

Dipartimento di Matematica Corso di Laurea Triennale in Matematica

Il gruppo affine di Cremona

Tesi di Laurea Triennale

Candidato

Relatore

Marco D'Addezio

Prof. Angelo Vistoli

Indice

1	Automorfismi polinomiali		5
	1.1	Algebre e automorfismi	5
	1.2	Automorfismi moderati	6
2	Derivazioni		9
	2.1	Prime definizioni	9
	2.2	Anello delle costanti	10
	2.3	Derivazioni localmente nilpotenti e triangolari	12
	2.4	Funzione grado indotta da una derivazione	13
	2.5	Algebre graduate e derivazioni omogenee	15
	2.6	Azione di coniugio	17
	2.7	Automorfismi esponenziali	18
3	Il problema dei generatori moderati		20
	3.1	Prodotto amalgamato	21
	3.2	Teorema di struttura	22
	3.3	Teoremi di Rentschler e di Jung, van der Kulk	25
	3.4	Controesempio di Nagata, Shestakov, Umirbaev	29
4	Problema di linearizzazione		31
	4.1	Varietà e gruppi algebrici affini	31
	4.2	Rappresentazioni	35
	4.3	Rappresentazioni razionali e regolari	36
	1.1	Problema di linearizzazione	38

Introduzione

Nell'elaborato intendiamo presentare alcuni risultati di geometria algebrica affine riguardanti gli automorfismi polinomiali dello spazio affine. In particolare cercheremo un buon insieme di generatori del gruppo di questi automorfismi.

Prendiamo un campo \mathbb{K} e una n-upla di polinomi in n variabili a coefficienti in \mathbb{K} , questa induce un endomorfismo di \mathbb{K} -algebre dell'anello dei polinomi. Focalizziamo la nostra attenzione sugli endomorfismi invertibili, questo è un gruppo ed è chiamato gruppo affine di Cremona.

Alcuni esempi di automorfismi dell'algebra dei polinomi ci vengono forniti dall'algebra lineare, ovvero gli automorfismi lineari e più in generale tutte le affinità. Automorfismi di grado più alto si possono ottenere ad esempio prendendo $f \in \mathbb{K}[x_1, \dots, \widehat{x}_i, \dots, x_n]$ e definendo l'endomorfismo che manda ogni generatore in se stesso, ad eccezione di x_i che va in x_i+f . Questo genere di endomorfismi sono invertibili e li chiameremo automorfismi elementari.

Proviamo a considerare una classe più ampia di automorfismi, quelli ottenuti componendo affinità e automorfismi elementari, chiamati automorfismi moderati. Capire se tutti gli automorfismi sono moderati diventa un problema molto più complesso ed è noto come il problema dei generatori moderati.

Nel 1942 Heinrich W. E. Jung provò che per ogni campo \mathbb{K} di caratteristica zero, in dimensione due, tutti gli automorfismi sono moderati. Nel 1953 Wouter van der Kulk generalizzò tale risultato a campi di caratteristica positiva e dimostrò che il gruppo affine di Cremona in dimensione due è isomorfo al prodotto amalgamato sull'intersezione del gruppo delle affinità e del gruppo delle $mappe\ triangolari$.

Nel 1968 Rudolf Rentschler classificò le derivazioni localmente nilpotenti dell'anello dei polinomi in due variabili in caratteristica zero. Nel suo articolo Rentschler mostrò che il risultato ottenuto aveva come conseguenza il teorema di Jung [1].

Nel corso dell'elaborato introdurremo le derivazioni localmente nilpotenti e faremo agire gli automorfismi moderati di $\mathbb{K}[x,y]$ sullo spazio vettoriale di queste derivazioni. Grazie a concetti come quello di ω -graduazione, riusciremo a trovare in ogni orbita una derivazione triangolare di un certo tipo (Teorema di Rentschler). Mostreremo come il teorema di Jung segua dal

teorema di Rentschler e dimostreremo il teorema di struttura di van der Kulk.

Nel 1972 Masayoshi Nagata congetturò che l'automorfismo

$$\sigma = (x + 2y(xz - y^2) + z(xz - y^2)^2, \ y + z(xz - y^2), z)$$

non fosse moderato, e che quindi in dimensione tre non fosse vero che tutti gli automorfismi fossero moderati. La congettura si è rivelata vera, ed è stata dimostrata nel 2002 dai matematici Ualbai U. Umirbaev e Ivan P. Shestakov [5], [6].

Non daremo la dimostrazione del teorema di Umirbaev, Shestakov, tuttavia faremo vedere che l'automorfismo di Nagata diventa moderato se lo si estende ad un algebra di polinomi in quattro variabili.

Un motivo per cui vengono studiati gli automorfismi polinomiali e le derivazioni è per meglio comprendere le azioni dei gruppi algebrici sullo spazio affine. Dato un campo \mathbb{K} algebricamente chiuso di caratteristica zero ed un gruppo algebrico G, lo scopo è quello di classificare tutte le rappresentazioni algebriche. In dimensione tre o maggiore si sa poco al riguardo, ma in dimensione due vi è un risultato di Tatsuji Kambayashi [2] che mostra, grazie al teorema di Jung, van der Kulk, che se $\varphi: G \to GA_2(\mathbb{K})$, allora $\varphi(G)$ è coniugato ad un sottogruppo delle affinità oppure del gruppo degli automorfismi triangolari. Come conseguenza si ha che ogni azione di un gruppo algebrico linearmente riduttivo è linearizzabile, ovvero $\varphi(G)$ è coniugato ad un sottogruppo degli automorfismi lineari.

