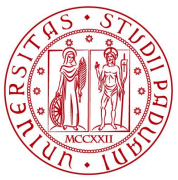

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Triennale in Matematica

Una introduzione alla Teoria di Galois Differenziale

Relatore:
Prof. Riccardo Colpi

Laureando: Edoardo Tacchetti
Matricola: 2002965

Anno Accademico 2022/2023

22 Settembre 2023

Indice

Introduzione

La Teoria di Galois Differenziale, detta anche Teoria di Picard-Vessiot, nasce nella seconda metà del diciannovesimo secolo da un'idea del matematico norvegese Sophus Lie (1842-1899). Egli voleva ricercare le soluzioni di una equazione differenziale andando a studiare un particolare gruppo di automorfismi ad essa correlato.

Il parallelismo con la Teoria di Galois classica è immediato. Il matematico francese Évariste Galois (1811-1832) aveva già sviluppato la sua teoria all'inizio del diciannovesimo secolo studiando le relazioni presenti tra le radici di un polinomio irriducibile $P(X) \in \mathbb{Q}[X]$, il suo campo di spezzamento ed il cosiddetto gruppo di Galois dell'estensione (ovvero il gruppo degli automorfismi che fissano gli elementi di $\mathbb{Q}$).

Le idee di Galois e Lie vennero riprese dai matematici francesi Émile Picard (1856-1941) ed Ernest Vessiot (1865-1952), i quali svilupparono una teoria analoga a quella di Galois ma avente per soggetto le equazioni differenziali: le nozioni di campo di spezzamento, gruppo di Galois e risolubilità per radicali fecero spazio a quelli di estensione di Picard-Vessiot, gruppo di Galois differenziale e risolubilità per quadrature.

Tale teoria venne infine rivisitata dal matematico americano Ellis Kolchin (1916-1991). Egli formalizzò la Teoria di Picard-Vessiot utilizzando la sua teoria dei gruppi algebrici lineari e gli strumenti dell'Algebra Differenziale sviluppati dal matematico americano Joseph Fels Ritt (1893-1951). Ciò portò a risultati importanti per la Teoria di Galois Differenziale, ad esempio la dimostrazione che il gruppo di Galois differenziale è un gruppo algebrico lineare ed il Teorema Fondamentale.

Negli ultimi anni la Teoria di Picard-Vessiot è stata centro di rinnovato interesse a causa delle connessioni e delle applicazioni con altre aree della matematica: dall'Analisi (Equazioni Fuchsiane) all'Algebra (Teoria dei Numeri), dalla Statistica (Teoria Asintotica) ai Sistemi Dinamici (integrabilità di sistemi Hamiltoniani e Teoria di Morales-Ramis) e così via.

Lo scopo di questa tesi è introdurre la Teoria di Galois Differenziale in maniera chiara ed accessibile dimostrando i risultati incontrati e fornendo esempi nel corso della trattazione per facilitare la comprensione dell'argomento.

Nel Capitolo 1 verranno introdotti gli strumenti e le nozioni utili per lo sviluppo della Teoria di Galois Differenziale. Si definiranno quindi le derivazioni su un anello arbitrario, i concetti di anello, campo ed estensione differenziale e tutte le proprietà ad essi collegate. Saranno poi descritti gli operatori differenziali a cui vengono associate le equazioni differenziali, argomento centrale nella discussione successiva. Si introdurrà infine la nozione di prodotto tensoriale tra anelli differenziali da un punto di vista più mirato alla trattazione della Teoria di Picard-Vessiot.

Nel Capitolo 2 si descriveranno le proprietà delle equazioni differenziali lineari omogenee introducendo il concetto di determinante Wronksiano. Verrà poi definita l'estensione di Picard-Vessiot per una data equazione differenziale e si dimostrerà il Teorema di Esistenza ed Unicità per le estensioni di Picard-Vessiot.

Nel Capitolo 3 si introdurrà il concetto di gruppo di Galois differenziale di una estensione di campi differenziali. Dopo aver presentato alcuni degli esempi più classici, si dimostrerà che il gruppo di Galois differenziale è un gruppo algebrico lineare. Infine verranno discusse altre importanti proprietà di tale gruppo.

Nel Capitolo 4 verrà esposto il Teorema Fondamentale della Teoria di Picard-Vessiot e se ne darà una dimostrazione andando a discutere e giustificare ogni implicazione presente.

Nel Capitolo 5 si introdurranno le estensioni di Liouville e le estensioni di Liouville generalizzate e si dimostreranno alcune loro importanti proprietà. In conclusione, verrà dimostrato un criterio di risolubilità per quadrature generalizzate di una equazione differenziale, legato alla risolubilità della componente identità del gruppo di Galois differenziale dell'estensione di Picard-Vessiot associata all'equazione.

Sono infine presenti due Appendici in cui vengono presentati gli strumenti e le nozioni utili relativi alle varietà affini e ai gruppi algebrici che vengono usati durante l'esposizione della teoria.

Capitolo 1

Anelli differenziali

1.1 Derivazioni

Definizione 1.1. Una *derivazione (o derivata)* su un anello A è una mappa $\partial\colon A \to A$ tale che, dati $a, b \in A$, si ha

$$\partial(a+b) = \partial(a) + \partial(b) \qquad\qquad \partial(ab) = \partial(a)\, b + a\, \partial(b)$$

Per indicare la derivata di un elemento si userà anche $a' = \partial(a)$ mentre $a'', a''', \ldots, a^{(n)}$ saranno utilizzati per derivate successive.

Per induzione si può dimostrare la regola di Leibniz

$$(ab)^{(n)} = a^{(n)}b + \cdots + \binom{n}{i} a^{(n-i)}b^{(i)} + \cdots + ab^{(n)}$$

Se a' commuta con a si ha che $(a^n)' = na^{n-1}a'$.
Se A è anello con identità 1, allora si deve avere necessariamente $\partial(1) = 0$, infatti

$$\partial(1) = \partial(1 \cdot 1) = \partial(1) \cdot 1 + 1 \cdot \partial(1) \implies \partial(1) = 0$$

Se $a \in A$ è invertibile con inverso a^{-1} si ha che

$$a \cdot a^{-1} = 1 \implies a'a^{-1} + a(a^{-1})' = 0 \implies (a^{-1})' = -a^{-1}a'a^{-1}$$

Dunque se a' commuta con a si ha che $(a^{-1})' = -a'/a^2$

Proposizione 1.2. *Se A è un dominio d'integrità, una derivazione ∂ di A si estende in modo unico al suo campo dei quozienti $Qt(A)$.*

Dimostrazione. Per ogni elemento $\dfrac{a}{b} \in Qt(A)$ si deve avere $\left(\dfrac{a}{b}\right)' = \dfrac{a'b - ab'}{b^2}$ cosicché vi sia unicità.

Si estende la derivazione a $Qt(A)$ definendo $\left(\frac{a}{b}\right)' := \frac{a'b - ab'}{b^2}$
Se $c \in A \setminus \{0\}$ si ha

$$\left(\frac{ac}{bc}\right)' = \frac{(ac)'bc - ac(bc)'}{b^2c^2} = \frac{(a'c + ac')bc - ac(b'c + bc')}{b^2c^2} = \frac{a'b - ab'}{b^2}$$

Dunque la definizione non dipende dalla scelta dei rappresentanti. Si hanno quindi

$$\begin{aligned}\left(\frac{a}{b} + \frac{c}{d}\right)' = \left(\frac{ad + bc}{bd}\right)' &= \frac{(ad + bc)'bd - (ad + bc)(bd)'}{b^2d^2} \\ &= \frac{(a'd + ad' + b'c + bc')bd - (ad + bc)(b'd + bd')}{b^2d^2} \\ &= \frac{a'b - ab'}{b^2} + \frac{c'd - cd'}{d^2} = \left(\frac{a}{b}\right)' + \left(\frac{c}{d}\right)'\end{aligned}$$

e anche

$$\begin{aligned}\left(\frac{a}{b} \cdot \frac{c}{d}\right)' = \left(\frac{ac}{bd}\right)' &= \frac{(ac)'bd - ac(bd)'}{b^2d^2} = \frac{(a'c + ac')bd - ac(b'd + bd')}{b^2d^2} \\ &= \frac{(a'b - ab')c}{b^2d} + \frac{(c'd - cd')a}{d^2b} = \frac{a'b - ab'}{b^2} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{c'd - cd'}{d^2} \\ &= \left(\frac{a}{b}\right)' \cdot \frac{c}{d} + \frac{a}{b} \cdot \left(\frac{c}{d}\right)'\end{aligned}$$

□

Osservazione 1.3. Se A è un anello commutativo senza divisori di zero dotato di una derivazione e S è un sistema moltiplicativo di A, seguendo gli stessi passaggi della dimostrazione si può mostrare che la derivazione di A si estende in modo unico all'anello $S^{-1}A$.

1.2 Anelli differenziali

Definizione 1.4. Un *anello differenziale* è un anello commutativo con identità dotato di una derivazione. Un *campo differenziale* è un anello differenziale che è un campo.

Esempio 1.5. 1. Ogni anello commutativo A con identità può essere visto come un anello differenziale con *derivazione banale* definita da

$$\partial(a) = 0 \quad \forall a \in A$$

Su $\mathbb{Z}$ e $\mathbb{Q}$ la derivazione banale è l'unica possibile poiché $\partial(1) = 0$, quindi per induzione si ha che $\partial(n) = \partial((n-1)+1) = 0$, da cui anche $\partial(n/m) = 0$.

2. L'anello delle funzioni infinitamente differenziabili sull'asse reale con la derivata usuale è un anello differenziale.

3. L'anello delle funzioni analitiche sul piano complesso con la derivata usuale è un anello differenziale. In questo caso si ha un dominio di integrità, quindi la derivata si estende al suo campo dei quozienti che è il campo delle funzioni meromorfe.

4. Siano A un anello differenziale e $A[X]$ l'anello dei polinomi su A con indeterminata X. Una derivazione su $A[X]$ che estenda quella di A deve soddisfare $(\sum a_i X^i)' = \sum (a_i' X^i + a_i i X^{i-1} X')$. Si può dunque estendere la derivazione di A a $A[X]$ assegnando ad X' un arbitrario valore in $A[X]$. Analogamente, se A è un campo, si può dunque estendere la sua derivazione al campo delle funzioni razionali $A(X)$.

   Iterando tale procedimento si può dare una struttura differenziale a $A[X_1, \ldots, X_n]$ (per un anello differenziale A) ed a $A(X_1, \ldots, X_n)$ (per un campo differenziale A).

5. Sia A un anello differenziale. Si considera l'anello dei polinomi $A[X_i]$ nelle indeterminate X_i, $i \in \mathbb{N}$. Definendo $X_i' = X_{i+1}$ si determina in modo unico una derivazione su $A[X_i]$. Si cambierà notazione indicando

$$X = X_0 \qquad X^{(n)} = X_n$$

   Tale procedura è detta *aggiunta di una indeterminata differenziale* e si indicherà il risultante anello differenziale con $A\{X\}$. I suoi elementi sono detti *polinomi differenziali* in X (sono ordinari polinomi in X e nelle sue derivate).

   Se A è un campo differenziale allora $A\{X\}$ è un dominio d'integrità e la sua derivazione si estende in modo unico al suo campo dei quozienti. Si denota tale campo con $A\langle X\rangle$ e i suoi elementi sono detti *funzioni differenziali razionali* in X.

   Iterando il procedimento precedente, si definisce l'anello dei polinomi differenziali in n indeterminate differenziali $X_1, \ldots, X_n$ su A ponendo

$$A\{X_1, \ldots, X_n\} = A\{X_1, \ldots, X_{n-1}\}\{X_n\}$$

   Se A è un campo differenziale, il campo dei quozienti di tale anello sarà il campo differenziale $A\langle X_1, \ldots, X_n\rangle$.

6. Se A è anello differenziale si può definire una derivazione sull'anello $M_{n\times n}(A)$ delle matrici quadrate $n \times n$, definendo la derivata di una matrice come la matrice ottenuta applicando la derivazione di A a tutte le entrate. Per $n \geq 2$ si ha che $M_{n\times n}(A)$ è un anello differenziale non commutativo.

Definizione 1.6. Dato un anello differenziale A, si definisce *l'anello delle costanti* C_A come l'insieme degli elementi di A con derivata nulla

$$C_A := \{a \in A \mid \partial(a) = 0\}$$

C_A è sottoanello di A. Se A è un campo lo è anche C_A (detto *campo delle costanti*).

L'anello delle costanti contiene l'immagine del morfismo $\mathbb{Z} \to A$, $1 \mapsto 1_A$.

In seguito C_K denoterà il campo delle costanti di un campo differenziale K.

Definizione 1.7. Sia I un ideale di un anello differenziale A. Si dice che I è un *ideale differenziale* se $a \in I \implies a' \in I$, ovvero $\partial(I) \subseteq I$.

Se I è ideale differenziale per l'anello differenziale A, si può definire una derivazione sull'anello quoziente A/I imponendo

$$\partial(\bar{a}) \colon = \overline{\partial(a)} \qquad \bar{a} \in A/I$$

Si vede facilmente che tale definizione non dipende dalla scelta del rappresentante nella classe laterale e dunque definisce una derivazione in A/I.

Definizione 1.8. Se A e B sono anelli differenziali, una mappa $f \colon A \to B$ è detta *morfismo differenziale* se soddisfa:

1. $f(a+b) = f(a) + f(b) \qquad f(ab) = f(a)f(b) \qquad f(1) = 1 \quad \forall a, b \in A$
2. $f(a)' = f(a') \quad \forall a \in A$

Le definizioni di isomorfismo differenziale ed automorfismo differenziale sono chiare.

Se I è ideale differenziale, il morfismo naturale $A \to A/I$ è un morfismo differenziale.

Proposizione 1.9. *Se $f \colon A \to B$ è un morfismo differenziale, allora* $\operatorname{Ker} f$ *è un ideale differenziale e la mappa $\bar{f} \colon A/\operatorname{Ker} f \to \operatorname{Im} f$ è un isomorfismo differenziale.*

Dimostrazione. Per $a \in \operatorname{Ker} f$ si ha $f(a') = f(a)' = 0$, quindi $a' \in \operatorname{Ker} f$, dunque $\operatorname{Ker} f$ è un ideale differenziale.

Per ogni $a \in A$ si ha $(\bar{f}(\bar{a}))' = (f(a))' = f(a') = \bar{f}(\bar{a}')$, quindi $\bar{f}$ è un isomorfismo differenziale. □

1.3 Estensioni differenziali

Definizione 1.10. Dati A, B anelli differenziali, con A sottoanello di B, l'inclusione $A \subseteq B$ è detta *estensione di anelli differenziali* se la derivazione su B si restringe alla derivazione su A.

Se S è un sottoinsieme di B si denota con $A\{S\}$ la A-sottoalgebra differenziale di B generata da S su A, che è il più piccolo sottoanello di B contenente A, gli elementi di S e le loro derivate.

Se $K \subseteq L$ è estensione di campi differenziali e S è un sottoinsieme di L, si denota con $K\langle S\rangle$ il sottocampo differenziale di L generato da S su K.
Se S è sottoinsieme finito, si dirà che l'estensione $K \subseteq K\langle S\rangle$ è *finitamente generata differenzialmente.*

Proposizione 1.11. *Se K è un campo differenziale e $K \subseteq L$ una estensione di campi algebrica separabile, allora la derivazione di K si estende in modo unico ad L. Inoltre ogni K-automorfismo di L è differenziale.*

Dimostrazione. Se $K \subseteq L$ è un'estensione finita si ha che $L = K(\alpha)$ per qualche $\alpha \in L$ per il Teorema dell'elemento primitivo. Se $P(X)$ è il polinomio minimo di α su K, derivando l'espressione $P(\alpha) = 0$ si ottiene $P^\partial(\alpha) + P'(\alpha)\,\alpha' = 0$ dove P^∂ denota il polinomio ottenuto da P derivando i suoi coefficienti mentre P' è il polinomio derivato. Si ha dunque $\alpha' = -P^\partial(\alpha)/P'(\alpha)$ e la derivazione si estende in modo unico.

Si verifica l'esistenza. Si ha che $L \cong K[X]/(P)$. Si può estendere la derivazione di K a $K[X]$ definendo $X' := -P^\partial(X)h(X)$ con $h(X) \in K[X]$ tale che $h(X)P'(X) \equiv 1 \pmod{P}$. Se $h(X)P'(X) = 1 + k(X)P(X)$ si ha che

$$\begin{aligned}\partial(P(X)) &= P^\partial(X) + P'(X)X' \\ &= P^\partial(X) + P'(X)(-P^\partial(X)h(X)) \\ &= -P^\partial(X)(1 + P'(X)h(X)) = -P^\partial(X)k(X)P(X)\end{aligned}$$

Dunque (P) è un ideale differenziale e il quoziente $K[X]/(P)$ è un anello differenziale.

