal{R} -modulo. Quando tali strutture sono compatibili, diremo che \mathcal{S} è una *\mathcal{R} -algebra commutativa*. Date due \mathcal{R} -algebre \mathcal{M} e \mathcal{N} , diremo che $f : \mathcal{M} \rightarrow \mathcal{N}$ è un *omomorfismo di \mathcal{R} -algebre* se è sia un omomorfismo di anelli, sia un omomorfismo di \mathcal{R} -moduli.

Esempio 1.2. *Ogni anello commutativo con unità \mathcal{R} è una \mathbb{Z} -algebra, con l'omomorfismo*

$$\begin{aligned} \phi : \mathbb{Z} &\rightarrow \mathcal{R} \\ n &\mapsto n1_{\mathcal{R}}. \end{aligned}$$

Siano \mathcal{M}, \mathcal{N} due \mathcal{R} -algebre, con gli omomorfismi $\phi_{\mathcal{M}} : \mathcal{R} \rightarrow \mathcal{M}$, $\phi_{\mathcal{N}} : \mathcal{R} \rightarrow \mathcal{N}$. Poiché \mathcal{M} e \mathcal{N} sono \mathcal{R} -moduli, è possibile definire il prodotto tensoriale $\mathcal{M} \otimes \mathcal{N}$: vogliamo dotare quest'ultimo anche della struttura di anello commutativo. Osserviamo che ci basta definire il prodotto sui tensori di rango 1, e quindi estendere per linearità. Consideriamo la mappa

$$\begin{aligned} \mathcal{P} : \mathcal{M} \times \mathcal{N} \times \mathcal{M} \times \mathcal{N} &\rightarrow \mathcal{M} \otimes \mathcal{N} \\ (m, n, m', n') &\mapsto (mm') \otimes (nn'). \end{aligned}$$

Dato che \mathcal{P} è \mathcal{R} -multilineare, sfruttando l'associatività del prodotto tensoriale è allora ben definito il seguente prodotto:

$$\mu : \mathcal{T} \times \mathcal{T} \rightarrow \mathcal{T}$$

$$\left(\sum_{i=1}^{N_1} m_i \otimes n_i, \sum_{j=1}^{N_2} m'_j \otimes n'_j \right) \mapsto \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} m_i m'_j \otimes n_i n'_j.$$

Semplici verifiche mostrano che con questa operazione \mathcal{T} è un anello commutativo con unità, l'elemento $1 \otimes 1$, e quindi una \mathcal{R} -algebra, con l'omomorfismo

$$\phi : \mathcal{R} \rightarrow \mathcal{T}$$

$$x \mapsto \phi_{\mathcal{M}}(x) \otimes \phi_{\mathcal{N}}(x).$$

1.2. Localizzazione

Sia \mathcal{R} un anello commutativo con unità, e sia \mathcal{S} un suo qualsiasi sottoinsieme.

Teorema 1.2. (Esistenza e unicità della localizzazione) *Esistono una \mathcal{R} -algebra \mathcal{L} e un omomorfismo di \mathcal{R} -algebra $h : \mathcal{R} \rightarrow \mathcal{L}$, che verificano le seguenti proprietà:*

- Per ogni $s \in \mathcal{S}$, $h(s)$ è invertibile in \mathcal{L} ;
- Per ogni \mathcal{R} -algebra \mathcal{A} e per ogni omomorfismo di \mathcal{R} -algebra $\phi : \mathcal{R} \rightarrow \mathcal{A}$ tale che, per ogni $s \in \mathcal{S}$, $\phi(s)$ è invertibile in \mathcal{A} , esiste un unico omomorfismo di \mathcal{R} -algebra $\phi' : \mathcal{L} \rightarrow \mathcal{A}$ tale che il diagramma seguente è commutativo:

$$\begin{array}{ccc} \mathcal{R} & \xrightarrow{\phi} & \mathcal{A} \\ h \downarrow & \circlearrowleft & \nearrow \phi' \\ \mathcal{L} & & \end{array}$$

Figura 1.2:
Localizzazione di un anello

Inoltre, \mathcal{L} e h sono univocamente determinati a meno di isomorfismo.

Dimostrazione

Proveremo soltanto l'esistenza: l'unicità a meno di isomorfismo si dimostra esattamente come nel Teorema 1.1.

Consideriamo un insieme di variabili $X = \{x_s : s \in \mathcal{S}\}$, ognuna delle quali in corrispondenza con un elemento di \mathcal{S} , e sia $\mathcal{R}[X]$ l'anello di polinomi nelle variabili X . Sia poi \mathcal{I} l'ideale di $\mathcal{R}[X]$ generato, al variare di $s \in \mathcal{S}$, dagli elementi della forma $sx_s - 1$.

Consideriamo il quoziente $\mathcal{L} = \mathcal{R}[X]/\mathcal{I}$, e la mappa $h = \pi \circ \iota$, dove $\iota : \mathcal{R} \rightarrow \mathcal{R}[X]$ è la naturale mappa di inclusione e $\pi : \mathcal{R}[X] \rightarrow \mathcal{L}$ è la mappa di proiezione al quoziente. \mathcal{L} è chiaramente

una \mathcal{R} -algebra e h è un omomorfismo di \mathcal{R} -algebre. Proviamo che \mathcal{L} e h soddisfano le proprietà richieste:

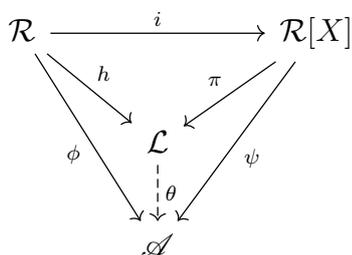


Figura 1.3:
Esistenza della localizzazione

- Per ogni $s \in \mathcal{S}$ si ha $(s + \mathcal{I})(x_s + \mathcal{I}) = 1 + \mathcal{I}$. In altre parole, $h(s) = \pi \circ i(s)$ è invertibile in \mathcal{L} ;
- Sia \mathcal{A} una \mathcal{R} -algebra, e sia $\phi : \mathcal{R} \rightarrow \mathcal{A}$ un omomorfismo di \mathcal{R} -algebre tale che $\phi(s)$ è invertibile in \mathcal{A} per ogni $s \in \mathcal{S}$. Studiamo il diagramma a sinistra, dove ψ è l'omomorfismo di \mathcal{R} -algebre

$$\begin{aligned} \psi : \mathcal{R}[X] &\rightarrow \mathcal{A} \\ x_s &\mapsto \phi(s)^{-1} \end{aligned}$$

Il triangolo superiore è chiaramente commutativo. Inoltre $\mathcal{I} \subset \text{Ker}(\psi)$, dato che, per ogni $s \in \mathcal{S}$,

$$\psi(sx_s - 1) = \phi(s)\psi(x_s) - \psi(1) = \phi(s)\phi(s)^{-1} - 1 = 1 - 1 = 0.$$

Allora, per il primo teorema di omomorfismo, è ben definito un omomorfismo di \mathcal{R} -algebre $\theta : \mathcal{L} \rightarrow \mathcal{A}$ che fa commutare il triangolo a destra, e conseguentemente

$$\theta \circ h = \theta \circ \pi \circ i = \psi \circ i = \phi.$$

Infine, osserviamo che θ è univocamente determinato, in quanto $\text{Im}(h) \cup \{h(s)^{-1} : s \in \mathcal{S}\}$ genera \mathcal{L} come \mathcal{R} -algebra. □

Chiameremo \mathcal{L} la *localizzazione* di \mathcal{R} in \mathcal{S} , e la denoteremo con $\mathcal{S}^{-1}\mathcal{R}$, e chiameremo $h : \mathcal{R} \rightarrow \mathcal{S}^{-1}\mathcal{R}$ la *mappa di localizzazione*. La seconda proprietà richiesta nel teorema precedente è nota come la *proprietà universale della localizzazione*.

Esempio 1.3. Nel caso in cui \mathcal{S} sia un sottoinsieme di \mathcal{R} moltiplicativamente chiuso, un modo alternativo di costruire $\mathcal{S}^{-1}\mathcal{R}$ è di definirlo come l'insieme quoziente della seguente relazione di equivalenza su $\mathcal{R} \times \mathcal{S}$

$$(x, s_1) \sim (y, s_2) \Leftrightarrow \text{Esiste } u \in \mathcal{S} \text{ tale che } u(xs_2 - ys_2) = 0,$$

e poi dotarlo della struttura di \mathcal{R} -algebra: in tal caso, $\mathcal{S}^{-1}\mathcal{R}$ è detto anello delle frazioni di \mathcal{R} rispetto a \mathcal{S} . La mappa di localizzazione è data da

$$\begin{aligned} h : \mathcal{R} &\rightarrow \mathcal{S}^{-1}\mathcal{R} \\ x &\mapsto [(x, 1)]. \end{aligned}$$

Nell'esempio precedente, se \mathcal{S} non è moltiplicativamente chiuso, si può comunque prendere il più piccolo sottoinsieme di \mathcal{R} con questa proprietà e contenente \mathcal{S} , che denotiamo con $\bar{\mathcal{S}}$. In tal caso si può dimostrare che $\bar{\mathcal{S}}^{-1}\mathcal{R}$ e $\mathcal{S}^{-1}\mathcal{R}$ sono isomorfi (si veda ad esempio [Rot03]).

Esempio 1.4. Se \mathcal{R} è un dominio di integrità, l'insieme $\mathcal{S} = \mathcal{R} - \{0\}$ è moltiplicativamente chiuso, e $\mathcal{S}^{-1}\mathcal{R}$ è un campo, detto campo delle frazioni di \mathcal{R} . Ad esempio, $(\mathbb{Z} - \{0\})^{-1}\mathbb{Z} \cong \mathbb{Q}$.

Concludiamo questa sezione con la seguente proprietà, che ci permette di visualizzare gli elementi di $\mathcal{S}^{-1}\mathcal{R}$ come frazioni:

Proposizione 1.1. *Sia \mathcal{R} un anello commutativo, e sia \mathcal{S} un suo sottoinsieme. Denotiamo, al solito, con $h : \mathcal{R} \rightarrow \mathcal{S}^{-1}\mathcal{R}$ la mappa di localizzazione. Comunque si prenda $z \in \mathcal{S}^{-1}\mathcal{R}$, esistono $a \in \mathcal{R}$ e $b \in \overline{\mathcal{S}}$ tali che $z = h(a)h(b)^{-1}$.*

Dimostrazione

Per il Teorema 1.2, mantenendo le stesse notazioni, z è della forma $z = f(x_1, \dots, x_n) + \mathcal{I}$, con $x_k \in X$ per ogni $k = 1, \dots, n$.

Procediamo per induzione su $n = 0, 1, \dots$. Il passo base ($n = 0$) è immediato: in tal caso f è costantemente uguale a un elemento $a \in \mathcal{R}$, e $z = h(a)$. Proviamo il passo induttivo: supponiamo che la proposizione sia verificata per $n - 1$; poniamo $J = (x_1, \dots, x_{n-1})$. Possiamo vedere $f(x_1, \dots, x_n)$ come polinomio in x_n , ovvero

$$f(x_1, \dots, x_n) = \phi_0(J) + \phi_1(J)x_n + \dots + \phi_m(J)x_n^m,$$

con $\phi_k(J) \in \mathcal{R}[J]$ per ogni $k = 1, \dots, m$. Ma in $\mathcal{S}^{-1}\mathcal{R}$ si ha $x_n = h(s)^{-1}$, per qualche $s \in \mathcal{S}$, e per ipotesi induttiva possiamo scrivere $\phi_k(J) = h(a_k)h(b_k)^{-1}$, con $a_k \in \mathcal{R}$ e $b_k \in \mathcal{S}$ per ogni $k = 0, \dots, m$. Pertanto,

$$z = \sum_{k=0}^m h(a_k)h(b_k)^{-1}h(s)^{-k} = h(s)^{-m} \sum_{k=0}^m h(a_k)h(b_k)^{-1}h(s)^{m-k} = h(a)h(b)^{-1},$$

con $a \in \mathcal{R}^2$ e $b = b_0 \dots b_m s^m$.

□

1.3. Algebra differenziale

1.3.1. Derivazioni

Sia \mathcal{R} un anello. Diremo che un'applicazione $\mathcal{D}_{\mathcal{R}} : \mathcal{R} \rightarrow \mathcal{R}$ è una *derivazione* di \mathcal{R} se verifica le seguenti proprietà: per ogni $x, y \in \mathcal{R}$,

$$\mathcal{D}_{\mathcal{R}}(x + y) = \mathcal{D}_{\mathcal{R}}(x) + \mathcal{D}_{\mathcal{R}}(y); \quad (1.1)$$

$$\mathcal{D}_{\mathcal{R}}(xy) = x\mathcal{D}_{\mathcal{R}}(y) + \mathcal{D}_{\mathcal{R}}(x)y. \quad (1.2)$$

Nel caso in cui non ci siano ambiguità, scriveremo \mathcal{D} al posto di $\mathcal{D}_{\mathcal{R}}$, denoteremo con x' la derivazione di $x \in \mathcal{R}$, e con $x'', \dots, x^{(n)}$ le sue derivazioni successive.

Esempio 1.5. *La derivata usuale è una derivazione dell'anello $\mathcal{C}^\infty(\mathbb{R})$.*

²Si ha

$$a = \sum_{k=0}^m a_k s^{m-k} \prod_{\substack{0 \leq j \leq m \\ j \neq k}} b_j$$

Esempio 1.6. *La mappa*

$$\begin{aligned} \mathcal{D}_{\text{Triv}} : \mathcal{R} &\rightarrow \mathcal{R} \\ x &\mapsto 0 \end{aligned}$$

è una derivazione di qualsiasi anello \mathcal{R} : la chiameremo derivazione banale.

Esempio 1.7. *Sia \mathcal{A} l'anello delle funzioni aritmetiche³. La mappa*

$$\begin{aligned} \mathcal{D} : \mathcal{A} &\rightarrow \mathcal{A} & \mathcal{D}\{f\} : \mathbb{N} &\rightarrow \mathbb{C} \\ f &\mapsto \mathcal{D}\{f\}, & n &\mapsto \log(n)f(n). \end{aligned}$$

è una derivazione di \mathcal{A} : infatti, la proprietà (1.1) nella definizione è banalmente verificata, e inoltre

$$\begin{aligned} \mathcal{D}\{f \star g\}(n) &= \log(n) \sum_{\substack{d \in \mathbb{N} \\ d|n}} f(d)g\left(\frac{n}{d}\right) \\ &= \sum_{\substack{d \in \mathbb{N} \\ d|n}} \log(d)f(d)g\left(\frac{n}{d}\right) + \sum_{\substack{d \in \mathbb{N} \\ d|n}} f(d) \log\left(\frac{n}{d}\right)g\left(\frac{n}{d}\right) \\ &= \mathcal{D}\{f\} \star g(n) + f \star \mathcal{D}\{g\}(n) \end{aligned}$$

(e in realtà si ha lo stesso se al posto del logaritmo utilizziamo una qualsiasi altra funzione completamente additiva).

Possiamo generalizzare una formula nota per il calcolo delle derivate successive al caso di una generica derivazione.

Proposizione 1.2. (Leibniz, derivazioni successive) *Per ogni $x, y \in \mathcal{R}$, $n \in \mathbb{N}$, vale la formula*

$$(xy)^{(n)} = \sum_{k=0}^n \binom{n}{k} x^{(n-k)} y^{(k)}.$$

Dimostrazione

Procediamo per induzione su n : il passo base ($n = 1$) è verificato per la definizione di derivazione. Supponiamo che la formula sia verificata per n : allora

$$\begin{aligned} (xy)^{(n+1)} &= ((xy)^{(n)})' = \left(\sum_{k=0}^n \binom{n}{k} x^{(n-k)} y^{(k)} \right)' \\ &= \sum_{k=0}^n \binom{n}{k} x^{(n-k+1)} y^{(k)} + \sum_{k=0}^n \binom{n}{k} x^{(n-k)} y^{(k+1)} \end{aligned}$$

³Una *funzione aritmetica* è una qualsiasi applicazione $f : \mathbb{N} \rightarrow \mathbb{C}$. Le operazioni in \mathcal{A} sono l'usuale somma tra funzioni e la convoluzione moltiplicativa:

$$\begin{aligned} \star : \mathcal{A} \times \mathcal{A} &\rightarrow \mathcal{A} & f \star g : \mathbb{N} &\rightarrow \mathbb{C} \\ (f, g) &\mapsto f \star g, & n &\mapsto \sum_{\substack{d \in \mathbb{N} \\ d|n}} f(d)g\left(\frac{n}{d}\right). \end{aligned}$$

$$\begin{aligned}
&= x^{(n+1)} + y^{(n+1)} + \sum_{k=1}^n \left[\binom{n}{k} + \binom{n}{k-1} \right] x^{(n-k+1)} y^{(k)} \\
&= x^{(n+1)} + y^{(n+1)} + \sum_{k=1}^n \binom{n+1}{k} x^{(n-k+1)} y^{(k)} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^{(n-k+1)} y^{(k)}.
\end{aligned}$$

□

Per la proposizione precedente, se $x \in \mathcal{R}$ e la sua derivazione commutano, allora

$$(x^2)' = 2xx' = 2x'x.$$

In generale, però, questo è falso.

Esempio 1.8. Sia $\mathbb{R}[x]$ l'anello dei polinomi a coefficienti reali. Una derivazione di tale anello è la derivata usuale. Definiamo sull'anello $\mathcal{R} = \mathcal{M}(2, \mathbb{R}[x])$ delle matrici di ordine 2 a coefficienti in $\mathbb{R}[x]$ la seguente applicazione:

$$\begin{aligned}
\mathcal{D} : \quad \mathcal{R} &\rightarrow \mathcal{R} \\
\begin{bmatrix} a(x) & b(x) \\ c(x) & d(x) \end{bmatrix} &\mapsto \begin{bmatrix} a'(x) & b'(x) \\ c'(x) & d'(x) \end{bmatrix}.
\end{aligned}$$

Le verifiche che \mathcal{D} sia effettivamente una derivazione di \mathcal{R} sono immediate. Tuttavia, si ha

$$\begin{aligned}
\mathcal{D} \left(\begin{bmatrix} 0 & 0 \\ 1 & x \end{bmatrix}^2 \right) &= \begin{bmatrix} 0 & 0 \\ 1 & 2x \end{bmatrix}, \\
2\mathcal{D} \left(\begin{bmatrix} 0 & 0 \\ 1 & x \end{bmatrix} \right) \begin{bmatrix} 0 & 0 \\ 1 & x \end{bmatrix} &= \begin{bmatrix} 0 & 0 \\ 2 & 2x \end{bmatrix}, \\
2 \begin{bmatrix} 0 & 0 \\ 1 & x \end{bmatrix} \mathcal{D} \left(\begin{bmatrix} 0 & 0 \\ 1 & x \end{bmatrix} \right) &= \begin{bmatrix} 0 & 0 \\ 0 & 2x \end{bmatrix}.
\end{aligned}$$

Nel seguito, supporremo che \mathcal{R} sia un anello commutativo con unità a caratteristica 0. Denoteremo con 1 l'elemento neutro del prodotto e con 0 l'elemento neutro della somma. Osserviamo subito che la derivazione di 1 è 0 : infatti

$$1' = (1 \cdot 1)' = 1 \cdot 1' + 1' \cdot 1 = 2 \cdot 1'.$$

Similmente, si verifica che anche $0' = 0$. Inoltre, se x è un elemento invertibile con inverso x^{-1} , dall'identità $xx^{-1} = 1$ si ricava $x'x^{-1} + x(x^{-1})' = 0$, e quindi

$$(x^{-1})' = -x'x^{-2}. \tag{1.3}$$

Più in generale:

Proposizione 1.3. *Se \mathcal{R} è un dominio di integrità, una derivazione \mathcal{D} di \mathcal{R} si estende univocamente al campo delle frazioni di \mathcal{R} , $\mathcal{F}(\mathcal{R})$.*

Dimostrazione

Estendiamo la derivazione \mathcal{D} nel modo seguente:

$$\mathcal{D} : \mathcal{F}(\mathcal{R}) \rightarrow \mathcal{F}(\mathcal{R})$$

$$\frac{x}{y} \mapsto \frac{x'y - xy'}{y^2}.$$

Osserviamo che, se $z \in \mathcal{R} - \{0\}$,

$$\left(\frac{xz}{yz}\right)' = \frac{(xz)'yz - xz(yz)'}{y^2z^2} = \frac{x'yz^2 + xyzz' - xy'z^2 - xyz'z'}{y^2z^2} = \frac{x'y - xy'}{y^2},$$

quindi la mappa è ben definita, in quanto non dipende dalla scelta del rappresentante. Inoltre,

$$\begin{aligned} \left(\frac{x}{y} + \frac{z}{t}\right)' &= \left(\frac{xt + yz}{yt}\right)' = \frac{(xt + yz)'yt - (xt + yz)(yt)'}{y^2t^2} \\ &= \frac{x'yt^2 + y^2z't - xy't^2 - y^2zt'}{y^2t^2} = \frac{x'y - xy'}{y^2} + \frac{z't - zt'}{t^2} = \left(\frac{x}{y}\right)' + \left(\frac{z}{t}\right)', \\ \left(\frac{xz}{yt}\right)' &= \left(\frac{xz}{yt}\right)' = \frac{(xz)'yt - xz(yt)'}{y^2t^2} = \frac{x'yzt + xyz't - xy'zt - xyz't'}{y^2t^2} \\ &= \frac{x'y - xy'}{y^2} \frac{z}{t} + \frac{x}{y} \frac{z't - zt'}{t^2} = \left(\frac{x}{y}\right)' \frac{z}{t} + \frac{x}{y} \left(\frac{z}{t}\right)'. \end{aligned}$$

Che tale estensione sia univocamente determinata è una immediata conseguenza dell'identità (1.3). □

1.3.2. Anelli e campi differenziali

Un *anello differenziale* è un anello commutativo con unità dotato di una derivazione, mentre un *campo differenziale* è un anello differenziale che è anche un campo. Dati due campi differenziali \mathbb{L}, \mathbb{K} con $\mathbb{K} \subset \mathbb{L}$, diremo che quest'ultima è un' *estensione differenziale* se $\mathcal{D}_{\mathbb{L}|\mathbb{K}} = \mathcal{D}_{\mathbb{K}}$.

Esempio 1.9. *Per l'Esempio 1.6, ogni anello commutativo con unità può essere visto come anello differenziale: basta dotarlo della sua derivazione banale.*

Esempio 1.10. *Per la Proposizione 1.3, il campo delle frazioni di un anello differenziale che è anche un dominio di integrità è un campo differenziale.*

Esempio 1.11. *L'anello delle funzioni analitiche in una variabile nel piano complesso, dotato della derivata usuale, è un anello differenziale. Essendo quest'ultimo anche un dominio di integrità, per la Proposizione 1.3 è possibile estendere univocamente tale derivazione al suo campo delle frazioni, ovvero al campo delle funzioni meromorfe in una variabile.*

Dato un anello differenziale \mathcal{R} , diremo che un suo elemento x è una *costante* se $x' = 0$. Denoteremo con $\mathcal{C}_{\mathcal{R}}$ l'insieme delle costanti in \mathcal{R} . Abbiamo già visto che 0 e 1 sono costanti, e in generale non saranno gli unici elementi dell'anello ad esserlo:

Proposizione 1.4. $\mathcal{C}_{\mathcal{R}}$ è un sottoanello di \mathcal{R} . Se \mathcal{R} è anche un campo, $\mathcal{C}_{\mathcal{R}}$ è un suo sottocampo.