Nello stesso articolo Kambayashi congetturò che quest'ultimo fatto fosse vero in generale, anche in dimensione maggiore di due, ma questa congettura si è rivelata falsa. Nel 1989 Gerry Schwarz trovò due azioni non linearizzabili una di $O_2(\mathbb{K})$ su \mathbb{K}^4 e una di $SL_2(\mathbb{K})$ su \mathbb{K}^7 [4].

Studieremo l'azione di un gruppo algebrico sulla \mathbb{K} -algebra di funzioni regolari di una G-varietà, in particolare quando G è linearmente riduttivo. Dimostreremo quindi il teorema di Kambayashi combinando il risultato di Jung, van der Kulk ed un teorema di Serre [9] sui sottogruppi limitati di un prodotto amalgamato sull'intersezione.

Notazioni

Nel corso della trattazione si adotteranno le seguenti notazioni:

- Tutti gli anelli saranno commutativi con identità ed R indicherà sempre un anello con queste proprietà. Diremo che R_1 è sottoanello di R_2 se $R_1 \subseteq R_2$ e $1_{R_1} = 1_{R_2}$. Con R^* indicheremo gli elementi invertibili di R. Con la lettera \mathbb{K} denoterò sempre un campo.
- Gli elementi di R^n potranno rappresentare n-uple su cui poter valutare polinomi, e allora li noteremo con P, oppure vettori colonna quando vorremo applicargli funzioni lineari, e allora li noteremo con una lettera minuscola sottolineata, ad esempio \underline{w} . Indicheremo inoltre $M_n(R)$ l'anello delle matrici $n \times n$ a coefficienti in R.
- Per ogni $n \in \mathbb{N}$ e per ogni anello commutativo R con identità, $R[x_1, \ldots, x_n]$ sarà l'anello dei polinomi, dove si intende che per n=0 l'anello è R. In R[x] chiameremo termine di testa il monomio di grado massimo e coefficiente di testa il coefficiente del termine di testa. Se $f \in R[x_1, \ldots, x_n]$ la funzione $\deg_{x_i}(f)$ indicherà il più alto esponente con cui appare x_i tra i monomi di un polinomio con coefficiente non nullo. Indicheremo con $\partial_{x_1}, \ldots, \partial_{x_n}$ le usuali derivazioni parziali $\partial_{x_i}(x_j) = \delta_{ij}$.
- Dato un automorfismo dell'algebra dei polinomi $F = (F_1, ..., F_n)$, chiameremo $\deg(F) = \max_{1 \leq i \leq n} \{\deg(F_i)\}$ e chiameremo inoltre multigrado di F e lo denoteremo $\operatorname{mdeg}(F)$ il vettore di \mathbb{N}^n , $(\deg(F_1), ..., \deg(F_n))$.

Capitolo 1

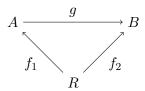
Automorfismi polinomiali

In questo capitolo daremo le primissime definizioni riguardanti le mappe polinomiali di $R[x_1, \ldots, x_n]$. Introdurremo inoltre il problema dei generatori moderati, questione che verrà ripresa poi nel capitolo tre.

1.1 Algebre e automorfismi

Iniziamo definendo un'algebra.

Definizione 1.1. Siano A ed R due anelli ed f_1 un omomorfismo di anelli, allora diremo che A è una R-algebra, inoltre se B è una seconda R-algebra con omomorfismo f_2 , diremo che un omomorfismo di anelli $g: A \to B$ è un omomorfismo di R-algebre se il seguente diagramma commuta.



L'anello R agisce su A tramite moltiplicazione, quindi una R-algebra ha una struttura canonica di R-modulo.

Nel corso della trattazione studieremo il gruppo di automorfismi di R-algebra di $R[x_1, \ldots, x_n]$. L'anello R sarà spesso un campo ma ci metteremo anche in ipotesi più generali di R dominio.

I generatori x_1, \ldots, x_n sono liberi da relazioni, perciò preso $(F_1, \ldots, F_n) \in R[x_1, \ldots, x_n]^n$ esiste un unico endomorfismo di R-algebra $F: R[x_1, \ldots, x_n] \to R[x_1, \ldots, x_n]$ tale che $x_i \mapsto F_i(x_1, \ldots, x_n)$. Viceversa, se abbiamo un endomorfismo F, possiamo sempre prendere il vettore $(F(x_1), \ldots, F(x_n)) \in R[x_1, \ldots, x_n]^n$. Per brevità scriveremo F_i per indicare $F(x_i)$.

Definizione 1.2. Definisco gruppo lineare generale su R di dimensione n il gruppo degli isomorfismi del modulo libero R^n e lo denoteremo $GL_n(R)$. Allo

stesso modo definisco il gruppo di automorfismi generale su R di dimensione n, il gruppo degli automorfismi di R-algebra di $R[x_1, \ldots, x_n]$ e lo denoteremo $GA_n(R)$.