Il caso generale $K \subseteq L$ algebrico si ottiene dal caso finito applicando il Lemma di Zorn.

Infine se σ è un K-automorfismo di L, anche $\sigma^{-1}\partial\sigma$ è una derivazione di L che estende quella di K e per unicità si ottiene che $\sigma^{-1}\partial\sigma = \partial$ ovvero $\partial\sigma = \sigma\partial$, dimostrando che σ è un automorfismo differenziale. □

Osservazione 1.12. Sia K un campo differenziale con caratteristica positiva p (ad esempio $\mathbb{F}_p(T)$ con derivazione data da $T' = 1$), sia $P(X) = X^p - a \in K[X]$, con $a \notin K^p$ e sia α una radice di P. Se l'elemento $a \in K$ non è una costante, allora non è possibile estendere la derivazione di K a $L := K(\alpha)$. Se invece a è una costante si può estendere la derivazione di K a L assegnando a α' un valore arbitrario in L.

Definizione 1.13. Se $K \subseteq L$ è una estensione di campi differenziali, un elemento $\alpha \in L$ è detto:

- *elemento primitivo (o integrale)* su K se $\alpha' \in K$;
- *elemento esponenziale* su K se $\alpha'/\alpha \in K$.

1.4 Anello degli operatori differenziali

Definizione 1.14. Sia K un campo differenziale con una derivazione ∂ non banale. Un *operatore differenziale lineare* $\mathcal{L}$ con coefficienti in K è un polinomio nella variabile ∂

$$\mathcal{L} = a_n\partial^n + a_{n-1}\partial^{n-1} + \cdots + a_1\partial + a_0 \quad \text{con} \ \ a_i \in K$$

Se $a_n \neq 0$ si dice che $\mathcal{L}$ ha ordine (o grado) n. Se $a_n = 1$ si dice che $\mathcal{L}$ è monico.

L'*anello degli operatori differenziali lineari* con coefficienti in K è l'anello non commutativo $K[\partial]$ dei polinomi nella variabile ∂ con coefficienti in K, con ∂ che soddisfa

$$\partial a = a' + a\partial$$

per ogni elemento $a \in K$.

Si ha che $\deg(\mathcal{L}_1\mathcal{L}_2) = \deg \mathcal{L}_1 + \deg \mathcal{L}_2$ e dunque gli unici elementi invertibili a destra o sinistra di $K[\partial]$ sono gli elementi di $K \setminus \{0\}$.

Un operatore differenziale agisce su K e sulle estensioni differenziali di K scrivendo $\partial(y) = y'$. Quindi, fissato un operatore differenziale

$$\mathcal{L} = a_n\partial^n + a_{n-1}\partial^{n-1} + \cdots + a_1\partial + a_0$$

ad esso si associa l'equazione differenziale lineare

$$\mathcal{L}(Y) = a_nY^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1Y' + a_0Y = 0$$

Come per l'anello dei polinomi in una variabile su un campo K, si ha un algoritmo per la divisione (sia a destra che a sinistra).

Lemma 1.15. *Dati $\mathcal{L}_1, \mathcal{L}_2 \in K[\partial]$, con $\mathcal{L}_2 \neq 0$, esistono e sono unici degli operatori differenziali Q_s, R_s (risp. Q_d, R_d) in $K[\partial]$ tali che*

$$\mathcal{L}_1 = Q_s\mathcal{L}_2 + R_s \quad con \quad \deg R_s < \deg \mathcal{L}_2$$

$$(risp.\ \mathcal{L}_1 = \mathcal{L}_2 Q_r + R_r \quad con \quad \deg R_r < \deg \mathcal{L}_2)$$

La dimostrazione di tale proprietà è analoga al caso polinomiale.

Corollario 1.16. *Per ogni ideale sinistro (risp. destro) I di $K[\partial]$ esiste un elemento $\mathcal{L} \in K[\partial]$, unico a meno di un fattore in $K \setminus \{0\}$, tale che $I = K[\partial]\mathcal{L}$ (risp. $I = \mathcal{L}K[\partial]$).*

Da tale corollario si deduce che dati due operatori differenziali lineari $\mathcal{L}_1, \mathcal{L}_2$ il loro MCD sinistro è l'unico generatore monico di $K[\partial]\mathcal{L}_1 + K[\partial]\mathcal{L}_2$ e il loro *mcm* sinistro è l'unico generatore monico di $K[\partial]\mathcal{L}_1 \cap K[\partial]\mathcal{L}_2$. Analogamente si definiscono MCD destro e *mcm* destro. Si possono calcolare i MCD destro e sinistro tramite una versione modificata dell'algoritmo di Euclide.

1.5 Prodotto tensoriale di anelli differenziali

Sia K campo differenziale e siano R, S anelli differenziali con $K \subseteq R, K \subseteq S$. Si vuole definire il prodotto tensoriale tra anelli differenziali $R \otimes_K S$.

Sia $\{x_i\}_{i\in I}$ una base di R (come spazio vettoriale) su K e sia $\{y_j\}_{j\in J}$ una base di S su K. Considerando tutte le coppie del tipo (x_i, y_j) (con $i \in I, j \in J$), $R \otimes_K S$ è l'insieme delle somme formali finite

$$\sum_{i,j} a_{ij}(x_i, y_j) \quad \text{con} \quad a_{ij} \in K$$

$R \otimes_K S$ è spazio vettoriale su K con base data da $\{(x_i, y_j)\}_{i\in I, j\in J}$.

Se $x = \sum_i a_i x_i \in R$ e $y = \sum_j b_j y_j \in S$ si scriverà

$$x \otimes y = \sum_{i,j} a_i b_j (x_i, y_j) \in R \otimes_K S$$

con le proprietà ($x, \bar{x} \in R$, $y, \bar{y} \in S$, $a \in K$):

1. $(x + \bar{x}) \otimes y = x \otimes y + \bar{x} \otimes y$
2. $x \otimes (y + \bar{y}) = x \otimes y + x \otimes \bar{y}$
3. $a(x \otimes y) = ax \otimes y = x \otimes ay$

Si definisce poi il prodotto

$$(x \otimes y)(\bar{x} \otimes \bar{y}) := x\bar{x} \otimes y\bar{y} \quad \text{con } x, \bar{x} \in R, y, \bar{y} \in S$$

e la derivata

$$(x \otimes y)' := x' \otimes y + x \otimes y' \quad \text{con } x \in R, y \in S$$

In tal modo si ha che $R \otimes_K S$ è anello differenziale.

Si hanno le mappe canoniche di inclusione

$$\begin{array}{ll} \alpha \colon R \to R \otimes_K S & \beta \colon S \to R \otimes_K S \\ r \mapsto r \otimes 1 & s \mapsto 1 \otimes s \end{array}$$

Capitolo 2

Estensioni di Picard-Vessiot

2.1 Equazioni differenziali lineari omogenee

D'ora in poi si indicherà con K un campo di caratteristica zero ($\operatorname{char} K = 0$).

Sia $\mathcal{L}(Y)$ un'equazione differenziale lineare omogenea (si può supporre monica) su un campo differenziale K, con campo delle costanti C_K:

$$\mathcal{L}(Y) := Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1 Y' + a_0 Y = 0 \qquad a_i \in K$$

Se $K \subseteq L$ è un'estensione differenziale, l'insieme delle soluzioni di $\mathcal{L}(Y) = 0$ in L è un C_L-spazio vettoriale (con C_L campo delle costanti di L).

Definizione 2.1. Siano $y_1, y_2, \ldots, y_n$ elementi di un campo differenziale K. Si definisce il *(determinante) Wronksiano* di $y_1, y_2, \ldots, y_n$ come il determinante

$$W = W(y_1, y_2, \ldots, y_n) := \begin{vmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{vmatrix}$$

Proposizione 2.2. *Sia K un campo differenziale con campo delle costanti C_K e siano $y_1, y_2, \ldots, y_n \in K$. Allora $y_1, y_2, \ldots, y_n$ sono linearmente indipendenti su C_K se e solo se $W(y_1, \ldots, y_n) \neq 0$.*

Dimostrazione. Si assuma che $y_1, y_2, \ldots, y_n$ siano linearmente dipendenti su C_K, ovvero $\sum_{i=1}^n c_i y_i = 0$ con $c_i \in C_K$ non tutti nulli. Derivando $n-1$ volte tale uguaglianza si ottengono le espressioni $\sum_{i=1}^n c_i y_i^{(k)} = 0$ al variare di $k = 0, \ldots, n-1$. Dunque le colonne del Wronksiano sono linearmente dipendenti, da cui $W(y_1, \ldots, y_n) = 0$.

Viceversa sia $W(y_1, \ldots, y_n) = 0$. Si hanno n uguaglianze $\sum_{i=1}^{n} c_i y_i^{(k)} = 0$ con $k = 0, \ldots, n-1$ e $c_i \in K$ non tutti zero. Si può assumere di avere $c_1 = 1$ e $W(y_2, \ldots, y_n) \neq 0$. Derivando la k-esima uguaglianza si ottiene che $\sum_{i=1}^{n} c_i y_i^{(k+1)} + \sum_{i=2}^{n} c_i' y_i^{(k)} = 0$. Sottraendo a tale espressione l'uguaglianza $(k+1)$-esima si trova $\sum_{i=2}^{n} c_i' y_i^{(k)} = 0$ con $k = 0, \ldots, n-2$. Si ha dunque un sistema di equazioni lineari omogenee in $c_2', \ldots, c_n'$ con determinante $W(y_2, \ldots, y_n) \neq 0$, perciò $c_2' = \cdots = c_n' = 0$ cioè $c_i \in C_K \ \forall i = 1, \ldots, n$. □

Da tale proposizione si può parlare di lineare (in)dipendenza sul campo delle costanti senza ambiguità poiché la condizione di (non) annullamento del Wronksiano è indipendente dal campo.

Proposizione 2.3. *Sia $\mathcal{L}(Y) = 0$ una equazione differenziale lineare omogenea di ordine n su un campo differenziale K. Se $y_1, \ldots, y_{n+1}$ sono soluzioni di $\mathcal{L}(Y) = 0$ in una estensione differenziale L di K, allora $W(y_1, \ldots, y_{n+1}) = 0$.*

Dimostrazione. L'ultima riga del Wronksiano è formata da $(y_1^{(n)}, \ldots, y_{n+1}^{(n)})$, che è una combinazione lineare non banale delle righe precedenti, infatti da $\mathcal{L}(y_i) = y_i^{(n)} + a_{n-1} y_i^{(n-1)} + \cdots + a_1 y_i' + a_0 y_i = 0 \quad \forall i$, si ha

$$y_i^{(n)} = -(a_{n-1} y_i^{(n-1)} + \cdots + a_1 y_i' + a_0 y_i) \quad \forall i$$ □

Corollario 2.4. *$\mathcal{L}(Y) = 0$ ha al più n soluzioni in L linearmente indipendenti sul campo delle costanti.*

Sia $\mathcal{L}(Y) = 0$ una equazione differenziale lineare omogenea di ordine n su un campo differenziale K, $y_1, \ldots, y_n$ siano n soluzioni di $\mathcal{L}(Y) = 0$ in una estensione differenziale L di K, linearmente indipendenti sul campo delle costanti. Si dice che $\{y_1, \ldots, y_n\}$ è un *insieme fondamentale di soluzioni* per $\mathcal{L}(Y) = 0$ in L. Ogni altra soluzione di $\mathcal{L}(Y) = 0$ in L è combinazione lineare (con coefficienti costanti) di $y_1, \ldots, y_n$.

La seguente proposizione si dimostra facilmente utilizzando le proprietà del determinante.

Proposizione 2.5. *Sia $\mathcal{L}(Y) = 0$ una equazione differenziale lineare omogenea di ordine n su un campo differenziale K e sia $\{y_1, \ldots, y_n\}$ una base dello spazio delle soluzioni di $\mathcal{L}(Y) = 0$ in una estensione differenziale L di K. Siano $z_j = \sum_{i=1}^{n} c_{ij} y_i, \ (j = 1, \ldots, n)$ con c_{ij} costanti, allora*

$$W(z_1, \ldots, z_n) = \det(c_{ij}) \cdot W(y_1, \ldots, y_n)$$

2.2 Esistenza e unicità delle estensioni di Picard-Vessiot

Si definirà ora l'estensione di Picard-Vessiot di una equazione differenziale lineare omogenea, che può essere pensata come l'analogo del campo di spezzamento di un polinomio.

Definizione 2.6. Data una equazione differenziale lineare omogenea $\mathcal{L}(Y) = 0$ di ordine n su un campo differenziale K, una estensione differenziale $K \subseteq L$ è una *estensione di Picard-Vessiot* per $\mathcal{L}$ se

1. $L = K\langle y_1, \ldots, y_n \rangle$, dove $y_1, \ldots, y_n$ è un insieme fondamentale di soluzioni per $\mathcal{L}(Y) = 0$ in L.

2. Ogni costante di L è in K, cioè $C_K = C_L$.

Osservazione 2.7. Siano F un campo differenziale, $K = F\langle z \rangle$ con $z' = z$ e si consideri l'equazione differenziale $Y' - Y = 0$. Poiché z è soluzione dell'equazione, pensando in modo analogo ai campi di spezzamento, è naturale supporre che l'estensione di Picard-Vessiot per tale equazione sia l'estensione banale di K. Aggiungendo ora una seconda indeterminata differenziale e considerando $L = K\langle y \rangle$ con $y' = y$, l'estensione $K \subseteq L$ soddisfa la condizione 1 nella Definizione 2.6. Si ha dunque che $(y/z)' = 0$, ovvero l'estensione $K \subseteq L$ aggiunge una nuova costante y/z.

Quindi la condizione 2 nella definizione delle estensioni di Picard-Vessiot ne garantisce la minimalità.

Si dimostrerà ora che, quando K è un campo differenziale con campo delle costanti C_K algebricamente chiuso, esiste una estensione di Picard-Vessiot L di K per una data equazione differenziale lineare omogenea $\mathcal{L}$ definita su K e che essa è unica a meno di K-isomorfismi differenziali.

L'idea per dimostrare l'esistenza è costruire una K-algebra differenziale contenente un insieme fondamentale di soluzioni per l'equazione differenziale $\mathcal{L}(Y) = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1 Y' + a_0 Y = 0$ e poi farne il quoziente con un ideale differenziale massimale per ottenere un'estensione che non aggiunge costanti.

Si considera l'anello dei polinomi in n^2 indeterminate

$$K[Y_{ij}, 0 \leq i \leq n-1, 1 \leq j \leq n]$$

e si estende la derivazione di K a $K[Y_{ij}]$ definendo $(\forall j)$

$$\begin{aligned} Y'_{ij} &:= Y_{i+1,j} \quad \text{per} \quad 0 \leq i \leq n-2 \\ Y'_{n-1,j} &:= -(a_{n-1}Y_{n-1,j} + \cdots + a_1 Y_{1j} + a_0 Y_{0j}) \end{aligned}$$

Tale definizione è corretta in quanto si può ottenere $K[Y_{ij}]$ definendo l'anello $K\{X_1, \ldots, X_n\}$ in n indeterminate differenziali e facendo il quoziente con l'ideale differenziale generato dagli elementi

$$X_j^{(n)} + a_{n-1}X_j^{(n-1)} + \cdots + a_1X_j' + a_0X_j \quad 1 \leq j \leq n$$

cioè l'ideale generato da tali elementi e dalle loro derivate.
Sia $R := K[Y_{ij}][W^{-1}]$ la localizzazione di $K[Y_{ij}]$ nel sistema moltiplicativo delle potenze di $W = \det(Y_{ij})$. La derivazione di $K[Y_{ij}]$ si estende in modo unico ad R (Osservazione 1.3).
L'algebra R è detta *algebra universale completa delle soluzioni* per $\mathcal{L}$.

Dalle due proposizioni che seguono si otterrà che un ideale differenziale massimale P dell'algebra universale completa delle soluzioni R è un ideale primo, da cui R/P è un dominio di integrità, e che il campo dei quozienti di R/P ha lo stesso campo delle costanti di K.