Dimostrazione

Abbiamo già dimostrato che $0, 1 \in \mathcal{C}_{\mathcal{R}}$ (quindi in particolare $\mathcal{C}_{\mathcal{R}} \neq \emptyset$). Inoltre, dalla definizione di derivazione, è immediato osservare che se x è costante allora lo è anche $-x$, e che la somma e il prodotto di due costanti sono ancora delle costanti. Infine, se \mathcal{R} è un campo, come conseguenza dell'equazione (1.3) si ha che $\mathcal{C}_{\mathcal{R}}$ è un suo sottocampo. □

Tra i sottogruppi additivi di un anello, hanno particolare rilevanza gli ideali: dato un anello differenziale \mathcal{R} , diremo che $\mathcal{I} \subset \mathcal{R}$ è un *ideale differenziale* se è un ideale di \mathcal{R} e gode della seguente proprietà:

$$x \in \mathcal{I} \Rightarrow x' \in \mathcal{I},$$

ovvero se $\mathcal{D}(\mathcal{I}) \subset \mathcal{I}$. Osserviamo che grazie a quest'ultima proprietà è possibile definire una derivazione dell'anello quoziente \mathcal{R}/\mathcal{I} :

$$\begin{aligned} \overline{\mathcal{D}}: \mathcal{R}/\mathcal{I} &\rightarrow \mathcal{R}/\mathcal{I} \\ \overline{x} &\mapsto \overline{\mathcal{D}(x)}. \end{aligned}$$

Infatti se $\overline{x} = \overline{y}$, allora $x - y \in \mathcal{I}$, e dunque

$$\overline{\mathcal{D}(\overline{x})} - \overline{\mathcal{D}(\overline{y})} = \overline{\mathcal{D}(x)} - \overline{\mathcal{D}(y)} = \overline{\mathcal{D}(x) - \mathcal{D}(y)} = \overline{\mathcal{D}(x - y)} = \overline{0}.$$

Concludiamo questa sezione introducendo gli omomorfismi differenziali: se \mathcal{R} e \mathcal{S} sono due anelli differenziali, diremo che un'applicazione $f: \mathcal{R} \rightarrow \mathcal{S}$ è un *omomorfismo differenziale* se è un omomorfismo di anelli e, per ogni $x \in \mathcal{R}$, verifica la seguente proprietà:

$$f(x)' = f(x'). \tag{1.4}$$

Un omomorfismo differenziale che è anche un isomorfismo si dirà *isomorfismo differenziale*. Un isomorfismo differenziale da un anello in se stesso si dirà *automorfismo differenziale*.

Esempio 1.12. Se \mathcal{I} è un ideale differenziale, la mappa di proiezione al quoziente $\pi: \mathcal{R} \rightarrow \mathcal{R}/\mathcal{I}$ è un omomorfismo differenziale: infatti sappiamo per la teoria degli anelli che è un omomorfismo, e la proprietà (1.4) è verificata per la definizione di derivazione sull'anello quoziente.

Il primo teorema di omomorfismo si adatta bene agli anelli differenziali.

Teorema 1.3. (Primo teorema di omomorfismo per anelli differenziali) Siano \mathcal{R} e \mathcal{S} due anelli differenziali, e sia $f: \mathcal{R} \rightarrow \mathcal{S}$ un omomorfismo differenziale. Allora $\text{Ker}(f)$ è un ideale differenziale di \mathcal{R} , e

$$\begin{aligned} \overline{f}: \mathcal{R}/\text{Ker}(f) &\rightarrow \text{Im}(f) \\ \overline{x} &\mapsto f(x). \end{aligned}$$

è un isomorfismo differenziale.

Dimostrazione

Per la teoria degli anelli, $\text{Ker}(f)$ è un ideale di \mathcal{R} . Se $x \in \text{Ker}(f)$, $f(x') = f(x)' = 0$, cioè $x' \in \text{Ker}(f)$.

$$\begin{array}{ccc} \mathcal{R} & \xrightarrow{f} & \text{Im}(f) \subset \mathcal{S} \\ \pi \downarrow & \circlearrowleft & \nearrow \bar{f} \\ \mathcal{R}/\text{Ker}(f) & & \end{array}$$

Figura 1.4:

Il primo teorema di omomorfismo

Concludiamo che $\text{Ker}(f)$ è un ideale differenziale. Inoltre, per il primo teorema di omomorfismo, sappiamo che \bar{f} è un isomorfismo: infine, poiché per ogni $x \in \mathcal{R}$

$$\bar{f}(\bar{x})' = f(x)' = f(x') = \bar{f}(\bar{x}') = \bar{f}(\bar{x}'),$$

la mappa \bar{f} è un isomorfismo differenziale. \square

1.3.3. Operatori differenziali

Sia \mathbb{K} un campo differenziale con derivazione \mathcal{D} non banale: chiameremo *operatore differenziale lineare* omogeneo a coefficienti in \mathbb{K} una qualsiasi espressione della forma

$$\mathcal{L} = \sum_{k=0}^{+\infty} a_k \mathcal{D}^{(k)},$$

con $a_k \in \mathbb{K}$ per ogni $k \in \mathbb{N} \cup \{0\}$ e $a_k \neq 0$ solo per un numero finito di indici. Chiameremo *grado* dell'operatore differenziale il numero $\deg \mathcal{L} = \max\{k \in \mathbb{N} \cup \{0\} : a_k \neq 0\}$. Il termine $a_0 \mathcal{D}^{(0)} = a_0 \text{Id}$ si dirà *termine noto* dell'operatore differenziale: converremo di scrivere più semplicemente a_0 per indicare il termine noto. Diremo infine che un operatore differenziale lineare di grado n è *monico* se $a_n = 1$.

L'insieme $\mathbb{K}[\mathcal{D}]$ degli operatori differenziali lineari omogenei a coefficienti in \mathbb{K} gode di una naturale struttura di anello, che è però non commutativo: il prodotto di due operatori si svolge tenendo conto della distributività rispetto alla somma e della seguente relazione, che segue dalla Proposizione 1.2:

$$\mathcal{D}^{(\alpha)} \circ x \mathcal{D}^{(\beta)} = \sum_{k=0}^{\alpha} \binom{\alpha}{k} \mathcal{D}^{(k)}(x) \mathcal{D}^{(\alpha-k+\beta)}. \quad (1.5)$$

Esempio 1.13. Consideriamo il campo delle funzioni razionali $\mathbb{C}(z)$: due operatori differenziali lineari a coefficienti in $\mathbb{C}(z)$ sono, ad esempio,

$$\mathcal{L}_1 = z \frac{d}{dz}, \quad \mathcal{L}_2 = \frac{d}{dz} + z.$$

$$\mathcal{L}_1 \circ \mathcal{L}_2 = z \frac{d}{dz} \circ \left(\frac{d}{dz} + z \right) = z \frac{d}{dz} (1) \frac{d}{dz} + z \frac{d^2}{dz^2} + z \frac{d}{dz} (z) + z^2 \frac{d}{dz} = z \frac{d^2}{dz^2} + z^2 \frac{d}{dz} + z,$$

mentre

$$\mathcal{L}_2 \circ \mathcal{L}_1 = \left(\frac{d}{dz} + z \right) \circ z \frac{d}{dz} = \frac{d}{dz} \circ z \frac{d}{dz} + z^2 \frac{d}{dz} = \frac{d}{dz} (z) \frac{d}{dz} + z \frac{d^2}{dz^2} + z^2 \frac{d}{dz} = z \frac{d^2}{dz^2} + (z^2 + 1) \frac{d}{dz}.$$

Osserviamo che, in particolare, $\mathcal{L}_1 \circ \mathcal{L}_2 \neq \mathcal{L}_2 \circ \mathcal{L}_1$.

Estensioni di Picard-Vessiot

Introduzione

Definiamo le estensioni di Picard-Vessiot, e analizziamo le proprietà richieste nella definizione. A tal fine, introduciamo il Wronskiano, che ci permette di avere una condizione necessaria e sufficiente per la dipendenza lineare di alcuni elementi su un campo. In seguito, affrontiamo il problema dell'esistenza e unicità delle estensioni di Picard-Vessiot.

Dove non è altrimenti specificato, supponiamo che \mathbb{K} sia un campo differenziale con derivazione \mathcal{D} non banale e a caratteristica 0, che il suo campo delle costanti sia algebricamente chiuso, e che gli operatori differenziali siano lineari e omogenei, a coefficienti in \mathbb{K} .

2.1. Definizioni

Dato un operatore differenziale di grado n ,

$$\mathcal{L} = \sum_{k=0}^n a_k \mathcal{D}^{(k)}, \quad (2.1)$$

possiamo associargli l'equazione differenziale

$$\mathcal{L}(x) = \sum_{k=0}^n a_k x^{(k)} = 0. \quad (2.2)$$

Denoteremo con $\mathcal{V}_{\mathcal{L}}$ l'insieme delle soluzioni dell'equazione (2.2): si verifica immediatamente che $\mathcal{V}_{\mathcal{L}}$ è un $\mathcal{C}_{\mathbb{K}}$ -spazio vettoriale.

Vogliamo definire un qualcosa di analogo al campo di spezzamento di un polinomio nella teoria di Galois classica per gli operatori differenziali lineari omogenei. Diremo che un'estensione di campi differenziali $\mathbb{L} \supset \mathbb{K}$ è un'estensione di Picard-Vessiot per \mathcal{L} se valgono le seguenti condizioni:

- ◇ esistono n soluzioni $\mathcal{C}_{\mathbb{K}}$ -linearmente indipendenti per l'equazione (2.2), $x_1, \dots, x_n \in \mathbb{L}$ tali che $\mathbb{L} = \mathbb{K}(x_1, \dots, x_n)$;
- ◇ $\mathcal{C}_{\mathbb{L}} = \mathcal{C}_{\mathbb{K}}$.

Analizziamo le proprietà nella definizione: se la seconda proprietà è soddisfatta, parleremo di *estensioni senza costanti*. La richiesta che un'estensione di Picard-Vessiot sia senza costanti è resa chiara dall'esempio seguente.

Esempio 2.1. Consideriamo il campo differenziale $\mathbb{K} = \mathbb{C}(e^z)$, dotato della derivazione usuale, e sia u una variabile formale, tale che $u' = u$. Poniamo $\mathbb{L} = \mathbb{K}(u)$. Chiaramente, u è una nuova soluzione dell'equazione differenziale $x' - x = 0$, indipendente da e^z . L'elemento $\frac{e^z}{u}$ è però una nuova costante in \mathbb{L} :

$$\left(\frac{e^z}{u}\right)' = \frac{e^z u - e^z u'}{u^2} = 0.$$

Dall'esempio precedente, deduciamo quindi che la seconda proprietà è necessaria al fine di garantire la minimalità dell'estensione. Pertanto, è utile avere qualche criterio per stabilire se un'estensione sia senza costanti: uno di questi, ad esempio, è il seguente.

Proposizione 2.1. Sia $\mathbb{K} \subset \mathcal{R}$ un'estensione di anelli differenziali, tale che \mathcal{R} sia un dominio di integrità, finitamente generato come \mathbb{K} -algebra. Sia \mathbb{L} il campo delle frazioni di \mathcal{R} : se \mathcal{R} non ha ideali differenziali propri non banali, allora l'estensione $\mathbb{L} \supset \mathbb{K}$ è senza costanti.

Dimostrazione

Si veda [CH11].

□

2.2. Il Wronskiano

Introduciamo adesso un nuovo strumento, che ci consentirà di stabilire se la prima proprietà nella definizione di estensione di Picard-Vessiot è soddisfatta o meno. Data una m -upla (x_1, \dots, x_m) di elementi di un anello differenziale \mathcal{R} , definiamo il loro *Wronskiano* come

$$W = W(x_1, \dots, x_m) = \det \left(\left(x_i^{(j)} \right)_{\substack{1 \leq i \leq m \\ 0 \leq j < m}} \right) = \det \begin{bmatrix} x_1 & x_2 & \dots & x_m \\ x_1' & x_2' & \dots & x_m' \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{(m-1)} & x_2^{(m-1)} & \dots & x_m^{(m-1)} \end{bmatrix}.$$

La matrice che definisce il Wronskiano sarà detta la *matrice Wronskiana* associata alla m -upla (x_1, \dots, x_m) .

Esempio 2.2. Supponiamo che x_1, \dots, x_m siano tali che $x_j' = a_j x_j$ per ogni $j = 1, \dots, m$, dove a_1, \dots, a_m sono costanti. Allora

$$\begin{aligned} \mathcal{W}(x_1, \dots, x_m) &= \det \begin{bmatrix} x_1 & x_2 & \dots & x_m \\ a_1 x_1 & a_2 x_2 & \dots & a_m x_m \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{m-1} x_1 & a_2^{m-1} x_2 & \dots & a_m^{m-1} x_m \end{bmatrix} \\ &= x_1 \dots x_m \det \begin{bmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_m \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{m-1} & a_2^{m-1} & \dots & a_m^{m-1} \end{bmatrix} = x_1 \dots x_m \prod_{1 \leq i < j \leq m} (a_i - a_j), \end{aligned}$$

dove abbiamo usato la formula per il calcolo del determinante di una matrice di Vandermonde.

Essendo \mathcal{W} combinazione lineare finita di prodotti di elementi di \mathcal{R} , anche \mathcal{W} è un elemento di \mathcal{R} : pertanto, possiamo calcolare la sua derivazione. A questo scopo, introduciamo una notazione più comoda: dato che il Wronskiano è a tutti gli effetti un determinante, possiamo vederlo come applicazione sulle righe della matrice; denoteremo con $\underline{x} = (x_1, \dots, x_m)$ un generico vettore riga di m elementi di \mathcal{R} , e con $\underline{x}^{(j)}$ il vettore delle j -esime derivazioni dei suoi elementi.

Scriviamo \mathcal{W} mediante la formula di Leibniz:

$$\mathcal{W}(x_1, \dots, x_m) = \mathcal{W}(\underline{x}) = \det(\underline{x}, \dots, \underline{x}^{(m-1)}) = \sum_{\sigma \in \mathcal{S}_m} \text{sign}(\sigma) \prod_{i=1}^m x_i^{(\sigma(i))},$$

dove \mathcal{S}_m è il gruppo simmetrico con m elementi. Sfruttando le proprietà (1.1) e (1.2) delle derivazioni, si ottiene

$$\begin{aligned} \mathcal{D}(\mathcal{W}(\underline{x})) &= \sum_{\sigma \in \mathcal{S}_m} \text{sign}(\sigma) \sum_{i=1}^m x_i^{(\sigma(i)+1)} \prod_{\substack{1 \leq j \leq m \\ j \neq i}} x_j^{(\sigma(j))} = \sum_{i=1}^m \sum_{\sigma \in \mathcal{S}_m} \text{sign}(\sigma) x_i^{(\sigma(i)+1)} \prod_{\substack{1 \leq j \leq m \\ j \neq i}} x_j^{(\sigma(j))} \\ &= \det(\underline{x}^{(1)}, \underline{x}^{(1)}, \dots, \underline{x}^{(m-1)}) + \det(\underline{x}, \underline{x}^{(2)}, \underline{x}^{(2)}, \dots, \underline{x}^{(m-1)}) + \dots + \\ &\quad + \det(\underline{x}^{(1)}, \dots, \underline{x}^{(m-1)}, \underline{x}^{(m-1)}) + \det(\underline{x}^{(1)}, \dots, \underline{x}^{(m-2)}, \underline{x}^{(m)}) \\ &= \det(\underline{x}, \underline{x}^{(1)}, \dots, \underline{x}^{(m-2)}, \underline{x}^{(m)}), \end{aligned}$$

dove i primi $m - 1$ termini nella somma sono nulli, in quanto ci sono righe uguali nella matrice Wronskiana corrispondente. Quindi, in pratica, per calcolare la derivazione del Wronskiano di una m -upla basta sostituire all'ultima riga della matrice Wronskiana il vettore riga delle derivazioni dei suoi elementi, e calcolare il determinante di questa nuova matrice.

Il Wronskiano è uno strumento utilissimo per stabilire se degli elementi di un campo differenziale sono linearmente dipendenti sul campo delle costanti.

Teorema 2.1. (Indipendenza degli elementi di un campo differenziale) $x_1, \dots, x_n \in \mathbb{K}$ sono $\mathcal{C}_{\mathbb{K}}$ -linearmente dipendenti se e solo se $\mathcal{W}(x_1, \dots, x_n) = 0$.

Dimostrazione

\Rightarrow Supponiamo che x_1, \dots, x_n siano $\mathcal{C}_{\mathbb{K}}$ -linearmente dipendenti, e siano $c_1, \dots, c_n \in \mathcal{C}_{\mathbb{K}}$ non tutti nulli tali che $\sum_{i=1}^n c_i x_i = 0$. Se deriviamo quest'ultima identità per $n - 1$ volte, otteniamo che, per ogni $j = 0, \dots, n - 1$,

$$\sum_{i=1}^n c_i x_i^{(j)} = 0. \quad (2.3)$$

Osserviamo che queste relazioni esprimono una relazione di dipendenza lineare tra le colonne della matrice Wronskiana associata a x_1, \dots, x_n : pertanto, $\mathcal{W}(x_1, \dots, x_n) = 0$.

\Leftarrow Procediamo per induzione su n : il passo base ($n = 1$) è immediato; supponiamo che la proposizione sia verificata per $n - 1$, e che $\mathcal{W}(x_1, \dots, x_n) = 0$; di conseguenza, avremo una relazione di dipendenza lineare fra le colonne della matrice Wronskiana associata a x_1, \dots, x_n , espressa dalle condizioni (2.3), ma stavolta sappiamo a priori soltanto che $c_1, \dots, c_n \in \mathbb{K}$, e che tali elementi non sono tutti nulli. Possiamo assumere, a meno di riordinare e di moltiplicare per inversi, che $c_1 = 1$. Fissiamo allora $0 \leq j \leq n - 2$, e deriviamo la corrispondente relazione tra le condizioni (2.3): otteniamo

$$\sum_{i=1}^n c_i x_i^{(j+1)} + \sum_{i=2}^n c'_i x_i^{(j)} = 0.$$

Osserviamo che la prima somma è uguale a 0: otteniamo quindi

$$\sum_{i=2}^n c'_i x_i^{(j)} = 0.$$

Al variare di $j = 0, \dots, n - 2$, queste ultime identità ci dicono che c'_2, \dots, c'_n sono soluzioni del sistema di equazioni differenziali lineari

$$\begin{bmatrix} x_2 & x_3 & \dots & x_n \\ x_2^{(1)} & x_3^{(1)} & \dots & x_n^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ x_2^{(n)} & x_3^{(n)} & \dots & x_n^{(n)} \end{bmatrix} \begin{bmatrix} c'_2 \\ c'_3 \\ \vdots \\ c'_n \end{bmatrix} = 0.$$

Il determinante della matrice che definisce il sistema è uguale a $\mathcal{W}(x_2, \dots, x_n)$: se quest'ultimo è uguale a 0, concludiamo per ipotesi induttiva; se invece è diverso da 0, si ha che $c'_2 = \dots = c'_n = 0$, ovvero c_2, \dots, c_n sono costanti. In ogni caso, si ha la tesi. \square

Consideriamo adesso un operatore differenziale \mathcal{L} di grado n , come nell'equazione (2.1). Nel caso, molto frequente, che \mathcal{L} sia monico, il seguente risultato ha delle conseguenze importanti sullo spazio delle soluzioni dell'equazione associata.

Teorema 2.2. *Supponiamo che, in una qualche estensione differenziale $\widehat{\mathbb{K}}$ di \mathbb{K} , esistano degli elementi $x_1, \dots, x_{n+1} \in \widehat{\mathbb{K}}$ soluzioni dell'equazione differenziale $\mathcal{L}(x) = 0$. Allora il Wronskiano $\mathcal{W}(x_1, \dots, x_{n+1})$ è nullo, ovvero tali soluzioni sono $\mathbb{C}_{\mathbb{K}}$ -linearmente dipendenti. In particolare, se \mathcal{L} è un operatore differenziale monico di grado n , il $\mathbb{C}_{\mathbb{K}}$ -spazio vettoriale $\mathcal{V}_{\mathcal{L}}$ di soluzioni dell'equazione differenziale associata ha dimensione finita su $\mathbb{C}_{\mathbb{K}}$, di dimensione minore o uguale a n su $\mathbb{C}_{\mathbb{K}}$.*

Dimostrazione

Poiché $\mathcal{W}(x_1, \dots, x_{n+1}) = \det(\underline{x}, \underline{x}^{(1)}, \dots, \underline{x}^{(n)})$, e per ipotesi l'ultima riga è combinazione lineare delle precedenti, tale determinante è uguale a 0. Tutto il resto è immediata conseguenza del teorema precedente. \square

Nel seguito, supporremo che $\dim_{\mathbb{C}_{\mathbb{K}}} \mathcal{V}_{\mathcal{L}} = n$, ovvero che esistano n elementi $x_1, \dots, x_n \in \mathcal{V}_{\mathcal{L}}$ tali che $\mathcal{W}(x_1, \dots, x_n) \neq 0$: in tal caso, diremo che $\{x_1, \dots, x_n\}$ è un *insieme massimale di soluzioni*. Avere a disposizione un insieme massimale di soluzioni è molto utile, in quanto quest'ultimo determina univocamente l'equazione differenziale:

Corollario 2.1. *Dati $x_1, \dots, x_n \in \mathbb{K}$ che siano $\mathbb{C}_{\mathbb{K}}$ -linearmente indipendenti, esiste un unico operatore differenziale \mathcal{L} , monico e di grado n , tale che $\mathcal{L}(x_j) = 0$ per ogni $j = 1, \dots, n$.*

Dimostrazione

Unicità Supponiamo che

$$\mathcal{L}_1 = \mathcal{D}^{(n)} + \sum_{i=0}^{n-1} a_i \mathcal{D}^{(i)}, \quad \mathcal{L}_2 = \mathcal{D}^{(n)} + \sum_{i=0}^{n-1} b_i \mathcal{D}^{(i)},$$

siano due operatori differenziali come nelle ipotesi, tali che $\mathcal{L}_1(x_j) = \mathcal{L}_2(x_j) = 0$ per ogni $j = 1, \dots, n$, e supponiamo che esista $0 \leq j \leq n-1$ tale che $a_j \neq b_j$: prendiamo il massimo j che verifica questa proprietà.

Consideriamo l'operatore differenziale $\mathcal{L} = (b_j - a_j)^{-1}(\mathcal{L}_1 - \mathcal{L}_2)$: quest'ultimo è un operatore differenziale lineare monico omogeneo, di grado $m < n$: per il Teorema 2.2,

$$\dim_{\mathbb{C}_{\mathbb{K}}} \mathcal{V}_{\mathcal{L}} \leq m < n.$$

Osserviamo che $\mathcal{L}(x_k) = 0$ per ogni $k = 1, \dots, n$: per non contraddire il teorema precedente, dato che tali elementi sono linearmente indipendenti sul campo delle costanti, si ha necessariamente $\mathcal{L} = 0$, cioè $\mathcal{L}_1 = \mathcal{L}_2$.