Nel caso $R = \mathbb{K}$, $GA_n(\mathbb{K})$ è il gruppo affine di Cremona. Ogni elemento di $GL_n(R)$ può essere pensato come un automorfismo di R-algebra di $R[x_1, \ldots, x_n]$, perciò $GL_n(R) \hookrightarrow GA_n(R)$. Sono elementi di $GA_n(R)$ anche le traslazioni delle variabili di $R[x_1, \ldots, x_n]$ per un elemento di R^n . Chiamo affinità ciascun elemento del gruppo generato da $GL_n(R)$ e dalle traslazioni e lo denoteremo $Af_n(R)$.

1.2 Automorfismi moderati

Per costruire automorfismi che non sono affinità, si può procedere nel modo seguente:

Definizione 1.3. Per ogni $i \in f \in R[x_1, \dots, \widehat{x}_i, \dots, x_n]$ sia

$$E_i(f) := (x_1, \dots, x_i + f, \dots, x_n).$$

Tale endomorfismo ha come inversa $E_i(-f)$, perciò è un elemento di $GA_n(R)$. Più in generale E_i è un omomorfismo dal gruppo additivo di $\mathbb{K}[x_1,\ldots,\widehat{x}_i,\ldots,x_n]$ in $GA_n(\mathbb{K})$. Chiameremo queste mappe automorfismi elementari. Denoteremo con $EA_n(R)$ il gruppo generato da questi automorfismi. Chiameremo inoltre gruppo degli automorfismi moderati il gruppo $TA_n(R) := \langle Af_n(R), EA_n(R) \rangle$.

Nel caso n=1, gli automorfismi moderati sono solo le affinità, poiché gli automorfismi elementari sono traslazioni. Inoltre vale il seguente lemma.

Lemma 1.4. Se R è dominio e sia F un endomorfismo di R-algebre di R[x] con inversa sinistra, allora F è un'affinità.

Dimostrazione. Sia G tale che $G \circ F = id_{R[x]}$ e siano $F_1, G_1 \in R[x]$ i polinomi corrispondenti. Vale che $G_1(F_1(x)) = x$ e poiché il prodotto dei coefficienti di testa è non nullo, $\deg_x(G_1) \deg_x(F_1) = \deg_x(x) = 1$, da cui $\deg_x(F_1) = \deg_x(G_1) = 1$. I coefficienti di testa di F_1 e G_1 dovranno inoltre essere invertibili, perciò si ha la tesi.

Corollario 1.5. Se R è dominio $GA_1(R) = Af_1(R)$, perciò se $f, g \in R[x_1, ..., x_n]$ tali che R[f] = R[g], allora esistono $a \in R^*$ e $b \in R$ tali che f = ag + b.

Osservazione. L'ipotesi R dominio è necessaria, infatti in $GA_1(\mathbb{Z}/4\mathbb{Z})$ l'endomorfismo che manda x in $2x^2 + x$ è un'involuzione, eppure ha grado due.

Studiamo un'altra classe di automorfismi. Diciamo che una mappa $F \in GA_n(R)$ è un automorfismo triangolare o un automorfismo di Jonquière se $F(x_i) \in R[x_1, \ldots, x_i]$. Denoteremo con $J_n(R)$ il gruppo generato dagli automorfismi triangolari.

Lemma 1.6. Sia R un dominio e F un automorfismo triangolare, allora esistono $a_1, \ldots, a_n \in R^*$, $f_1 \in R$ e $per <math>2 \le i \le n$, $f_i \in R[x_1, \ldots, x_{i-1}]$ tali che

$$F = (a_1x_1 + f_1, \dots, a_nx_n + f_n).$$

Dimostrazione. Dimostriamo la tesi per induzione su n. Nel caso n=1 l'automorfismo è affine per il lemma precedente. Se $n \geq 2$ e F è un automorfismo triangolare di $\mathrm{GA}_n(R)$, allora (F_1,\ldots,F_{n-1}) è un automorfismo triangolare di $\mathrm{GA}_{n-1}(R)$, perciò esistono $a_1,\ldots,a_{n-1}\in R^*,\ f_1\in R$ e per $2\leq i\leq n-1,$ $f_i\in R[x_1,\ldots,x_{i-1}]$ tali che $F=(a_1x_1+f_1,\ldots,a_{n-1}x_{n-1}+f_{n-1},F_n)$. Se specializziamo la variabile x_n , possiamo vedere F_n come un elemento di $\mathrm{GA}_1(\mathbb{K}[x_1,\ldots,x_{n-1}])$, perciò esiste $a_n\in (R[x_1,\ldots,x_{n-1}])^*$ e $f_n\in R[x_1,\ldots,x_{n-1}]$ tali che $F_n=a_nx_n+f_n$. Ma R è un dominio, perciò $(R[x_1,\ldots,x_{n-1}])^*=R^*$, quindi abbiamo la tesi.

Lemma 1.7. Se $R \ \dot{e} \ un \ dominio, \ allora \ \langle Af_n(R), J_n(R) \rangle = TA_n(R).$

Dimostrazione. Per dimostrare $\langle Af_n(R), J_n(R) \rangle \supseteq TA_n(R)$, devo far vedere che $\langle Af_n(R), J_n(R) \rangle \supseteq EA_n(R)$. Per ogni $f \in R[x_1, \ldots, x_{n-1}], E_n(f)$ è triangolare. Coniugando per l'automorfismo che permuta le variabili x_i e x_n posso ottenere un qualsiasi $E_i(g)$ con $g \in R[x_1, \ldots, \hat{x_i}, \ldots, x_n]$.