Proposizione 2.8. *Siano K un campo differenziale e $K \subseteq R$ una estensione di anelli differenziali. Sia I un elemento massimale nell'insieme degli ideali differenziali propri di R. Allora I è un ideale primo.*

Dimostrazione. Passando al quoziente R/I si può supporre che R non abbia ideali differenziali propri. Dunque basta dimostrare che R è un dominio di integrità. Siano a, b elementi non nulli di R tali che $ab = 0$. Si vede che $\partial^k(a)b^{k+1} = 0\ \forall k \in \mathbb{N}$, infatti $ab = 0 \implies 0 = \partial(ab) = a\partial(b) + \partial(a)b$ e moltiplicando tale espressione per b si ha che $\partial(a)b^2 = 0$. Per induzione, se ciò vale per k allora $0 = \partial(\partial^k(a)b^{k+1}) = \partial^{k+1}(a)b^{k+1} + (k+1)\partial^k(a)b^k\partial(b)$ e moltiplicando per b si ottiene $\partial^{k+1}(a)b^{k+2} = 0$.

Sia ora J l'ideale differenziale generato da a, ovvero l'ideale generato da a e dalle sue derivate. Si suppone per assurdo che nessuna potenza di b sia zero (cioè $b^n \neq 0\, \forall n \in \mathbb{N}$). Da $\partial^k(a)b^{k+1} = 0\, \forall k \in \mathbb{N}$ si ha che tutti gli elementi di J sono divisori di zero. In particolare $J \neq R$ e, poiché J contiene l'elemento non nullo a, J è un ideale differenziale proprio di R, ma ciò contraddice l'ipotesi iniziale. Dunque vi deve essere almeno una potenza di b che dia 0.

Visto che b era un divisore di zero arbitrario si conclude che tutti i divisori di zero di R sono nilpotenti, in particolare $a^n = 0\ \exists n$. Scegliendo n minimo si ha $0 = \partial(a^n) = na^{n-1}\partial(a)$. Poiché $K \subseteq R$ (char $K = 0$) si ha $na^{n-1} \neq 0$, quindi $\partial(a)$ è un divisore di zero. Si è dimostrato che la derivata di un divisore di zero è ancora un divisore di zero, dunque a e tutte le sue derivate sono divisori di zero quindi nilpotenti. In particolare $J \neq R$, perciò J sarebbe un ideale differenziale proprio di R e ciò porterebbe di nuovo ad una contraddizione. Si conclude quindi che R è dominio d'integrità. □

Proposizione 2.9. *Sia K un campo differenziale con campo delle costanti C_K e sia $K \subseteq R$ una estensione di anelli differenziali con R dominio d'integrità finitamente generato come K-algebra. Sia L il campo dei quozienti di R. Si assume che C_K sia algebricamente chiuso e che R non abbia ideali differenziali propri. Allora L non contiene nuove costanti, cioè $C_L = C_K$.*

Dimostrazione. 1. Si dimostra che gli elementi in $C_L \setminus C_K$ non possono essere algebrici su K. Se $\alpha \in \overline{K} \setminus K$ dalla dimostrazione della Proposizione 1.11 si ha che $\alpha' = -P^{\partial}(\alpha)/P'(\alpha)$ per $P(X) = X^k + a_{k-1}X^{k-1} + \cdots + a_1X + a_0$ polinomio minimo di α su K. Allora $\alpha' = 0 \implies P^{\partial}(X) = a'_{k-1}X^{k-1} + \cdots + a'_1X + a'_0 = 0$, quindi $P(X) \in C_K[X]$ e $\alpha \in C_K$.

2. Si ha $C_L \subseteq R$. Infatti per ogni $b \in C_L$ si ha che $b = f/g$ con $f, g \in R$. Si considera l'ideale dei denominatori di b, $J = \{h \in R \mid hb \in R\}$. Si ha $h \in J \implies hb \in R \implies (hb)' = h'b \in R \implies h' \in J$. Quindi J è un ideale differenziale. Per ipotesi R non ha ideali propri, dunque $J = R$, da cui $b \in R$.

3. Si mostra che per ogni $b \in C_L$ esiste un elemento $c \in C_K$ tale che $b - c$ è non invertibile in R. Allora l'ideale $(b-c)R$ è un ideale differenziale diverso da R e dunque è nullo. Così $b = c \in C_K$.

Si useranno ora risultati di geometria algebrica. Sia $\overline{K}$ la chiusura algebrica di K e $\overline{R} = R \otimes_K \overline{K}$. Se l'elemento $b \otimes 1 - c \otimes 1 = (b-c) \otimes 1$ non è invertibile in $\overline{R}$, allora $(b - c)$ non è invertibile in R. Si può dunque assumere K algebricamente chiuso. Sia V una varietà algebrica affine con anello delle coordinate R. Allora b definisce una funzione f a valori in K su V. Dal Teorema di Chevalley (Teorema A.15) la sua immagine $f(V)$ è un insieme costruibile nella retta affine $\mathbb{A}^1$ e quindi o un insieme finito di punti o il complementare di un insieme finito di punti. Nel secondo caso, poiché C_K è infinito, esiste $c \in C_K$ tale che $f(v) = c$ per qualche $v \in V$, cosicché $f - c$ si annulla in v e quindi $(b - c)$ appartiene all'ideale massimale di v. Dunque $(b - c)$ non è invertibile. Se invece $f(V)$ fosse finito consisterebbe di un singolo punto, visto che V sarebbe irriducibile essendo R un dominio. Allora f sarebbe costante e b apparterebbe a K, dunque a C_K. □

Si dimostra ora l'esistenza delle estensioni di Picard-Vessiot:

Teorema 2.10. *Sia K un campo differenziale con campo delle costanti C_K algebricamente chiuso. Sia $\mathcal{L}(Y) = 0$ un'equazione differenziale lineare omogenea definita su K. Sia R l'algebra universale completa delle soluzioni per $\mathcal{L}$ e sia P un ideale differenziale massimale di R. Allora P è un ideale primo e il campo dei quozienti L del dominio di integrità R/P è una estensione di Picard-Vessiot di K per $\mathcal{L}$.*

Dimostrazione. Si ha che R è generato differenzialmente su K dalle soluzioni dell'equazione differenziale $\mathcal{L}(Y) = 0$ e dall'inverso del Wronksiano, dunque ciò vale anche per R/P. Dalla Proposizione 2.8, l'ideale P è primo. Poiché P è ideale differenziale massimale, R/P non ha ideali differenziali propri dunque dalla Proposizione 2.9 si ha $C_L = C_K$. Inoltre il Wronksiano è invertibile in R/P e quindi in particolare è non nullo in L. Dunque L contiene un insieme fondamentale di soluzioni per $\mathcal{L}$ ed è generato differenzialmente da esso su K. Perciò L è una estensione di Picard-Vessiot di K per $\mathcal{L}$. □

Per ottenere l'unicità delle estensioni di Picard-Vessiot è necessario prima dimostrare una proprietà di normalità.

Proposizione 2.11. *Siano L_1, L_2 estensioni di Picard-Vessiot di K per un'equazione differenziale lineare omogenea $\mathcal{L}(Y) = 0$ di ordine n e sia $K \subseteq L$ una estensione di campi differenziali con $C_L = C_K$. Siano inoltre $\sigma_i \colon L_i \to L$ K-morfismi differenziali $(i = 1, 2)$. Allora $\sigma_1(L_1) = \sigma_2(L_2)$.*

Dimostrazione. Si considerino gli insiemi $V_i := \{y \in L_i \mid \mathcal{L}(y) = 0\}$, $i = 1, 2$, e $V := \{y \in L \mid \mathcal{L}(y) = 0\}$. Si ha che V_i è uno C_K-spazio vettoriale di dimensione n e V è un C_K-spazio vettoriale di dimensione al più n. Dato che σ_i è morfismo differenziale si ha $\sigma_i(V_i) \subseteq V$, $i = 1, 2$, da cui $\sigma_1(V_1) = \sigma_2(V_2) = V$. Da $L_i = K\langle V_i \rangle$, $i = 1, 2$, si ha $\sigma_1(L_1) = \sigma_2(L_2)$. □

Da tale proposizione derivano i seguenti corollari:

Corollario 2.12. *Siano $K \subseteq L \subseteq M$ campi differenziali. Si suppone che L sia una estensione di Picard-Vessiot di K e che M abbia lo stesso campo delle costanti di K (cioè $C_M = C_K$). Allora ogni K-automorfismo di M manda L in sé stesso.*

Corollario 2.13. *Sia K un campo differenziale con campo delle costanti C_K algebricamente chiuso. Se L è una estensione di Picard-Vessiot algebrica di K, allora L è una estensione algebrica normale di K, cioè ogni automorfismo di una chiusura algebrica di L che fissa K è un automorfismo di L.*

Dimostrazione. Sia M una chiusura algebrica di L, con $K \subseteq L \subseteq M$. Dunque M è una estensione algebrica di K, perciò dalla Proposizione 1.11 si ha che M è una estensione differenziale di K ed ogni K-automorfismo di M è differenziale.

Si vede che l'estensione $C_K \subseteq C_M$ è algebrica. Infatti, preso $\alpha \in C_M$ con $P(X) = X^k + a_{k-1}X^{k-1} + \cdots + a_1X + a_0$ il suo polinomio minimo su K, si ha

$$\begin{aligned} \alpha' = 0,\ P(\alpha) = 0 &\implies P^\partial(\alpha) + P'(\alpha)\alpha' = 0 \\ &\implies P^\partial(\alpha) = a'_{k-1}X^{k-1} + \cdots + a'_1X + a'_0 = 0 \end{aligned}$$

da cui $P(X) \in C_K[X]$. Dal punto 1 della Dimostrazione della Proposizione 2.9 si ha inoltre $C_K = C_M$. Da ciò si conclude per il Corollario 2.12. □

Si stabilisce ora l'unicità a meno di K-isomorfismi delle estensioni di Picard-Vessiot:

Teorema 2.14. *Sia K un campo differenziale con campo delle costanti C_K algebricamente chiuso. Sia $\mathcal{L}(Y) = 0$ una equazione differenziale lineare omogenea definita su K. Siano L_1, L_2 due estensioni di Picard-Vessiot di K per $\mathcal{L}$. Allora esiste un K-isomorfismo differenziale da L_1 in L_2.*

Dimostrazione. Si può supporre che L_1 sia l'estensione di Picard-Vessiot precedentemente considerata nel Teorema 2.10. L'idea della dimostrazione è di costruire un'estensione differenziale $K \subseteq E$ con $C_E = C_K$, K-morfismi differenziali $L_1 \to E$, $L_2 \to E$ e applicare la Proposizione 2.11.

Si consideri l'anello $A := (R/P) \otimes_K L_2$ (con R e P definiti come nel Teorema 2.10). A è un anello differenziale finitamente generato come una L_2-algebra, con derivazione definita da $\partial(x \otimes y) := \partial(x) \otimes y + x \otimes \partial(y)$. Sia Q un ideale differenziale massimale proprio di A. La sua preimmagine in R/P, tramite la mappa $R/P \to A$, $a \mapsto a \otimes 1$, è nulla dato che R/P non contiene ideali differenziali propri e non può essere uguale a R/P poiché, in tal caso, Q sarebbe uguale ad A (in contraddizione col fatto che Q è proprio). Quindi R/P si immerge iniettivamente in A/Q tramite $a \mapsto \overline{a \otimes 1}$ e anche la mappa $L_2 \hookrightarrow A/Q$ data da $b \mapsto \overline{1 \otimes b}$ è iniettiva. Dalla Proposizione 2.8 si ha che Q è primo, dunque A/Q è un dominio di integrità. Sia E il suo campo dei quozienti. Si può ora applicare la Proposizione 2.9 alla L_2-algebra A/Q per ottenere che $C_E = C_K = C_{L_2}$ (la seconda uguaglianza segue dal fatto che L_2 è estensione di Picard-Vessiot su K). Applicando la Proposizione 2.11 alle mappe $L_1 \hookrightarrow A/Q \hookrightarrow E$ e $L_2 \hookrightarrow A/Q \hookrightarrow E$ si ottiene che esiste un K-isomorfismo differenziale $L_1 \to L_2$. □

Enunciando insieme i teoremi 2.10 e 2.14 si ha il Teorema di Esistenza e Unicità per le estensioni di Picard-Vessiot:

Teorema di Esistenza e Unicità 2.15. *Sia K un campo differenziale con campo delle costanti C_K algebricamente chiuso e sia*

$$\mathcal{L}(Y) = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1 Y' + a_0 Y = 0$$

una equazione differenziale lineare omogenea definita su K.
Allora esiste una estensione di Picard-Vessiot L di K per $\mathcal{L}$ ed è unica a meno di K-isomorfismi differenziali.

Capitolo 3

Gruppo di Galois differenziale

Definizione 3.1. Se $K \subseteq L$ è una estensione di campi differenziali, si chiama *gruppo di Galois differenziale* dell'estensione $K \subseteq L$

$$Gal(L/K)$$

il gruppo dei K-automorfismi differenziali di L.

Se $K \subseteq L$ è una estensione di Picard-Vessiot per $\mathcal{L}(Y) = 0$, il gruppo $Gal(L/K)$ è detto anche gruppo di Galois (differenziale) di $\mathcal{L}$ su K. Si usa la notazione $Gal_K(\mathcal{L})$ oppure $Gal(\mathcal{L})$ se il campo base è chiaro dal contesto.

3.1 Esempi di gruppi di Galois differenziali

Si vedranno ora alcuni esempi importanti di gruppi di Galois differenziali.

Esempio 3.2. Si consideri l'estensione di campi differenziali $L = K\langle\alpha\rangle$, con $\alpha' = a \in K$ tale che a non è una derivata in K. Si dice che L è ottenuto da K per *aggiunta di un integrale*. Si dimostra che α è trascendente su K, $K \subseteq K\langle\alpha\rangle$ è una estensione di Picard-Vessiot e $Gal(K\langle\alpha\rangle/K)$ è isomorfo al gruppo additivo di C_K.

Sia per assurdo α algebrico su K e sia $P(X) = X^n + \sum_{i=1}^{n} b_i X^{n-i}$ il suo polinomio minimo su K. Allora $0 = P(\alpha) = \alpha^n + \sum_{i=1}^{n} b_i \alpha^{n-i}$, derivando si ha $0 = n\alpha^{n-1}a + b_1'\alpha^{n-1} + (\text{termini di grado} < n-1) \implies na + b_1' = 0 \implies a = -b_1'/n = (-b_1/n)'$ che dà una contraddizione, dunque α è trascendente su K.

Si vede che $K\langle\alpha\rangle$ non contiene nuove costanti. Si suppone che il polinomio $\sum_{i=0}^{n} b_i \alpha^{n-i}$, con $b_i \in K$, sia costante. Derivando si ottiene che $0 = b_0'\alpha^n + (nb_0a + b_1')\alpha^{n-1} + (\text{termini di grado} < n-1) \implies b_0' = 0$, $nb_0a + b_1' = 0 \implies a = -b_1'/nb_0 = (-b_1/nb_0)'$, contraddicendo l'ipotesi.

Si supponga ora che la funzione razionale $f(\alpha)/g(\alpha)$ sia costante, con g monico di grado ≥ 1 minimo. Derivando si ha che

$$0 = \frac{f(\alpha)'g(\alpha)a - f(\alpha)g(\alpha)'a}{g(\alpha)^2} \implies \frac{f(\alpha)}{g(\alpha)} = \frac{f(\alpha)'}{g(\alpha)'}$$

con $g(\alpha)'$ polinomio non nullo di grado minore rispetto a g, poiché $g(\alpha)$ non è costante e g è monico. Questa è una contraddizione.

Si osserva che 1 e α sono soluzioni di $Y'' - \frac{a'}{a}Y' = 0$ linearmente indipendenti sul campo delle costanti C_K, dunque $K \subsetneq K\langle\alpha\rangle = L$ è una estensione di Picard-Vessiot.

Un K-automorfismo differenziale di $K\langle\alpha\rangle$ manda α in $\alpha + c$ con $c \in C_K$ e una mappa $\alpha \mapsto \alpha + c$ induce un K-automorfismo differenziale di $K\langle\alpha\rangle$ per ogni $c \in C_K$. Dunque si ha

$$Gal(K\langle\alpha\rangle/K) \cong C_K \cong \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}, c \in C_K \right\} \subset \mathrm{GL}(2, C_K)$$

Esempio 3.3. Si consideri l'estensione di campi differenziali $L = K\langle\alpha\rangle$, con $\alpha'/\alpha = a \in K \setminus \{0\}$. Si dice che L è ottenuto da K per *aggiunta dell'esponenziale di un integrale*. È chiaro che $K\langle\alpha\rangle = K(\alpha)$ e α è un insieme fondamentale di soluzioni per l'equazione differenziale $Y' - aY = 0$. Si assume che $C_L = C_K$.

Si vede che se α è algebrico su K allora $\alpha^n \in K$ per qualche $n \in \mathbb{N}$ e inoltre il gruppo di Galois $Gal(L/K)$ è isomorfo ad un gruppo ciclico finito. Invece se α è trascendente su K, il gruppo $Gal(L/K)$ è isomorfo al gruppo moltiplicativo di C_K.