Esistenza L'operatore differenziale

$$\mathcal{L} = (-1)^n \frac{\mathcal{W}(\text{Id}, x_1, \dots, x_n)}{\mathcal{W}(x_1, \dots, x_n)} = \frac{(-1)^n}{\mathcal{W}(x_1, \dots, x_n)} \det \begin{bmatrix} \text{Id} & x_1 & \dots & x_n \\ \mathcal{D} & x_1' & \dots & x_n' \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{D}^{(n)} & x_1^{(n)} & \dots & x_n^{(n)} \end{bmatrix}$$

è lineare monico omogeneo di grado n , e inoltre, per ogni $j = 1, \dots, n$, si ha

$$\mathcal{L}(x_j) = \frac{\mathcal{W}(x_j, x_1, \dots, x_n)}{\mathcal{W}(x_1, \dots, x_n)} = 0.$$

2.3. Esistenza di un'estensione di Picard-Vessiot

Supponiamo che \mathcal{L} sia un operatore differenziale come in (2.1): consideriamo il seguente anello dei polinomi in n^2 indeterminate

$$\mathcal{P} = \mathbb{K}[x_{i,j} : 0 \leq i \leq n-1, 1 \leq j \leq n].$$

Possiamo estendere la derivazione di \mathbb{K} a una derivazione di \mathcal{P} ponendo

$$\begin{aligned} x'_{i,j} &= x_{i+1,j} & 0 \leq i \leq n-2, & \quad 1 \leq j \leq n, \\ x'_{n-1,j} &= - \sum_{k=0}^{n-1} a_k x_{k,j} & 1 \leq j \leq n. \end{aligned}$$

Questa costruzione non è banale: identificando $x_{0,1}, \dots, x_{0,n}$ con delle soluzioni y_1, \dots, y_n dell'equazione differenziale (2.2), e scrivendo le variabili in una matrice, otteniamo proprio la matrice Wronskiana associata alla n -upla (y_1, \dots, y_n) (l'indice i indica l'ordine di derivazione):

$$\begin{bmatrix} y_1 & y_2 & \cdots & y_n \\ y_1^{(1)} & y_2^{(1)} & \cdots & y_n^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{bmatrix} = \begin{bmatrix} x_{0,1} & x_{0,2} & \cdots & x_{0,n} \\ x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n-1,1} & x_{n-1,2} & \cdots & x_{n-1,n} \end{bmatrix}.$$

Denotiamo con \mathcal{S} l'insieme delle potenze del Wronskiano $\mathcal{W} = \mathcal{W}(y_1, \dots, y_n)$. Osserviamo che questo insieme è moltiplicativamente chiuso. Localizziamo \mathcal{P} rispetto a questo sottoinsieme:

$$\mathcal{V} = \mathcal{S}^{-1}\mathcal{P} = \mathcal{P}[\mathcal{W}^{-1}] = \mathbb{K}[x_{i,j} : 0 \leq i \leq n-1, 1 \leq j \leq n][\mathcal{W}^{-1}].$$

Esattamente come nella Proposizione 1.3, la derivazione di \mathcal{P} si estende in modo unico a una derivazione di \mathcal{V} . Diremo che \mathcal{V} è un'algebra di soluzioni universale massimale per \mathcal{L} .

Vogliamo dimostrare che è possibile costruire, a partire da \mathcal{V} , un'estensione di \mathbb{K} di Picard-Vessiot per \mathcal{L} . Premettiamo un lemma:

Lemma 2.1. *Sia $\mathcal{R} \supset \mathbb{K}$ un'estensione di anelli differenziali. Esiste un ideale differenziale proprio di \mathcal{R} che è anche primo.*

Dimostrazione

Supponiamo inizialmente che \mathcal{R} non abbia ideali propri non banali, e proviamo che in tal caso \mathcal{R} è un dominio di integrità (così, il lemma è provato con l'ideale nullo). Supponiamo per assurdo che esistano due elementi non nulli $x, y \in \mathcal{R}$ tali che $xy = 0$. Osserviamo che, per ogni $k \in \mathbb{N}$, si ha $x^{(k)}y^{k+1} = 0$: infatti, derivando la relazione precedente si ottiene

$$x'y + xy' = 0,$$

e moltiplicando per y quest'ultima, si ottiene $x'y^2 = 0$. Procedendo induttivamente, è immediato provare quanto affermato sopra. Sia \mathcal{J} l'ideale differenziale generato da x : per l'ipotesi

aggiuntiva su \mathcal{R} , si ha $\mathcal{J} = \mathcal{R}$. Ma allora esiste necessariamente $k \in \mathbb{N}$ tale che $y^k = 0$: infatti, per quanto appena provato, se così non fosse, tutti gli elementi di \mathcal{J} sarebbero divisori di 0, e quindi \mathcal{J} sarebbe un ideale proprio non banale di \mathcal{R} ; poiché y è generico, abbiamo provato che ogni divisore di 0 è nilpotente.

Sia m il più piccolo intero positivo tale che $x^m = 0$. Ma allora $(x^m)' = mx^{m-1}x' = 0$, e poiché $mx^{m-1} \neq 0$, si ha che x' è un divisore di 0. Induttivamente, concludiamo che x , e tutte le sue derivazioni, sono divisori di 0, e quindi nilpotenti: di conseguenza si avrebbe che \mathcal{J} è un ideale proprio non banale di \mathcal{R} , assurdo. Quindi \mathcal{R} è un dominio di integrità.

Nel caso generale, possiamo ricondurci al precedente: sia \mathcal{F} la famiglia di tutti gli ideali propri di \mathcal{R} : osserviamo che questa famiglia è non vuota (in quanto contiene l'ideale nullo) e che possiamo dotarla di un ordinamento parziale con la relazione di contenimento, rispetto alla quale ogni catena possiede un maggiorante (dato dall'unione degli elementi della catena): per il lemma di Zorn, esiste almeno un elemento massimale (rispetto al contenimento) in \mathcal{F} , sia esso \mathcal{I} . Per costruzione, \mathcal{R}/\mathcal{I} non possiede ideali propri non banali: dunque, per quanto provato precedentemente, \mathcal{R}/\mathcal{I} è un dominio di integrità, ovvero \mathcal{I} è un ideale primo. □

Teorema 2.3. (Esistenza di un'estensione di Picard-Vessiot) *Sia \mathcal{L} un operatore differenziale di grado n , e siano \mathcal{V} un'algebra di soluzioni universale massimale per \mathcal{L} , \mathcal{P} un ideale proprio di \mathcal{V} , massimale rispetto al contenimento. Allora \mathcal{P} è primo, e il campo delle frazioni \mathbb{L} di \mathcal{V}/\mathcal{P} è un'estensione di \mathbb{K} di Picard-Vessiot per \mathcal{L} .*

Dimostrazione

Osserviamo che, per costruzione, \mathcal{V} è generata su \mathbb{K} dalle soluzioni dell'equazione (2.2) e dall'inverso del Wronskiano di un insieme massimale di soluzioni, quindi a maggior ragione lo è anche \mathcal{V}/\mathcal{P} . Inoltre, per il Lemma 2.1, \mathcal{P} è un ideale primo, e quindi \mathcal{V}/\mathcal{P} è un dominio di integrità.

Poiché \mathcal{P} è anche massimale rispetto al contenimento, \mathcal{V}/\mathcal{P} non ha ideali differenziali propri non banali e quindi, per la Proposizione 2.1, $\mathcal{C}_{\mathbb{L}} = \mathcal{C}_{\mathbb{K}}$. Infine, il Wronskiano è invertibile in \mathbb{L} , e quindi è in particolare non nullo. Grazie al Teorema 2.1, possiamo concludere che \mathbb{L} ha tutte le proprietà nella definizione di estensione di Picard-Vessiot, e si ha quindi la tesi. □

2.4. Unicità di un'estensione di Picard-Vessiot

Iniziamo con un lemma:

Lemma 2.2. (Normalità delle estensioni di Picard-Vessiot) *Sia \mathcal{L} un operatore differenziale come in (2.1), e siano $\mathbb{L}_1, \mathbb{L}_2$ due estensioni di \mathbb{K} di Picard-Vessiot per \mathcal{L} . Supponiamo di avere un'ulteriore estensione differenziale $\mathbb{L} \supset \mathbb{K}$ senza costanti. Se $\sigma_1 : \mathbb{L}_1 \rightarrow \mathbb{L}$, $\sigma_2 : \mathbb{L}_2 \rightarrow \mathbb{L}$ sono due \mathbb{K} -morfismi differenziali, allora $\sigma_1(\mathbb{L}_1) = \sigma_2(\mathbb{L}_2)$.*

Dimostrazione

Poniamo

$$\begin{aligned} \mathcal{V}_1 &= \{x \in \mathbb{L}_1 : \mathcal{L}(x) = 0\}, & \mathcal{V}_2 &= \{x \in \mathbb{L}_2 : \mathcal{L}(x) = 0\}, \\ \mathcal{V} &= \{x \in \mathbb{L} : \mathcal{L}(x) = 0\}. \end{aligned}$$

Sappiamo che \mathcal{V}_1 e \mathcal{V}_2 sono $\mathbb{C}_{\mathbb{K}}$ -spazi vettoriali di dimensione n , mentre \mathcal{V} è anch'esso un $\mathbb{C}_{\mathbb{K}}$ -spazio vettoriale, ma possiamo solo concludere, per il Teorema 2.2 che la sua dimensione è al più n . Essendo σ_1, σ_2 \mathbb{K} -morfismi differenziali, osserviamo che $\sigma_1(\mathcal{V}_1), \sigma_2(\mathcal{V}_2)$ sono contenuti in \mathcal{V} . Ma allora, ad esempio per la formula di Grassmann, osserviamo che l'unica possibilità è $\dim_{\mathbb{C}_{\mathbb{K}}} \sigma_1(\mathcal{V}_1) = \dim_{\mathbb{C}_{\mathbb{K}}} \sigma_2(\mathcal{V}_2) = n$, e quindi

$$\sigma_1(\mathcal{V}_1) = \sigma_2(\mathcal{V}_2) = \mathcal{V}.$$

Quindi, usando le proprietà nella definizione di estensione di Picard-Vessiot, otteniamo che

$$\sigma_1(\mathbb{L}_1) = \sigma_1(\mathbb{K}(\mathcal{V}_1)) = \sigma_2(\mathbb{K}(\mathcal{V}_2)) = \sigma_2(\mathbb{L}_2).$$

□

Teorema 2.4. (Unicità delle estensioni di Picard-Vessiot) *Sia \mathcal{L} un operatore differenziale come in (2.1), e siano $\mathbb{L}_1, \mathbb{L}_2$ due estensioni di \mathbb{K} di Picard-Vessiot per \mathcal{L} . Allora esiste un \mathbb{K} -isomorfismo differenziale $\psi : \mathbb{L}_1 \rightarrow \mathbb{L}_2$.*

Dimostrazione

L'idea che useremo per dimostrare questo risultato è di costruire un'estensione differenziale senza costanti $\mathbb{E} \supset \mathbb{K}$, e due immersioni differenziali da \mathbb{L}_1 e \mathbb{L}_2 in \mathbb{E} : una volta fatto ciò, si avrà immediatamente la tesi per il lemma precedente.

Possiamo assumere che \mathbb{L}_1 sia l'estensione di \mathbb{K} di Picard-Vessiot per \mathcal{L} costruita nel Teorema 2.3: mantenendo le stesse notazioni, consideriamo l'anello $\mathcal{A} = \mathcal{V}/\mathcal{P} \otimes_{\mathbb{K}} \mathbb{L}_2$, e dotiamolo della struttura di anello differenziale (finitamente generato come \mathbb{L}_2 -algebra) mediante la seguente applicazione, che si verifica subito essere una derivazione, e che definiamo sui tensori di rango 1 ed estendiamo per linearità:

$$\begin{aligned} \mathcal{D} : \quad \mathcal{A} &\rightarrow \mathcal{A} \\ x \otimes y &\mapsto \mathcal{D}_{\mathcal{V}/\mathcal{P}}(x) \otimes y + x \otimes \mathcal{D}_{\mathbb{L}_2}(y). \end{aligned}$$

Le verifiche che \mathcal{D} sia effettivamente una derivazione sono immediate, per via delle regole di calcolo sui tensori di rango 1. Consideriamo l'omomorfismo di immersione

$$\begin{aligned} \iota : \mathcal{V}/\mathcal{P} &\rightarrow \mathcal{A} \\ x &\mapsto x \otimes 1, \end{aligned}$$

e sia \mathcal{Q} un ideale proprio di \mathcal{A} , massimale rispetto al contenimento. Per il Lemma 2.1, \mathcal{Q} è un ideale primo, e inoltre la sua controimmagine in \mathcal{V}/\mathcal{P} tramite ι è l'ideale nullo: infatti quest'ultimo non possiede ideali propri non banali, e se fosse $\iota^{-1}(\mathcal{Q}) = \mathcal{V}/\mathcal{P}$, si avrebbe anche $\mathcal{Q} = \mathcal{A}$. È quindi ben definita l'immersione

$$\begin{aligned} \bar{\iota}_1 : \mathcal{V}/\mathcal{P} &\rightarrow \mathcal{A}/\mathcal{Q} \\ x &\mapsto \overline{x \otimes 1}, \end{aligned}$$

Sia \mathbb{E} il campo delle frazioni di \mathcal{A}/\mathcal{Q} : per le proprietà universali della localizzazione, la mappa $\bar{\iota}_1$ si estende in modo univoco a un'immersione $\phi_1 : \mathbb{L}_1 \rightarrow \mathbb{E}$, come mostrato nel diagramma a lato. In modo simile si costruisce l'immersione

$$\begin{aligned} \bar{\iota}_2 : \mathbb{L}_2 &\rightarrow \mathcal{A}/\mathcal{Q} \\ x &\mapsto \overline{1 \otimes x}, \end{aligned}$$

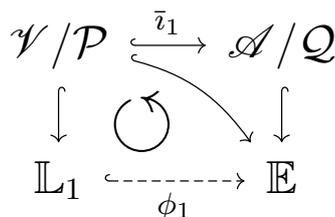


Figura 2.1:
Unicità dell'estensione di Picard-Vessiot

e la si estende a un'immersione $\phi_2 : \mathbb{L}_2 \rightarrow \mathbb{E}$. Ma per la Proposizione 2.1 si ha $\mathcal{C}_{\mathbb{E}} = \mathcal{C}_{\mathbb{L}_2} = \mathcal{C}_{\mathbb{K}}$, quindi possiamo concludere applicando il Lemma 2.2. □

Anche solo da queste prime proprietà, le estensioni di Picard-Vessiot appaiono come l'analogo dei campi di spezzamento per i polinomi in $\mathbb{Q}[x]$. Il Lemma 2.2 è l'analogo del seguente risultato della teoria di Galois classica:

Lemma 2.3. *Siano \mathbb{K} un campo, $p(x) \in \mathbb{K}[x]$ un polinomio monico di grado n . Consideriamo un campo di spezzamento $\mathbb{L} \supset \mathbb{K}$ di $p(x)$, e sia $\overline{\mathbb{K}}$ la chiusura algebrica di \mathbb{K} . Se $\sigma_1, \sigma_2 : \mathbb{L} \rightarrow \overline{\mathbb{K}}$ sono delle \mathbb{K} -immersioni, allora $\sigma_1(\mathbb{L}) = \sigma_2(\mathbb{L})$.*

Il teorema precedente ci garantisce che, dato un operatore differenziale \mathcal{L} , è univocamente determinata a meno di isomorfismo l'estensione di Picard-Vessiot ad esso associata: tuttavia, nulla vieta che esistano due operatori differenziali a cui è associata la stessa estensione di Picard-Vessiot. Nel prossimo capitolo, cercheremo di costruire un apparato teorico simile a quello della teoria di Galois classica, per poter affrontare più nel dettaglio questo e altri problemi.

Il gruppo di Galois differenziale

Introduzione

Richiamiamo le principali nozioni della teoria di Galois classica, di cui cercheremo di mettere in luce le principali analogie con la teoria di Picard-Vessiot. Dopo aver introdotto il concetto di gruppo di Galois differenziale, vediamo degli esempi concreti e ne studiamo le principali proprietà, in particolare il fatto che può essere visto come gruppo algebrico. Forniamo inoltre una seconda caratterizzazione delle estensioni di Picard-Vessiot, che ha il pregio di non riferirsi esplicitamente a un operatore differenziale.

Dove non è altrimenti specificato, e ad eccezione della prima sezione, supponiamo che \mathbb{K} sia un campo differenziale con derivazione \mathcal{D} non banale e a caratteristica 0, che il suo campo delle costanti sia algebricamente chiuso, e che gli operatori differenziali siano lineari e omogenei, a coefficienti in \mathbb{K} .

3.1. Richiami di teoria di Galois

Richiamiamo le definizioni e gli enunciati principali della teoria di Galois classica per le estensioni algebriche. Per una trattazione più completa si veda ad esempio [Gai17].

Data un'estensione di campi $\mathbb{L} \supset \mathbb{K}$, un elemento $z \in \mathbb{L}$ si dice *algebrico* su \mathbb{K} se esiste un polinomio $p(t) \in \mathbb{K}[t]$ tale che $p(z) = 0$; in caso contrario, diremo che z è *trascendente* su \mathbb{K} . L'estensione si dice *algebrica* se ogni elemento di \mathbb{L} è algebrico su \mathbb{K} .

Diremo inoltre che un polinomio irriducibile $p(t) \in \mathbb{K}[t]$ è *separabile* se ha derivata non nulla: se \mathbb{K} è a caratteristica 0, ciò equivale a richiedere che non sia costante. Essendo $p(t)$ irriducibile, non ha radici multiple in un campo di spezzamento. Più in generale, diremo che un polinomio $p(t) \in \mathbb{K}[t]$ è *separabile* se è prodotto di polinomi irriducibili separabili.

Denoteremo con $\text{Aut}(\mathbb{L})$ il gruppo¹ degli automorfismi di \mathbb{L} , e con $\text{Aut}(\mathbb{L}/\mathbb{K})$, $\text{Fix}(\mathbb{L}/\mathbb{K})$, rispettivamente, gli insiemi

$$\text{Aut}(\mathbb{L}/\mathbb{K}) = \{\sigma \in \text{Aut}(\mathbb{L}) : \sigma|_{\mathbb{K}} = \text{Id}_{\mathbb{K}}\}, \quad (3.1)$$

$$\text{Fix}(\mathbb{L}/\mathbb{K}) = \{x \in \mathbb{L} : \sigma(x) = x, \forall \sigma \in \text{Aut}(\mathbb{L}/\mathbb{K})\}. \quad (3.2)$$

¹Con la composizione di applicazioni

È immediato verificare che (3.1) è un sottogruppo di $\text{Aut}(\mathbb{L})$, e che (3.2) è un sottocampo di \mathbb{L} , contenente \mathbb{K} . Più in generale, dato un qualsiasi sottogruppo \mathcal{H} di $\text{Aut}(\mathbb{L}/\mathbb{K})$, denoteremo con $\text{Fix}(\mathcal{H})$ l'insieme

$$\text{Fix}(\mathcal{H}) = \{x \in \mathbb{L} : \sigma(x) = x, \forall \sigma \in \mathcal{H}\}.$$

Anche in questo caso, si verifica facilmente che $\text{Fix}(\mathcal{H})$ è un sottocampo di \mathbb{L} , contenente \mathbb{K} . Questi oggetti sono legati dai prossimi risultati.

Proposizione 3.1. *Sia \mathbb{L} il campo di spezzamento su \mathbb{K} di un polinomio separabile $p(t)$ a coefficienti in \mathbb{K} . Comunque si prenda $x \in \mathbb{L} - \mathbb{K}$, esiste $\sigma \in \text{Fix}(\mathbb{L}/\mathbb{K})$ tale che $\sigma(x) \neq x$.*

Proposizione 3.2. *Sia $\mathbb{L} \supset \mathbb{K}$ un'estensione finita² di campi. Allora $|\text{Aut}(\mathbb{L}/\mathbb{K})| < +\infty$.*

Diremo che $\mathbb{L} \supset \mathbb{K}$ è un'estensione di Galois se è finita e $\text{Fix}(\mathbb{L}/\mathbb{K}) = \mathbb{K}$. In tal caso, chiameremo $\text{Aut}(\mathbb{L}/\mathbb{K})$ il gruppo di Galois dell'estensione, e lo denoteremo con $\text{Gal}(\mathbb{L}/\mathbb{K})$. Per la Proposizione 3.2, tale gruppo è finito, e i suoi elementi sono completamente determinati da come agiscono su dei generatori dell'estensione. I seguenti teoremi forniscono, rispettivamente, una condizione necessaria affinché un'estensione sia di Galois, e una caratterizzazione di queste ultime.

Teorema 3.1. *Se $\mathbb{L} \supset \mathbb{K}$ è un'estensione di Galois, allora ogni elemento $x \in \mathbb{L}$ è radice di un polinomio irriducibile separabile $p(t) \in \mathbb{K}[t]$. Inoltre, \mathbb{L} contiene un campo di spezzamento di $p(t)$.*

Teorema 3.2. *Sia $\mathbb{L} \supset \mathbb{K}$ un'estensione di campi. L'estensione è di Galois se e solo se \mathbb{L} è il campo di spezzamento su \mathbb{K} di un polinomio $p(t) \in \mathbb{K}[t]$ separabile.*

Osserviamo che, in particolare, se $\mathbb{L} \supset \mathbb{F} \supset \mathbb{K}$ sono delle estensioni di campi, tali che $\mathbb{L} \supset \mathbb{K}$ è di Galois, allora anche $\mathbb{L} \supset \mathbb{F}$ è di Galois: infatti, per il Teorema 3.2, \mathbb{L} è il campo di spezzamento di un polinomio $p(t) \in \mathbb{K}[t]$ separabile, e tale polinomio può essere visto anche come polinomio a coefficienti in $\mathbb{F}[t]$, dove rimane separabile.

L'idea attorno alla quale ruota la teoria di Galois è quella di far corrispondere ai sottocampi di un'estensione di Galois i sottogruppi del gruppo di Galois corrispondente. A questo scopo, consideriamo un'estensione di Galois $\mathbb{L} \supset \mathbb{K}$, denotiamo con $\mathcal{C}_{\mathbb{L}/\mathbb{K}}$ la famiglia dei sottocampi dell'estensione, ovvero dei campi \mathbb{F} tali che $\mathbb{L} \supset \mathbb{F} \supset \mathbb{K}$, con $\mathcal{G}_{\mathbb{L}/\mathbb{K}}$ la famiglia dei sottogruppi di $\text{Gal}(\mathbb{L}/\mathbb{K})$, e definiamo le seguenti mappe:

$$\begin{aligned} \alpha : \mathcal{C}_{\mathbb{L}/\mathbb{K}} &\rightarrow \mathcal{G}_{\mathbb{L}/\mathbb{K}} & \beta : \mathcal{G}_{\mathbb{L}/\mathbb{K}} &\rightarrow \mathcal{C}_{\mathbb{L}/\mathbb{K}} \\ \mathbb{F} &\mapsto \text{Gal}(\mathbb{L}/\mathbb{F}), & \mathcal{H} &\mapsto \text{Fix}(\mathcal{H}). \end{aligned} \quad (3.3)$$

²Ovvero, \mathbb{L} è un \mathbb{K} -spazio vettoriale di dimensione finita. In genere, in questo contesto, si denota $\dim_{\mathbb{K}} \mathbb{L}$ con $[\mathbb{L} : \mathbb{K}]$.

Teorema 3.3. *Sia $\mathbb{L} \supset \mathbb{K}$ un'estensione di Galois. Allora:*

- ◇ **(Corrispondenza di Galois, versione classica)** *Le mappe definite in (3.3) sono una l'inversa dell'altra.*
- ◇ *Preso $\mathbb{F} \in \mathcal{C}_{\mathbb{L}/\mathbb{K}}$, l'estensione $\mathbb{F} \supset \mathbb{K}$ è di Galois se e solo se $\alpha(\mathbb{F})$ è un sottogruppo normale del gruppo di Galois dell'estensione, e in tal caso*

$$\text{Gal}(\mathbb{F}/\mathbb{K}) \cong \text{Gal}(\mathbb{L}/\mathbb{K})/\alpha(\mathbb{F}).$$

- ◇ *Preso $\mathbb{F} \in \mathcal{C}_{\mathbb{L}/\mathbb{K}}$, si ha*

$$|\text{Gal}(\mathbb{L}/\mathbb{F})| = [\mathbb{L} : \mathbb{F}].$$

Nel seguito del capitolo, cercheremo di studiare quali analogie e le differenze ci sono fra la teoria di Galois classica e la teoria di Picard-Vessiot.