Per l'altra inclusione devo dimostrare che se F è un automorfismo triangolare, allora è moderato. Per il lemma precedente esistono $a_1, \ldots, a_n \in R^*$, $f_1 \in R$ e $f_i \in R[x_1, \ldots, x_{i-1}]$ tali che $F = (a_1x_1 + f_1, \ldots, a_nx_n + f_n)$. Siano L_i le affinità che mandano $x_i \mapsto a_ix_i$.

Prendiamo $G_1 = E_1(f_1) \circ L_1$ e H_1 l'inverso di G_1 . Continuiamo induttivamente definendo

$$G_{i+1} = E_{i+1}(f_{i+1}(H_i(x_1), \dots, H_i(x_i), \widehat{x_{i+1}}, x_{i+2}, \dots, x_n)) \circ L_{i+1} \circ G_i$$

e H_{i+1} l' inverso. Si dimostra per induzione che

$$G_i = (a_1x_1 + b_1, \dots, a_ix_i + b_i, x_{i+1}, \dots, x_n)$$

e che quindi G_n è della forma voluta.

Perciò se R è un dominio tutti gli automorfismi che abbiamo trovato finora sono moderati. Riusciamo ad uscire fuori da questo gruppo? In sintesi:

Problema (dei generatori moderati). Se R è un dominio, allora è vero che $GA_n(R) = TA_n(R)$?

Nel caso n=1 abbiamo già visto che è vero. Già per dimensione due il problema non è affatto banale. Nel capitolo tre dimostreremo che la risposta è affermativa se R è un campo di caratteristica zero e che è falso per ogni dominio che non sia un campo.

Parleremo inoltre del problema in dimensione tre e vedremo che è stata data una risposta negativa se $\mathbb K$ è un campo di caratteristica zero.

Capitolo 2

Derivazioni

In questo capitolo definiamo uno degli strumenti più utilizzati per lo studio dell'algebra dei polinomi: le derivazioni ed in particolare le derivazioni localmente nilpotenti di un anello A. Daremo una struttura di A-modulo sinistro a questi endomorfismi e introdurremo l'anello delle costanti.

Una derivazione induce naturalmente una funzione grado. Grazie a questa dimostreremo ad esempio che l'anello delle costanti è un anello fattorialmente chiuso, daremo quindi la definizione di derivazione K-lineari.

Vedremo in seguito degli strumenti che utilizzeremo per dimostrare il teorema di Rentshler, come il concetto di ω -graduazione di un anello e di derivazione ω -omogenea di $\mathbb{K}[x_1,\ldots,x_n]$. Mostreremo cosa succede se una derivazione localmente nilpotente ammette una decomposizione in derivazioni ω -omogenee e che ad esempio le derivazioni \mathbb{K} -lineari ammettono una decomposizione in derivazioni ω -omogenee.

Un altro punto importante che presenteremo è l'azione di coniugio degli automorfismi di \mathbb{K} -algebra di A sullo spazio vettoriale delle derivazioni di A. Questa mappa è molto importante perché lega automorfismi e derivazioni.

Infine parleremo degli automorfismi esponenziali per \mathbb{K} -algebre con \mathbb{K} di caratteristica zero. L'automorfismo di Nagata sarà proprio l'automorfismo esponenziale indotto da una certa derivazione.

2.1 Prime definizioni

Definizione 2.1. Sia A un anello, una mappa $D: A \to A$ si dice una derivazione di A, se soddisfa per ogni $f, g \in A$,

$$D(f+g) = D(f) + D(g)$$

$$D(fg) = fD(g) + D(f)g$$
(2.1)

La condizione (2.1) è chiamata regola di Leibniz o regola del prodotto.

Esempio 2.2. La mappa che manda ogni elemento di A in zero è una derivazione. La chiameremo derivazione nulla.

Annoteremo con Der(A) l'insieme delle derivazioni di A.

Osservazione. Si dimostra per induzione che per ogni derivazione D di A e per ogni $f, g \in A$ e $n, m \in \mathbb{Z}^+$ valgono le seguenti identità :

$$D^{n}(fg) = \sum_{i=0}^{n} {n \choose i} D^{i}(f) D^{n-i}(g)$$
 (2.2)

$$D(f^{m}) = mf^{m-1}D(f). (2.3)$$

Lemma 2.3. Se $D, D' \in Der(A)$ e $h \in A$, allora D + D' e hD sono derivazioni, dove con l'ultima intendo $hD : A \to A$ tale che per ogni $f \in A$, $hD(f) := h \cdot D(f)$. Il gruppo abeliano (Der(A), +) ha quindi una naturale struttura di A-modulo sinistro.

2.2 Anello delle costanti

In questa sezione daremo la definizione di anello delle costanti e di derivazione \mathbb{K} -lineare e vedremo che $\partial_1, \ldots, \partial_n$ è una base dello spazio vettoriale $\mathrm{Der}_{\mathbb{K}}(A)$, con A una \mathbb{K} -algebra.

Definizione 2.4. Se $D \in Der(A)$, allora $Ker D := \{a \in A \mid Da = 0\}$ è l'insieme delle *costanti* della derivazione.

Equivalentemente le costanti sono gli elementi $a \in A$, tali che D(af) = aD(f) per ogni $f \in A$.

Lemma 2.5. Le costanti Ker D sono un sottoanello di A.