Si suppone α algebrico su K, con $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ il suo polinomio minimo. Derivando si ottiene

$$0 = P(\alpha)' = P^{\partial}(\alpha) + P'(\alpha)\alpha' = P^{\partial}(\alpha) + P'(\alpha)a\alpha = an\alpha^n + \sum_{k=0}^{n-1}(a_k' + aka_k)\alpha^k$$

Quest'ultimo polinomio è diviso da P (polinomio minimo di α), quindi si ha $a_k' + aka_k = ana_k \implies a_k' = a(n-k)a_k$, $0 \leq k \leq n-1$. Dunque $(\alpha^{n-k}/a_k)' = 0$ e in particolare $\alpha^n = ca_0$ per qualche $c \in C_L = C_K$, da cui $\alpha^n = b \in K$. Allora $P(X)$ divide $X^n - b$, quindi $P(X) = X^n - b$.

Per $\sigma \in Gal(L/K)$ si ha $\sigma(\alpha)' = \sigma(\alpha') = \sigma(a\alpha) = a\sigma(\alpha)$. Si ha quindi $(\sigma(\alpha)/\alpha)' = 0 \implies \sigma(\alpha) = c\alpha$ per qualche $c \in C_L = C_K$. Se α è trascendente su K, per ogni $c \in C_K$ si può definire un K-automorfismo differenziale di L dato da $\alpha \mapsto c\alpha$. Se α è algebrico allora $\alpha^n = b \in K$, da cui si ha che $c^n\alpha^n = \sigma(\alpha)^n = \sigma(\alpha^n) = \sigma(b) = b = \alpha^n \implies c^n = 1 \implies c$ deve essere una radice n-esima dell'unità e $Gal(L/K)$ è un gruppo ciclico finito.

Esempio 3.4. Si considerino un campo differenziale K (con campo delle costanti C_K algebricamente chiuso), un polinomio irriducibile $P(X) \in K[X]$ di grado n ed un campo di spezzamento L di $P(X)$ su K. Si vede che $K \subseteq L$ è una estensione di Picard-Vessiot.

Per la Proposizione 1.11 si può estendere la derivazione di K a L in modo unico definendo $x' := -P^{\partial}(x)h(x)$ per ogni radice x di $P(X)$ in L, con $h(X) \in K[X]$ tale che $h(X)P'(X) \equiv 1 \pmod{P}$. Inoltre, riducendo modulo P, si può ottenere una espressione per x' come polinomio in x di grado minore di n. Derivando tale espressione polinomiale di x' si ottiene un'espressione per x'' come polinomio in x il quale, riducendo ancora modulo P, avrà grado minore di n. Iterando tale processo si ottengono espressioni polinomiali in x di grado minore di n per tutte le successive derivate di x. Perciò $x, x', \ldots, x^{(n-1)}$ sono linearmente dipendenti su K. Scrivendo tale relazione di dipendenza si ottiene una equazione differenziale lineare omogenea con coefficienti in K soddisfatta da tutte le radici del polinomio P. Si assuma che, calcolando le derivate successive di una radice x di P, la prima relazione di lineare dipendenza trovata dia l'equazione differenziale

$$\mathcal{L}(Y) = Y^{(k)} + a_{k-1}Y^{(k-1)} + \cdots + a_1Y' + a_0Y = 0,\ a_i \in K,\ k \leq n$$

Allora esistono k radici $x_1, \ldots, x_k$ di P con $W(x_1, \ldots, x_k) \neq 0$, poiché altrimenti si sarebbe trovata un'equazione differenziale di ordine minore di k soddisfatta da tutte le radici di P.

Dunque L è una estensione di Picard-Vessiot di K per l'equazione $\mathcal{L}(Y) = 0$ e per la Proposizione 1.11 il gruppo di Galois differenziale di $K \subseteq L$ coincide con il suo gruppo di Galois algebrico.

3.2 Gruppo di Galois differenziale come gruppo algebrico lineare

Si vuole dimostrare che il gruppo di Galois differenziale per una estensione di Picard-Vessiot è un gruppo algebrico lineare. D'ora in poi si assumerà che il campo delle costanti C_K di K sia algebricamente chiuso.

Per prima cosa si vede che il gruppo di Galois di una equazione differenziale lineare omogenea di ordine n definita sul campo differenziale K è isomorfo ad un sottogruppo del gruppo generale lineare $\mathrm{GL}(n, C_K)$ sul campo delle costanti C_K di K.
Infatti se $y_1, \ldots, y_n$ è un insieme fondamentale di soluzioni di $\mathcal{L}(Y) = 0$, per ogni $\sigma \in Gal_K(\mathcal{L})$ e per ogni $j \in \{1, \ldots, n\}$, $\sigma(y_j)$ è ancora una soluzione di $\mathcal{L}(Y) = 0$, quindi $\sigma(y_j) = \sum_{i=1}^{n} c_{ij}y_i$, per qualche $c_{ij} \in C_K$. Dunque si può

associare ad ogni $\sigma \in Gal_K(\mathcal{L})$ la matrice $(c_{ij}) \in \mathrm{GL}(n, C_K)$. Inoltre, visto che $L = K\langle y_1, \ldots, y_n \rangle$, un K-automorfismo differenziale di L è determinato dall'immagine delle y_j. Da ciò si ottiene un morfismo iniettivo

$$Gal_K(\mathcal{L}) \to \mathrm{GL}(n, C_K) \quad \text{con} \quad \sigma \mapsto (c_{ij})$$

Nella Proposizione 3.5 si vede che $Gal_K(\mathcal{L})$ è chiuso in $\mathrm{GL}(n, C_K)$ rispetto alla topologia di Zariski (si veda Appendice A).

Proposizione 3.5. *Siano K un campo differenziale con campo delle costanti C_K, $L = K\langle y_1, \ldots, y_n \rangle$ una estensione di Picard-Vessiot di K. Allora esiste un insieme S di polinomi $F(X_{ij}), 1 \leq i, j \leq n$, con coefficienti in C_K tale che*

1. *Se σ è un K-automorfismo differenziale di L e $\sigma(y_j) = \sum_{i=1}^n c_{ij} y_i$, allora $F(c_{ij}) = 0$, $\forall F \in S$.*
2. *Data una matrice $(c_{ij}) \in GL(n, C_K)$ con $F(c_{ij}) = 0$, $\forall F \in S$, esiste un K-automorfismo differenziale σ di L tale che $\sigma(y_j) = \sum_{i=1}^n c_{ij} y_i$.*

Dimostrazione. Sia $K\{Z_1, \ldots, Z_n\}$ l'anello dei polinomi differenziali in n indeterminate su K. Si definisce un K-morfismo differenziale

$$\varphi \colon K\{Z_1, \ldots, Z_n\} \to L \quad \text{dato da} \quad Z_j \mapsto y_j$$

Il suo nucleo $\Gamma := \operatorname{Ker} \varphi$ è un ideale differenziale primo di $K\{Z_1, \ldots, Z_n\}$. Sia $L[X_{ij}], 1 \leq i, j \leq n$ l'anello dei polinomi nelle indeterminate X_{ij}, con derivata data da $X'_{ij} := 0$. Si definisce un K-morfismo differenziale

$$\psi \colon K\{Z_1, \ldots, Z_n\} \to L[X_{ij}] \quad \text{tale che} \quad Z_j \mapsto \sum_{i=1}^n X_{ij} y_i$$

Sia $\Delta := \psi(\Gamma)$ l'immagine di Γ tramite ψ. Sia $\{w_k\}$ una base del C_K-spazio vettoriale L. Si scrive ogni polinomio in Δ come combinazione lineare dei w_k con coefficienti polinomiali in $C_K[X_{ij}]$. Si definisce S come l'insieme di tutti questi coefficienti polinomiali.

1. Sia σ un K-automorfismo di L con $\sigma(y_j) = \sum_{i=1}^n c_{ij} y_i$. Si considera il diagramma

$$\begin{array}{ccc} K\{Z_1, \ldots, Z_n\} & \xrightarrow{\varphi} & L \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \sigma} \\ L[X_{ij}] & \xrightarrow{\nu} & L \end{array}$$

dove $\nu\colon L[X_{ij}] \to L$, $X_{ij} \mapsto c_{ij}$ (K-morfismo differenziale). Tale diagramma è commutativo, infatti

$$\sigma(\varphi(Z_j)) = \sigma(y_j) = \sum_{i=1}^{n} c_{ij} y_i = \nu(\sum_{i=1}^{n} X_{ij} y_i) = \nu(\psi(Z_j))$$

L'immagine di Γ tramite $\sigma \circ \varphi$ è 0 (infatti $\sigma(\varphi(\gamma)) = \sigma(0) = 0\ \forall \gamma \in \Gamma$), mentre tramite $\nu \circ \psi$ è $\Delta(= \psi(\Gamma))$ valutato in $X_{ij} = c_{ij}$. Perciò tutti i polinomi di Δ si annullano nei c_{ij}. Scrivendo tali polinomi nella base $\{w_k\}$ si conclude che tutti i polinomi di S si annullano nei c_{ij}.

2. Sia data ora una matrice $(c_{ij}) \in \mathrm{GL}(n, C_K)$ tale che $F(c_{ij}) = 0$ per ogni F in S. Si considera il morfismo differenziale

$$\begin{array}{rcl} \mu\colon K\{Z_1, \ldots, Z_n\} & \to & K\{y_1, \ldots, y_n\} \\ Z_j & \mapsto & \sum_i c_{ij} y_i \end{array}$$

con $\mu := \nu \circ \psi$ (ν e ψ definite precedentemente). Dalle ipotesi su (c_{ij}) e dalla definizione dell'insieme S si vede che $\operatorname{Ker}\varphi = \Gamma \subseteq \operatorname{Ker}\mu$, quindi si ha un K-morfismo (non nullo)

$$\begin{array}{rcl} \tilde{\sigma}\colon K\{y_1, \ldots, y_n\} & \to & K\{y_1, \ldots, y_n\} \\ y_j & \mapsto & \sum_i c_{ij} y_i \end{array}$$

Bisogna dimostrare che è biettivo. Sia per assurdo $I := \operatorname{Ker}\tilde{\sigma} \neq \{0\}$. Se u è un elemento non nullo di I allora non può essere algebrico su K poiché in tal caso il termine noto del polinomio minimo di u su K apparterrebbe ad I e quindi I sarebbe l'intero anello. Ma se u fosse trascendente si avrebbe

$$\mathrm{trdeg}[K\{y_1, \ldots, y_n\}\colon K] > \mathrm{trdeg}[K\{\tilde{\sigma}(y_1), \ldots, \tilde{\sigma}(y_n)\}\colon K]$$

D'altra parte

$$\mathrm{trdeg}[K\{y_j, \tilde{\sigma}(y_j)\}\colon K] = \mathrm{trdeg}[K\{y_j, c_{ij}\}\colon K] = \mathrm{trdeg}[K\{y_j\}\colon K]$$

e analogamente $\mathrm{trdeg}[K\{y_j, \tilde{\sigma}(y_j)\}\colon K] = \mathrm{trdeg}[K\{\tilde{\sigma}(y_j)\}\colon K]$, da cui si ha un assurdo. Dunque $\tilde{\sigma}$ è iniettivo. Visto che la matrice (c_{ij}) è invertibile, l'immagine di $\tilde{\sigma}$ contiene $y_1, \ldots, y_n$ e quindi $\tilde{\sigma}$ è suriettiva.

Perciò il morfismo $\tilde{\sigma}$ è biettivo e può essere esteso ad un K-automorfismo

$$\sigma\colon K\langle y_1, \ldots, y_n\rangle \ \to \ K\langle y_1, \ldots, y_n\rangle \qquad \square$$

Si è dunque dimostrato che $Gal(L/K)$ è un sottogruppo chiuso (nella topologia di Zariski) di $\mathrm{GL}(n, C_K)$ e dunque un gruppo algebrico lineare (si veda la definizione nell'Esempio B.3).

Osservazione 3.6. I sottogruppi chiusi propri di $\mathrm{GL}(1, C_K) \cong C_K^*$ sono finiti e quindi gruppi ciclici. Allora per una equazione differenziale lineare omogenea di ordine 1 gli unici gruppi di Galois differenziali possibili sono C_K^* oppure un gruppo ciclico finito, come visto nell'Esempio 3.3.

Osservazione 3.7. Nell'Esempio 3.2, l'elemento α è soluzione per l'equazione lineare non omogenea $Y' - a = 0$ e si è visto che $K \subseteq K\langle\alpha\rangle$ è una estensione di Picard-Vessiot per l'equazione $Y'' - \dfrac{a'}{a}Y' = 0$

Più in generale si può associare ad una equazione differenziale lineare non omogenea $\mathcal{L}(Y) = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1Y' + a_0Y = b$, l'equazione omogenea $\overline{\mathcal{L}}(Y) = 0$ con $\overline{\mathcal{L}} = (\partial - \dfrac{b'}{b})\mathcal{L}$. Si vede facilmente che se $y_1, \ldots, y_n$ è un insieme fondamentale di soluzioni per $\mathcal{L}(Y) = 0$ e y_0 è una soluzione particolare per $\mathcal{L}(Y) = b$, allora $y_0, y_1, \ldots, y_n$ è un insieme fondamentale di soluzioni per $\overline{\mathcal{L}}(Y) = 0$.

Osservazione 3.8. L'algebra universale completa delle soluzioni, data da $R = K[Y_{ij}][W^{-1}]$, costruita prima della Proposizione 2.8, è chiaramente isomorfa come K-algebra a $K \otimes_{C_K} C_K[\mathrm{GL}(n, C_K)]$, dove si denota con $C_K[\mathrm{GL}(n, C_K)] = C_K[X_{ij}, 1/\det(X_{ij})]$ l'anello delle coordinate del gruppo algebrico $\mathrm{GL}(n, C_K)$ (si veda l'Esempio B.3). L'isomorfismo è dato da

$$\begin{array}{ccc} K[Y_{ij}][W^{-1}] & \to & K \otimes_{C_K} C_K[\mathrm{GL}(n, C_K)] \\ Y_{ij} & \mapsto & X_{i+1,j} \end{array}$$

Lasciando agire $\mathrm{GL}(n, C_K)$ su sé stesso tramite traslazione a destra si ha

$$\begin{array}{ccc} \mathrm{GL}(n, C_K) \times \mathrm{GL}(n, C_K) & \to & \mathrm{GL}(n, C_K) \\ (g, h) & \mapsto & hg^{-1} \end{array}$$

e la corrispondente azione di $\mathrm{GL}(n, C_K)$ su $C_K[\mathrm{GL}(n, C_K)]$ è

$$\begin{array}{ccc} \mathrm{GL}(n, C_K) \times C_K[\mathrm{GL}(n, C_K)] & \to & C_K[\mathrm{GL}(n, C_K)] \\ (g, f) & \mapsto & \rho_g(f)\colon h \mapsto f(hg) \end{array}$$

(si veda Osservazione B.5). Prendendo f come la funzione X_{ij} che manda una matrice di $\mathrm{GL}(n, C_K)$ nella sua entrata ij-esima, si ha

$$\rho_g(X_{ij})(h) = X_{ij}(hg) = (hg)_{ij} = \sum_{k=1}^{n} h_{ik}g_{kj}$$

Tramite il K-isomorfismo di algebre tra $K \otimes_{C_K} C_K[\mathrm{GL}(n, C_K)]$ e $K[Y_{ij}][W^{-1}]$, si può far agire $\mathrm{GL}(n, C_K)$ sull'algebra universale completa delle soluzioni

$R = K[Y_{ij}][W^{-1}]$. Allora, se P è l'ideale differenziale massimale di R considerato nel Teorema 2.10 e y_{ij} denota l'immagine degli elementi Y_{ij} nel quoziente R/P, ad ogni elemento $\sigma \in Gal(L/K)$, tale che $\sigma(y_{ij}) = \sum g_{kj} y_{ik}$, si associa la matrice $(g_{ij}) \in \mathrm{GL}(n, C_K)$.

Allora il gruppo di Galois differenziale $Gal(L/K)$ può essere definito come

$$Gal(L/K) = \{\sigma \in \mathrm{GL}(n, C_K) \mid \sigma(P) = P\}$$

Quindi il gruppo di Galois differenziale è lo stabilizzatore del C_K-sottospazio vettoriale P di R.