3.2. Il gruppo di Galois differenziale

Data un'estensione $\mathbb{L} \supset \mathbb{K}$ di campi differenziali, denoteremo con $\text{Aut}^{\text{Diff}}(\mathbb{L})$ il gruppo³ degli automorfismi differenziali di \mathbb{L} , e con $\text{Aut}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$, $\text{Fix}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$, rispettivamente, gli insiemi

$$\text{Aut}^{\text{Diff}}(\mathbb{L}/\mathbb{K}) = \{\sigma \in \text{Aut}^{\text{Diff}}(\mathbb{L}) : \sigma|_{\mathbb{K}} = \text{Id}_{\mathbb{K}}\} \quad (3.4)$$

$$\text{Fix}^{\text{Diff}}(\mathbb{L}/\mathbb{K}) = \{x \in \mathbb{L} : \sigma(x) = x, \forall \sigma \in \text{Aut}^{\text{Diff}}(\mathbb{L}/\mathbb{K})\}. \quad (3.5)$$

Come in precedenza, è immediato verificare che (3.4) è un sottogruppo di $\text{Aut}^{\text{Diff}}(\mathbb{L})$, e che (3.5) è un sottocampo differenziale di \mathbb{L} , contenente \mathbb{K} . I gruppi (3.4) e (3.5) sono il corrispondente dei gruppi (3.1) e (3.2). Per continuare con l'analogia, è necessario che $\text{Fix}^{\text{Diff}}(\mathbb{L}/\mathbb{K}) = \mathbb{K}$: in effetti, le estensioni di Picard-Vessiot verificano questa proprietà, e ciò è conseguenza immediata del prossimo risultato, che è l'analogo della Proposizione 3.1.

Proposizione 3.3. *Sia $\mathbb{L} \supset \mathbb{K}$ un'estensione di Picard-Vessiot per un operatore differenziale lineare \mathcal{L} , di grado n . Comunque si prenda $x \in \mathbb{L} - \mathbb{K}$, esiste $\sigma \in \text{Aut}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$ tale che $\sigma(x) \neq x$.*

Dimostrazione

Si veda [CH11].

□

Corollario 3.1. *Sia $\mathbb{L} \supset \mathbb{K}$ un'estensione di Picard-Vessiot per \mathcal{L} . Allora $\text{Fix}^{\text{Diff}}(\mathbb{L}/\mathbb{K}) = \mathbb{K}$.*

Dimostrazione

L'inclusione $\mathbb{K} \subset \text{Fix}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$ segue subito dalla definizione. L'altra inclusione è immediata conseguenza della proposizione precedente.

□

³Con la composizione di applicazioni

Dunque, le estensioni di Picard-Vessiot possiedono proprietà analoghe alle estensioni di Galois classiche, e pertanto le chiameremo anche *estensioni di Galois differenziali*. Coerentemente, chiameremo $\text{Aut}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$ il *gruppo di Galois differenziale* associato all'estensione, e lo denoteremo con $\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$.

Lemma 3.1. *Se $\sigma \in \text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$ e y è una soluzione dell'equazione differenziale associata ad \mathcal{L} , ovvero $\mathcal{L}(y) = 0$, allora si ha anche $\mathcal{L}(\sigma(y)) = 0$.*

Dimostrazione

Poniamo $\mathcal{L} = \sum_{k=0}^n a_k \mathcal{D}^{(k)}$. Partendo dall'identità

$$\sum_{k=0}^n a_k y^{(k)} = 0$$

ed applicando σ ad entrambi i membri otteniamo

$$0 = \sigma(0) = \sigma\left(\sum_{k=0}^n a_k y^{(k)}\right) = \sum_{k=0}^n \sigma(a_k y^{(k)}) = \sum_{k=0}^n \sigma(a_k) \sigma(y^{(k)}) = \sum_{k=0}^n a_k \sigma(y)^{(k)},$$

ovvero $\mathcal{L}(\sigma(y)) = 0$. □

In particolare, se $\{y_1, \dots, y_n\}$ è un insieme massimale di soluzioni, ogni elemento del gruppo di Galois differenziale manda, al variare di $j = 1, \dots, n$ ognuno degli y_j in una loro combinazione lineare (a coefficienti in \mathbb{K}). Questo fatto può essere espresso in notazione matriciale nel modo seguente:

$$\sigma \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \quad (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}(n, \mathbb{K}).$$

Chiameremo quest'ultima matrice la *matrice associata* a σ rispetto all'insieme massimale di soluzioni $\{y_1, \dots, y_n\}$. Gli elementi del gruppo di Galois differenziale sono di conseguenza completamente determinati da come agiscono su un insieme massimale di soluzioni per \mathcal{L} , ovvero su un insieme di generatori dell'estensione di Picard-Vessiot associata. Ci chiediamo adesso come sono legate le matrici associate a due insiemi massimali di soluzioni diversi.

Proposizione 3.4. *Siano $\{y_1, \dots, y_n\}$ e $\{z_1, \dots, z_n\}$ due insiemi massimali di soluzioni. Le matrici associate a σ rispetto ad essi sono simili.*

Dimostrazione

Chiamiamo $\mathcal{Y}, \mathcal{Z} \in \mathcal{M}(n, \mathbb{K})$ rispettivamente le matrici associate a σ rispetto ai due insiemi massimali di soluzioni. Osserviamo che deve esistere una terza matrice $\mathcal{C} \in \mathcal{M}(n, \mathbb{K})$ tale che $\underline{z}^T = \mathcal{C} \underline{y}^T$. Dato che deve sussistere una relazione analoga quando scambiamo \underline{z} e \underline{y} , la matrice \mathcal{C} deve essere invertibile. Ma allora

$$\sigma \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} = \sigma \left(\mathcal{C} \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \right) = \mathcal{C} \sigma \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \mathcal{C} \mathcal{Y} \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \mathcal{C} \mathcal{Y} \mathcal{C}^{-1} \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}.$$

Quindi, $\mathcal{Z} = \mathcal{C} \mathcal{Y} \mathcal{C}^{-1}$, cioè la tesi. □

Viceversa, fissato l'insieme massimale di soluzioni, è evidente che ogni elemento del gruppo di Galois differenziale è in corrispondenza biunivoca con la matrice associata.

3.2.1. Un'ulteriore caratterizzazione delle estensioni di Picard-Vessiot

Abbiamo provato, grazie ai teoremi di esistenza 2.3 e unicità 2.4 delle estensioni di Picard-Vessiot, che esiste ed è unica a meno di isomorfismo l'estensione $\mathbb{L} \supset \mathbb{K}$ di Picard-Vessiot per un operatore differenziale \mathcal{L} . Tuttavia, è possibile che una stessa estensione di campi $\mathbb{L} \supset \mathbb{K}$ sia di Picard-Vessiot per due operatori differenziali distinti.

Esempio 3.1. *I campi differenziali $\mathbb{K} = \mathbb{C}(x)$ e $\mathbb{L} = \mathbb{C}(x, e^x)$ (con la derivazione usuale) sono tali che l'estensione $\mathbb{L} \supset \mathbb{K}$ è senza costanti. Inoltre gli operatori*

$$\mathcal{L}_1 = \frac{d}{dx} - 1, \quad \mathcal{L}_2 = \frac{d^2}{dx^2} - \frac{x+1}{x} \frac{d}{dx}$$

sono distinti, e le equazioni differenziali associate ammettono come insiemi massimali di soluzioni, rispettivamente, $\{e^x\}$ e $\{1, (x-1)e^x\}$. Di conseguenza, l'estensione $\mathbb{L} \supset \mathbb{K}$ è di Picard-Vessiot sia per \mathcal{L}_1 sia per \mathcal{L}_2 .

Il prossimo risultato caratterizza le estensioni di Picard-Vessiot senza riferirle a un operatore differenziale:

Teorema 3.4. *Un'estensione $\mathbb{L} \supset \mathbb{K}$ di campi differenziali è di Picard-Vessiot per un qualche operatore differenziale \mathcal{L} se e solo se valgono le seguenti condizioni*

- ◇ $\mathbb{L} = \mathbb{K}(\mathbb{V})$, dove $\mathbb{V} \subset \mathbb{L}$ è un $\mathbb{C}_{\mathbb{K}}$ -spazio vettoriale di dimensione finita.
- ◇ Esiste un sottogruppo \mathcal{G} di $\text{Aut}^{\text{Diff}}(\mathbb{L})$ tale che $\text{Fix}^{\text{Diff}}(\mathcal{G}) = \mathbb{K}$ e, per ogni $\phi \in \mathcal{G}$, \mathbb{V} è ϕ -invariante.
- ◇ L'estensione è senza costanti.

In particolare, se tali condizioni sono soddisfatte, e se $\{y_1, \dots, y_n\}$ è una $\mathbb{C}_{\mathbb{K}}$ -base di \mathbb{V} , allora $\mathbb{L} \supset \mathbb{K}$ è un'estensione di Picard-Vessiot per l'operatore differenziale monico

$$\mathcal{L} = (-1)^n \frac{\mathcal{W}(\text{Id}, y_1, \dots, y_n)}{\mathcal{W}(y_1, \dots, y_n)},$$

e inoltre $\mathcal{L}(x) = 0$ se e solo se $x \in \mathbb{V}$.

Dimostrazione

⇒ Supponiamo che $\mathbb{L} \supset \mathbb{K}$ sia un'estensione di Picard-Vessiot per \mathcal{L} . Per definizione, tale estensione è senza costanti. Consideriamo il $\mathbb{C}_{\mathbb{K}}$ -spazio vettoriale

$$\mathcal{V}_{\mathcal{L}} = \{x \in \mathbb{L} : \mathcal{L}(x) = 0\}.$$

Per il Teorema 2.2, $\mathcal{V}_{\mathcal{L}}$ ha dimensione finita, e per definizione di estensione di Picard-Vessiot genera \mathbb{L} su \mathbb{K} . Inoltre, osserviamo che per il Lemma 3.1 $\mathcal{V}_{\mathcal{L}}$ è ϕ -invariante per ogni $\phi \in \text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$. Infine, per il Corollario 3.1, $\text{Fix}^{\text{Diff}}(\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})) = \mathbb{K}$.

⇐ Poniamo $n = \dim_{\mathbb{C}_{\mathbb{K}}} \mathbb{V}$, e sia $\{x_1, \dots, x_n\}$ una base di \mathbb{V} come $\mathbb{C}_{\mathbb{K}}$ -spazio vettoriale. Per il Teorema 2.1, il Wronskiano $\mathcal{W}(x_1, \dots, x_n)$ è non nullo. Consideriamo il seguente operatore differenziale, già visto nel Corollario 2.1:

$$\mathcal{L} = (-1)^n \frac{\mathcal{W}(\text{Id}, x_1, \dots, x_n)}{\mathcal{W}(x_1, \dots, x_n)} = \frac{(-1)^n}{\mathcal{W}(x_1, \dots, x_n)} \det \begin{bmatrix} \text{Id} & x_1 & \dots & x_n \\ \mathcal{D} & x_1' & \dots & x_n' \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{D}^{(n)} & x_1^{(n)} & \dots & x_n^{(n)} \end{bmatrix}.$$

\mathcal{L} è un operatore differenziale lineare monico omogeneo di grado n , e inoltre $\mathcal{L}(y_j) = 0$ per ogni $j = 1, \dots, n$. Per concludere, basta provare che \mathcal{L} è a coefficienti in \mathbb{K} . Poniamo $\mathcal{L} = \mathcal{D}^{(n)} + a_{n-1}\mathcal{D}^{(n-1)} + \dots + a_1\mathcal{D} + a_0$: un calcolo diretto mostra che

$$a_1 = \frac{(-1)^{n+1}}{\mathcal{W}(x_1, \dots, x_n)} \mathcal{W}(x_1', \dots, x_n'),$$

e più in generale, per ogni $j = 2, \dots, n - 1$,

$$a_j = \frac{(-1)^{n+j}}{\mathcal{W}(x_1, \dots, x_n)} \det(\dots, \underline{x}^{(j-1)}, \underline{x}^{(j+1)}, \dots).$$

Prendiamo $\sigma \in \mathcal{G}$, e poniamo, per ogni $j = 1, \dots, n$, $y_j = \sigma(x_j)$. Dato che, per ipotesi $\sigma(\mathbb{V}) = \mathbb{V}$, ognuno degli y_j si può scrivere come combinazione lineare (a coefficienti in $\mathbb{C}_{\mathbb{K}}$) degli x_j ; in altri termini, esiste una matrice $M \in \text{GL}(n, \mathbb{C}_{\mathbb{K}})$ tale che

$$\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = M \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

A questo punto, essendo tale matrice a coefficienti costanti, è facile vedere, ad esempio nel caso di a_1 , che

$$\sigma(a_1) = \frac{(-1)^{n+1}}{\det M \cdot \mathcal{W}(x_1, \dots, x_n)} \det M \cdot \mathcal{W}(x_1', \dots, x_n') = a_1.$$

Per gli altri coefficienti il procedimento è lo stesso.

□

3.2.2. Esempi

Vediamo adesso qualche esempio concreto: questo ci permetterà di osservare più da vicino le somiglianze, ma anche qualche differenza, con la teoria di Galois classica. Fino alla fine di questa sezione, dove non è altrimenti specificato, prenderemo $\mathbb{K} = \mathbb{C}(x)$ come campo differenziale, dotato della derivazione usuale.

Esempio 3.2. Consideriamo l'equazione differenziale

$$y'' + \frac{1}{x}y' = 0,$$

corrispondente all'operatore differenziale $\mathcal{L} = \frac{d^2}{dx^2} + \frac{1}{x} \frac{d}{dx}$. È facile verificare che $\{\log x, 1\}$ è un insieme massimale di soluzioni. L'estensione

$$\mathbb{K}(\log x) = \mathbb{L} \supset \mathbb{K}$$

è dunque di Picard-Vessiot per \mathcal{L} .

Fissiamo $\sigma \in \text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$: poiché σ deve mandare soluzioni in altre soluzioni, devono esistere $\alpha, \beta \in \mathbb{C}$ tali che

$$\begin{aligned}\sigma(\log x) &= \beta \log x + \alpha \\ \sigma(1) &= 1,\end{aligned}$$

Inoltre, dato che σ è un automorfismo differenziale che lascia fissati gli elementi in $\mathbb{K} = \mathbb{C}(x)$, i seguenti elementi

$$\begin{aligned}\sigma\left(\frac{d}{dx}(\log x)\right) &= \sigma\left(\frac{1}{x}\right) = \frac{1}{x}, \\ \frac{d}{dx}(\sigma(\log x)) &= \frac{d}{dx}(\beta \log x + \alpha) = \beta \frac{1}{x},\end{aligned}$$

devono essere uguali, pertanto $\beta = 1$. Non ci sono invece restrizioni su α . A questo punto si verifica agevolmente che $\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$ è costituito, al variare di $\alpha \in \mathbb{C}$, da tutte le mappe σ tali che

$$\begin{aligned}\sigma(\log x) &= \log x + \alpha, \\ \sigma(1) &= 1.\end{aligned}$$

Esiste un isomorfismo naturale fra $\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$ e \mathbb{C} (visto come gruppo additivo). Passando alle matrici associate, a un tale σ corrisponde la matrice

$$\begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}.$$

Le matrici aventi questa forma formano un sottogruppo, $U(2, \mathbb{C})$ di $GL(2, \mathbb{C})$: infatti, per ogni $\alpha, \beta \in \mathbb{C}$,

$$\begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha + \beta \\ 0 & 1 \end{bmatrix}.$$

Dunque abbiamo che $\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K}) = U(2, \mathbb{C}) \cong \mathbb{C}$.

In generale, dato un campo \mathbb{K} , denoteremo con

$$\begin{aligned}T(n, \mathbb{K}) &= \left\{ (a_{i,j})_{1 \leq i,j \leq n} \in GL(n, \mathbb{K}) : a_{i,j} = 0, i > j \right\}, \\ U(n, \mathbb{K}) &= \left\{ (a_{i,j})_{1 \leq i,j \leq n} \in GL(n, \mathbb{K}) : a_{i,i} = 1, a_{i,j} = 0, i > j \right\},\end{aligned}$$

rispettivamente, il gruppo delle matrici triangolari superiori e il gruppo delle matrici triangolari superiori unipotenti, detti anche *gruppo triangolare superiore* e *gruppo triangolare superiore unipotente* (a coefficienti in \mathbb{K}).

L'esempio precedente ci permette di trovare una differenza con la teoria classica (si veda la Proposizione 3.2):

Proposizione 3.5. *Il gruppo di Galois differenziale non è in generale un gruppo finito.*

Esempio 3.3. *Consideriamo l'equazione differenziale*

$$y'' + y = 0,$$

corrispondente all'operatore differenziale $\mathcal{L} = \frac{d^2}{dx^2} + 1$. Anche in questo caso, si verifica immediatamente che $\{\sin x, \cos x\}$ è un insieme massimale di soluzioni, e che l'estensione

$$\mathbb{K}(\sin x, \cos x) = \mathbb{L} \supset \mathbb{K}$$

è di Picard-Vessiot per \mathcal{L} .

Come nell'esempio precedente, dato $\sigma \in \text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$ devono esistere $a_{1,1}, a_{1,2}, a_{2,1}, a_{2,2} \in \mathbb{C}$ tali che

$$\begin{aligned}\sigma(\sin x) &= a_{1,1} \sin x + a_{1,2} \cos x, \\ \sigma(\cos x) &= a_{2,1} \sin x + a_{2,2} \cos x,\end{aligned}$$

Analogamente a prima, imponiamo inoltre che σ e la derivazione commutino:

$$\begin{aligned}\sigma(\cos x) &= \frac{d}{dx} \sigma(\sin x), \\ a_{2,1} \sin x + a_{2,2} \cos x &= a_{1,1} \cos x - a_{1,2} \sin x,\end{aligned}$$

da cui si deve avere, data l'indipendenza lineare delle soluzioni, $a_{1,1} = a_{2,2}$, e $a_{2,1} = -a_{1,2}$. Imponendo che $\sigma(-\sin x) = \frac{d}{dx} \sigma(\cos x)$, si trovano le stesse condizioni. A questo punto, facili verifiche mostrano che $\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$ è costituito, al variare di $\alpha, \beta \in \mathbb{C}$ (non entrambi nulli) da mappe σ tali che

$$\begin{aligned}\sigma(\sin x) &= \alpha \sin x - \beta \cos x, \\ \sigma(\cos x) &= \beta \sin x + \alpha \cos x.\end{aligned}$$

È nuovamente comodo passare in notazione matriciale: a una tale σ corrisponde la matrice

$$\begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix};$$

osserviamo che le matrici aventi questa forma formano un sottogruppo di $\text{GL}(2, \mathbb{C})$: infatti, per ogni $\alpha, \beta, \gamma, \delta \in \mathbb{C}$,

$$\begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix} \begin{bmatrix} \gamma & -\delta \\ \delta & \gamma \end{bmatrix} = \begin{bmatrix} \alpha\gamma - \beta\delta & -(\alpha\delta + \beta\gamma) \\ \alpha\delta + \beta\gamma & \alpha\gamma - \beta\delta \end{bmatrix}.$$

Infine, dato che

$$1 = \sigma(1) = \sigma(\cos^2 x + \sin^2 x) = \sigma(\cos x)^2 + \sigma(\sin x)^2 = \alpha^2 + \beta^2,$$

si ricava che

$$\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K}) \cong \left\{ \begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix} \in \text{GL}(2, \mathbb{C}) : \alpha^2 + \beta^2 = 1 \right\}.$$

Esempio 3.4. Dato $a \in \mathbb{R} - \{0\}$, consideriamo l'equazione differenziale

$$y' - \frac{a}{x}y = 0,$$

corrispondente all'operatore differenziale $\mathcal{L} = \frac{d}{dx} - \frac{a}{x}$. Un insieme massimale di soluzioni è dato da $\{x^a\}$, e l'estensione

$$\mathbb{K}(x^a) = \mathbb{L} \supset \mathbb{K}$$

è di Picard-Vessiot per \mathcal{L} . Come in precedenza, se $\sigma \in \text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$, deve esistere $\alpha \in \mathbb{C}$ tale che $\sigma(x^a) = \alpha x^a$. Ci sono due possibilità:

$a \in \mathbb{Q}$ In tal caso, possiamo scrivere $a = \frac{n}{m}$, con $n \in \mathbb{N}$, $m \in \mathbb{Z} - \{0\}$. Osserviamo che x^a è algebrico su $\mathbb{K} = \mathbb{C}(x)$, con polinomio minimo $p(t) = t^m - x^n$. Se $y(x) = \alpha x^a$ è un'altra soluzione deve valere $p(y) = 0$, da cui $\alpha^m = 1$. Abbiamo dunque trovato un vincolo su α : deve essere una radice m -esima dell'unità, ovvero

$$\alpha \in \left\{ e^{\frac{2k\pi i}{m}} : k = 0, \dots, m-1 \right\}.$$

Osserviamo che quest'ultimo è un sottogruppo di $\text{GL}(1, \mathbb{C})$, isomorfo a $\mathbb{Z}/m\mathbb{Z}$ e al gruppo di Galois differenziale.

$a \notin \mathbb{Q}$ In tal caso, osserviamo che x^a è trascendente su \mathbb{K} , e $\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$ è costituito, al variare di $\alpha \in \mathbb{C} - \{0\} = \mathbb{C}^*$ da tutte le mappe σ tali che $\sigma(x^a) = \alpha x^a$; dunque

$$\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K}) \cong \mathbb{C}^* \cong \text{GL}(1, \mathbb{C}).$$

Esempio 3.5. Consideriamo l'equazione differenziale

$$y^{(3)} - y = 0,$$

corrispondente all'operatore differenziale $\mathcal{L} = \frac{d^3}{dx^3} - 1$. Anche in questo caso, è facile verificare che un insieme massimale di soluzioni è dato da $\{e^x, e^{\zeta_3 x}, e^{\zeta_3^2 x}\}$, dove $\zeta_3 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$. Dunque, l'estensione

$$\mathbb{K}(e^x, e^{\zeta_3 x}, e^{\zeta_3^2 x}) = \mathbb{L} \supset \mathbb{K}$$

è di Picard-Vessiot per \mathcal{L} . Procedendo al solito modo, si ottiene che il gruppo di Galois differenziale corrispondente può essere visto come un sottogruppo di

$$\left\{ \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{bmatrix} : \alpha, \beta, \gamma \in \mathbb{C} - \{0\} \right\}.$$

Infine, imponendo che $1 = \sigma(e^x e^{\zeta_3 x} e^{\zeta_3^2 x}) = \alpha\beta\gamma e^x e^{\zeta_3 x} e^{\zeta_3^2 x} = \alpha\beta\gamma$, si ricava

$$\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K}) \cong \left\{ \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \frac{1}{\alpha\beta} \end{bmatrix} \in \text{GL}(3, \mathbb{C}) : \alpha, \beta \in \mathbb{C} - \{0\} \right\}.$$

In generale, dato un campo \mathbb{K} , denoteremo con

$$D(n, \mathbb{K}) = \left\{ (a_{i,j})_{1 \leq i,j \leq n} \in \text{GL}(n, \mathbb{K}) : a_{i,j} = 0, i \neq j \right\}$$

il gruppo delle matrici diagonali, o gruppo diagonale (a coefficienti in \mathbb{K}).