Dimostrazione. Se
$$a, b \in \text{Ker } D$$
, $D(a+b) = D(a) + D(b) = 0$, $D(ab) = aD(b) + D(a)b = 0$ e $D(1_A) = D(1_A \cdot 1_A) = D(1_A) + D(1_A)$, quindi $D(1_A) = 0$

Definizione 2.6. Se R è un sottoanello di A, diremo che D è R-lineare oppure che D è una R-derivazione se $R \subseteq \text{Ker}(D)$. Denoteremo con $\text{Der}_R(A)$ l'insieme delle R-derivazioni.

Vediamo ora un lemma che ci permette di dimostrare rapidamente se due derivazioni sono uguali ed in particolare se una derivazione è nulla.

Lemma 2.7. Sia $S \subseteq A$ e supponiamo che A := R[S]. Se D_1 e D_2 sono R-derivazioni, tali che $D_1(s) = D_2(s)$ per ogni $s \in S$, allora $D_1 = D_2$.

Dimostrazione. Sia $D' := (D_1 - D_2)$, allora $R \subseteq \text{Ker}(D')$ poiché D_1 e D_2 sono derivazioni R-lineari, inoltre per ipotesi $S \subset \text{Ker}(D')$. Poiché le costanti sono un sottoanello, segue che $R[S] \subseteq \text{Ker}(D')$ e che quindi D' = 0.

Esempio 2.8. Nel caso $A = \mathbb{K}[x_1, \dots, x_n]$, posso definire in modo unico, in virtù del lemma 2.7, le derivazioni $\partial_{x_1}, \dots, \partial_{x_n}$ come quelle \mathbb{K} -derivazioni tali che per ogni i, j $\partial_{x_i} x_j = \delta_{ij}$.

Lemma 2.9. Sia $A := \mathbb{K}[x_1, \dots, x_n]$, allora le derivazioni $\partial_{x_1}, \dots, \partial_{x_n}$ sono una base del \mathbb{K} -spazio vettoriale $\mathrm{Der}_{\mathbb{K}}(A)$.

Dimostrazione. Supponiamo che esistano $(a_i)_{1 \leq i \leq n} \subseteq \mathbb{K}$ tali che $\sum_{i=1}^n a_i \partial_{x_i} = 0$, allora, valutando in x_i , otteniamo che tutti gli a_i sono nulli. Se $D \in \mathrm{Der}_{\mathbb{K}}(A)$, definiamo $D' := D - \sum_{i=1}^n D(x_i) \partial_{x_i}$. Allora D' è \mathbb{K} -lineare e fa zero sugli x_i , perciò per il 2.7, è la derivazione nulla.

Osservazione. Le derivate parziali ci dimostrano che Der(A) in generale non è un anello. Notiamo infatti che $\partial_{x_1}^2$ non è una derivazione. Applicando la formula di Leibniz otteniamo

$$\partial_{x_1}^2(x_1^2) = 2x_1 \partial_{x_1}(x_1).$$

A sinistra viene 2 mentre a destra $2x_1$.

Lemma 2.10. Sia $s \in A$ e $p(t) \in \text{Ker}(D)[t]$, allora D(p(s)) = p'(s)D(s), dove con p'(t) indico la derivata formale del polinomio p(t).

Dimostrazione. Mi basta dimostrarlo su un monomio, infatti per additività di D si può estendere il risultato ad un qualsiasi polinomio. Preso $a \in \text{Ker}(D)$,

$$D(as^n) = aD(s^n) = ans^{n-1}D(s).$$

Osservazione. Prendiamo un campo \mathbb{K} di caratteristica zero e calcoliamo Ker (∂_{x_n}) nell'anello $\mathbb{K}[x_1,\ldots,x_n]$. Sia $R:=\mathbb{K}[x_1,\ldots,x_{n-1}]\subset\mathbb{K}[x_1,\ldots,x_n]$, allora R è costituito solo da costanti di ∂_{x_n} . Sia ora $p(x_n)\in R[x_n]$. Per il corollario precedente se $\deg_{x_n}(p(x_n))>0$, allora $p(x_n)\not\in \mathrm{Ker}(\partial_{x_n})$. Perciò $\mathrm{Ker}(\partial_{x_n})=\mathbb{K}[x_1,\ldots,x_{n-1}]$ e più in generale per ogni i,

$$\operatorname{Ker}\left(\partial_{x_i}\right) = \mathbb{K}[x_1, \dots, \widehat{x}_i, \dots, x_n].$$

Definizione 2.11. Se $f \in A$ è tale che Df = 1, diremo che f è un elemento fondamentale.

Osservazione. Non tutte le derivazioni hanno elementi fondamentali, ad esempio se la derivazione $x\partial_x\in \mathrm{Der}_{\mathbb{K}}[x]$ avesse elementi fondamentali, allora x sarebbe invertibile.

Siano R ed A due \mathbb{K} -algebre, con \mathbb{K} di caratteristica zero.

Lemma 2.12. Per ogni derivazione D e per ogni elemento f di A, se $R \subseteq \text{Ker}(D)$, allora D(R[f]) = D(f)R[f].

Dimostrazione. Per il lemma 2.10 $D(R[f]) \subseteq D(f)R[f]$. Voglio dimostrare ora l'altra inclusione, sia $p(f) \in R[f]$, allora posso scrivere $p(f) = \sum_{i=0}^{k} a_i f^i$. Preso $q(f) := \sum_{i=0}^{k} \frac{a_i}{i+1} f^{i+1}$, D(q(f)) = D(f)p(f).