Si definisce l'annullatore di un ideale differenziale I di R l'insieme

$$Ann(I) := \{r \in R \mid r \cdot x = 0 \quad \forall x \in I\}$$

che è chiaramente un'ideale di R. È inoltre un ideale differenziale di R. Infatti derivando l'uguaglianza $r \cdot x = 0$ (con $r \in Ann(I)$, $x \in I$) si ha $0 = r' \cdot x + r \cdot x' = r' \cdot x$, perché $x' \in I$ essendo I ideale differenziale, da cui $r \cdot x' = 0$. Dunque $r' \in Ann(I)$ $\forall r \in Ann(I)$.

Tornando all'ideale differenziale massimale P di R si ha che

$$P \subseteq Ann(Ann(P)) = \{r \in R \mid r \cdot a = 0 \quad \forall a \in Ann(P)\}$$

infatti $p \cdot a = 0$, $\forall a \in Ann(P)$ $\forall p \in P$ (per definizione di annullatore). Poiché $Ann(Ann(P))$ è ancora un ideale differenziale di R e P è ideale differenziale massimale si ha che $P = Ann(Ann(P))$. Dunque, prendendo una base $\{v_j\}_{j \in J}$ di P su C_K, si ha che

$$\begin{aligned} Gal(L/K) &= \{\sigma \in \mathrm{GL}(n, C_K) \mid \sigma(P) = P\} \\ &= \{\sigma \in \mathrm{GL}(n, C_K) \mid \sigma(v_j) \in P = Ann(Ann(P)) \ \forall j \in J\} \\ &= \{\sigma \in \mathrm{GL}(n, C_K) \mid \sigma(v_j) \cdot a = 0 \quad \forall a \in Ann(P) \ \forall j \in J\} \end{aligned}$$

da cui si trovano equazioni per $Gal(L/K)$ in $\mathrm{GL}(n, C_K)$.

Ciò fornisce una seconda dimostrazione del fatto che $Gal(L/K)$ sia un sottogruppo chiuso del gruppo algebrico $\mathrm{GL}(n, C_K)$, ovvero un gruppo algebrico lineare.

Si vedranno ora delle proprietà del gruppo di Galois differenziale analoghe a quelle della Teoria di Galois classica.

Proposizione 3.9. *(a) Se $K \subseteq L$ è una estensione di Picard-Vessiot per $\mathcal{L}(Y) = 0$ e $x \in L \setminus K$, allora esiste un K-automorfismo differenziale σ di L tale che $\sigma(x) \neq x$.*

(*b*) *Siano $K \subseteq L \subseteq M$ estensioni di campi differenziali con $K \subseteq L$ e $K \subseteq M$ estensioni di Picard-Vessiot. Allora ogni $\sigma \in Gal(L/K)$ può essere esteso ad un automorfismo differenziale di M.*

Dimostrazione. (*a*) Si può assumere che L sia il campo dei quozienti di R/P con R algebra universale completa delle soluzioni per $\mathcal{L}$ e P un ideale differenziale massimale di R. Sia $x = a/b$ con $a, b \in R/P$. Si definisca $A := (R/P)[b^{-1}] \subseteq L$ e si consideri la K-algebra $T = A \otimes_K A \subseteq L \otimes_K L$. Sia $z = x \otimes 1 - 1 \otimes x \in T$. Poiché $x \notin K$ si ha $z \neq 0$, $z' \neq 0$ (se z fosse una costante apparterrebbe a K) e z non è nilpotente ($z^n = 0$ con n minimo implicherebbe $nz^{n-1}z' = 0$ creando una contraddizione). Si localizza T a z e si passa al quoziente $T[1/z]/Q$ con Q ideale differenziale massimale di $T[1/z]$. Poiché z è invertibile, la sua immagine $\bar{z}$ in $T[1/z]/Q$ è non nulla. Si hanno le mappe $\tau_i \colon A \to T[1/z]/Q$, $i = 1, 2$, indotte da $w \mapsto w \otimes 1, w \mapsto 1 \otimes w$. La massimalità di P implica che R/P non ha ideali differenziali non banali, dunque neanche A, quindi le τ_i sono iniettive. Perciò si possono estendere entrambe le mappe a K-immersioni differenziali di L nel campo dei quozienti E di $T[1/z]/Q$. Dalla Proposizione 2.9 E è un'estensione di K senza nuove costanti quindi dalla Proposizione 2.11 si ha $\tau_1(L) = \tau_2(L)$. D'altra parte $\tau_1(x) - \tau_2(x) = \bar{z} \neq 0$, così $\tau_1(x) \neq \tau_2(x)$. Dunque $\tau := \tau_1^{-1}\tau_2$ è un K-automorfismo differenziale di L con $\tau(x) \neq x$.

(*b*) Si ha che $L \subseteq M$ è estensione di Picard-Vessiot (basta prendere la stessa equazione differenziale $\mathcal{L}$ dell'estensione $K \subseteq M$ e considerarla con coefficienti in L). Si può quindi assumere che M sia il campo dei quozienti di R_1/P dove $R_1 := L \otimes_K R$ con R algebra universale completa delle soluzioni per $\mathcal{L}$ e P ideale differenziale massimale per R_1. Allora l'estensione di $\sigma \in Gal(L/K)$ ad M è indotta da $\sigma \otimes Id_R$. □

Si presenteranno ora due lemmi necessari per la dimostrazione della Proposizione 3.12.

Lemma 3.10. *Sia L un campo differenziale con campo delle costanti C_L. Sia $A := L[Y_{ij}, 1/\det(Y_{ij})]$ (con Y_{ij}, $1 \leq i, j \leq n$, indeterminate) e si estende la derivazione di L ad A definendo $Y'_{ij} = 0$. Si consideri $B := C_L[Y_{ij}, 1/\det(Y_{ij})]$ come sottoanello di A. Allora la mappa $I \mapsto IA$ dall'insieme degli ideali di B all'insieme degli ideali differenziali di A è una biezione, la cui mappa inversa è data da $J \mapsto J \cap B$.*

Dimostrazione. Sia $\{v_s\}_{s \in S_1}$ una base di L su C_L che includa 1. Allora $\{v_s\}_{s \in S_1}$ è anche una base libera del B-modulo A. L'ideale differenziale IA consiste nelle somme finite $\sum_s \lambda_s v_s$ con $\lambda_s \in I$. Dunque $IA \cap B = I$.

Si vede ora che ogni ideale differenziale J di A è generato da $I = J \cap B$. Sia $\{u_s\}_{s \in S_2}$ una base di B su C_L. Ogni elemento $b \in J$ può essere scritto in

modo unico come una somma finita $\sum_s \mu_s u_s$ con $\mu_s \in L$. Con la lunghezza $l(b)$ di b si indicherà il numero di sottoindici s con $\mu_s \neq 0$. Per induzione sulla lunghezza di b si mostra che $b \in IA$. Se $l(b) = 0, 1$ il risultato è chiaro. Si assuma ora $l(b) > 1$. Si può supporre che $\mu_{s_1} = 1$ per qualche $s_1 \in S_2$ e che $\mu_{s_2} \in L \setminus C_L$ per qualche $s_2 \in S_2$. Allora $b' = \sum_s \mu'_s u_s$ ha una lunghezza minore di $l(b)$, dunque per induzione $b' \in IA$. Analogamente $(\mu_{s_2}^{-1} b)' \in IA$. Perciò $(\mu_{s_2}^{-1})' b = (\mu_{s_2}^{-1} b)' - \mu_{s_2}^{-1} b' \in IA$. Poiché C_L è il campo delle costanti di L, si ha che $(\mu_{s_2}^{-1})' \neq 0$ e dunque $b \in IA$. □

Lemma 3.11. *Siano K un campo differenziale con campo delle costanti C_K e $K \subseteq L$ una estensione di Picard-Vessiot con gruppo di Galois differenziale $Gal(L/K)$. Si considerino $A := L[Y_{ij}, 1/\det(Y_{ij})]$ e $B := K[Y_{ij}, 1/\det(Y_{ij})]$. Allora la mappa $I \mapsto IA$ dall'insieme degli ideali di B all'insieme degli ideali $Gal(L/K)$-invarianti di A è una biezione, la cui mappa inversa è data da $J \mapsto J \cap B$.*

Dimostrazione. La dimostrazione è simile a quella del Lemma 3.10. Bisogna verificare che ogni ideale $Gal(L/K)$-invariante J di A è generato da $I = J \cap B$. Sia $\{u_s\}_{s \in S}$ una base di B su K. Ogni elemento $b \in J$ può essere scritto in modo unico come una somma finita $\sum_s \mu_s u_s$ con $\mu_s \in L$. Con la lunghezza $l(b)$ di b si indicherà il numero di sottoindici s con $\mu_s \neq 0$. Per induzione sulla lunghezza di b si mostra che $b \in IA$. Se $l(b) = 0, 1$ il risultato è chiaro. Si assuma ora $l(b) > 1$. Si può supporre che $\mu_{s_1} = 1$ per qualche $s_1 \in S$. Se si avesse $\mu_s \in K$ per ogni s allora $b \in IA$. Altrimenti esiste qualche $s_2 \in S$ con $\mu_{s_2} \in L \setminus K$. Per ogni $\sigma \in Gal(L/K)$ la lunghezza di $\sigma(b) - b$ è minore di $l(b)$. Dunque per induzione $\sigma(b) - b \in IA$. Dalla Proposizione 3.9 (a) esiste un σ con $\sigma(\mu_{s_2}) \neq \mu_{s_2}$. In modo analogo a quanto visto per $\sigma(b) - b$, si trova che $\sigma(\mu_{s_2}^{-1} b) - \mu_{s_2}^{-1} b \in IA$. Allora si ha $(\sigma(\mu_{s_2}^{-1}) - \mu_{s_2}^{-1}) b = \sigma(\mu_{s_2}^{-1} b) - \mu_{s_2}^{-1} b - \sigma(\mu_{s_2}^{-1})(\sigma(b) - b) \in IA$. Poiché $\sigma(\mu_{s_2}^{-1}) - \mu_{s_2}^{-1} \in L^*$ si conclude che $b \in IA$. □

Proposizione 3.12. *Siano K un campo differenziale con campo delle costanti C_K e $K \subseteq L$ una estensione di Picard-Vessiot con gruppo di Galois differenziale $G = Gal(L/K)$. Sia T la K-algebra R/P considerata nel* Teorema 2.10. *Si ha un isomorfismo di $\overline{K}[G]$-moduli $\overline{K} \otimes_K T \cong \overline{K} \otimes_{C_K} C_K[G]$, dove $\overline{K}$ indica la chiusura algebrica del campo K.*

Dimostrazione. Si considera la K-algebra $R = K[Y_{ij}, 1/\det(Y_{ij})]$ con derivata definita da (come fatto prima della Proposizione 2.8)

$$Y'_{ij} := Y_{i+1,j} \quad \text{per} \quad 0 \leq i \leq n-2$$
$$Y'_{n-1,j} := -(a_{n-1} Y_{n-1,j} + \cdots + a_1 Y_{1j} + a_0 Y_{0j})$$

$\forall j = 1, \ldots, n$. Sia inoltre $L[Y_{ij}, 1/\det(Y_{ij})]$ la L-algebra con derivazione definita dalla derivazione di L e dalle formule precedenti. Si consideri ora la C_K-algebra $C_K[X_{st}, 1/\det(X_{st})]$ (con X_{st}, $1 \leq s, t \leq n$ indeterminate), che si ricorda essere l'anello delle coordinate $C_K[\mathrm{GL}(n, C_K)]$ del gruppo algebrico $\mathrm{GL}(n, C_K)$. Prendendo l'azione di traslazione a sinistra del gruppo G su $\mathrm{GL}(n, C_K)$

$$\begin{array}{ccc} G \times \mathrm{GL}(n, C_K) & \to & \mathrm{GL}(n, C_K) \\ (g, h) & \mapsto & gh \end{array}$$

si ha la corrispondente azione di G su $C_K[\mathrm{GL}(n, C_K)]$ (si veda Osservazione B.5)

$$\begin{array}{ccc} G \times C_K[\mathrm{GL}(n, C_K)] & \to & C_K[\mathrm{GL}(n, C_K)] \\ (g, f) & \mapsto & \lambda_g(f) \colon h \mapsto f(g^{-1}h) \end{array}$$

Prendendo f pari a X_{st}, l'azione di un elemento $\sigma \in G$ su X_{st} corrisponde alla moltiplicazione a sinistra per l'inversa della matrice di σ visto come elemento in $\mathrm{GL}(n, C_K)$. Si considerano $C_K[X_{st}, 1/\det(X_{st})]$ con questa azione di G e l'inclusione $C_K[X_{st}, 1/\det(X_{st})] \subseteq L[X_{st}, 1/\det(X_{st})]$. Si definisce ora la relazione tra le indeterminate Y_{ij} e X_{st} scrivendo $(Y_{ij}) = (r_{ab})(X_{st})$, dove r_{ab} sono le immagini delle Y_{ab} nel quoziente R/P dell'anello R sul suo ideale massimale P. Si osserva che l'azione di G definita sulle X_{st} è compatibile con l'azione di G su L se le Y_{ij} sono prese G-invarianti. Ora per la definizione di r_{ab} e per la definizione della derivata delle Y_{ij} si ha che $X'_{st} = 0$. Si hanno dunque gli anelli

$$K[Y_{ij}, \frac{1}{\det(Y_{ij})}] \subseteq L[Y_{ij}, \frac{1}{\det(Y_{ij})}] = L[X_{st}, \frac{1}{\det(X_{st})}] \supseteq C_K[X_{st}, \frac{1}{\det(X_{st})}]$$

ognuno dei quali è dotato di una derivazione e di una azione di G che sono compatibili con quelle degli altri anelli. Utilizzando insieme i risultati dei lemmi 3.10 e 3.11 si ottiene una biezione tra l'insieme degli ideali differenziali di $K[Y_{ij}, 1/\det(Y_{ij})]$ e l'insieme degli ideali G-invarianti di $C_K[X_{st}, 1/\det(X_{st})]$. Un ideale differenziale massimale del primo anello corrisponde ad un ideale G-invariante massimale del secondo. Quindi si ha che $Q = PL[Y_{ij}, 1/\det(Y_{ij})] \cap C_K[X_{st}, 1/\det(X_{st})]$ è un ideale G-invariante massimale dell'anello $C_K[X_{st}, 1/\det(X_{st})]$. Per la sua massimalità, Q è un ideale radicale e quindi definisce una sottovarietà W di $\mathrm{GL}(n, C_K)$ (si veda Appendice A), la quale è minimale rispetto alla G-invarianza. Allora W è una classe laterale sinistra in $\mathrm{GL}(n, C_K)$ per il gruppo $G = Gal(L/K)$ visto come sottogruppo di $\mathrm{GL}(n, C_K)$. Passando ora alla chiusura algebrica

$\overline{K}$ di K, si ha un isomorfismo tra $G_{\overline{K}}$ e $W_{\overline{K}}$, da cui si ha l'isomorfismo $\overline{K} \otimes_{C_K} C_K[G] \cong \overline{K} \otimes_{C_K} C_K[W]$ tra i loro anelli delle coordinate. D'altra parte, si hanno gli isomorfismi di anelli

$$\begin{aligned} L \otimes_K T &= L \otimes_K (K[Y_{ij}, \frac{1}{\det(Y_{ij})}]/P) \cong L[Y_{ij}, \frac{1}{\det(Y_{ij})}]/(PL[Y_{ij}, \frac{1}{\det(Y_{ij})}]) \\ &\cong L \otimes_{C_K} (C_K[X_{st}, \frac{1}{\det(X_{st})}]/Q) \end{aligned}$$

e quindi $L \otimes_K T \cong L \otimes_{C_K} C_K[W]$. Si ha dunque $\overline{L} \otimes_K T \cong \overline{L} \otimes_{C_K} C_K[W]$ per $\overline{L}$ chiusura algebrica di L. Ciò corrisponde ad un isomorfismo di varietà affini $V_{\overline{L}} \cong W_{\overline{L}}$, dove V è la sottovarietà affine di $\mathrm{GL}(n, K)$ corrispondente all'ideale P di $K[Y_{ij}, 1/\det(Y_{ij})]$. Entrambe V e W sono però definite su K, quindi per la Proposizione A.10 si ottiene $V_{\overline{K}} \cong W_{\overline{K}}$. Considerando i corrispondenti anelli delle coordinate si ottiene $\overline{K} \otimes_K T \cong \overline{K} \otimes_{C_K} C_K[W]$ e utilizzando l'isomorfismo precedente ($\overline{K} \otimes_{C_K} C_K[G] \cong \overline{K} \otimes_{C_K} C_K[W]$) si conclude che $\overline{K} \otimes_K T \cong \overline{K} \otimes_{C_K} C_K[G]$. □

Corollario 3.13. *Sia $K \subseteq L$ una estensione di Picard-Vessiot con gruppo di Galois differenziale $Gal(L/K)$. Si ha che*

$$\dim Gal(L/K) = \mathrm{trdeg}[L : K]$$

Dimostrazione. La dimensione della varietà affine $G = Gal(L/K)$ è uguale alla dimensione di Krull del suo anello delle coordinate $C_K[G]$ (si veda A.11). Si può dimostrare che la dimensione di Krull di una C_K-algebra rimane invariata facendo un prodotto tensoriale con una estensione di campi di C_K. La Proposizione 3.12 dice dunque che la dimensione di Krull di $C_K[G]$ è pari alla dimensione di Krull dell'algebra T (dove T denota, come nella Proposizione 3.12, la K-algebra R/P considerata nel Teorema 2.10) la quale, per il Lemma di normalizzazione di Noether A.12 (insieme all'Osservazione A.13), è uguale al grado di trascendenza $\mathrm{trdeg}[L : K]$ di L su K. □

Capitolo 4

Teorema Fondamentale

In questo capitolo verrà esposto il Teorema Fondamentale della Teoria di Picard-Vessiot, il quale è analogo al Teorema Fondamentale della Teoria di Galois classica.