Esempio 3.6. Consideriamo l'equazione differenziale

$$y'' + 2xy' = 0,$$

corrispondente all'operatore differenziale $\mathcal{L} = \frac{d^2}{dx^2} + 2x \frac{d}{dx}$. Un insieme massimale di soluzioni è dato da $\{1, \mathcal{N}(x)\}$, dove

$$\begin{aligned} \mathcal{N} : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto \int_{-\infty}^x e^{-t^2} dt, \end{aligned}$$

e quindi l'estensione

$$\mathbb{K}(\mathcal{N}(x)) = \mathbb{L} \supset \mathbb{K}$$

è di Picard-Vessiot per \mathcal{L} . Si verifica facilmente che

$$\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K}) \cong \left\{ \begin{bmatrix} 1 & \alpha \\ 0 & \beta \end{bmatrix} \in \text{GL}(2, \mathbb{C}) \right\}.$$

Osserviamo che, a differenza di tutti gli esempi precedenti, questa volta il gruppo di Galois differenziale non è abeliano. In effetti si può verificare che $\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$ è il prodotto semidiretto secondo il coniugio di

$$\mathcal{H}_1 \cong \left\{ \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} \in \text{GL}(2, \mathbb{C}) \right\} \triangleleft \text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$$

e

$$\mathcal{H}_2 \cong \left\{ \begin{bmatrix} 1 & 0 \\ 0 & \beta \end{bmatrix} \in \text{GL}(2, \mathbb{C}) \right\} < \text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K});$$

in altre parole, dato che $\mathcal{H}_1 \cong \mathbb{C}$ e $\mathcal{H}_2 \cong \mathbb{C}^*$, e $\mathcal{H}_1 \cap \mathcal{H}_2 = \{\text{Id}\}$,

$$\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K}) \cong \mathbb{C} \rtimes \mathbb{C}^*.$$

In tutti gli esempi precedenti, abbiamo visto il gruppo di Galois differenziale come un sottogruppo di $\text{GL}(n, \mathbb{C})$, con n il grado dell'operatore differenziale associato all'equazione differenziale e $\mathbb{C} = \mathcal{C}_{\mathbb{K}}$, caratterizzato da relazioni di tipo polinomiale tra le componenti della matrice. Torneremo in seguito su questo fatto.

3.3. Estensioni particolari

Studiamo adesso alcune tipologie di estensioni di Picard-Vessiot da un punto di vista più generale, quelle ottenute con l'aggiunta di un solo elemento.

Estensioni con aggiunta di un integrale Diremo che $\mathbb{K}(\alpha) \supset \mathbb{K}$ è un'estensione con aggiunta di un integrale se $\alpha' \in \mathbb{K} - \{0\}$ e non esiste un elemento in \mathbb{K} la cui derivazione sia α' . L'estensione nell'esempio 3.2 è di questo tipo: infatti, un integrale

$$\mathcal{D}(\log x) = \frac{1}{x} \in \mathbb{K}.$$

Proposizione 3.6. Se $\mathbb{K}(\alpha) \supset \mathbb{K}$ è un'estensione con aggiunta di un integrale, allora α è trascendente su \mathbb{K} , l'estensione è di Picard-Vessiot e il gruppo di Galois differenziale è isomorfo a \mathbb{C} (visto come gruppo additivo).

Dimostrazione

Iniziamo con il provare che α è trascendente su \mathbb{K} . Se α fosse algebrico su \mathbb{K} , esisterebbe il suo polinomio minimo

$$p(x) = x^n + \sum_{k=1}^n b_k x^{n-k} \in \mathbb{K}[x].$$

Partendo dalla relazione $p(\alpha) = 0$ e derivando, si ottiene

$$0 = n\alpha' \alpha^{n-1} + \sum_{k=1}^n b'_k \alpha^{n-k} + \sum_{k=1}^{n-1} (n-k) b_k \alpha' \alpha^{n-1-k}.$$

Osserviamo che, dato che $\alpha' \in \mathbb{K}$ per ipotesi, il polinomio

$$q(x) = n\alpha' x^{n-1} + \sum_{k=1}^n b'_k x^{n-k} + \sum_{k=1}^{n-1} (n-k) b_k \alpha' x^{n-1-k}$$

è a coefficienti in \mathbb{K} , di grado minore di n , e si annulla in α . Per non avere subito un assurdo, annulliamo il coefficiente del termine di grado più alto: $n\alpha' + b'_n = 0$. Poiché la precedente relazione implica l'esistenza di un elemento in \mathbb{K} la cui derivazione è α' , otteniamo anche in questo caso un assurdo; quindi α non può essere algebrico su \mathbb{K} .

Proviamo adesso che l'estensione è senza costanti. Come prima, se $\sum_{k=0}^n b_k \alpha^k \in \mathbb{K}(\alpha)$ fosse costante, derivando si otterrebbe una relazione di dipendenza fra le potenze di α . Per quanto appena provato, dobbiamo imporre che tutti i coefficienti siano nulli, e in particolare

$$b'_n = nb_n \alpha' + b'_{n-1} = 0.$$

Dunque si avrebbe una contraddizione, dato che questo implica

$$\alpha' = -\frac{b'_{n-1}}{nb_n} = -\left(\frac{b_{n-1}}{nb_n}\right)' \in \mathbb{K}.$$

Similmente, si dimostra che nemmeno un generico elemento di $\mathbb{K}(\alpha)$ della forma $\frac{f(\alpha)}{g(\alpha)}$ può essere costante. Per concludere, basta osservare che 1 e α sono soluzioni dell'equazione differenziale

$$y'' - \frac{\alpha'}{\alpha} y' = 0.$$

Procedendo esattamente come nell'Esempio 3.2, si prova che il gruppo di Galois differenziale associato è isomorfo a \mathbb{C} (visto come gruppo additivo). □

Estensioni con aggiunta dell'esponenziale di un integrale Diremo che $\mathbb{K}(\alpha) \supset \mathbb{K}$ è un'estensione con aggiunta dell'esponenziale di un integrale se $\alpha \neq 0$, e inoltre $\frac{\alpha'}{\alpha} \in \mathbb{K} - \{0\}$. Un tale α verifica l'equazione differenziale $y' - \frac{\alpha'}{\alpha}y = 0$. Le estensioni negli Esempi 3.4 e 3.5 sono di questo tipo: ad esempio, nel primo caso si ha

$$\frac{ax^{a-1}}{x^a} = \frac{a}{x} \in \mathbb{K}.$$

un integrale

Nel caso dell'Esempio 3.5, abbiamo una catena di tre estensioni con aggiunta dell'esponenziale di un integrale.

Per quest'ultimo tipo di estensioni, vale il seguente risultato, la cui dimostrazione ripercorre esattamente quanto fatto nell'Esempio 3.4:

Proposizione 3.7. *Sia $\mathbb{K}(\alpha) \supset \mathbb{K}$ un'estensione con aggiunta dell'esponenziale di un integrale. Supponiamo che l'estensione sia senza costanti. Allora l'estensione è di Picard-Vessiot, e il gruppo di Galois differenziale è isomorfo a un sottogruppo del gruppo moltiplicativo $C_{\mathbb{K}} - \{0\}$.*

3.4. Gruppi algebrici

Vogliamo caratterizzare maggiormente i gruppi di Galois differenziale. Per fare questo, richiamiamo alcune nozioni sui gruppi algebrici. Dato un campo \mathbb{K} , e fissato $n \in \mathbb{N}$, chiameremo \mathbb{K}^n spazio affine di dimensione n . Vogliamo definire una topologia su \mathbb{K}^n : diremo che un sottoinsieme di \mathbb{K}^n è chiuso se è l'insieme degli zeri di una famiglia di polinomi $\{p_i(\underline{x})\}_{i \in \mathcal{I}}$ in $\mathbb{K}[x_1, \dots, x_n]$. Osserviamo che la famiglia \mathcal{Z} di tali insiemi di zeri è la famiglia dei chiusi di una topologia su \mathbb{K}^n :

$\emptyset, \mathbb{K}^n \in \mathcal{Z}$ Basta prendere come famiglie rispettivamente $\mathbb{K}[x_1, \dots, x_n]$ e quella costituita dal solo polinomio nullo;

\mathcal{Z} è stabile per unione finita Se \mathcal{C}_1 e \mathcal{C}_2 sono rispettivamente gli insiemi di zeri delle famiglie di polinomi $\{p_i(\underline{x})\}_{i \in \mathcal{I}}$ e $\{q_j(\underline{x})\}_{j \in \mathcal{J}}$, allora $\mathcal{C}_1 \cup \mathcal{C}_2$ è l'insieme di zeri della famiglia $\{p_i q_j(\underline{x})\}_{(i,j) \in \mathcal{I} \times \mathcal{J}}$;

\mathcal{Z} è stabile per intersezione qualsiasi Sia $\{\mathcal{C}_i\}_{i \in \mathcal{I}}$ una famiglia arbitraria di chiusi: per ogni $i \in \mathcal{I}$, sia Ω_i la famiglia di cui \mathcal{C}_i è l'insieme degli zeri. Allora

$$\bigcap_{i \in \mathcal{I}} \mathcal{C}_i$$

è l'insieme degli zeri di $\bigcup_{i \in \mathcal{I}} \Omega_i$.

Chiamiamo questa topologia la *topologia di Zariski* su \mathbb{K}^n . In questa topologia, si può dimostrare (si veda ad esempio [Wat79]) che una base per gli aperti è data dagli insiemi della forma

$$\mathcal{A}_p = \{z \in \mathbb{K}^n : p(z) \neq 0\},$$

detti *aperti principali*, al variare di $p(\underline{x}) \in \mathbb{K}[x_1, \dots, x_n]$.

Dati due chiusi \mathcal{S}, \mathcal{T} , diremo che

$$\phi : \mathcal{S} \rightarrow \mathcal{T}$$

$$\begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix} \mapsto \begin{bmatrix} \phi_1(s_1, \dots, s_n) \\ \vdots \\ \phi_n(s_1, \dots, s_n) \end{bmatrix}$$

è una *mappa polinomiale* se, per ogni $j = 1, \dots, n$, $\phi_j(\underline{s})$ è un polinomio. Le mappe polinomiali godono di buone proprietà, come vedremo nel prossimo risultato.

Proposizione 3.8. *Se poniamo su \mathbb{K}^n e \mathbb{K}^m ($m, n \in \mathbb{N}$) la topologia di Zariski, ogni mappa polinomiale $\phi : \mathbb{K}^n \rightarrow \mathbb{K}^m$ è continua.*

Dimostrazione

Basta provare che la controimmagine di un aperto principale in \mathbb{K}^m è un aperto in \mathbb{K}^n . Se $p(\underline{s})$ è un polinomio in $\mathbb{K}[x_1, \dots, x_m]$, si ha

$$\phi^{-1}(\mathcal{A}_p) = \{x \in \mathbb{K}^n : \phi(x) \in \mathcal{A}_p\} = \{x \in \mathbb{K}^n : p \circ \phi(x) \neq 0\} = \mathcal{A}_{p \circ \phi}.$$

□

Chiameremo *gruppo algebrico lineare* in \mathbb{K}^n un qualsiasi sottoinsieme chiuso $\mathcal{S} \in \mathbb{K}^n$ (rispetto alla topologia di Zariski) dotato di una struttura di gruppo e tale che le due mappe di composizione e di inversione

$$\begin{aligned} \star : \mathcal{S} \times \mathcal{S} &\rightarrow \mathcal{S} & \iota : \mathcal{S} &\rightarrow \mathcal{S} \\ (x, y) &\mapsto x \star y & x &\mapsto x^{-1} \end{aligned}$$

sono polinomiali.

Esempio 3.7. *Possiamo dotare \mathbb{K}^3 della struttura di gruppo algebrico lineare ad esempio con l'usuale somma di vettori, ma anche con le seguenti mappe:*

$$\begin{aligned} \star : \mathbb{K}^3 \times \mathbb{K}^3 &\rightarrow \mathbb{K}^3 & \iota : \mathbb{K}^3 &\rightarrow \mathbb{K}^3 \\ \left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}, \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} \right) &\mapsto \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 + x_1 y_2 \end{bmatrix} & \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} &\mapsto \begin{bmatrix} -x_1 \\ -x_2 \\ x_1 x_2 - x_3 \end{bmatrix}. \end{aligned}$$

Come era lecito aspettarsi, la struttura di gruppo algebrico lineare dipende dalla legge di composizione.

Il motivo per cui abbiamo introdotto questi nuovi oggetti è che possiamo identificare $\mathcal{M}(n, \mathbb{K})$ con \mathbb{K}^{n^2} , e dotarlo della topologia di Zariski. In questo senso, possiamo affermare che il determinante $\det : \mathcal{M}(n, \mathbb{K}) \rightarrow \mathbb{K}$ è una mappa polinomiale, e

$$\begin{aligned} \text{GL}(n, \mathbb{K}) &= \{A \in \mathcal{M}(n, \mathbb{K}) : \det(A) \neq 0\}, \\ \text{SL}(n, \mathbb{K}) &= \{A \in \mathcal{M}(n, \mathbb{K}) : \det(A) = 1\}. \end{aligned}$$

sono rispettivamente un aperto principale e un chiuso in $\mathcal{M}(n, \mathbb{K})$. In particolare, $\text{SL}(n, \mathbb{K})$ e i suoi sottogruppi sono tutti gruppi algebrici lineari in $\mathcal{M}(n, \mathbb{K})$.

Esempio 3.8. *Il gruppo triangolare superiore unipotente è un gruppo algebrico lineare in $\mathcal{M}(n, \mathbb{K})$.*

Concludiamo questa presentazione dei gruppi algebrici lineari mostrando che anche $\mathrm{GL}(n, \mathbb{K})$ può essere visto come tale, a patto di aumentare la dimensione dello spazio affine.

Teorema 3.5. $\mathrm{GL}(n, \mathbb{K})$ è isomorfo (come gruppo) e omeomorfo a un chiuso di $\mathrm{SL}(n+1, \mathbb{K})$.

Dimostrazione

La mappa

$$\begin{aligned} \psi : \mathrm{GL}(n, \mathbb{K}) &\rightarrow \mathrm{SL}(n+1, \mathbb{K}) \\ A &\mapsto \left[\begin{array}{c|c} A & 0 \\ \hline 0 & 1/\det A \end{array} \right] \end{aligned}$$

è un omomorfismo di gruppi, in quanto, per ogni $A, B \in \mathrm{GL}(n, \mathbb{K})$

$$\psi(A)\psi(B) = \left[\begin{array}{c|c} A & 0 \\ \hline 0 & 1/\det A \end{array} \right] \left[\begin{array}{c|c} B & 0 \\ \hline 0 & 1/\det B \end{array} \right] = \left[\begin{array}{c|c} AB & 0 \\ \hline 0 & 1/\det AB \end{array} \right] = \psi(AB).$$

Inoltre, ψ è chiaramente iniettiva. Per il primo teorema di omomorfismo, $\mathrm{GL}(n, \mathbb{K})$ è isomorfo alla sua immagine \mathcal{I} in $\mathrm{SL}(n+1, \mathbb{K})$ mediante la mappa

$$\begin{aligned} \tilde{\psi} : \mathrm{GL}(n, \mathbb{K}) &\rightarrow \mathcal{I} \\ A &\mapsto \psi(A). \end{aligned}$$

Osserviamo che \mathcal{I} è chiuso, in quanto è descritto dalle equazioni polinomiali

$$\begin{cases} x_{n+1,1} = \cdots = x_{n+1,n} = 0 \\ x_{1,n+1} = \cdots = x_{n,n+1} = 0 \\ \det(x_{i,j})_{1 \leq i,j \leq n} - x_{n+1,n+1} = 0. \end{cases}$$

Più in generale, l'immagine di ogni sottoinsieme $\mathcal{S} \subset \mathrm{GL}(n, \mathbb{K})$ relativamente chiuso in $\mathrm{GL}(n, \mathbb{K})$ ⁴ è relativamente chiusa in \mathcal{I} . Similmente, se \mathcal{C} è un chiuso in $\mathrm{SL}(n+1, \mathbb{K})$ allora $\psi^{-1}(\mathcal{C} \cap \mathcal{I})$ è ancora un chiuso. Quindi, la mappa $\tilde{\psi}$ è anche un omeomorfismo. \square

Possiamo caratterizzare i gruppi di Galois differenziali mediante i gruppi algebrici lineari, come mostra il prossimo risultato.

Teorema 3.6. (Kolchin) Sia $\mathbb{L} = \mathbb{K}(y_1, \dots, y_n) \supset \mathbb{K}$ un'estensione di Picard-Vessiot (per il Teorema 3.4, non è necessario specificare per quale operatore differenziale). Allora esiste una famiglia di polinomi

$$\mathcal{S} \subset \mathcal{C}_{\mathbb{K}}[(x_{i,j})_{1 \leq i,j \leq n}]$$

tale che

◇ Se $\sigma \in \mathrm{Gal}^{\mathrm{Diff}}(\mathbb{L}/\mathbb{K})$ e

$$\sigma \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = C \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \quad C = (c_{i,j})_{1 \leq i,j \leq n} \in \mathrm{GL}(n, \mathcal{C}_{\mathbb{K}}),$$

allora $F(C) = 0$ per ogni $F \in \mathcal{S}$.

⁴Ovvero, esiste un chiuso \mathcal{C} in $\mathcal{M}(n, \mathbb{K})$ tale che $\mathcal{C} \cap \mathrm{GL}(n, \mathbb{K}) = \mathcal{S}$.

◇ Se $C \in GL(n, \mathbb{C}_{\mathbb{K}})$ è tale che $F(C) = 0$ per ogni $F \in \mathcal{S}$, allora esiste $\sigma \in \text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$ tale che

$$\sigma \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = C \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$$

In particolare, $\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$ è sottogruppo chiuso di $GL(n, \mathbb{C}_{\mathbb{K}})$, e quindi un gruppo algebrico lineare.

Dimostrazione

Si veda [CH11].

□

3.5. La corrispondenza di Galois

Concludiamo questo capitolo con il teorema fondamentale della teoria di Galois differenziale, che vedremo essere completamente analogo a quello della teoria di Galois classica. Sia $\mathbb{L} \supset \mathbb{K}$ un'estensione di Picard-Vessiot: denotiamo con $\mathcal{C}_{\mathbb{L}/\mathbb{K}}^{\text{Diff}}$ la famiglia dei sottocampi differenziali dell'estensione, con $\overline{\mathcal{G}}_{\mathbb{L}/\mathbb{K}}$ la famiglia dei sottogruppi chiusi di $\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$.

Osserviamo che se $\mathbb{F} \in \mathcal{C}_{\mathbb{L}/\mathbb{K}}^{\text{Diff}}$, allora anche $\mathbb{L} \supset \mathbb{F}$ è un'estensione di Picard-Vessiot (è sufficiente considerare lo stesso operatore differenziale dell'estensione $\mathbb{L} \supset \mathbb{K}$, e considerarlo a coefficienti in \mathbb{F}), con gruppo di Galois differenziale

$$\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{F}) = \{\sigma \in \text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K}) : \sigma|_{\mathbb{F}} = \text{Id}_{\mathbb{F}}\}.$$

Definiamo le seguenti mappe:

$$\begin{array}{ccc} \alpha' : \mathcal{C}_{\mathbb{L}/\mathbb{K}}^{\text{Diff}} & \rightarrow & \overline{\mathcal{G}}_{\mathbb{L}/\mathbb{K}} \\ \mathbb{F} & \mapsto & \text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{F}) \end{array} \qquad \begin{array}{ccc} \beta' : \overline{\mathcal{G}}_{\mathbb{L}/\mathbb{K}} & \rightarrow & \mathcal{C}_{\mathbb{L}/\mathbb{K}}^{\text{Diff}} \\ \mathcal{H} & \mapsto & \text{Fix}^{\text{Diff}}(\mathcal{H}) \end{array} \qquad (3.6)$$

Teorema 3.7. (Kolchin) Sia $\mathbb{L} \supset \mathbb{K}$ un'estensione di Picard-Vessiot, con gruppo di Galois differenziale $\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$. Allora:

- ◇ **(Corrispondenza di Galois, versione differenziale)** Le mappe definite in (3.6) sono una l'inversa dell'altra.
- ◇ Preso $\mathbb{F} \in \mathcal{C}_{\mathbb{L}/\mathbb{K}}^{\text{Diff}}$, l'estensione $\mathbb{F} \supset \mathbb{K}$ è di Galois se e solo se $\alpha'(\mathbb{F})$ è un sottogruppo normale del gruppo di Galois dell'estensione, e in tal caso

$$\text{Gal}(\mathbb{F}/\mathbb{K}) \cong \text{Gal}(\mathbb{L}/\mathbb{K}) / \alpha(\mathbb{F}).$$

Dimostrazione

Dimostreremo solo la corrispondenza di Galois. Per una dimostrazione completa si veda [CH11].

Dalle definizioni, si vede che per ogni $\mathbb{F}_1, \mathbb{F}_2 \in \mathcal{C}_{\mathbb{L}/\mathbb{K}}^{\text{Diff}}$ e $\mathcal{H}_1, \mathcal{H}_2 \in \overline{\mathcal{G}}_{\mathbb{L}/\mathbb{K}}^{\text{Diff}}$ tali che $\mathcal{H}_1 \subset \mathcal{H}_2$, $\mathbb{F}_1 \subset \mathbb{F}_2$, si ha

$$\alpha'(\mathbb{F}_1) \supset \alpha'(\mathbb{F}_2), \quad \beta'(\mathcal{H}_1) \supset \beta'(\mathcal{H}_2).$$

Inoltre, è facile vedere che per ogni $\mathbb{F} \in \mathcal{C}_{\mathbb{L}/\mathbb{K}}^{\text{Diff}}$ si ha

$$\text{Fix}^{\text{Diff}}(\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{F})) = \mathbb{F},$$

cioè che $\beta' \circ \alpha'$ è l'identità su $\mathcal{C}_{\mathbb{L}/\mathbb{K}}^{\text{Diff}}$: infatti abbiamo già osservato che l'estensione $\mathbb{L} \supset \mathbb{F}$ è di Picard-Vessiot, e dunque concludiamo per il Corollario 3.1.

Resta da provare che, per ogni sottogruppo chiuso \mathcal{H} di $\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$, si ha l'uguaglianza

$$\text{Gal}^{\text{Diff}}(\mathbb{L}/\text{Fix}^{\text{Diff}}(\mathcal{H})) = \mathcal{H}.$$

Dalle definizioni è chiaro che vale l'inclusione $\text{Gal}^{\text{Diff}}(\mathbb{L}/\text{Fix}^{\text{Diff}}(\mathcal{H})) \supset \mathcal{H}$. Per provare anche l'uguaglianza, dimostreremo che, preso un sottogruppo qualsiasi \mathcal{H} di $\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$, allora

$$\mathcal{H}' = \text{Gal}^{\text{Diff}}(\mathbb{L}/\text{Fix}^{\text{Diff}}(\mathcal{H}'))$$

è la sua chiusura. Osserviamo che, per quanto appena provato,

$$\text{Fix}^{\text{Diff}}(\mathcal{H}') = \text{Fix}^{\text{Diff}}(\text{Gal}^{\text{Diff}}(\mathbb{L}/\text{Fix}^{\text{Diff}}(\mathcal{H}')))) = \text{Fix}^{\text{Diff}}(\mathcal{H}).$$

Nel seguito, supporremo che $\mathbb{L} = \mathbb{K}(y_1, \dots, y_n) \supset \mathbb{K}$ sia di Picard-Vessiot per un operatore differenziale di grado n , e considereremo $\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$ come un gruppo algebrico lineare: in particolare, vedremo i suoi elementi come matrici, le cui componenti sono legate da relazioni di tipo polinomiale; per ogni $\sigma \in \text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$, denotiamo con \mathcal{M}_σ la matrice tale che

$$\sigma \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \mathcal{M}_\sigma \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}.$$

Supponiamo per assurdo che $\overline{\mathcal{H}} \neq \mathcal{H}'$: allora, esiste $f : \text{GL}(n, \mathbb{C}_{\mathbb{K}}) \rightarrow \mathbb{L}$ tale che $f|_{\mathcal{H}} = 0$ ma $f|_{\mathcal{H}'} \neq 0$. Denotiamo con u_1, \dots, u_n delle indeterminate differenziali, e sia U la matrice Wronskiana associata ad esse. Sia poi A la matrice Wronskiana associata alla n -upla (y_1, \dots, y_n) : per il Teorema 2.1, tale matrice è invertibile. Poniamo $F(u_1, \dots, u_n) = f(UA^{-1})$: per le ipotesi su f , si ha

$$F \left(\sigma \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \right) = f(\mathcal{M}_\sigma AA^{-1}) = f(\mathcal{M}_\sigma) = 0$$

per ogni $\sigma \in \mathcal{H}$, ma non per tutti i $\sigma \in \mathcal{H}'$. Senza perdere in generalità, possiamo scegliere F tra tutti i polinomi con le precedenti proprietà in modo tale che abbia il numero minimo di monomi non nulli. Possiamo anche assumere che almeno un monomio di F abbia coefficiente uguale a 1.