Corollario 2.13. Se f è un elemento fondamentale $D|_{R[f]}:R[f]\to R[f]$ è suriettiva.

Osservazione. L'ipotesi char $\mathbb{K}=0$ è essenziale. In $\mathbb{F}_p[x]$, ∂_x non sarà suriettiva, in quanto x^{p-1} non è nell'immagine della derivazione.

2.3 Derivazioni localmente nilpotenti e triangolari

In questa breve sezione introdurremo i concetti di derivazione localmente nilpotente e triangolare e dimostreremo che le derivazioni triangolari sono localmente nilpotenti.

Definizione 2.14. Diremo che $D \in Der(A)$ è *nilpotente* rispetto ad un certo elemento f di A se esiste un intero positivo n tale che $D^n f = 0$. Diremo inoltre che D è *localmente nilpotente* se è nilpotente rispetto ad ogni elemento di A.

Sia Nil(D) l'insieme degli elementi nilpotenti rispetto a D, sia LND(A) l'insieme di derivazioni localmente nilpotenti e sia LND_R(A) := LND(A) \cap Der_R(A). É chiaro che una derivazione $D \in \text{LND}(A)$ se e solo se Nil(D) = A.

Lemma 2.15. L'insieme Nil(D) è un sottoanello di A.

Dimostrazione. Per ogni coppia di elementi $f, g \in A$ se $m, n \in \mathbb{N}$ tali che $D^m(f) = 0$ e $D^n(g) = 0$, allora $D^{\max\{m,n\}}(f+g) = 0$. Vale anche che $D^{m+n}(fg) = 0$, poiché sviluppando con la (2.2) otteniamo monomi della forma $c_i D^i(f) D^{m+n-i}(g)$ e per ogni $i, 0 \le i \le m+n$ vale $i \ge m$ oppure $m+n-i \ge n$. Perciò ogni addendo è 0. Infine $1_A \in \text{Nil}(A)$, poiché come abbiamo già visto $1_A \in \text{Ker}(D)$.

Corollario 2.16. Se S è un insieme di generatori dell'anello A e $S \subseteq Nil(D)$, allora D è localmente nilpotente. Se D' è una R-derivazione ed esiste $T \subseteq Nil(D')$ tale che R[T] = A, allora $D' \in LND(A)$.

Esempio 2.17. Sia $A:=\mathbb{K}[[x_1,\ldots,x_n]]$, allora $\partial_{x_1},\cdots,\partial_{x_n}$ sono \mathbb{K} -derivazioni, ma non sono localmente nilpotenti. Preso ad esempio $\sum_{i=0}^{\infty}x_1^i\in A$, non esiste $m\in\mathbb{Z}^+$ tale che $\partial_1^m\sum_{i=0}^{\infty}x_1^i=0$. Un discorso diverso vale per $\mathbb{K}[x_1,\ldots,x_n]$. Le \mathbb{K} -derivazioni $\partial_{x_1},\cdots,\partial_{x_n}$ sono nilpotenti rispetto a $\{x_i\}_{1\leq i\leq n}$, perciò sono nilpotenti rispetto a tutto $\mathbb{K}[x_1,\ldots,x_n]$. Possiamo comunque trovare derivazioni non localmente nilpotenti. Ad esempio $x_1\partial_{x_1}$.

Vediamo delle particolari derivazioni di $A := \mathbb{K}[x_1, \dots, x_n]$.

Definizione 2.18. Siano f_i con $1 \le i \le n$ una famiglia di polinomi tali che $f_i \in \mathbb{K}[x_1, \dots, x_{i-1}]$ per $i \ge 2$ e $f_1 \in \mathbb{K}$, e sia

$$D := f_1 \partial_{x_1} + \dots + f_n \partial_{x_n}.$$

Allora D è detta derivazione triangolare.

Lemma 2.19. Le derivazioni triangolari sono localmente nilpotenti.

Dimostrazione. Dimostriamolo per induzione: il caso n=1 l'abbiamo già visto nell'esempio. Sia $n \geq 2$, prendo $D \in \operatorname{Der}_{\mathbb{K}}(\mathbb{K}[x_1,\ldots,x_n])$ e sia $D_0 \in \operatorname{Der}_{\mathbb{K}}(\mathbb{K}[x_1,\ldots,x_{n-1}])$ tale che $D=D_0+f_n\partial x_n$. Mi basta dimostrare che è nilpotente rispetto ai generatori dell'algebra. Per ipotesi induttiva D_0 è localmente nilpotente, perciò x_1,\ldots,x_{n-1} sono nilpotenti. Per x_n vale che $D(x_n)=f_n\in\operatorname{Nil}(D)$, perciò $x_n\in\operatorname{Nil}(D)$. Questo termina la dimostrazione.

2.4 Funzione grado indotta da una derivazione

D'ora in poi gli anelli saranno domini e \mathbb{K} sarà di caratteristica zero. In questo modo potremo definire una funzione grado della derivazione. Questa ci permetterà di dimostrare ad esempio che gli invertibili dell'algebra sono costanti nel caso le derivazioni siano localmente nilpotenti.

Definizione 2.20. Dato un dominio R, chiamiamo funzione grado una qualsiasi funzione deg: $R \to \mathbb{N} \cup \{-\infty\}$, tale che per ogni $x, y \in R$,

- (i) $deg(x) = -\infty$ se e solo se deg(x) = 0;
- (ii) $\deg(x+y) \le \max\{\deg(x), \deg(y)\};$
- (iii) deg(xy) = deg(x) + deg(y).