Sia $K \subseteq L$ una estensione di Picard-Vessiot e F un campo differenziale intermedio, ovvero $K \subseteq F \subseteq L$. Si ha che $F \subseteq L$ è estensione di Picard-Vessiot (basta prendere la stessa equazione differenziale $\mathcal{L}$ dell'estensione $K \subseteq L$ e considerarla con coefficienti in F) con gruppo di Galois differenziale

$$Gal(L/F) = \{\sigma \in Gal(L/K) \mid \sigma_{|F} = Id_F\}$$

Se H è un sottogruppo di $Gal(L/K)$, si denota con L^H il sottocampo di L tenuto fisso dall'azione di H, ovvero

$$L^H = \{x \in L \mid \sigma(x) = x \quad \forall \sigma \in H\}$$

Tale L^H è stabile per la derivazione di L.

Lemma 4.1. *Se $K \subseteq L$ è una estensione di Picard-Vessiot con gruppo di Galois differenziale $G = Gal(L/K)$ allora si ha*

$$L^G = K$$

cioè il sottocampo di L tenuto fisso dall'azione di $Gal(L/K)$ è uguale a K.

Dimostrazione. L'inclusione $K \subseteq L^G$ è ovvia (per definizione di G) mentre l'inclusione $L^G \subseteq K$ è data dalla Proposizione 3.9 (a). □

Proposizione 4.2. *Sia $K \subseteq L$ una estensione di Picard-Vessiot con $Gal(L/K)$ il suo gruppo di Galois differenziale. Le corrispondenze*

$$H \mapsto L^H \qquad F \mapsto Gal(L/F)$$

definiscono delle mappe biettive tra l'insieme dei sottogruppi H di $Gal(L/K)$ chiusi per la topologia di Zariski e l'insieme dei campi differenziali intermedi F, con $K \subseteq F \subseteq L$. Tali mappe biettive invertono le inclusioni e sono una l'inversa dell'altra.

Dimostrazione. Dati due sottogruppi H_1, H_2 di $Gal(L/K)$ è chiaro che

$$H_1 \subseteq H_2 \implies L^{H_1} \supseteq L^{H_2}$$

e analogamente dati F_1, F_2 campi differenziali intermedi

$$F_1 \subseteq F_2 \implies Gal(L/F_1) \supseteq Gal(L/F_2)$$

(tali inversioni delle inclusioni seguono direttamente dalle definizioni date).

Si vede inoltre che se H è sottogruppo di $Gal(L/K)$ si ha l'uguaglianza

$$L^{Gal(L/L^H)} = L^H$$

e se F è campo differenziale intermedio si ha

$$Gal(L/L^{Gal(L/F)}) = Gal(L/F)$$

Infatti dalle definizioni si trova che $H \subseteq Gal(L/L^H)$ per ogni H sottogruppo di $Gal(L/K)$ e $F \subseteq L^{Gal(L/F)}$ per ogni F campo differenziale intermedio. Tramite l'inversione delle inclusioni si ottiene che $L^H \supseteq L^{Gal(L/L^H)}$ e $Gal(L/F) \supseteq Gal(L/L^{Gal(L/F)})$. Ora L^H è campo differenziale intermedio e $Gal(L/F)$ è sottogruppo di $Gal(L/K)$, dunque si ha anche $L^H \subseteq L^{Gal(L/L^H)}$ e $Gal(L/F) \subseteq Gal(L/L^{Gal(L/F)})$, da cui si conclude.

Bisogna ora dimostrare che $L^{Gal(L/F)} = F$ per ogni campo intermedio F di $K \subseteq L$ e $H = Gal(L/L^H)$ per ogni sottogruppo H di $Gal(L/K)$ chiuso per la topologia di Zariski.

La prima uguaglianza segue dal fatto che $F \subseteq L$ è una estensione di Picard-Vessiot (osservato in precedenza) e dal Lemma 4.1.

Per la seconda uguaglianza si è già visto che $H \subseteq Gal(L/L^H)$. Bisogna dunque mostrare che se H è un sottogruppo di $Gal(L/K)$ (non necessariamente chiuso) allora $H' := Gal(L/L^H)$ è la chiusura di H in $Gal(L/K)$ nella topologia di Zariski. Si suppone per assurdo che esista un polinomio f su $\mathrm{GL}(n, C_K)$ tale che $f_{|H} = 0$ e $f_{|H'} \neq 0$ (dove n è l'ordine dell'equazione differenziale legata all'estensione di Picard-Vessiot $K \subseteq L$). Sia $L = K\langle y_1, \ldots, y_n \rangle$ e si considerino le matrici $A = (y_j^{(i)})_{0 \leq i \leq n-1, 1 \leq j \leq n}$, $B = (u_j^{(i)})_{0 \leq i \leq n-1, 1 \leq j \leq n}$, con $u_1, \ldots, u_n$ indeterminate differenziali. Si lascia agire il gruppo di Galois a destra, ovvero dato $\sigma \in Gal(L/K)$ si definisce la matrice M_σ tale che

$(\sigma(y_1), \ldots, \sigma(y_n)) = (y_1, \ldots, y_n)M_\sigma$. Si nota che, poiché $W(y_1, \ldots, y_n) \neq 0$, la matrice A è invertibile. Si definisce dunque il polinomio

$$F(u_1, \ldots, u_n) := f(A^{-1}B) \in L\{u_1, \ldots, u_n\}$$

che soddisfa $F(\sigma(y_1), \ldots, \sigma(y_n)) = 0$ per ogni $\sigma \in H$ ma non per tutti i $\sigma \in H'$. Si assume di prendere tra tutti i polinomi F con tale proprietà quello con il minor numero di monomi non nulli. Si può inoltre assumere che almeno un coefficiente di F sia 1. Dato $\tau \in H$, sia τF il polinomio ottenuto applicando τ ai coefficienti di F. Allora per ogni $\sigma \in H$ si ha

$$(\tau F)(\sigma(y_1), \ldots, \sigma(y_n)) = \tau(F(\tau^{-1}\sigma(y_1), \ldots, \tau^{-1}\sigma(y_n))) = 0$$

Dunque $F - \tau F$ è più corto di F e si annulla in $(\sigma(y_1), \ldots, \sigma(y_n))$ per ogni $\sigma \in H$. Per l'assunzione di minimalità su F, si ha che $F - \tau F$ deve annullarsi in $(\sigma(y_1), \ldots, \sigma(y_n))$ per ogni $\sigma \in H'$. Se $F - \tau F$ non è identicamente nullo, si può trovare un elemento $a \in L$ tale che $F - a(F - \tau F)$ è più corto di F ed ha la sua stessa proprietà. Quindi $F - \tau F \equiv 0$, per ogni $\tau \in H$, ovvero i coefficienti di F sono H-invarianti quindi sono in $L^H = L^{H'}$. Ora, dato $\sigma \in H'$ si ha

$$F(\sigma(y_1), \ldots, \sigma(y_n)) = (\sigma F)(\sigma(y_1), \ldots, \sigma(y_n)) = \sigma(F(y_1, \ldots, y_n)) = 0$$

Da tale contraddizione si conclude la dimostrazione. □

Proposizione 4.3. *Sia $K \subseteq L$ una estensione di campi differenziali con gruppo di Galois differenziale $G = Gal(L/K)$.*

(a) *Se H è sottogruppo normale di G allora L^H è G-invariante (cioè $G(L^H) \subseteq L^H$).*

(b) *Se F è un campo differenziale intermedio per l'estensione $K \subseteq L$ ed è G-invariante, allora $Gal(L/F)$ è sottogruppo normale di G. Inoltre il morfismo di restrizione*

$$\begin{array}{ccc} Gal(L/K) & \to & Gal(F/K) \\ \sigma & \mapsto & \sigma_{|F} \end{array}$$

induce un isomorfismo dal quoziente $G/Gal(L/F)$ al gruppo di tutti i K-automorfismi differenziali di F che possono essere estesi a L.

Dimostrazione. (a) Per $\sigma \in G$, $a \in L^H$ si vuole vedere che $\sigma(a) \in L^H$. Se $\tau \in H$ si ha $\tau(\sigma(a)) = \sigma(a) \iff \sigma^{-1}\tau\sigma(a) = a$ e l'ultima uguaglianza è vera perché $a \in L^H$ e $\sigma^{-1}\tau\sigma \in H$ per la normalità di H.

(b) Per vedere che $Gal(L/F)$ è normale in G è necessario mostrare che per $\sigma \in G$, $\tau \in Gal(L/F)$, $\sigma^{-1}\tau\sigma$ appartiene a $Gal(L/F)$, ovvero fissa ogni elemento $a \in F$. Si ha $\sigma^{-1}\tau\sigma(a) = a \iff \tau(\sigma(a)) = \sigma(a)$ e quest'ultima uguaglianza è vera poiché $\sigma(a) \in F$, visto che F è G-invariante. Sempre per la G-invarianza di F si può definire il morfismo $\varphi\colon Gal(L/K) \to Gal(F/K)$ dato da $\sigma \mapsto \sigma_{|F}$. Il nucleo di φ è $Gal(L/F)$ e la sua immagine consiste dei K-automorfismi differenziali di F che possono essere estesi a L. □

Si introduce ora la nozione di normalità per una estensione di campi differenziali.

Definizione 4.4. Una estensione di campi differenziali $K \subseteq L$ si dice *normale* se per ogni $x \in L \setminus K$ esiste un elemento $\sigma \in Gal(L/K)$ tale che $\sigma(x) \neq x$.

Proposizione 4.5. *Sia $K \subseteq L$ una estensione di Picard-Vessiot con gruppo di Galois differenziale $G = Gal(L/K)$.*

1. *Sia H un sottogruppo chiuso di G. Se H è normale in G allora l'estensione di campi differenziali $K \subseteq F := L^H$ è normale.*

2. *Sia F è un campo differenziale intermedio con $K \subseteq F \subseteq L$. Se $K \subseteq F$ è una estensione di Picard-Vessiot allora il sottogruppo $H = Gal(L/F)$ è normale in $Gal(L/K)$. In questo caso il morfismo di restrizione*

$$\begin{array}{ccc} Gal(L/K) & \to & Gal(F/K) \\ \sigma & \mapsto & \sigma_{|F} \end{array}$$

induce un isomorfismo $Gal(L/K)/Gal(L/F) \cong Gal(F/K)$.

Dimostrazione. 1. Dalla Proposizione 3.9 (a) per $x \in F \setminus K$ esiste $\sigma \in G$ tale che $\sigma(x) \neq x$. Dalla Proposizione 4.3 (a) si ha che $F = L^H$ è G-invariante, quindi $\sigma_{|F}$ è un automorfismo di F.

2. Dal Corollario 2.12 si ha che F è G-invariante. Allora dalla Proposizione 4.3 (b), $H = Gal(L/F)$ è sottogruppo normale di $G = Gal(L/K)$.

Ricordando ancora il punto (b) della Proposizione 4.3, rimane solo da dimostrare che l'immagine del morfismo di restrizione coincide con il gruppo $Gal(F/K)$ e ciò segue dalla Proposizione 3.9 (b). □

La prossima proposizione costituisce la parte più difficile del Teorema Fondamentale, ovvero la dimostrazione che il campo intermedio F corrispondente ad un sottogruppo normale di $Gal(L/K)$ è una estensione di Picard-Vessiot. La dimostrazione proposta si basa su assunzioni valide. Per consultare la dimostrazione completa si vedano [1] e [2].

Proposizione 4.6. *Sia $K \subseteq L$ una estensione di Picard-Vessiot con gruppo di Galois differenziale $G = Gal(L/K)$. Se H è un sottogruppo normale chiuso di $Gal(L/K)$, allora l'estensione $K \subseteq L^H$ è una estensione di Picard-Vessiot.*

Dimostrazione. Si assuma di avere una K-sottoalgebra T di L finitamente generata che soddisfi le seguenti condizioni:

a) T è G-invariante e il suo campo dei quozienti $Qt(T)$ è uguale a L;

b) per ogni $t \in T$, il C_K-spazio vettoriale generato da $\{\sigma(t) \mid \sigma \in G\}$ ha dimensione finita;

c) la sottoalgebra $T^H = \{t \in T \mid \sigma(t) = t \ \forall \sigma \in H\}$ è una K-algebra finitamente generata;

d) $F := L^H$ è il campo dei quozienti di T^H, cioè $F = Qt(T^H)$.

Con tali assunzioni si dimostra che l'algebra T^H è generata su K dallo spazio delle soluzioni di una equazione differenziale lineare omogenea con coefficienti in K.

Per prima cosa si osserva che, poiché H è normale in G, T^H è G-invariante. Infatti dati $t \in T^H$ e $\tau \in G$ si vuole vedere che $\tau(t) \in T^H$. Per $\sigma \in H$ si ha $\sigma(\tau(t)) = \tau(t) \iff \tau^{-1}\sigma\tau(t) = t$ e l'ultima uguaglianza è valida in quanto la normalità di H implica che $\tau^{-1}\sigma\tau \in H$. Dunque T^H è una sottoalgebra G-invariante di T e la restrizione dell'azione di G a T^H definisce un'azione del gruppo quoziente G/H su T^H.

Sia ora $V_1 \subseteq T^H$ il sottospazio finito dimensionale su $C_K (= C_L)$ che genera T^H come K-algebra ed è G-invariante. Tale sottospazio V_1 esiste per le condizioni b) e c). Sia $z_1, \ldots, z_m$ una base di V_1, allora il Wronksiano $W(z_1, \ldots, z_m)$ non è zero. L'equazione differenziale in Z

$$\frac{W(Z, z_1, \ldots, z_m)}{W(z_1, \ldots, z_m)} = 0$$

è soddisfatta da ogni $z \in V_1$. Sviluppando il determinante al numeratore rispetto alla prima colonna si vede che ogni coefficiente dell'equazione è un quoziente di due determinanti. Inoltre, sotto l'azione di un elemento $\sigma \in G$, tali determinanti sono tutti moltiplicati dallo stesso fattore $\det \sigma_{|V_1}$. Quindi i coefficienti dell'equazione sono fissati dall'azione di G e dunque per il Lemma 4.1 appartengono a K. Allora $T^H = K\langle V_1 \rangle$ dove V_1 è lo spazio delle soluzioni di una equazione differenziale lineare omogenea con coefficienti in K. Si conclude che $F = L^H = Qt(T^H)$ è una estensione di Picard-Vessiot su K. $\square$

Unendo i risultati delle proposizioni 4.2, 4.5, 4.6 si ottiene il Teorema Fondamentale della Teoria di Picard-Vessiot:

Teorema Fondamentale 4.7. *Sia $K \subseteq L$ una estensione di Picard-Vessiot con $Gal(L/K)$ il suo gruppo di Galois differenziale.*

1. *Le corrispondenze*

$$H \mapsto L^H \qquad\qquad F \mapsto Gal(L/F)$$

definiscono delle mappe biettive tra l'insieme dei sottogruppi H di $Gal(L/K)$ chiusi per la topologia di Zariski e l'insieme dei campi differenziali intermedi F, con $K \subseteq F \subseteq L$. Tali mappe biettive invertono le inclusioni e sono una l'inversa dell'altra.

2. *Il campo differenziale intermedio F è una estensione di Picard-Vessiot di K se e solo se il sottogruppo $H = Gal(L/F)$ è normale in $Gal(L/K)$. In questo caso il morfismo di restrizione*

$$\begin{array}{ccc} Gal(L/K) & \to & Gal(F/K) \\ \sigma & \mapsto & \sigma_{|F} \end{array}$$

induce un isomorfismo $Gal(L/K)/Gal(L/F) \cong Gal(F/K)$.