Preso $\tau \in \mathcal{H}$, denotiamo con τF il polinomio ottenuto a partire da F applicando τ a tutti i suoi coefficienti. In particolare, si ha

$$(\tau F) \left(\sigma \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \right) = \tau \left(F \left(\tau^{-1} \sigma \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \right) \right).$$

Ma allora $F - \tau F$ è un polinomio costituito da un numero inferiore di monomi rispetto a F , e si annulla su $(\sigma(y_1, \dots, y_n))^T$ per ogni $\sigma \in \mathcal{H}$. Per le ipotesi di minimalità su F , $F - \tau F$ deve annullarsi anche su $(\sigma(y_1, \dots, y_n))^T$ per ogni $\sigma \in \mathcal{H}'$: osserviamo che $F - \tau F$ deve essere identicamente nullo, dato che altrimenti potremmo trovare un $x \in \mathbb{L}$ tale che $F - x(F - \tau F)$ sia costituito da un numero inferiore di monomi rispetto a F e possieda le stesse proprietà di quest'ultimo.

Di conseguenza, $F - \tau F$ è il polinomio nullo per ogni $\tau \in \mathcal{H}$, e questo implica che i coefficienti di F non vengono modificati dall'azione di \mathcal{H} , cioè sono in $\text{Fix}^{\text{Diff}}(\mathcal{H}) = \text{Fix}^{\text{Diff}}(\mathcal{H}')$. Ma allora, preso un qualsiasi $\sigma \in \mathcal{H}'$, si ha

$$F \left((\sigma(y_1), \dots, \sigma(y_n))^T \right) = (\sigma F) \left((\sigma(y_1), \dots, \sigma(y_n))^T \right) = \sigma \left(F(y_1, \dots, y_n) \right) = 0,$$

e questo è assurdo, per le ipotesi su F . □

Esempio 3.9. Prendiamo $\mathbb{K} = \mathbb{C}(x)$, dotato della derivazione usuale, e consideriamo l'equazione differenziale

$$y' - y = 0,$$

corrispondente all'operatore differenziale $\mathcal{L} = \frac{d}{dx} - 1$. L'estensione di Picard-Vessiot associata è $\mathbb{L} = \mathbb{K}(e^x)$. Osserviamo che quest'ultima è un'estensione con aggiunta dell'esponenziale di un integrale: per la Proposizione 3.7, il suo gruppo di Galois differenziale è isomorfo a un sottogruppo del gruppo moltiplicativo \mathbb{C}^* : in realtà, procedendo allo stesso modo degli esempi precedenti, si verifica che il gruppo di Galois differenziale è proprio isomorfo a \mathbb{C}^* .

Operatore differenziale associato	Estensione di Picard-Vessiot $\mathbb{E} \supset \mathbb{K}$	Gruppo di Galois differenziale $\text{Gal}^{\text{Diff}}(\mathbb{E}/\mathbb{K})$
$\frac{d}{dx} - 1$	$\mathbb{K}(e^x)$	$\{1\}$
	\cup	\cap
$\frac{d}{dx} - m$	$\mathbb{K}(e^{mx})$	\mathcal{U}_m
	\cup	\cap
$\frac{d}{dx} - n$	$\mathbb{K}(e^{nx})$	\mathcal{U}_n
	\cup	\cap
	\mathbb{K}	\mathbb{C}^*

Figura 3.1: Un esempio di corrispondenza di Galois

Grazie al teorema fondamentale dell'algebra, si vede che tutti i sottogruppi chiusi di \mathbb{C}^* sono i gruppi, al variare di $n \in \mathbb{N}$,

$$\mathcal{U}_n = \left\{ e^{\frac{2ik\pi}{n}} : k = 0, \dots, n-1 \right\}.$$

Essendo \mathbb{C}^* abeliano, questi sottogruppi sono tutti normali, e quindi sono delle estensioni di $\mathbb{C}(x)$ di Picard-Vessiot per qualche operatore. Nella figura è descritta la corrispondenza di Galois per la catena di estensioni $\mathbb{K} \subset \mathbb{K}(e^{nx}) \subset \mathbb{K}(e^{mx}) \subset \mathbb{L}$ (con m divisore di n).

Equazioni differenziali Fuchsiane

Introduzione

Dopo aver introdotto le equazioni differenziali Fuchsiane, una sottoclasse delle equazioni differenziali a coefficienti in $\mathbb{C}(z)$ con alcune ipotesi di regolarità sui coefficienti, dimostriamo che, per queste ultime, in un intorno di ciascun punto $P \in \mathbb{P}^1(\mathbb{C})$ esiste almeno una soluzione esprimibile nella forma di una serie di potenze. In seguito vediamo come tali soluzioni si raccordano: introduciamo il gruppo di monodromia e dimostriamo il teorema di Schlesinger, che mette in relazione quest'ultimo con il gruppo di Galois differenziale associato all'estensione di Picard-Vessiot corrispondente all'equazione differenziale Fuchsiana. Dopo un primo studio dell'equazione ipergeometrica di Gauss, equazione che ha una discreta importanza in quanto tutta una classe di equazioni Fuchsiane si può ricondurre a quest'ultima, concludiamo il capitolo vedendo come, mediante alcune proprietà legate al gruppo di Galois differenziale, la teoria di Picard-Vessiot sia in grado di dare delle risposte sul tipo di soluzioni dell'equazione Fuchsiana.

Dove non è altrimenti specificato, consideriamo il campo $\mathbb{C}(z)$ come campo differenziale munito della derivazione usuale, e denotiamo con $\infty \in \mathbb{P}^1(\mathbb{C})$ il punto all'infinito.

4.1. Definizioni e prime proprietà

Consideriamo un operatore differenziale lineare monico omogeneo a coefficienti in $\mathbb{C}(z)$,

$$\mathcal{D} = \frac{d^n}{dz^n} + a_1(z) \frac{d^{n-1}}{dz^{n-1}} + \dots + a_{n-1}(z) \frac{d}{dz} + a_n(z),$$

e consideriamo l'equazione differenziale lineare associata

$$\mathcal{D}(Y) = 0. \tag{4.1}$$

Diremo che $P \in \mathbb{C}$ è un *punto regolare* per l'equazione differenziale (4.1) se tutti i coefficienti sono funzioni analitiche in P , mentre diremo che è un *punto singolare* se non è regolare. Similmente, diremo che ∞ è un punto regolare, o singolare, per l'equazione (4.1) se $z_0 = 0$ lo è per l'equazione differenziale ottenuta mediante la sostituzione $z \mapsto \frac{1}{z}$.

Esempio 4.1. Consideriamo un'equazione differenziale di ordine 2 :

$$Y'' + a_1(z)Y' + a_2(z)Y = 0. \tag{4.2}$$

Mediante il cambio di variabili $z = \frac{1}{x}$, otteniamo l'equazione differenziale¹

$$\begin{aligned} x^4 Y'' + \left(2x^3 - a_1 \left(\frac{1}{x} \right) x^2 \right) Y' + a_2 \left(\frac{1}{x} \right) Y &= 0, \\ Y'' + \left(\frac{2x - a_1 \left(\frac{1}{x} \right)}{x^2} \right) Y' + \frac{a_2 \left(\frac{1}{x} \right)}{x^4} Y &= 0, \\ Y'' + b_1(x) Y' + b_2(x) Y &= 0. \end{aligned}$$

Nel caso in cui $P \in \mathbb{C}$ sia un punto singolare per (4.1), diremo che P è un *punto singolare regolare* se, per ogni $k = 1, \dots, n$, esistono e sono finiti i limiti

$$\lim_{z \rightarrow P} (z - P)^k a_k(z).$$

Analogamente a prima, diremo che ∞ è singolare regolare se $z_0 = 0$ lo è per l'equazione differenziale ottenuta mediante la sostituzione $z \mapsto \frac{1}{z}$.

Un'equazione differenziale della forma (4.1) è *Fuchsiana* se ogni punto $P \in \mathbb{P}^1(\mathbb{C})$ è regolare oppure singolare regolare.

Esempio 4.2. Consideriamo l'equazione differenziale

$$Y' - \frac{1}{z} Y = 0.$$

Mediante il cambio di variabili $z = \frac{1}{x}$, otteniamo l'equazione differenziale

$$\begin{aligned} -x^2 Y' - x Y &= 0, \\ Y' + \frac{1}{x} Y &= 0. \end{aligned}$$

I punti $0, \infty$ sono singolari regolari per l'equazione di partenza. Tutti gli altri punti sono regolari.

La seguente proposizione caratterizza i coefficienti di un'equazione differenziale Fuchsiana con un numero finito di punti singolari regolari in \mathbb{C} :

Proposizione 4.1. Se l'equazione (4.1) è Fuchsiana, con un numero finito di punti singolari regolari $P_1, \dots, P_m \in \mathbb{C}$, allora, per ogni $k = 1, \dots, n$, esiste un polinomio $A_k(z) \in \mathbb{C}[z]$, di grado minore o uguale a $k(m-1)$ tale che

$$a_k(z) = \frac{A_k(z)}{\prod_{s=1}^m (z - P_s)}.$$

¹Applichiamo la regola della derivazione a catena:

$$\begin{aligned} \frac{dY}{dz} &= \frac{dY}{dx} \frac{dx}{dz} = -x^2 \frac{dY}{dx}, \\ \frac{d^2 Y}{dz^2} &= \frac{d}{dz} \left(\frac{dY}{dx} \frac{dx}{dz} \right) = \frac{d^2 Y}{dx^2} \left(\frac{dx}{dz} \right)^2 + \frac{dY}{dx} \frac{d^2 x}{dz^2} = x^4 \frac{d^2 Y}{dx^2} + 2x^3 \frac{dY}{dx}. \end{aligned}$$

In particolare, esistono delle costanti $A_{1,1}, \dots, A_{1,m} \in \mathbb{C}$ tali che

$$a_1(z) = \sum_{s=1}^m \frac{A_{1,s}}{(z - P_s)}.$$

Dimostrazione

Fissiamo $k \in \{1, \dots, n\}$. Per definizione di punto singolare regolare, e dato che per ipotesi non ci sono altri punti singolari, esiste una funzione intera $A_k : \mathbb{C} \rightarrow \mathbb{C}$ tale che

$$a_k(z) = A_k(z) \prod_{s=1}^m (z - P_s)^{-k}.$$

Inoltre, sempre per ipotesi, il punto all'infinito è al più un polo per $a_k(z)$: pertanto, $A_k(z)$ è un polinomio, di grado minore o uguale a $k(m-1)$, dovendo essere finito il limite

$$\lim_{z \rightarrow \infty} z^k a_k(z).$$

Nel caso $k = 1$, A_1 è un polinomio di grado $m-1$, quindi è completamente determinato dal valore che esso assume sugli m punti singolari regolari: dato che $a_1(z)$ e

$$\sum_{s=1}^m \frac{A_1(P_s)}{\prod_{\substack{1 \leq p \leq m \\ p \neq s}} (P_s - P_t)} \frac{1}{z - P_s}$$

assumono lo stesso valore su tali punti, essi devono necessariamente coincidere. Quindi, prendendo

$$A_{1,s} = \frac{A_1(P_s)}{\prod_{\substack{1 \leq p \leq m \\ p \neq s}} (P_s - P_t)}$$

per ogni $s = 1, \dots, m$, si ha la tesi. □

4.2. Soluzioni formali ed equazione indiciale

Vogliamo studiare il problema dell'esistenza locale di soluzioni di un'equazione differenziale Fuchsiana nell'intorno di un punto, sia esso regolare o singolare regolare. Questo richiede un lavoro preliminare.

Consideriamo l'operatore differenziale $\mathcal{L} = z \frac{d}{dz}$: vogliamo scrivere l'equazione (4.1) in termini di quest'ultimo operatore.

Lemma 4.1. Per ogni $r \in \mathbb{N}$, valgono le uguaglianze

$$\frac{d^r}{dz^r} \circ z = r \frac{d^{r-1}}{dz^{r-1}} + z \frac{d^r}{dz^r}, \quad (4.3)$$

$$z^r \frac{d^r}{dz^r} = \mathcal{L} \circ (\mathcal{L} - 1) \circ \cdots \circ (\mathcal{L} - r + 1). \quad (4.4)$$

Dimostrazione

Iniziamo con (4.3) e procediamo per induzione su r : il passo base ($r = 1$) segue immediatamente:

$$\frac{d}{dz} \circ z = \frac{d}{dz}(z) + z \frac{d}{dz} = 1 + z \frac{d}{dz}.$$

Supponiamo che (4.3) sia verificata per r , allora

$$\begin{aligned} \frac{d^{r+1}}{dz^{r+1}} \circ z &= \frac{d}{dz} \circ \left(\frac{d^r}{dz^r} \circ z \right) = \frac{d}{dz} \circ \left(r \frac{d^{r-1}}{dz^{r-1}} + z \frac{d^r}{dz^r} \right) \\ &= r \frac{d^r}{dz^r} + \frac{d}{dz}(z) \frac{d^r}{dz^r} + z \frac{d^{r+1}}{dz^{r+1}} = (r+1) \frac{d^r}{dz^r} + z \frac{d^{r+1}}{dz^{r+1}}. \end{aligned}$$

Per il principio di induzione, (4.3) è dimostrata per ogni $r \in \mathbb{N}$.

Proviamo allo stesso modo la seconda identità: il passo base ($r = 1$) è verificato per definizione di \mathcal{L} . Supponiamo che la (4.4) sia verificata per r : allora, tenendo conto dell'identità (1.5),

$$\begin{aligned} &\mathcal{L} \circ (\mathcal{L} - 1) \circ \cdots \circ (\mathcal{L} - r + 1) \circ (\mathcal{L} - r) \\ &= z^r \frac{d^r}{dz^r} \circ (\mathcal{L} - r) = z^r \frac{d^r}{dz^r} \circ z \frac{d}{dz} - z^r \frac{d^r}{dz^r} \circ r \\ &= z^r \sum_{h=0}^r \binom{r}{h} \frac{d^h}{dz^h}(z) \frac{d^{r-h+1}}{dz^{r-h+1}} - r z^r \frac{d^r}{dz^r} \\ &= z^r \left(z \frac{d^{r+1}}{dz^{r+1}} + r \frac{d^r}{dz^r} \right) - r z^r \frac{d^r}{dz^r} = z^{r+1} \frac{d^{r+1}}{dz^{r+1}}. \end{aligned}$$

□

Ripartiamo dall'equazione differenziale (4.1), e moltiplichiamola per z^n :

$$z^n \frac{d^n Y}{dz^n} + z a_1(z) z^{n-1} \frac{d^{n-1} Y}{dz^{n-1}} + \cdots + z^{n-1} a_{n-1}(z) z \frac{dY}{dz} + a_n(z) Y = 0.$$

Usando l'identità (4.4), è possibile riscrivere quest'ultima equazione nella forma

$$\mathcal{L}^{(n)}(Y) + b_1(z) \mathcal{L}^{(n-1)}(Y) + \cdots + b_{n+1}(z) \mathcal{L}(Y) + b_n(z) Y = 0, \quad (4.5)$$

dove

$$\begin{aligned} b_1(z) &= z a_1(z) - \sum_{r_1=1}^{n-1} r_1 = z a_1(z) - \frac{n(n-1)}{2}, \\ b_n(z) &= z^n a_n(z) \end{aligned}$$

e, per ogni $j = 2, \dots, n-1$,

$$\begin{aligned} b_j(z) &= z^j a_j(z) + \sum_{1 \leq r_1 < \cdots < r_j \leq n-1} (-1)^j r_1 \cdots r_j + \\ &+ \sum_{k=1}^{j-1} (-1)^{j-k} z^k a_k(z) \sum_{1 \leq r_1 < \cdots < r_{j-k} \leq n-k-1} r_1 \cdots r_{j-k}. \end{aligned} \quad (4.6)$$

Proposizione 4.2. *Le seguenti due affermazioni sono equivalenti:*

- ◇ Per ogni $j = 1, \dots, n$, esistono, e sono finiti, i limiti $\lim_{z \rightarrow 0} z^j a_j(z)$;
- ◇ Per ogni $j = 1, \dots, n$, la funzione $b_j(z)$ è olomorfa in un intorno di $z_0 = 0$, oppure è prolungabile analiticamente a una funzione olomorfa in un intorno di $z_0 = 0$.

Dimostrazione

⇒ Per ipotesi, $b_j(z)$ è somma finita di funzioni olomorfe o prolungabili analiticamente a funzioni olomorfe in un intorno di $z_0 = 0$, e quindi è una funzione olomorfa o prolungabile analiticamente a una funzione olomorfa in un intorno di tale punto.

⇐ Dall'equazione (4.6), ricaviamo

$$za_1(z) = b_1(z) + \frac{n(n-1)}{2},$$

ed essendo $b_1(z)$ olomorfa in un intorno di $z_0 = 0$, o prolungabile analiticamente a una funzione olomorfa in un intorno di tale punto, si vede subito che esiste, finito, il limite $\lim_{z \rightarrow 0} za_1(z)$. Osserviamo che, sempre per (4.6), $b_2(z)$ è combinazione lineare (a coefficienti a interi) di $za_1(z)$ e $z^2 a_2(z)$, quindi, per quanto appena provato e poiché anche $b_2(z)$ è olomorfa in un intorno di $z_0 = 0$, o prolungabile analiticamente a una funzione olomorfa in un intorno di tale punto, anche il limite $\lim_{z \rightarrow 0} z^2 a_2(z)$ esiste, finito. Iterando il ragionamento, si arriva alla tesi. □

4.2.1. Soluzioni nell'intorno di un punto regolare

Il seguente teorema ci permette di vedere che possiamo ottenere delle soluzioni formali per l'equazione differenziale (4.1) in un intorno di un punto regolare. A meno di un cambio di variabili, possiamo supporre che tale punto sia $z_0 = 0$, in modo da poter usare quanto fatto finora.

Teorema 4.1. (Cauchy) *Sia $z_0 = 0$ un punto regolare per l'equazione differenziale (4.1). Allora esistono n serie di potenze con raggio di convergenza strettamente positivo $F_0(z), \dots, F_{n-1}(z)$, che sono soluzioni di tale equazione e sono linearmente indipendenti su \mathbb{C} . Inoltre, ogni serie di potenze che è soluzione dell'equazione differenziale (4.1) è combinazione lineare (a coefficienti in \mathbb{C}) di F_0, \dots, F_{n-1} .*

Dimostrazione

Come in precedenza, moltiplichiamo (4.1) per z^n e usiamo l'identità (4.4):

$$\begin{aligned} & \mathcal{L} \circ (\mathcal{L} - 1) \circ \dots \circ (\mathcal{L} - n + 1)(Y) + \\ & + \sum_{k=1}^n z^k a_k(z) \mathcal{L} \circ (\mathcal{L} - 1) \circ \dots \circ (\mathcal{L} - (n - k) + 1)(Y) = 0. \end{aligned} \quad (4.7)$$

Per ogni $k = 1, \dots, n$, e per ogni $j \in \mathbb{N}$, usando la Proposizione 4.2 poniamo

$$z^k a_k(z) = \sum_{j=k}^{\infty} a_{k,j} z^j,$$

$$Q_j(X) = \sum_{m=1}^j a_{m,j} X(X-1) \dots (X-(n-m)+1),$$

e cerchiamo soluzioni in forma di serie di potenze $Y = \sum_{k=0}^{\infty} c_k z^k$. Sostituendo nell'equazione (4.7) e andando a vedere i coefficienti si ottengono, al variare di $k = 0, 1, \dots$, delle relazioni per ricorrenza:

$$k(k-1) \dots (k-n+1)c_k + \sum_{j=1}^k Q_j(k)c_{k-j} = 0. \quad (4.8)$$

Osserviamo che, se $1 \leq j \leq k \leq n-1$, allora $Q_j(k-j) = 0$: dunque per $k = 0, \dots, n-1$ la corrispondente equazione per ricorrenza è banale. Pertanto, possiamo scegliere i coefficienti c_0, \dots, c_{n-1} in modo arbitrario: una volta fatta questa scelta, le relazioni (4.8) determinano univocamente i restanti coefficienti. In questo modo, si ottengono n soluzioni formali dell'equazione (4.7), linearmente indipendenti su \mathbb{C} : una possibile scelta potrebbe essere quella di prendere, al variare di $j = 0, \dots, n-1$, la soluzione F_j ottenuta scegliendo $c_k = \delta_{j,k}$, al variare di $k = 0, \dots, n-1$.

Proviamo adesso che le serie di potenze che abbiamo visto essere soluzioni formali dell'equazione differenziale hanno raggio di convergenza strettamente positivo; per farlo, è sufficiente vedere che i rispettivi coefficienti sono esponenzialmente limitati. Sia C un numero reale maggiore di 1 tale che siano soddisfatte le seguenti condizioni:

◇ per ogni $j, k \in \mathbb{N}$,

$$|Q_j(k)| < C^j k^{n-1};$$

◇ per ogni $k = 0, 1, \dots, n-1$,

$$|c_k| < C^{2k+1};$$

◇ per ogni $k \geq n$,

$$\frac{1}{k(k-1) \dots (k-n+1)} < \frac{C}{k^n}.$$

Proviamo per induzione su k che per ogni $k \in \mathbb{N}$ vale la seguente disuguaglianza, che implica immediatamente la tesi:

$$|c_k| < C^{2k+1}.$$

Il passo base ($k = 1$) è immediato, dato che per $k < n$ la precedente disuguaglianza è verificata per ipotesi.

Supponiamo adesso che quest'ultima sia verificata per $j = 1, \dots, k-1$, con $k \geq n$: dalla

relazione (4.8) ricaviamo allora

$$\begin{aligned}
 |c_k| &= \frac{1}{k(k-1)\dots(k-n+1)} \left| \sum_{j=1}^k Q_j(k) c_{k-j} \right| \\
 &\leq \frac{C}{k^n} \sum_{j=1}^k |Q_j(k)| |c_{k-j}| < \frac{C}{k^n} \sum_{j=1}^k C^j k^{n-1} C^{2(k-j)+1} \\
 &= \frac{C}{k^n} k^{n-1} C^{2k+1} \sum_{j=1}^k C^{-j} < \frac{C}{k^n} k^{n-1} C^{2k+1} \frac{k}{C} = C^{2k+1}.
 \end{aligned}$$

□

4.2.2. Soluzioni nell'intorno di un punto singolare regolare

Supponiamo adesso che $z_0 = 0$ sia un punto singolare regolare per l'equazione differenziale (4.1). Anche in questo caso, cerchiamo delle soluzioni in forma di serie di potenze, ma con un fattore correttivo davanti:

$$Y = z^\rho \sum_{k=0}^{\infty} c_k z^k,$$

dove supponiamo $c_0 \neq 0$.