Dove si intende che $(-\infty)+(-\infty)=(-\infty)$ e per ogni $n\in\mathbb{N}$ $n+(-\infty)=-\infty$.

Definizione 2.21. Definiamo per $D \in \text{Der}(A), v_D : \text{Nil}(D) \to \mathbb{N} \cup \{-\infty\}$ tale che se $f \in A - 0$

$$v_D(f) := \min\{n \in \mathbb{N} \mid D^{n+1}f = 0\}$$

e $v_D(0) = -\infty$. Chiameremo $v_D(\cdot)$, funzione grado indotta da D.

In particolare se $D \in \text{LND}(A)$, $v_D(\cdot)$ sarà definita su tutta l'algebra.

Lemma 2.22. La funzione v_D è una funzione grado.

Dimostrazione. La prima proprietà vale per definizione. Prendiamo $f, g \in Nil(D)$ e verifichiamo la (2) e la (3). Notiamo che se f = 0 oppure g = 0, allora le due proprietà valgono banalmente. Quindi supponiamo $f \neq 0$ e $g \neq 0$. Allora la (2) segue dall'additività di D. Detto $M := \max\{v_D(f), v_D(g)\}$,

$$D^{M+1}(f+g) = D^{M+1}(f) + D^{M+1}(g).$$

Per dimostrare il punto (3) applichiamo la (2.2) su $D^{N+1}(fg)$ e $D^{N}(fg)$, con $N = v_D(f) + v_D(g)$, ottenendo:

$$D^{N+1}(fg) = \sum_{i=0}^{N+1} \binom{N+1}{i} D^{i}(f) D^{N-i+1}(g) = 0$$

poiché per ogni $i, i > v_D(f)$ oppure $N - i + 1 > v_D(g)$.

$$D^{N}(fg) = \sum_{i=0}^{N} {N \choose i} D^{i}(f) D^{N-i}(g) = {N \choose v_{D}(f)} D^{v_{D}(f)}(f) D^{v_{D}(g)}(g) \neq 0$$

Nell'ultimo passaggio sfrutto l'ipotesi di dominio e l'ipotesi sulla caratteristica di \mathbb{K} . Il risultato ottenuto ci dice che $v_D(fg) = N$.

Iniziamo dimostrando:

Lemma 2.23. Le costanti Ker(D) formano un sottoanello fattorialmente chiuso, ovvero se $f, g \in A - \{0\}$, allora $fg \in Ker(D)$ implica $f, g \in Ker(D)$.

Dimostrazione. Usiamo la funzione grado appena introdotta. Se $fg \in \text{Ker}(D)$, allora $v_D(fg) = 0$, quindi $v_D(f) + v_D(g) = 0$. Quest'ultima uguaglianza è vera solo se $v_D(f) = 0$ e $v_D(g) = 0$, ovvero $f, g \in \text{Ker}(D)$.

Questo ci dice anche che $A^* \subseteq \mathrm{Ker}(D)$, quindi in particolare $\mathrm{Ker}(D)$ sarà anche una \mathbb{K} -algebra.

Osservazione. Sia $D \in \text{Der}(A)$, $f \in \text{Nil}(D)-\text{Ker}(D)$, allora per la definizione di $v_D(\cdot)$, $v_D(Df) = v_D(f) - 1$.

Lemma 2.24. Sia $D \in LND(A)$ e $f_1, f_2 \in A$, se $Df_1 \in f_2A$ e $Df_2 \in f_1A$, allora $Df_1 = 0$ oppure $Df_2 = 0$.

Dimostrazione. Supponiamo che esistono $g_1,g_2\in A$ tali che $Df_1=f_2g_1$ e $Df_2=f_1g_2$ e per assurdo che $Df_1\neq 0$ e $Df_2\neq 0$. Per l'osservazione

$$v_D(f_1) - 1 = v_D(Df_1) = v_D(f_2g_1) \ge v_D(f_2).$$

Allo stesso tempo $v_D(f_2) - 1 \ge v_D(f_1)$ e sommando le due disuguaglianze si ottiene un assurdo.

Lemma 2.25. Sia B = A[t], allora LND_A(B) = $A\partial_t$.

Dimostrazione. Un contenimento è banale: $A\partial_t$ sono tutte A-derivazioni localmente nilpotenti.

Per dimostrare che sono le sole, per 2.7, mi basta provare che per ogni D in $LND_A(B)$, $D(t) \in A$. Supponiamo $D(t) \notin A$, allora esiste $n \in \mathbb{Z}^+$ tale che $D^n(t) \in A$ e $D^{n-1}(t) \notin A$. Un tale n esiste perché D è localmente nilpotente. Sia $p(t) := D^{n-1}(t)$, allora $p'(t)D(t) = D(p(t)) \in A$. Ma A è fattorialmente chiuso, perciò $D(t) \in A$. Assurdo.