Capitolo 5

Estensioni di Liouville

In questo capitolo si caratterizzeranno le equazioni differenziali risolubili per quadrature, analogamente alla caratterizzazione delle equazioni algebriche risolubili per radicali.

5.1 Estensioni di Liouville

Definizione 5.1. Una estensione di campi differenziali $K \subseteq L$ si dice *estensione di Liouville* se esiste una catena di campi differenziali intermedi

$$K = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n = L \qquad \text{tale che} \qquad F_{i+1} = F_i\langle\alpha_i\rangle \ \ \forall i$$

dove ogni α_i è un elemento primitivo su F_i (cioè $\alpha_i' \in F_i$) oppure un elemento esponenziale su F_i (cioè $\alpha_i'/\alpha_i \in F_i$).

Proposizione 5.2. *Sia L una estensione di Liouville del campo differenziale K che ha il suo stesso campo delle costanti, $C_L = C_K$. Allora il gruppo di Galois differenziale $Gal(L/K)$ di L su K è risolubile.*

Dimostrazione. Si assuma che l'estensione $K \subseteq L$ abbia una catena di campi differenziali intermedi come nella Definizione 5.1. Dagli esempi 3.2 e 3.3 si ha che $K \subseteq F_2$ è una estensione di Picard-Vessiot con gruppo di Galois differenziale abeliano. Dal Corollario 2.12 ogni K-automorfismo differenziale di L manda F_2 in sé stesso. Dalla Proposizione 4.3 (b) , $Gal(L/F_2)$ è un sottogruppo normale di $Gal(L/K)$ e $Gal(L/K)/Gal(L/F_2)$ è sottogruppo di $Gal(F_2/K)$, dunque abeliano. Iterando tale procedimento si ottiene che $Gal(L/K)$ è risolubile. □

Per considerare anche l'implicazione inversa bisognerà introdurre le estensioni di Liouville generalizzate, che ammettono anche estensioni algebriche. Per fare ciò è necessaria la prossima proposizione.

Proposizione 5.3. *Sia $K \subseteq L$ una estensione normale di campi differenziali. Si suppone che esistano elementi $u_1, \ldots, u_n \in L$ tali che per ogni automorfismo differenziale σ di L si abbiano le equazioni*

$$\sigma(u_j) = a_{1j}u_1 + \cdots + a_{j-1,j}u_{j-1} + a_{jj}u_j \qquad j = 1, \ldots, n \tag{5.1}$$

con a_{ij} costanti in L (che dipendono da σ). Allora $K\langle u_1, \ldots, u_n\rangle$ è una estensione di Liouville su K.

Dimostrazione. La prima delle equazioni (5.1) è $\sigma(u_1) = a_{11}u_1$. Derivando si ottiene $\sigma(u_1') = a_{11}u_1'$ e quindi u_1'/u_1 è invariante per ogni σ (si può assumere $u_1 \neq 0$, altrimenti basterebbe non considerarlo). Dalla normalità di $K \subseteq L$ si ha che $u_1'/u_1 \in K$. Dunque l'aggiunta di u_1 in K è l'aggiunta di un esponenziale. Si divida ora ciascuna delle restanti $n-1$ equazioni (5.1) per l'equazione $\sigma(u_1) = a_{11}u_1$ e si derivi. Si ottiene

$$\sigma\left(\left(\frac{u_j}{u_1}\right)'\right) = \frac{a_{2j}}{a_{11}}\left(\frac{u_2}{u_1}\right)' + \cdots + \frac{a_{j-1,j}}{a_{11}}\left(\frac{u_{j-1}}{u_1}\right)' + \frac{a_{jj}}{a_{11}}\left(\frac{u_j}{u_1}\right)'$$

Si ha un insieme di equazioni della stessa forma delle (5.1) negli elementi $(u_j/u_1)'$ con $j = 2, \ldots, n$. Per induzione su n, l'aggiunta di $(u_j/u_1)'$ in K fornisce una estensione di Liouville. Allora l'aggiunta degli u_j/u_1 è l'aggiunta di integrali. □

5.2 Estensioni di Liouville generalizzate

Definizione 5.4. Una estensione di campi differenziali $K \subseteq L$ si dice *estensione di Liouville generalizzata* se esiste una catena di campi differenziali intermedi

$$K = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n = L \qquad \text{tale che} \qquad F_{i+1} = F_i\langle\alpha_i\rangle \ \ \forall i$$

dove ogni α_i è un elemento primitivo su F_i (cioè $\alpha_i' \in F_i$), un elemento esponenziale su F_i (cioè $\alpha_i'/\alpha_i \in F_i$) oppure un elemento algebrico su F_i.

Ogni elemento α di una estensione di Liouville generalizzata $K \subseteq L$ è detto *esprimibile per quadrature (generalizzate)* su K.

Teorema 5.5. *Sia K un campo differenziale con campo delle costanti C_K algebricamente chiuso. Sia L una estensione di Picard-Vessiot di K. Si suppone che la componente identità G^0 di $G = Gal(L/K)$ sia risolubile. Allora L può essere ottenuto da K tramite una estensione normale finita, seguita da una estensione di Liouville.*

Dimostrazione. Sia $F = L^{G^0}$. Dalla Proposizione B.7 si ha che G^0 è sottogruppo normale di G di indice finito. Allora $K \subseteq F$ è una estensione normale finita e $Gal(L/F) \cong G^0$. Allora per il Teorema di Lie-Kolchin B.10 si può applicare la Proposizione 5.3, da cui si ottiene che $F \subseteq L$ è una estensione di Liouville. □

Per dimostrare l'implicazione inversa è necessario il seguente lemma.

Lemma 5.6. *Sia K un campo differenziale con campo delle costanti C_K algebricamente chiuso. Sia L una estensione di Picard-Vessiot di K. Siano $L_1 = L\langle z\rangle$ un'estensione di L che non abbia nuove costanti e $K_1 = K\langle z\rangle$. Allora $K_1 \subseteq L_1$ è una estensione di Picard-Vessiot e il suo gruppo di Galois differenziale è isomorfo a $Gal(L/L \cap K_1)$.*

Dimostrazione. È chiaro che $K_1 \subseteq L_1$ è una estensione di Picard-Vessiot poiché entrambi i campi hanno lo stesso campo delle costanti e l'estensione è generata dalle soluzioni dell'equazione differenziale associata all'estensione di Picard-Vessiot $K \subseteq L$. Dal Corollario 2.12, ogni K-automorfismo differenziale di L_1 manda L in sé stesso. Dunque la restrizione a L definisce un morfismo $\varphi\colon Gal(L_1/K_1) \to Gal(L/K)$. Un automorfismo di L_1 in $\operatorname{Ker}\varphi$ fissa sia K_1 che L, quindi è l'identità. Perciò φ è iniettivo e $Gal(L_1/K_1)$ è isomorfo ad un sottogruppo chiuso di $Gal(L/K)$. Il campo differenziale intermedio corrispondente nell'estensione $K \subseteq L$ è $L \cap K_1$ e dal Teorema Fondamentale 4.7 si ha che $Gal(L_1/K_1) \cong Gal(L/L \cap K_1)$. □

Teorema 5.7. *Sia K un campo differenziale con campo delle costanti C_K algebricamente chiuso. Sia L una estensione di Picard-Vessiot di K. Si suppone che L possa essere immerso in un campo differenziale M che sia una estensione di Liouville generalizzata di K che non contiene nuove costanti. Allora la componente identità G^0 di $G = Gal(L/K)$ è risolubile (da cui per il Teorema 5.5 si ha che L può essere ottenuto da K tramite una estensione normale finita seguita da una estensione di Liouville).*

Dimostrazione. Si procede per induzione sul numero di elementi nella catena da K a M. Sia $K\langle z\rangle$ il primo elemento. Allora per induzione, il gruppo di Galois differenziale di $L\langle z\rangle$ su $K\langle z\rangle$ ha la componente identità risolubile e per il Lemma 5.6 è isomorfo al sottogruppo H di G corrispondente a $L \cap K\langle z\rangle$. Si suppone che z sia algebrico su K. Allora H ha indice finito in G e in tal caso, per la Proposizione B.7, $G^0 = H^0$, dunque è risolubile. Se invece z fosse un integrale o un esponenziale, dagli esempi 3.2 e 3.3, $K\langle z\rangle$ sarebbe una estensione di Picard-Vessiot di K con gruppo di Galois differenziale abeliano. Allora tutti i campi differenziali tra K e $K\langle z\rangle$ sarebbero normali su K. In particolare si avrebbe $L \cap K\langle z\rangle$ normale su K con gruppo di Galois

differenziale abeliano. Dunque H è normale in G con G/H abeliano, perciò dalla Proposizione B.9 la componente identità G^0 di G è risolubile. □

Dai Teoremi 5.5 e 5.7 si ha una caratterizzazione per le equazioni differenziali risolubili per quadrature generalizzate.

Teorema 5.8. *Siano K un campo differenziale con campo delle costanti C_K algebricamente chiuso e $K \subseteq L$ una estensione di Picard-Vessiot per l'equazione differenziale $\mathcal{L}(Y) = 0$.*

Allora $\mathcal{L}(Y) = 0$ è risolubile per quadrature generalizzate (cioè le sue soluzioni sono esprimibili per quadrature generalizzate ovvero L è contenuta in una estensione di Liouville generalizzata di K che non contiene nuove costanti) se e solo se la componente identità G^0 del gruppo di Galois differenziale $G = Gal(L/K)$ è risolubile.

Esempio 5.9. Sia $\mathbb{C}$ il campo dei numeri complessi e si consideri il campo differenziale $\mathbb{C}(X)$ delle funzioni razionali complesse con derivazione banale ∂ su $\mathbb{C}$ estesa a $\mathbb{C}(X)$ ponendo $\partial(X) := 1$.

Si consideri l'equazione di Airy

$$\mathcal{L}_A(Y) = Y'' - XY = 0$$

Sia $\mathbb{C}(X) \subseteq \mathbb{C}(X)\langle\alpha, \beta\rangle$ una estensione di Picard-Vessiot per $\mathcal{L}_A(Y) = 0$, dove α, β sono un insieme fondamentale di soluzioni per l'equazione di Airy. Si dimostra che il gruppo di Galois differenziale di tale equazione è (si veda Esempio 5.8 in [5])

$$Gal_{\mathbb{C}(X)}(\mathcal{L}_A) = \mathrm{SL}(2, \mathbb{C})$$

Tale gruppo è connesso (si veda Corollario 8.2 in [2]), quindi la componente identità corrisponde a tutto il gruppo. Inoltre $\mathrm{SL}(2, \mathbb{C})$ non è risolubile (essendo un gruppo perfetto). Dunque, per il Teorema 5.8, le soluzioni α, β dell'equazione di Airy $\mathcal{L}_A(Y) = 0$ non sono esprimibili per quadrature generalizzate sul campo $\mathbb{C}(X)$ delle funzioni razionali complesse.

Appendice A

Appendice varietà affini

In questa appendice verranno introdotte le varietà affini e tutti i risultati ausiliari che vengono utilizzati nella Teoria di Galois Differenziale. Le dimostrazioni di tali risultati possono essere trovate in [1], [2], [6], [8] e [9].

D'ora in poi si indicherà con C un campo algebricamente chiuso di caratteristica 0.

Definizione A.1. Si chiamerà *spazio affine n-dimensionale* l'insieme definito da $C^n = \underbrace{C \times \cdots \times C}_{n \text{ volte}}$ e verrà denotato con $\mathbb{A}^n_C$ oppure $\mathbb{A}^n$ (se il campo di base è chiaro dal contesto).

Si definisce una *varietà (algebrica) affine* come l'insieme degli zeri comuni in $\mathbb{A}^n$ di una collezione di polinomi in $C[X_1, \ldots, X_n]$.

Ad ogni ideale I di $C[X_1, \ldots, X_n]$ si associa l'insieme $\mathcal{V}(I)$ dei suoi zeri comuni in $\mathbb{A}^n$

$$\mathcal{V}(I) := \{x \in \mathbb{A}^n \mid f(x) = 0 \quad \forall f \in I\}$$

Tale insieme è detto *insieme algebrico associato ad I* ed in particolare è una varietà affine (per la definizione data).

Ad ogni sottoinsieme $S \subseteq \mathbb{A}^n$ si può associare la famiglia $\mathcal{I}(S)$ di tutti i polinomi che si annullano su S

$$\mathcal{I}(S) := \{f \in C[X_1, \ldots, X_n] \mid f(x) = 0 \quad \forall x \in S\}$$

Tale insieme è detto *ideale associato a S* (si vede facilmente che è un ideale). Si hanno le inclusioni (che non sono uguaglianze in generale)

$$S \subseteq \mathcal{V}(\mathcal{I}(S)) \qquad I \subseteq \mathcal{I}(\mathcal{V}(I))$$

Inoltre è facile vedere che le corrispondenze $\mathcal{V}$ e $\mathcal{I}$ invertono le inclusioni, ovvero dati I_1, I_2 ideali di $C[X_1, \ldots, X_n]$ e S_1, S_2 sottoinsiemi di $\mathbb{A}^n$ si ha

$$I_1 \subseteq I_2 \implies \mathcal{V}(I_1) \supseteq \mathcal{V}(I_2) \qquad S_1 \subseteq S_2 \implies \mathcal{I}(S_1) \supseteq \mathcal{I}(S_2)$$

Si definisce il radicale $\sqrt{I}$ di un ideale I

$$\sqrt{I} := \{f \in C[X_1, \ldots, X_n] \mid f^m \in I \text{ per qualche } m \geq 1\}$$

Si ha che $I \subseteq \sqrt{I}$ e anche $\sqrt{I} \subset \mathcal{I}(\mathcal{V}(I))$. Un ideale I è detto radicale se $I = \sqrt{I}$. Ad esempio gli ideali primi sono radicali e anche gli ideali della forma $\mathcal{I}(S)$, $S \subseteq \mathbb{A}^n$ sono ideali radicali di $C[X_1, \ldots, X_n]$.

Teorema A.2 (Nullstellensatz di Hilbert)**.** *Se I è un ideale di $C[X_1, \ldots, X_n]$ allora*

$$\sqrt{I} = \mathcal{I}(\mathcal{V}(I))$$

Proposizione A.3. *La mappa $\mathcal{V}$ ha le seguenti proprietà:*

1. $\mathcal{V}(0) = \mathbb{A}^n \quad , \quad \mathcal{V}(C[X_1, \ldots, X_n]) = \emptyset$
2. *Se I e J sono due ideali di $C[X_1, \ldots, X_n]$ allora*

$$\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$$

3. *Se I_α è una famiglia arbitraria di ideali di $C[X_1, \ldots, X_n]$ allora*

$$\bigcap_\alpha \mathcal{V}(I_\alpha) = \mathcal{V}\Big(\sum_\alpha I_\alpha\Big)$$

Si vede dunque che le varietà affini in $\mathbb{A}^n$ soddisfano gli assiomi per gli insiemi chiusi di una topologia. Questa topologia è detta *topologia di Zariski*.

Un *insieme aperto principale* di $\mathbb{A}^n$ è l'insieme dei punti in cui un polinomio non si annulla. Tali insiemi costituiscono una base per la topologia di Zariski.

Si ricorda che uno spazio topologico (non vuoto) si dice *riducibile* se può essere scritto come unione di due sottoinsiemi chiusi propri non vuoti. È dunque *irriducibile* se non è riducibile, equivalentemente se tutti i suoi sottoinsiemi aperti propri non vuoti sono densi.

Un sottoinsieme di uno spazio topologico è riducibile (rispettivamente irriducibile) se lo è come spazio topologico con la topologia indotta.

Proposizione A.4. *Un insieme chiuso V in $\mathbb{A}^n$ è irriducibile se e solo se il suo ideale associato $\mathcal{I}(V)$ è primo. In particolare $\mathbb{A}^n$ è irriducibile.*

Definizione A.5. Se V è chiuso in $\mathbb{A}^n$, ogni polinomio $f \in C[X_1, \ldots, X_n]$ definisce una funzione a valori in C su V. Polinomi diversi possono però

definire la stessa funzione. Si ha dunque una corrispondenza biettiva tra funzioni polinomiali su V e le classi resto dell'anello

$$C[V] := C[X_1, \ldots, X_n]/\mathcal{I}(\mathcal{V})$$

Questo anello è detto *anello delle coordinate* di V. È finitamente generato come C-algebra ed è ridotto (cioè non ha elementi nilpotenti non nulli) perché $\mathcal{I}(V)$ è ideale radicale.

Osservazione A.6. Se $V \subseteq \mathbb{A}^n$ è una varietà affine, si può considerare in V la topologia di Zariski indotta dalla topologia di $\mathbb{A}^n$, i cui insiemi chiusi sono definiti da $\mathcal{V}(I) = \{x \in V \mid f(x) = 0 \; \forall f \in I\}$ con I ideale di $C[V]$.