Per la Proposizione 4.2, è possibile sviluppare i coefficienti dell'equazione (4.5) in serie di Taylor:

$$b_k(z) = \sum_{j=0}^{\infty} b_{k,j} z^j.$$

Definiamo, inoltre, i polinomi

$$P_0(x) = x^n + \sum_{k=1}^n b_{k,j} x^{n-k},$$

e

$$P_j(x) = \sum_{k=1}^n b_{k,j} x^{n-k}$$

al variare di $j \in \mathbb{N}$; denotiamo infine con $P_j(\mathcal{L})$ i corrispondenti operatori differenziali lineari in $\mathbb{C}(z)[\mathcal{L}]$. Allora

$$\begin{aligned}
 0 &= \mathcal{L}^{(n)}(Y) + b_1(z)\mathcal{L}^{(n-1)}(Y) + \dots + b_{n+1}(z)\mathcal{L}(Y) + b_n(z)Y \\
 &= \sum_{j=0}^{\infty} P_j(\mathcal{L})(Y) z^j = \sum_{j=0}^{\infty} P_j(\mathcal{L}) \left(z^\rho \sum_{k=0}^{\infty} c_k z^k \right) z^j \\
 &= \sum_{k=0}^{\infty} \sum_{j=0}^{\infty} P_j(\mathcal{L})(c_k z^{\rho+k}) z^j = \sum_{k=0}^{\infty} c_k \sum_{j=0}^{\infty} P_j(\rho+k) z^{j+k+\rho},
 \end{aligned}$$

da cui, riordinando, si ricava

$$\sum_{m=0}^{\infty} \left[\sum_{j=0}^m c_j P_{m-j}(\rho + j) \right] z^{m+\rho} = 0.$$

Dunque, per ogni $m = 0, 1, \dots$, devono essere soddisfatte le relazioni seguenti:

$$\sum_{j=0}^m c_j P_{m-j}(\rho + j) = 0. \quad (4.9)$$

Dato che c_0 è non nullo, è necessario che ρ sia una soluzione dell'equazione polinomiale

$$P_0(x) = x^n + b_1(0)x^{n-1} + \dots + b_n(0) = 0, \quad (4.10)$$

che chiameremo *equazione indiciale* nel punto $z_0 = 0$. Chiameremo le sue soluzioni *esponenti locali* nel punto $z_0 = 0$. Se supponiamo che le radici di $P_0(x)$ siano tutte semplici, le soluzioni corrispondenti ai vari esponenti locali hanno tutte raggio di convergenza strettamente positivo, e formano una base di un \mathbb{C} -spazio vettoriale n -dimensionale di soluzioni: per una dimostrazione di questo fatto, si veda [Poo60].

Se invece due esponenti locali differiscono per un numero intero, oppure almeno uno di essi ha molteplicità strettamente maggiore di 1, ci possono essere delle complicazioni: ad esempio, può capitare che non si ottengano n soluzioni indipendenti, o che alcune delle condizioni (4.9) siano incompatibili: in tal caso si cercano soluzioni della forma

$$Y = z^\rho \sum_{k=0}^{\infty} \mathcal{L}_k(\log z) z^k,$$

dove, per ogni $k = 0, 1, \dots$, $\mathcal{L}_k(z)$ è un polinomio di grado strettamente minore di n . Per i nostri scopi non ci servirà approfondire ulteriormente questa eventualità, ma una trattazione più dettagliata si trova, ad esempio, in [Poo60] e [CH11].

È interessante riscrivere l'equazione indiciale anche in termini dei coefficienti dell'equazione differenziale di partenza (4.1): per l'identità (4.4), un calcolo diretto mostra che, dato un punto $P \in \mathbb{C}$ singolare regolare, l'equazione indiciale in tale punto è

$$\prod_{j=0}^{n-1} (x - j) + \lim_{z \rightarrow P} \left\{ (z - P)^n a_n(z) + \sum_{k=1}^{n-1} (z - P)^k a_k(z) \prod_{m=0}^{n-1-k} (x - m) \right\} = 0. \quad (4.11)$$

Similmente, se ∞ è un punto singolare regolare, l'equazione indiciale corrispondente è

$$\prod_{j=0}^{n-1} (x + j) + \lim_{z \rightarrow \infty} \left\{ (-1)^n z^n a_n(z) + \sum_{k=1}^{n-1} (-1)^k z^k a_k(z) \prod_{m=0}^{n-1-k} (x + m) \right\} = 0. \quad (4.12)$$

Se ripetiamo il ragionamento precedente per un punto regolare, si ottiene sempre la stessa equazione indiciale e gli stessi esponenti locali: $1, \dots, n-1$. Esiste una relazione molto semplice fra gli esponenti locali, nota come *relazione di Fuchs*.

Proposizione 4.3. (Fuchs) *Sia \mathcal{S} la famiglia dei punti singolari regolari dell'equazione differenziale (4.1). Denotiamo, per ogni punto $P \in \mathcal{S}$, con $\rho_1(P), \dots, \rho_n(P)$ gli esponenti locali nel punto P . Allora*

$$\sum_{P \in \mathcal{S}} \left[\sum_{k=1}^n \rho_k(P) - \binom{n}{2} \right] = -2 \binom{n}{2}.$$

Dimostrazione

Ricordiamo che, se $p(x)$ è un polinomio monico di grado n , allora il coefficiente del termine di grado $n-1$ è l'opposto della somma delle sue radici. Se $P \in \mathbb{C} \cap \mathcal{S}$, dall'equazione indiciale (4.11) segue che

$$\sum_{k=1}^n \rho_k(P) - \binom{n}{2} = - \lim_{z \rightarrow P} (z - P) a_1(z).$$

Similmente, se $P = \infty$, dall'equazione indiciale (4.12) si ricava

$$\sum_{k=1}^n \rho_k(\infty) - \binom{n}{2} = -2 \binom{n}{2} + \lim_{z \rightarrow \infty} z a_1(z).$$

Per un noto risultato di analisi complessa², si deve avere che

$$\sum_{P \in \mathcal{S} - \{\infty\}} \lim_{z \rightarrow P} (z - P) a_1(z) = \lim_{z \rightarrow \infty} z a_1(z).$$

Sommando al variare di $P \in \mathcal{S}$, si trova la relazione cercata. □

Esempio 4.3. *Consideriamo l'equazione differenziale*

$$Y'' - \frac{z+1}{z} Y' + \frac{1}{z} Y = 0,$$

e studiamone le soluzioni in un intorno di $z_0 = 0$. Osserviamo che tale punto è singolare regolare, dato che

$$\lim_{z \rightarrow 0} -z \frac{z+1}{z} = -1, \quad \lim_{z \rightarrow 0} z^2 \frac{1}{z} = 0.$$

Per (4.11), l'equazione indiciale in tale punto è

$$x(x-1) - x = 0,$$

e gli esponenti locali sono $\rho_1 = 0, \rho_2 = 2$.

²Se una funzione è meromorfa in $\mathbb{P}^1(\mathbb{C})$, la somma di tutti i suoi residui nei punti singolari (incluso, eventualmente, il punto all'infinito) è uguale a 0.

$\rho_1 = 0$ Cerchiamo soluzioni della forma:

$$Y = \sum_{k=0}^{\infty} c_k z^k.$$

Calcolando le derivate

$$Y' = \sum_{k=0}^{\infty} k c_k z^{k-1} = \sum_{k=1}^{\infty} k c_k z^{k-1} = \sum_{k=0}^{\infty} (k+1) c_{k+1} z^k$$

$$Y'' = \sum_{k=0}^{\infty} k(k+1) c_{k+1} z^{k-1} = \sum_{k=0}^{\infty} (k+1)(k+2) c_{k+2} z^k,$$

e sostituendo nell'equazione di partenza otteniamo

$$\sum_{k=0}^{\infty} \{ [(k+1)c_{k+1} + c_k] z^k + [(k+1)(k+2)c_{k+2} - (k+1)c_{k+1}] z^{k+1} \} = 0.$$

Imponendo, al variare di $k = 0, 1, \dots$, che il coefficiente di z^k sia nullo, otteniamo la seguente successione per ricorrenza:

$$c_{k+1} = \frac{1}{k+1} c_k,$$

dove $c_0 \neq 0$ è arbitrario. Prendendo $c_0 = 1$, si ricava, per ogni $k \in \mathbb{N}$, $c_k = \frac{1}{k!}$ e si ottiene la soluzione

$$Y_1 = \sum_{k=0}^{\infty} \frac{z^k}{k!} = e^z.$$

$\rho_2 = 2$ Cerchiamo soluzioni della forma:

$$Y = z^2 \sum_{k=0}^{\infty} c_k z^k.$$

Analogamente al caso precedente, si ricava, al variare di $k = 0, 1, \dots$, la seguente successione per ricorrenza:

$$c_{k+1} = \frac{1}{k+3} c_k,$$

dove $c_0 \neq 0$ è arbitrario. Prendendo $c_0 = 1$, si ricava, per ogni $k \in \mathbb{N}$, $c_k = \frac{2}{(k+2)!}$ e si ottiene la soluzione

$$Y_2 = 2 \sum_{k=0}^{\infty} \frac{z^{k+2}}{(k+2)!} = 2(e^z - 1 - z).$$

Osserviamo che, entrambe le soluzioni trovate sono olomorfe in z_0 : in generale, un punto singolare dove accade questo fenomeno è detto *punto singolare apparente*.

4.3. Monodromia

Consideriamo nuovamente l'equazione differenziale Fuchsiana (4.1). Abbiamo visto che, comunque si prenda $z_0 \in \mathbb{P}^1(\mathbb{C})$ esistono, almeno localmente, delle soluzioni: ci chiediamo quale sia il legame fra queste soluzioni a carattere locale. Per semplificare la trattazione, restringiamoci a un aperto connesso U in $\mathbb{P}^1(\mathbb{C})$ e supponiamo che ogni punto di U sia regolare per tale equazione. Fissiamo un punto $z_0 \in U$, e grazie al teorema di Cauchy 4.1 consideriamo le soluzioni $F_1(z), \dots, F_n(z)$ espresse in forma di serie di potenze che, al variare di $k = 1, \dots, n$ e $j = 0, \dots, n-1$ corrispondono alle condizioni iniziali³ $F_k^{(j)}(z_0) = \delta_{j+1,k}$. Denotiamo con \mathcal{V}_{z_0} il \mathbb{C} -spazio vettoriale di soluzioni generato da queste ultime.

Nel seguito, sarà conveniente trasformare l'equazione (4.1) in un sistema di equazioni differenziali di ordine 1 equivalente: nello specifico, introduciamo per $k = 1, \dots, n$ le variabili $Y_k = Y^{(k-1)}$ e la trasformiamo nel sistema

$$\begin{bmatrix} Y_1' \\ Y_2' \\ \vdots \\ Y_n' \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 \\ -a_n & -a_{n-1} & \dots & \dots & -a_1 \end{bmatrix} \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_n \end{bmatrix}$$

Usando questa notazione, le soluzioni $F_1(z), \dots, F_n(z)$ sono rappresentate da vettori n -dimensionali: denotiamo con \mathcal{F}_{z_0} la matrice la cui k -esima colonna è il vettore corrispondente alla soluzione $F_k(z)$, ovvero

$$\mathcal{F}_{z_0} = \begin{bmatrix} F_1(z) & F_2(z) & \dots & F_n(z) \\ F_1^{(1)}(z) & F_2^{(1)}(z) & \dots & F_n^{(1)}(z) \\ \vdots & \vdots & \dots & \vdots \\ F_1^{(n-1)}(z) & F_2^{(n-1)}(z) & \dots & F_n^{(n-1)}(z) \end{bmatrix}$$

Chiamiamo \mathcal{F}_{z_0} *matrice fondamentale di soluzioni* in z_0 .

Vediamo come questi spazi di soluzioni sono in relazione. Sia $z_1 \in U$ un secondo punto: dato che U è aperto e connesso, è anche connesso per archi, quindi esiste un arco continuo $\lambda : [0, 1] \rightarrow U$ che li congiunge: per ogni $t \in [0, 1]$ esiste un intorno aperto $\mathcal{O}_{\lambda(t)}$ di $\lambda(t)$ tale che gli elementi della matrice $\mathcal{F}_{\lambda(t)}$ sono serie convergenti in $\mathcal{O}_{\lambda(t)}$. Osserviamo che $\{\mathcal{O}_{\lambda(t)}\}_{t \in [0,1]}$ è un ricoprimento aperto di $\lambda([0, 1])$, quindi, essendo $[0, 1]$ compatto e λ continua, anche $\lambda([0, 1])$ è compatto, e possiamo trovare un ricoprimento aperto fatto da aperti di questa forma:

$$\{\mathcal{O}_{\lambda(t_0)}, \mathcal{O}_{\lambda(t_1)}, \dots, \mathcal{O}_{\lambda(t_m)} : t_0 = 0 < t_1 < \dots < t_m = 1\}.$$

Osserviamo che, per ogni $j = 0, \dots, m-1$, far corrispondere alle colonne della matrice $\mathcal{F}_{\lambda(t_j)}$, nell'ordine, le colonne della matrice $\mathcal{F}_{\lambda(t_{j+1})}$, induce un isomorfismo $\psi_j : \mathcal{V}_{\lambda(t_j)} \rightarrow \mathcal{V}_{\lambda(t_{j+1})}$. Si

³Osserviamo che, nelle notazioni usate nel Teorema 4.1, tali soluzioni si ottengono fissando i coefficienti c_0, \dots, c_{n-1} come nella dimostrazione del teorema.

può verificare che l'isomorfismo risultante dalla composizione,

$$\mathcal{M}_\lambda : \mathcal{V}_{z_0} \rightarrow \mathcal{V}_{z_1},$$

dipende soltanto dalla classe di omotopia di λ : chiameremo tale isomorfismo *prolungamento analitico* lungo λ .

Nel caso particolare in cui $z_0 = z_1$, si hanno conseguenze interessanti: infatti, in tal caso, come noto, l'insieme delle classi di omotopia degli archi in U formano un gruppo, il *gruppo fondamentale* $\pi_1(U, z_0)$, e la mappa \mathcal{M}_λ è un automorfismo, che può essere descritto mediante una matrice in $\mathrm{GL}(n, \mathbb{C})$, dato che le nuove soluzioni appartengono a \mathcal{V}_{z_0} , che è generato da $F_1(z), \dots, F_n(z)$, e quindi sono una loro combinazione lineare a coefficienti in \mathbb{C} . La mappa

$$\begin{aligned} \mathcal{M} : \pi_1(U) &\rightarrow \mathrm{GL}(n, \mathbb{C}) \\ [\lambda] &\mapsto \mathcal{M}_\lambda, \end{aligned}$$

che chiameremo anche *mappa di monodromia* è un omomorfismo di gruppi, e la sua immagine è detta *gruppo di monodromia*. Tale gruppo è univocamente determinato a meno di coniugio, a seconda del punto base scelto.

Osserviamo che l'estensione $\mathbb{C}(z)(F_1, \dots, F_n) \supset \mathbb{C}(z)$ è un'estensione di Picard-Vessiot, e dato che un elemento del corrispondente gruppo di Galois differenziale è determinato dalle immagini di un insieme massimale di soluzioni, possiamo vedere il gruppo di monodromia come un sottogruppo di quest'ultimo.

Data un'equazione differenziale Fuchsiana, il gruppo di monodromia e il gruppo di Galois differenziale associato sono strettamente.

Teorema 4.2. (Schlesinger) *Supponiamo che l'equazione differenziale (4.1) sia Fuchsiana. Denotiamo con \mathcal{G} il gruppo di Galois differenziale corrispondente all'estensione di Picard-Vessiot $\mathbb{L} \supset \mathbb{C}(z)$ associata, e con \mathcal{M} il gruppo di monodromia: allora \mathcal{G} è la chiusura di \mathcal{M} rispetto alla topologia di Zariski.*

Dimostrazione

Sia \mathbb{F} il sottocampo di \mathbb{L} fissato dal gruppo di monodromia. Per la corrispondenza di Galois 3.7, si ha $\mathrm{Gal}^{\mathrm{Diff}}(\mathbb{L}/\mathbb{F}) = \overline{\mathcal{M}}$. Per concludere, per il Teorema 3.7 basta provare che $\mathbb{F} = \mathbb{C}(z)$. A questo scopo, sia F un elemento in \mathbb{L} che rimane fissato sotto l'azione di \mathcal{M} : allora F è una funzione monodroma e analitica in $\mathbb{P}^1(\mathbb{C} - \mathcal{S})$, dove \mathcal{S} è l'insieme dei punti singolari dell'equazione differenziale. Per ipotesi, ogni elemento di \mathcal{S} è un punto singolare regolare, non ci sono singolarità essenziali, quindi F è meromorfa su $\mathbb{P}^1(\mathbb{C})$, e cioè una funzione razionale. □

Non approfondiremo oltre questo tema: una trattazione più dettagliata si trova, ad esempio, in [vdPS97] e [Hil76]. Tuttavia, mostriamo con un esempio che l'ipotesi che l'equazione differenziale sia Fuchsiana è necessaria.

Esempio 4.4. *Consideriamo l'equazione differenziale*

$$Y' - Y = 0.$$

Osserviamo che questa equazione non è Fuchsiana: mediante il cambio di variabili $z = \frac{1}{x}$, otteniamo l'equazione differenziale

$$\begin{aligned} -x^2 Y' - Y &= 0, \\ Y' + \frac{1}{x^2} Y &= 0, \end{aligned}$$

e da quest'ultima deduciamo che ∞ non è né regolare né singolare regolare. L'estensione di Picard-Vessiot associata è $\mathbb{C}(z)(e^z) \supset \mathbb{C}(z)$: osserviamo che quest'ultima è una estensione con aggiunta dell'esponenziale di un integrale, dato che il rapporto fra la derivata dell'esponenziale complesso e l'esponenziale complesso stesso è uguale a 1, che è una costante. Pertanto, per la Proposizione 3.7, il gruppo di Galois differenziale associato è isomorfo al gruppo moltiplicativo \mathbb{C}^* . D'altra parte, poiché l'esponenziale complesso è una funzione monodroma, il gruppo di monodromia è il gruppo banale, e coincide con la sua chiusura.

4.4. L'equazione ipergeometrica di Gauss

In questa sezione vediamo un esempio più dettagliato, che ha anche importanti applicazioni: l'equazione ipergeometrica di Gauss.

Siano $a, b, c \in \mathbb{R}$ tre parametri, con $c \notin \mathbb{Z} - \mathbb{N}$. Chiamiamo *equazione ipergeometrica di Gauss* (di parametri a, b, c) la seguente equazione differenziale:

$$Y'' + \frac{(a+b+1)z-c}{z(z-1)} Y' + \frac{ab}{z(z-1)} Y = 0. \quad (4.13)$$

Come abbiamo visto nell'esempio 4.1, mediante il cambio di variabili $z = \frac{1}{x}$ otteniamo l'equazione differenziale

$$\begin{aligned} Y'' + \frac{2z - \frac{(a+b+1)\frac{1}{z}-c}{\frac{1}{z}(\frac{1}{z}-1)}}{z^2} Y' + \frac{ab}{z^4 \frac{1}{z} (\frac{1}{z}-1)} Y &= 0, \\ Y'' + \frac{(c-2)z - a - b + 1}{z(1-z)} Y' + \frac{ab}{z^2(1-z)} Y &= 0. \end{aligned}$$

Dunque, è immediato osservare che i punti $z_1 = 0$, $z_2 = 1$, $z_3 = \infty$, sono tutti e soli i punti singolari per (4.13), e che sono singolari regolari. Quindi l'equazione differenziale (4.13) è Fuchsiana.

Mediante le equazioni (4.11), (4.12) viste nel capitolo precedente, possiamo ricavare gli esponenti locali:

$z_1 = 0$ L'equazione indiciale è

$$x(x-1) + \lim_{z \rightarrow 0} \left\{ z^2 \frac{ab}{z(z-1)} + z \frac{(a+b+1)z-c}{z(z-1)} x \right\} = x(x-1) + cx = 0,$$

e gli esponenti locali sono $\rho_1 = 0$, $\rho_2 = 1 - c$.

$z_2 = 1$ L'equazione indiciale è

$$\begin{aligned} x(x-1) + \lim_{z \rightarrow 1} \left\{ (z-1)^2 \frac{ab}{z(z-1)} + (z-1) \frac{(a+b+1)z-c}{z(z-1)} x \right\} \\ = x(x-1) + (a+b+1-c)x = 0, \end{aligned}$$

e gli esponenti locali sono $\rho_1 = 0$, $\rho_2 = c - a - b$.

$z_3 = \infty$ L'equazione indiciale è

$$x(x+1) + \lim_{z \rightarrow \infty} \left\{ z^2 \frac{ab}{z(z-1)} - z \frac{(a+b+1)z-c}{z(z-1)} x \right\} = x^2 - (a+b)x + ab = 0,$$

e gli esponenti locali sono $\rho_1 = a$, $\rho_2 = b$.

Cerchiamo adesso delle soluzioni per l'equazione ipergeometrica. A tale scopo, dato $x \in \mathbb{R}$, introduciamo il suo *simbolo di Pochhammer* $(x)_n$, al variare di $n = 0, 1, \dots$, definito ricorsivamente come segue:

$$\begin{aligned} (x)_0 &= 1, \\ (x)_n &= \prod_{k=0}^{n-1} (x+k) = (x+n-1)(x)_{n-1}, \end{aligned} \tag{4.14}$$

e consideriamo la serie di potenze formale

$$S(X) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n n!} X^n.$$

Lemma 4.2. *Se a, b non sono interi negativi, $S(X)$ ha raggio di convergenza uguale a 1.*

Dimostrazione

Se a, b sono interi negativi, $(a)_m$ e $(b)_n$ sono definitivamente nulli, e in tal caso $S(X)$ è un polinomio. Se invece a, b non sono interi negativi, applicando il criterio del rapporto otteniamo

$$\lim_{n \rightarrow \infty} \frac{(a)_{n+1} (b)_{n+1} (c)_n n!}{(a)_n (b)_n (c)_{n+1} (n+1)!} = \lim_{n \rightarrow \infty} \frac{(a+n)(b+n)}{(c+n)(n+1)} = 1.$$

Di conseguenza, il raggio di convergenza della serie $S(X)$ è uguale a 1. □

Per il lemma precedente, sono ben definite, al variare di a, b, c , le seguenti funzioni, note come *funzioni ipergeometriche di Gauss*:

$$\begin{aligned} F(a, b, c; \cdot) : \mathcal{B}(0, 1) &\rightarrow \mathbb{C} \\ z &\mapsto \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n n!} z^n, \end{aligned} \tag{4.15}$$

dove abbiamo denotato con $\mathcal{B}(0, 1)$ la palla aperta di centro l'origine e raggio unitario.

Il nome che abbiamo date alle funzioni (4.15) non è casuale:

Teorema 4.3. *La funzione ipergeometrica $F(a, b, c; \cdot)$ è una soluzione dell'equazione ipergeometrica (4.13) in un intorno dell'origine.*

Dimostrazione

Nel disco di convergenza, abbiamo

$$\begin{aligned}\frac{dF}{dz}(a, b, c; z) &= \sum_{n=1}^{\infty} \frac{(a)_n(b)_n}{(c)_n(n-1)!} z^{n-1} = \sum_{n=0}^{\infty} \frac{(a)_{n+1}(b)_{n+1}}{(c)_{n+1}n!} z^n, \\ \frac{d^2F}{dz^2}(a, b, c; z) &= \sum_{n=0}^{\infty} \frac{(a)_{n+2}(b)_{n+2}}{(c)_{n+2}n!} z^n, \\ \frac{1}{1-z} &= \sum_{n=0}^{\infty} z^n.\end{aligned}$$

Di conseguenza, posto

$$\begin{aligned}\Sigma_1 &= -\frac{ab}{z(z-1)}F(a, b, c; z) = ab \sum_{n=0}^{\infty} z^{n-1} \sum_{n=0}^{\infty} \frac{(a)_n(b)_n}{(c)_n n!} z^n, \\ \Sigma_2 &= -\frac{(a+b+1)z-c}{z(z-1)} \frac{dF}{dz}(a, b, c; z) \\ &= \left[(a+b+1) \sum_{n=0}^{\infty} z^n - c \sum_{n=0}^{\infty} z^{n-1} \right] \sum_{n=0}^{\infty} \frac{(a)_{n+1}(b)_{n+1}}{(c)_{n+1}n!} z^n,\end{aligned}$$

ci basta dimostrare che

$$\Sigma_1 + \Sigma_2 = \frac{d^2F}{dz^2}(a, b, c; z).$$

Per fare ciò, verifichiamo che le due serie di potenze abbiano gli stessi coefficienti. Riscriviamo Σ_1 e Σ_2 in serie di potenze:

$$\begin{aligned}\Sigma_1 &= ab \left(\sum_{n=0}^{\infty} z^n + \frac{1}{z} \right) \sum_{n=0}^{\infty} \frac{(a)_n(b)_n}{(c)_n n!} z^n = ab \sum_{N=0}^{\infty} \left(\sum_{h=0}^N \frac{(a)_h(b)_h}{(c)_h h!} \right) z^N + ab \sum_{n=0}^{\infty} \frac{(a)_n(b)_n}{(c)_n n!} z^{n-1} \\ &= \frac{ab}{z} + ab \sum_{N=0}^{\infty} \sum_{h=0}^{N+1} \frac{(a)_h(b)_h}{(c)_h h!} z^N,\end{aligned}$$

e similmente

$$\Sigma_2 = -\frac{ab}{z} + (a+b-c+1) \sum_{N=0}^{\infty} \left(\sum_{h=0}^N \frac{(a)_{h+1}(b)_{h+1}}{(c)_{h+1} h!} \right) z^N - c \sum_{N=0}^{\infty} \frac{(a)_{N+2}(b)_{N+2}}{(c)_{N+2}(N+1)!} z^N.$$

Sommando, si ricava $\Sigma_1 + \Sigma_2 = \sum_{N=0}^{\infty} \alpha_N z^N$, dove, per ogni $N = 0, 1, \dots$,

$$\alpha_N = ab \sum_{h=0}^{N+1} \frac{(a)_h(b)_h}{(c)_h h!} + (a+b-c+1) \sum_{h=0}^N \frac{(a)_{h+1}(b)_{h+1}}{(c)_{h+1} h!} - c \frac{(a)_{N+2}(b)_{N+2}}{(c)_{N+2}(N+1)!}.$$

Per concludere, proviamo per induzione su N che, per ogni $N = 0, 1, \dots$,

$$\alpha_N = \frac{(a)_{N+2}(b)_{N+2}}{(c)_{N+2}N!}.$$

Un semplice conto mostra che il passo base ($N = 0$) è verificato. Supponendo che l'identità precedente sia verificata per $N - 1$, allora,

$$\begin{aligned} \alpha_N &= ab \left(\sum_{h=0}^N \frac{(a)_h(b)_h}{(c_h)h!} + \frac{(a)_{N+1}(b)_{N+1}}{(c_{N+1})(N+1)!} \right) + \\ &\quad + (a+b-c+1) \left(\sum_{h=0}^{N-1} \frac{(a)_{h+1}(b)_{h+1}}{(c_{h+1})h!} + \frac{(a)_{N+1}(b)_{N+1}}{(c_{N+1})N!} \right) + \\ &\quad - c \frac{(a)_{N+1}(b)_{N+1}}{(c_{N+1})N!} + c \frac{(a)_{N+1}(b)_{N+1}}{(c_{N+1})N!} \\ &= \alpha_{N-1} + ab \frac{(a)_{N+1}(b)_{N+1}}{(c_{N+1})(N+1)!} + (a+b-c+1) \frac{(a)_{N+1}(b)_{N+1}}{(c_{N+1})N!} + \\ &\quad - c \frac{(a)_{N+2}(b)_{N+2}}{(c_{N+2})(N+1)!} + c \frac{(a)_{N+1}(b)_{N+1}}{(c_{N+1})N!} \\ &= \frac{(a)_{N+1}(b)_{N+1}}{(c)_{N+1}(N+1)!} \left[(N+a+b+1)(N+1) + ab - c \frac{(a+N+1)(b+N+1)}{c+N+1} \right] \\ &= \frac{(a)_{N+1}(b)_{N+1}}{(c)_{N+1}(N+1)!} \frac{(N+1)(a+N+1)(b+N+1)}{(c+N+1)} = \frac{(a)_{N+2}(b)_{N+2}}{(c)_{N+2}N!} \end{aligned}$$

□

Dalla dimostrazione del teorema precedente, è evidente che provare che le funzioni ipergeometriche siano soluzioni dell'equazione differenziale (4.13) è molto laborioso, ma ha conseguenze importanti: in effetti, si può dimostrare che le altre soluzioni dell'equazione in un intorno dei punti singolari regolari si esprimono in termini delle funzioni ipergeometriche: la soluzione relativa al punto $z_1 = 0$ con esponente locale $1 - c$ è

$$z^{1-c} F(a-c+1, b-c+1, 2-c; z),$$

mentre le soluzioni relative al punto $z_2 = 1$ sono

$$F(a, b, a+b-c; 1-z),$$

$$(1-z)^{c-a-b} F(c-a, c-b, c-a-b+1; 1-z),$$

entrambe con dominio di convergenza $\{z \in \mathbb{C} : 0 < |z| < 2\}$. Infine, le soluzioni relative al punto $z_3 = \infty$ sono

$$z^{-a} F\left(a, a-c+1, a-b+1; \frac{1}{z}\right),$$

$$z^{-b} F\left(b, b-c+1, b-a+1; \frac{1}{z}\right),$$

⁴Per semplicità, non riportiamo i facili passaggi intermedi.

con dominio di convergenza $\{z \in \mathbb{C} : |z| > 1\}$. Concludiamo osservando che, essendo l'equazione di ordine 2, non ci possono essere più di due soluzioni linearmente indipendenti. In effetti, vale ad esempio la seguente identità, dovuta a Klein:

$$F(a, b, c; z) = \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)} F(a, b, a+b-c+1; 1-z) + \frac{\Gamma(c)\Gamma(a+b-c)}{\Gamma(a)\Gamma(b)} (1-z)^{c-a-b} F(c-a, c-b, c-a-b+1; 1-z),$$

dove Γ è la funzione di Eulero.

Lo studio dell'equazione ipergeometrica di Gauss è molto importante: infatti, tutte le equazioni Fuchsiane di ordine 2 con tre punti singolari possono essere trasformate in un'equazione ipergeometrica mediante alcune trasformazioni, le *trasformazioni di Möbius*

$$\mu : \mathbb{P}^1(\mathbb{C}) \rightarrow \mathbb{P}^1(\mathbb{C})$$

$$z \mapsto \begin{cases} \frac{az+b}{cz+d} & \text{se } c \neq 0 \text{ e } z \neq -\frac{d}{c} \\ \infty & \text{se } c \neq 0 \text{ e } z = -\frac{d}{c}, \text{ oppure } c = 0 \text{ e } z = \infty, \\ \frac{a}{c} & \text{se } c \neq 0 \text{ e } z = \infty \end{cases}$$

dove $ad - bc \neq 0$. Mediante una trasformazione di Möbius, si portano i loro punti singolari nei tre punti $z_1 = 1, z_2 = 2, z_3 = \infty$ (in effetti, basta imporre questa condizione in quanto, come noto, basta fissare l'immagine di questi tre punti in $\mathbb{P}^1(\mathbb{C})$ per determinare univocamente una trasformazione di Möbius), e moltiplicando le soluzioni per un fattore della forma $z^{-\alpha}(1-z)^{-\beta}$, dove $\alpha, \beta \in \mathbb{C}$ sono coefficienti opportuni.

La generalizzazione delle equazioni ipergeometriche, è uno dei problemi di cui si occupa la moderna teoria analitica delle equazioni differenziali.

4.5. Alcuni risultati sul gruppo di Galois differenziale

Proposizione 4.4. *Data un'equazione differenziale a coefficienti in $\mathbb{C}(z)$,*

$$Y^{(n)} + a_{n-1}(z)Y^{(n-1)} + \dots + a_1(z)Y' + a_0(z)Y = 0,$$

esiste un cambio di variabili che trasforma quest'ultima equazione in un'equazione differenziale della forma

$$Z^{(n)} + b_{n-2}(z)Y^{(n-2)} + \dots + b_1(z)Z' + b_0(z)Z = 0.$$

Dimostrazione

Sia V una soluzione dell'equazione differenziale $nV' + a_{n-1}(z)V = 0$. Se poniamo $Y = VZ$, per ogni $k = 1, 2, \dots$ la proposizione 1.2 implica che

$$Y^{(k)} = \sum_{m=0}^k \binom{k}{m} V^{(m)} Z^{(k-m)}.$$

Se sostituiamo nell'equazione data, riordinando si ottiene che il coefficiente di $Z^{(n+1)}$ è

$$b_1 = \binom{n}{n-1} V' + a_{n-1} = nV' + a_{n-1} = 0.$$

□

Proposizione 4.5. Dato un operatore differenziale lineare monico a coefficienti in $\mathbb{C}(z)$,

$$\mathcal{L} = \frac{d^n}{dz^n} + a_{n-1}(z) \frac{d^{n-1}}{dz^{n-1}} + \dots + a_1(z) \frac{d}{dz} + a_0(z),$$

supponiamo che esista un insieme massimale di soluzioni dell'equazione differenziale associata, e sia \mathcal{W} il Wronskiano di questa n -upla. Se $a_{n-1}(z)$ è identicamente nulla, allora \mathcal{W} è una costante, e il gruppo di Galois differenziale dell'estensione di Picard-Vessiot corrispondente è isomorfo a un sottogruppo di $SL(n, \mathbb{C})$.

Dimostrazione

Sia $\{Y_1, \dots, Y_n\}$ un insieme massimale di soluzioni. Per quanto visto nel secondo capitolo, la derivazione del Wronskiano \mathcal{W} di questa n -upla è

$$\mathcal{W}' = \det \begin{bmatrix} Y_1 & Y_2 & \dots & Y_n \\ Y_1^{(1)} & Y_2^{(1)} & \dots & Y_n^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ Y_1^{(n-2)} & Y_2^{(n-2)} & \dots & Y_n^{(n-2)} \\ Y_1^{(n)} & Y_2^{(n)} & \dots & Y_n^{(n)} \end{bmatrix}.$$

L'ipotesi $a_{n-1}(z)$ identicamente nulla implica immediatamente che l'ultima riga è combinazione lineare delle precedenti. Pertanto, $\mathcal{W}' = 0$, e \mathcal{W} è una costante.

Sia ora σ un elemento del gruppo di Galois differenziale associato: se denotiamo con A_σ la matrice corrispondente a quest'ultimo elemento, dato che \mathcal{W} è costante si vede che

$$\mathcal{W} = \sigma(\mathcal{W}) = \det A_\sigma \cdot \mathcal{W},$$

e dato che $\mathcal{W} \neq 0$, essendo il Wronskiano associato a un insieme massimale di soluzioni, si ricava $\det A_\sigma = 1$: dunque $\text{Gal}^{\text{Diff}}(\mathcal{L})$ è un sottogruppo di $SL(n, \mathbb{C})$.

□

Esempio 4.5. Quest'ultima proposizione trova conferma negli esempi 3.3, 3.5.

Questo risultato non può essere migliorato, ovvero esistono operatori differenziali lineari che verificano le ipotesi della proposizione precedente, con gruppo di Galois differenziale associato isomorfo al gruppo lineare speciale.

Esempio 4.6. L'equazione di Airy

$$Y'' - zY = 0,$$

un'equazione che ha applicazioni nella meccanica quantistica, è un'equazione Fuchsiana: due sue soluzioni linearmente indipendenti su \mathbb{C} sono le seguenti, dette funzioni di Airy:

$$Ai : \mathbb{C} \rightarrow \mathbb{C} \\ z \mapsto \frac{1}{3^{2/3}\pi} \sum_{n=0}^{\infty} \frac{\Gamma(\frac{n+1}{3})}{n!} 3^{1/3n} \sin\left(\frac{2(n+1)\pi}{3}\right) z^n,$$

$$\begin{aligned}
 Bi : \mathbb{C} &\rightarrow \mathbb{C} \\
 z &\mapsto \frac{1}{3^{\frac{1}{6}}\pi} \sum_{n=0}^{\infty} \frac{\Gamma\left(\frac{n+1}{3}\right)}{n!} 3^{\frac{1}{3n}} \left| \sin\left(\frac{2(n+1)\pi}{3}\right) \right| z^n.
 \end{aligned}$$

Il gruppo di Galois differenziale associato all'equazione di Airy è $SL(2, \mathbb{C})$ (si veda [Mag97]).

4.6. Estensioni di Liouville

Sia $\mathbb{L} \supset \mathbb{K}$ l'estensione di Picard-Vessiot corrispondente a un'equazione differenziale lineare a coefficienti in \mathbb{K} . Diremo che l'estensione $\mathbb{L} \supset \mathbb{K}$ è un'estensione di Liouville, e che l'equazione è *risolubile per quadrature* se esiste una catena di sottocampi differenziali,

$$\mathbb{K} = \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_m = \mathbb{L}, \quad (4.16)$$

tale che ciascuna delle estensioni intermedie è un'estensione con aggiunta di un integrale, oppure un'estensione con aggiunta dell'esponenziale di un integrale. Similmente, diremo che l'estensione $\mathbb{L} \supset \mathbb{K}$ è un'estensione di Liouville generalizzata, e che l'equazione è *Liouvilliana*, se esiste una catena di sottocampi differenziali come in (4.16) tale che ciascuna delle estensioni intermedie è un'estensione con aggiunta di un integrale, oppure un'estensione con aggiunta dell'esponenziale di un integrale, oppure un'estensione algebrica. In altri termini, un'estensione di Picard-Vessiot è di Liouville generalizzata se, per ogni $j = 2, \dots, m$, esiste $x_j \in \mathbb{F}_j$ tale che $F_j = F_{j-1}(x_j)$ e vale una delle seguenti:

- (a) $x'_j \in \mathbb{F}_{j-1}$ (ovvero l'estensione è un'estensione con aggiunta di un integrale);
- (b) $x'_j/x_j \in \mathbb{F}_{j-1}$ (ovvero l'estensione è un'estensione con aggiunta dell'esponenziale di un integrale);
- (c) x_j è algebrico su \mathbb{F}_{j-1} (ovvero l'estensione è algebrica).

Infine, se la catena è ottenuta solo mediante estensioni con aggiunta di un integrale, diremo che l'equazione è *risolubile per integrali* mentre se è ottenuta solo mediante estensioni con aggiunta dell'esponenziale di un integrale, diremo che l'equazione è *risolubile per esponenziali*. I legami fra i vari tipi di estensioni sono evidenti.

Esempio 4.7. *L'equazione nell'esempio 3.5 è risolubile per integrali, in quanto l'estensione di Picard-Vessiot corrispondente è ottenibile mediante tre estensioni con aggiunta dell'esponenziale di un integrale.*

Una peculiarità della teoria di Picard-Vessiot è che permette di ottenere informazioni sulle soluzioni di un'equazione differenziale andando a vedere se il gruppo di Galois differenziale ad essa associato gode o meno di alcune proprietà.

Diremo che un gruppo \mathcal{G} è

- *risolubile* se esiste una catena di sottogruppi normali,

$$\{\text{Id}_{\mathcal{G}}\} = \mathcal{H}_1 \triangleleft \cdots \triangleleft \mathcal{H}_m = \mathcal{G}, \quad (4.17)$$

tale che, per ogni $j = 2, \dots, m$, il quoziente $\mathcal{H}_j/\mathcal{H}_{j-1}$ è abeliano;

- *diagonalizzabile* se esiste $n \in \mathbb{N}$ tale che \mathcal{G} è isomorfo al gruppo di matrici diagonali $D(n, \mathbb{K})$.

Per non complicare eccessivamente la trattazione, ci limiteremo a enunciare soltanto i seguenti risultati, dimostrati in [CH11] e [Kam]:

Teorema 4.4. *Sia $\mathbb{L} \supset \mathbb{K}$ un'estensione di Liouville di campi differenziali. Supponiamo che il campo delle costanti di \mathbb{L} coincida con il campo delle costanti di \mathbb{K} . Allora il gruppo di Galois differenziale associato all'estensione, $\text{Gal}^{\text{Diff}}(\mathbb{L}/\mathbb{K})$, è risolubile.*

Corollario 4.1. *Sia data un'equazione differenziale lineare a coefficienti in $\mathbb{C}(z)$. Se il gruppo di Galois corrispondente non è risolubile, allora l'equazione non è risolubile per quadrature.*

Teorema 4.5. *Sia data un'equazione differenziale su un campo differenziale \mathbb{K} , il cui campo delle costanti è algebricamente chiuso. Sia \mathcal{G} il gruppo di Galois differenziale associato all'equazione. Allora:*

- *l'equazione è risolubile per quadrature se e solo se \mathcal{G} è risolubile;*
- *l'equazione è risolubile per esponenziali se e solo se \mathcal{G} è diagonalizzabile;*

Concludiamo questa sezione, e questo lavoro, osservando che questi risultati sono l'analogo di quelli della teoria di Galois classica sulla risolubilità per radicali di un'equazione polinomiale: ricordiamo che, detto \mathbb{K} un campo a caratteristica 0, un polinomio $p(x) \in \mathbb{K}[x]$ si dice risolubile per radicali se, detto \mathbb{L} il suo campo di spezzamento su \mathbb{K} , esiste una catena di estensioni di campi,

$$\mathbb{K} = \mathbb{F}_0 \subset \mathbb{F}_1 = \mathbb{F}_0(\alpha_1) \subset \cdots \subset \mathbb{F}_n = \mathbb{F}_{n-1}(\alpha_n) = \mathbb{L}',$$

tale che $\mathbb{L} \subset \mathbb{L}'$ ed esistano dei numeri naturali m_1, \dots, m_n tali che, per ogni $j = 1, \dots, n$,

$$\alpha_j^{m_j} \in \mathbb{F}_{j-1}.$$

Teorema 4.6. *Se $p(x) \in \mathbb{K}[x]$ è un polinomio risolubile per radicali, allora il gruppo di Galois $\text{Gal}(\mathbb{L}/\mathbb{K})$ è risolubile.*

Bibliografia

- [AM69] M.F. Atiyah and I.G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley series in Mathematics, Addison-Wesley, 1969.
- [Car95] H. Cartan, *Elementary Theory of Analytic Functions of One or Several Complex Variables*, Dover Publications, 1995.
- [CH11] T. Crespo and Z. Hajto, *Algebraic Groups and Differential Galois Theory*, Graduate Studies in Mathematics, vol. 122, American Mathematical Society, 2011.
- [Gai17] G. Gaiffi, *Dispense del corso di Algebra I*, <http://people.dm.unipi.it/~gaiffi/Algebra1-2016/Pages/dispense1.pdf>, A.A. 2016-2017.
- [Hil76] E. Hille, *Ordinary Differential Equations in the Complex Domain*, Pure and Applied Mathematics, John Wiley and Sons, 1976.
- [Kam] M. Kamensky, *Differential Galois Theory*, <https://www.math.bgu.ac.il/~kamenskm/lectures/diffgalois.pdf>.
- [Kap57] I. Kaplansky, *An Introduction to Differential Algebra*, Actualités scientifiques et industrielles, vol. 1251, Paris: Hermann, 1957.
- [Mag97] A.R. Magid, *Lectures on Differential Galois Theory*, University Lectures Series, vol. 7, American Mathematical Society, 1997.
- [Mat] *Airy Functions*, <http://mathworld.wolfram.com/AiryFunctions.html>.
- [Nac96] M. Nacinovich, *Elementi di geometria analitica*, Serie di matematica e fisica, vol. 14, Liguori Editori, 1996.
- [Poo60] E.G.C. Poole, *Introduction to the Theory of Linear Differential Equations*, Dover Publications, 1960.
- [Rot03] J.J. Rotman, *Advanced Modern Algebra*, Prentice Hall, 2003.
- [Sim15] B. Simon, *An Introduction to Differential Galois Theory*, <http://math.sfsu.edu/serkan/expository/bruceSimonExpository.pdf>, 2015.
- [vdPS97] M. van der Put and M.F. Singer, *Galois Theory of Linear Differential Equations*, A Series of Comprehensive Studies in Mathematics, vol. 328, Springer-Verlag, 1997.
- [Wat79] W.C. Waterhouse, *Introduction to Affine Group Schemes*, Graduates Texts in Mathematics, vol. 66, Springer-Verlag, 1979.

- [Wil15] D. Wilson, *Differential Galois Theory through Examples*, <https://www.math.uchicago.edu/~dwilson/notes/differential-galois-grad-seminar.pdf>, 2015.
- [Zol06] H. Zoladek, *The Monodromy Group*, Monografie Matematyczne Instytut, vol. 67, Birkäuser, 2006.

A

Algebra	
Commutativa	3
Di soluzioni universale massimale	18
Anello differenziale	9
Aperto principale (topologia di Zariski)	34
Automorfismo differenziale	10

C

Campo	
Delle frazioni	5
Differenziale	9

D

Derivazione	6
Banale	7

E

Elemento	
Algebrico	23
Costante	10
Trascendente	23
Equazione	
Associata a un operatore differenziale	13
Di Airy	58
Fuchsiana	42
Indiciale	48
Ipergeometrica di Gauss	53
Liouvilliana	59
Risolubile	
Per esponenziali	59
Per integrali	59
Per quadrature	59
Esponenti	
Locali	48

Estensione

Con aggiunta	
Dell'esponenziale di un integrale	34
Di un integrale	33
Di Galois	24
Differenziale	26
Di Liouville	59
Generalizzata	59
Di Picard-Vessiot	13
Differenziale	9
Finita	24
Senza costanti	14

F

Formula di Leibniz	7
Funzione	
Aritmetica	7
Ipergeometrica di Gauss	54

G

Gruppo	
Algebrico	35
Di Galois	24
Differenziale	26
Di monodromia	52
Diagonale	32
Diagonalizzabile	60
Fondamentale	52
Risolubile	59
Triangolare superiore	29
Triangolare superiore unipotente	29

I

Ideale differenziale	10
Insieme	
Chiuso (topologia di Zariski)	34

massimale di soluzioni	17
Isomorfismo differenziale	10

L

Localizzazione di un anello	5
-----------------------------------	---

M

Mappa	
Di localizzazione	5
Di monodromia	52
Polinomiale	35
Matrice	
Associata a un automorfismo	26
Fondamentale di soluzioni	51
Wronskiana	14

O

Omomorfismo	
Di algebre	3
Differenziale	10
Operatore differenziale	
Grado	11
Lineare	11
Monico	11
Termine noto	11

P

Polinomio	
Risolubile per radicali	60
Separabile	23
Prodotto tensoriale di moduli	2
Prolungamento analitico lungo un arco ..	52
Proprietà	
Universale	
Della localizzazione	5
Di normalità	19
Universale	
Del prodotto tensoriale	2
Punto	
Regolare	41
Singolare	41

Singolare Apparente	50
Singolare Regolare	42

R

Relazione di Fuchs	49
--------------------------	----

S

Simbolo di Pochhammer	54
Spazio affine	34

T

Tensore	3
Teorema	
Di Cauchy (soluzioni formali di un'equazione Fuchsiana in un intorno di un punto regolare) ...	45
Di corrispondenza di Galois (versione classica)	25
Di esistenza	19
Di esistenza e unicità	
Del prodotto tensoriale	1
Della localizzazione	4
Di indipendenza degli elementi di un campo differenziale	15
Di Kolchin (Corrispondenza di Galois, versione differenziale)	37
di Kolchin (il gruppo di Galois differenziale è un gruppo algebrico lineare)	36
Di omomorfismo	10
Di Schlesinger (gruppo di monodromia)	52
Di unicità	20
Topologia di Zariski	34
Trasformazione di Möbius	57

W

Wronskiano	
Derivazione	15
Di una m -upla	14