Dunque data una varietà affine V essa è detta *varietà affine irriducibile* se (e solo se) $\mathcal{I}(V)$ è ideale primo (segue dalla Proposizione A.4).

Se V è irriducibile (equivalentemente se $\mathcal{I}(V)$ è ideale primo), $C[V]$ è un dominio d'integrità. Si può dunque considerare il suo campo dei quozienti $C(V)$ che è chiamato *campo delle funzioni* di V ed i suoi elementi sono detti *funzioni razionali* di V.

Dal Nullstellensatz di Hilbert (Teorema A.2) e dalla Proposizione A.4, le mappe $\mathcal{V}$ e $\mathcal{I}$ stabiliscono le seguenti corrispondenze biettive

$$\{\text{ideali radicali di } C[X_1, \ldots, X_n]\} \leftrightarrow \{\text{insiemi chiusi di } \mathbb{A}^n\}$$
$$\{\text{ideali primi di } C[X_1, \ldots, X_n]\} \leftrightarrow \{\text{insiemi chiusi irriducibili di } \mathbb{A}^n\}$$

Dall'Osservazione A.6, data una varietà V si hanno anche le corrispondenze

$$\{\text{ideali radicali di } C[V]\} \leftrightarrow \{\text{insiemi chiusi di } V\}$$
$$\{\text{ideali primi di } C[V]\} \leftrightarrow \{\text{insiemi chiusi irriducibili di } V\}$$

Osservazione A.7. Dati due sottoinsiemi chiusi $V \subseteq \mathbb{A}^n$ e $W \subseteq \mathbb{A}^m$ si ha che $V \times W \subseteq \mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$ è chiaramente un insieme chiuso, dunque il prodotto cartesiano di due varietà affini è una varietà affine. Si ha un isomorfismo $C[V \times W] \cong C[V] \otimes C[W]$.

Morfismi tra varietà affini

Definizione A.8. Siano $V \subseteq \mathbb{A}^n$, $W \subseteq \mathbb{A}^m$ varietà affini arbitrarie. Un *morfismo tra varietà affini* è una mappa

$$\varphi \colon V \to W \quad \text{definita da} \quad x = (x_1, \ldots, x_n) \mapsto (\varphi_1(x), \ldots, \varphi_m(x))$$

con $\varphi_i \in C[V]$.

Un morfismo $\varphi\colon V \to W$ è continuo per le topologie di Zariski coinvolte: infatti se $Z \subseteq W$ è l'insieme degli zeri di funzioni polinomiali f_i su W, allora $\varphi^{-1}(Z)$ è l'insieme degli zeri delle funzioni $f_i \circ \varphi$ su V.

Ad ogni morfismo $\varphi\colon V \to W$ è associato un morfismo di algebre

$$\varphi^*\colon C[W] \to C[V] \quad \text{definito da} \quad \varphi^*(f) = f \circ \varphi$$

Il morfismo $\varphi\colon V \to W$ è un isomorfismo se esiste un morfismo $\psi\colon W \to V$ tale che $\psi \circ \varphi = Id_V$ e $\varphi \circ \psi = Id_W$. In tal caso si dice che le due varietà affini sono isomorfe e si indica con $V \cong W$.

Estensione degli scalari per una varietà

Definizione A.9. Siano $V \subseteq \mathbb{A}^n_C$ una varietà affine e L un campo algebricamente chiuso che contiene C. Si indica con $V_L \subseteq \mathbb{A}^n_L$ la varietà affine definita da $V_L := \mathcal{V}(I_L)$ con $I_L = \mathcal{I}(V)L[X_1, \ldots, X_n]$. Si dice che V_L è la varietà ottenuta da V per *estensione degli scalari* a L. L'anello delle coordinate di V_L è $L[V] = L \otimes C[V]$.

È chiaro che se V, W sono varietà affini su C si ha $V \cong W \implies V_L \cong W_L$. L'implicazione inversa nel caso di campi algebricamente chiusi è data dalla seguente proposizione.

Proposizione A.10. *Siano K, L campi algebricamente chiusi con $K \subseteq L$. Siano V, W varietà affini definite su K. Siano V_L, W_L le varietà ottenute da V, W per estensione degli scalari a L. Se V_L e W_L sono isomorfe allora V e W sono isomorfe.*

Dimensione varietà affini

Dato uno spazio topologico noetheriano X si definisce la *dimensione di X* come l'estremo superiore di tutti gli interi n tale che esista una catena $Z_0 \subseteq Z_1 \subseteq \cdots \subseteq Z_n$ di distinti sottoinsiemi chiusi irriducibili di X.

Dato un anello A, si definisce la *dimensione di Krull* di A come l'estremo superiore di tutti gli interi n tale che esista una catena $P_0 \subseteq P_1 \subseteq \cdots \subseteq P_n$ di distinti ideali primi di A.

Definizione A.11. La *dimensione di una varietà affine* è la sua dimensione come spazio topologico. È chiaro che la dimensione di una varietà affine è il massimo delle dimensioni delle sue componenti irriducibili.

Se $V \subseteq \mathbb{A}^n$ è una varietà affine, dalla Proposizione A.4, i sottoinsiemi chiusi irriducibili di V corrispondono ad ideali primi di $C[X_1, \ldots, X_n]$ contenenti $\mathcal{I}(V)$ e questi sono in corrispondenza con gli ideali primi di $C[V]$. Dunque la dimensione di V è uguale alla dimensione di Krull del suo anello delle coordinate $C[V]$. Ad esempio si ha che $\dim C[X_1, \ldots . X_n] = n$ (si veda Teorema 22 in [6]), da cui $\dim \mathbb{A}^n = n$.

Lemma di normalizzazione d Noether A.12. *Sia C un campo arbitrario, $R = C[x_1, \ldots, x_n]$ una C-algebra finitamente generata. Allora esistono degli elementi $y_1, \ldots, y_d \in R$ ($d \leq n$) algebricamente indipendenti su C (cioè che non soddisfano nessuna equazione polinomiale non banale a coefficienti in C) tali che R è intero su $C[y_1, \ldots, y_d]$ (ovvero ogni elemento di R è radice di un polinomio monico a coefficienti in $C[y_1, \ldots, y_d]$).*

Osservazione A.13. Se R è dominio d'integrità e F è il suo campo dei quozienti, si ha che gli elementi $y_1, \ldots, y_d$ formano una base trascendentale di F su C, da cui $\mathrm{trdeg}[F : C] = d$.

Si può dimostrare che se un anello noetheriano R è intero su un sottoanello noetheriano S allora $\dim S = \dim R$ (si veda Teorema 20 in [6]). Nel caso del Lemma di normalizzazione di Noether, utilizzando la stessa notazione, si ha che $\dim R = d$. Dunque la dimensione di un dominio d'integrità R finitamente generato su C è pari al grado di trascendenza del suo campo dei quozienti su C (Osservazione A.13).

Perciò se V è varietà affine irriducibile, la dimensione di V è pari alla dimensione di Krull del suo anello delle coordinate $C[V]$ che è uguale al grado di trascendenza $\mathrm{trdeg}[C(V) : C]$ del campo delle funzioni $C(V)$ di V su C.

Insiemi costruibili

Definizione A.14. Un sottoinsieme di uno spazio topologico X è detto *localmente chiuso* se è l'intersezione di un insieme aperto e un insieme chiuso. Si chiama *insieme costruibile* una unione finita di insiemi localmente chiusi.

Teorema di Chevalley A.15. *Sia $\varphi \colon V \to W$ un morfismo di varietà. Allora φ manda insiemi costruibili in insiemi costruibili. In particolare $\varphi(V)$ è costruibile in W.*

Appendice B

Appendice gruppi algebrici

In questa appendice verrà introdotta la nozione di gruppo algebrico e verranno esposti alcuni importanti concetti ad esso correlati. I risultati delle proposizioni e dei teoremi esposti possono essere trovati in [1], [2] e [9].

In questa appendice si denoterà con C un campo algebricamente chiuso di caratteristica 0.

Definizione B.1. Un *gruppo algebrico (affine)* su C è una varietà (algebrica) affine G definita su C dotata di una struttura di gruppo e tale che le due mappe

$$\begin{aligned} \mu\colon G \times G \to G \quad &\text{con} \quad \mu(x,y) = xy \\ \iota\colon G \to G \quad &\text{con} \quad \iota(x) = x^{-1} \end{aligned}$$

sono morfismi di varietà.

Esempio B.2. Il *gruppo additivo* $\mathbb{G}_a$ è la retta affine $\mathbb{A}^1$ con legge di gruppo data da $\mu(x,y) = x + y$, con $\iota(x) = -x$ ed elemento neutro $e = 0$.
Il *gruppo moltiplicativo* $\mathbb{G}_m$ è l'insieme aperto principale $C^* \subseteq \mathbb{A}^1$ con legge di gruppo data da $\mu(x,y) = xy$, con $\iota(x) = x^{-1}$ ed elemento neutro $e = 1$.

Esempio B.3. Il *gruppo generale lineare* $\mathrm{GL}(n, C)$ è il gruppo di tutte le matrici $n \times n$ invertibili con entrate in C e con legge di gruppo data dalla moltiplicazione tra matrici. L'insieme $M(n, C)$ di tutte le matrici $n \times n$ su C può essere identificato con lo spazio affine $\mathbb{A}^{n^2}$ di dimensione n^2 e $\mathrm{GL}(n, C)$ con l'insieme aperto principale definito dal non annullamento del determinante. Per vedere $\mathrm{GL}(n, C)$ come varietà affine basta pensare all'inclusione in $\mathbb{A}^{n^2+1}$

$$\begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \dots & c_{nn} \end{pmatrix} \mapsto (c_{11}, \dots, c_{1n}, \dots, c_{n1}, \dots, c_{nn}, 1/\det(c_{ij})) \in \mathbb{A}^{n^2+1}$$

L'immagine di tale inclusione è un chiuso di $\mathbb{A}^{n^2+1}$ ed è l'insieme degli zeri di $\det(X_{ij})Y = 1$, dove Y è la (n^2+1)-esima coordinata. Pensandolo come varietà affine, $\mathrm{GL}(n, C)$ ha anello delle coordinate dato da $C[X_{ij}, 1/\det(X_{ij})]$ con $1 \leq i, j \leq n$ (n^2 indeterminate). Dalla moltiplicazione di matrici e dall'inversione è chiaro che $\mathrm{GL}(n, C)$ è un gruppo algebrico. Si noti inoltre che $\mathrm{GL}(1, C) = \mathbb{G}_m$.

Un *gruppo algebrico lineare* è un sottogruppo chiuso di $\mathrm{GL}(n, C)$. Si vede facilmente che un sottogruppo chiuso di un gruppo algebrico è ancora un gruppo algebrico.

Esempi di gruppi algebrici lineari sono:

1. $\mathrm{SL}(n, C) := \{A \in \mathrm{GL}(n, C) \mid \det(A) = 1\}$ (*gruppo speciale lineare*);
2. $\mathrm{Tr}(n, C) := \{(a_{ij}) \in \mathrm{GL}(n, C) \mid a_{ij} = 0,\ i > j\}$ (*gruppo triangolare superiore*);
3. $\mathrm{U}(n, C) := \{(a_{ij}) \in \mathrm{GL}(n, C) \mid a_{ii} = 1, a_{ij} = 0,\ i > j\}$ (*gruppo triangolare superiore unipotente*);
4. $\mathrm{D}(n, C) := \{(a_{ij}) \in \mathrm{GL}(n, C) \mid a_{ij} = 0,\ i \neq j\}$ (*gruppo diagonale*).

Azione di gruppi algebrici

Definizione B.4. Siano G un gruppo algebrico e V una varietà affine. Si dice che V è una *G-varietà* se G agisce su V, ovvero se si ha un morfismo di varietà

$$\begin{array}{ccc} G \times V & \to & V \\ (g, v) & \mapsto & g \cdot v \end{array}$$

che soddisfa

1. $e \cdot v = v$ per ogni $v \in V$
2. $g_1 \cdot (g_2 \cdot v) = (g_1 g_2) \cdot v$ per ogni $g_1, g_2 \in G$, $v \in V$

L'azione di G su V induce un'azione di G sull'anello delle coordinate $C[V]$ di V definito da

$$\begin{array}{ccc} G \times C[V] & \to & C[V] \\ (g, f) & \mapsto & g \cdot f \colon v \mapsto f(g^{-1} \cdot v) \end{array}$$

Osservazione B.5. In particolare si possono considerare due azioni differenti di G sul suo anello delle coordinate $C[G]$ associate alle azioni di traslazione sinistra e destra di G su sé stesso.
All'azione di traslazione sinistra di G su sé stesso definita da

$$\begin{array}{ccc} G \times G & \to & G \\ (g,h) & \mapsto & gh \end{array}$$

corrisponde l'azione

$$\begin{array}{ccc} G \times C[G] & \to & C[G] \\ (g,f) & \mapsto & \lambda_g(f)\colon h \mapsto f(g^{-1}h) \end{array}$$

Analogamente, all'azione di traslazione destra di G su sé stesso definita da

$$\begin{array}{ccc} G \times G & \to & G \\ (g,h) & \mapsto & hg^{-1} \end{array}$$

corrisponde l'azione

$$\begin{array}{ccc} G \times C[G] & \to & C[G] \\ (g,f) & \mapsto & \rho_g(f)\colon h \mapsto f(hg) \end{array}$$

Componente identità di un gruppo algebrico

Sia G un gruppo algebrico. Si vede che esiste una sola componente irriducibile di G che contiene l'elemento neutro e.
Infatti siano $X_1, \ldots, X_m$ le componenti irriducibili di G che contengono e. L'immagine della varietà irriducibile $X_1 \times \cdots \times X_m$ attraverso il morfismo prodotto è un sottoinsieme irriducibile $X_1 \cdots X_m$ di G che contiene ancora e. Quindi $X_1 \cdots X_m$ è contenuto in qualche X_i ma d'altra parte ogni componente $X_1, \ldots, X_m$ è chiaramente contenuta in $X_1 \cdots X_m$. Dunque si deve avere $m = 1$. Da ciò si definisce la componente identità di un gruppo algebrico.

Definizione B.6. Dato un gruppo algebrico G si definisce la *componente identità* G^0 di G come l'unica componente irriducibile di G che contiene l'elemento neutro e.
Un gruppo algebrico G si dice *connesso* se $G = G^0$.

Proposizione B.7. *Sia G un gruppo algebrico.*

1. *G^0 è un sottogruppo normale di indice finito in G.*
2. *Ogni sottogruppo chiuso di indice finito in G contiene G^0.*

Gruppi algebrici risolubili

Definizione B.8. Un gruppo algebrico G si dice *risolubile* se esiste una catena di sottogruppi chiusi

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

tale che $G_{i-1} \trianglelefteq G_i$ e G_i/G_{i-1} è abeliano, per $i = 1, \ldots, n$.

Proposizione B.9. *Siano G un gruppo algebrico e H un sottogruppo chiuso di G. Si suppone che H sia normale in G e che G/H sia abeliano. Si suppone inoltre che la componente identità H^0 di H sia risolubile. Allora la componente identità G^0 di G è risolubile.*

Teorema di Lie-Kolchin B.10. *Sia G un sottogruppo connesso risolubile di $GL(n, C)$, $n \geq 1$. Allora G è triangolarizzabile, ovvero esiste una matrice $M \in GL(n, C)$ tale che $MGM^{-1} \subseteq Tr(n, C)$.*

Bibliografia

[1] Teresa Crespo e Zbigniew Hajto. *Algebraic groups and differential Galois theory*. Vol. 122. American Mathematical Soc., 2011.

[2] Teresa Crespo, Zbigniew Hajto e Juan José Morales Ruiz. *Introduction to differential Galois theory*. Wydawnictwo PK Cracow, 2007.

[3] Jerald J. Kovacic. «Picard-Vessiot theory, algebraic groups and group schemes». In: *Department of Mathematics, the City College of the City University of New York* (2005).

[4] Andy Magid. «Differential galois theory». In: *Notices of the AMS* 46.9 (1999), pp. 1041–1049.

[5] Pau Martìnez Marìn. *Introduction to Differential Galois Theory*. 2021.

[6] Hideyuki Matsumura. *Commutative algebra*. Vol. 120. WA Benjamin New York, 1970.

[7] J. Murphy. *Differential Galois Theory*. 2010.

[8] Marius van der Put e Michael F. Singer. «Differential Galois Theory». In: *preprint* (2001).

[9] Tam Szamuely et al. *Lectures on linear algebraic groups*. 2006.