2.5 Algebre graduate e derivazioni omogenee

Definizione 2.26. Data un'algebra A definiamo graduazione una famiglia $\{A_i\}_{i\in\mathbb{N}}$ di sottospazi vettoriali di A, tale che $A=\bigoplus_{i\in\mathbb{N}}A_i$ e per ogni $i,j\in\mathbb{N},\ A_iA_j\subseteq A_{i+j}$. Un'algebra graduata è il dato di un'algebra A e una graduazione. Un elemento $f\in A$ lo chiameremo omogeneo di grado i se $f\in A_i$. Nel caso $A:=\mathbb{K}[x_1,\ldots,x_n]$, per ogni $\omega\in\mathbb{N}^n$, $\omega=(\omega_1,\ldots,\omega_n)$, chiameremo ω -graduazione la graduazione con sottospazi $A_i:=\langle x_1^{s_1}\cdots x_n^{s_n}\rangle_{\omega_1s_1+\cdots+\omega_ns_n=i}$ e ω -graduazione un polinomio omogeneo rispetto all' ω -graduazione.

Chiameremo graduazione standard la graduazione indotta da $(1, ..., 1) \in \mathbb{N}^n$ e diremo standard-omogeneo un elemento omogeneo rispetto questa graduazione e grado standard il grado indotto.

Nel resto della sezione $A = \mathbb{K}[x_1, \dots, x_n]$ e ω sarà un elemento di \mathbb{N}^n e A_i saranno i sottospazi ω -omogenei.

Definizione 2.27. Una derivazione D di A è detta ω -omogenea, di ω -grado $d \in \mathbb{Z}$ se per ogni $i \in \mathbb{N}$, $D(A_i) \subseteq A_{i+d}$.

Osservazione. Osserviamo che se D è ω -omogenea e $f \in A$ si decompone $\sum_{i \in \mathbb{N}} f_i$, con $f_i \in A_i$, allora Df = 0 se e solo se per ogni i, $Df_i = 0$. Questo vale perché $Df = \sum_{i \in \mathbb{N}} Df_i$ è una decomposizione in addendi omogenei.

Definizione 2.28. Definiamo $\deg_{\omega}: A \to \mathbb{N} \cup \{-\infty\}$ tale che

- $\deg_{\omega}(0) = -\infty$
- Se $f \in A \{0\}$ e $f := \sum_{i \in \mathbb{N}} f_i$, con f_i ω -omogenei, $\deg_{\omega}(f) := \max\{i \in \mathbb{N} \mid f_i \neq 0\}$.

Lemma 2.29. La funzione \deg_{ω} è una funzione grado.

Dimostrazione. La proprietà (1) è soddisfatta. Verifichiamo la (2) e la (3): siano $f,g \in A$ con $\deg_{\omega}(f) = M$ e $\deg_{\omega}(g) = N$ e supponiamo $M \geq N$. Scrivo $f = \sum_{i=0}^{M} f_i$ e $g = \sum_{i=0}^{N} g_i$ e sommo, ottengo

$$f + g = \sum_{i=0}^{M} (f_i + g_i)$$

allora $\deg_{\omega}(f+g) \leq M$. Vediamo il prodotto :

$$fg = \sum_{l=0}^{M+N} \sum_{i+j=l} f_i g_j.$$

Il termine ω -omogeneo di ω -grado massimo sarà $f_Mg_N\neq 0$ perché A dominio. Allora $\deg_\omega(fg)=M+N$.

Lemma 2.30. Sia D una derivazione localmente nilpotente non nulla e supponiamo esistano ℓ , $m \in \mathbb{Z}$ tale che D ammetta una decomposizione $D := \sum_{i=\ell}^m D_i$, con D_i ω -omogenee di grado i e con $D_\ell \neq 0$ e $D_m \neq 0$ e sia $f = \sum_{j=p}^q f_j$ con f_j ω -omogenei e f_p , $f_q \neq 0$.

- (i) La derivazione $D_{\ell}, D_m \in LND(A)$;
- (ii) Se $f \in \text{Ker}(D)$, allora $f_p \in \text{Ker}(D_\ell)$ e $f_q \in \text{Ker}(D_m)$.

Dimostrazione. Per la (1), se $t \in \mathbb{N}$ tale che $D^t = 0$, allora D^t avrà ancora una decomposizione finita in derivazioni omogenee della forma

$$D^t = D^t_\ell + D' + D^t_m$$

con D' derivazione decomponibile in derivazioni omogenee di gradi compresi tra $t\ell+1$ e tm-1. Poiché $D^t=0$ anche $D^t_\ell=D^t_m=0$. Passiamo alla (2): se Df=0, allora

$$\left(\sum_{i=\ell}^{m} D_i\right) \left(\sum_{j=p}^{q} f_j\right) = \sum_{\substack{1 \le i \le m \\ p \le j \le q}} D_i f_j$$

Il termine di ω -grado massimo sarà $D_p f_q$ e il termine di ω -grado minimo sarà $D_p f_q$. Entrambi dovranno essere nulli, perciò si ha la tesi.

Lemma 2.31. In A le derivazioni \mathbb{K} -lineari ammettono una decomposizione finita in derivazioni ω -omogenee per ogni ω .

Dimostrazione. Sia $D \in \operatorname{Der}_{\mathbb{K}}(A)$, per il lemma 2.9, esistono $f_1, \ldots, f_n \in A$ tali che $D = \sum_{i=1}^n f_i \partial_{x_i}$. Ogni $f_i = \sum_{j=0}^{m_i} f_{i,j}$ con tutti gli $f_{i,j}$ ω -omogenei e $m_i \in \mathbb{N}$. Allora

$$D = \sum_{i,j} f_{i,j} \partial_{x_i}$$

dove ogni addendo è una derivazione ω -omogenea.

2.6 Azione di coniugio

Andremo ora a definire l'azione di coniugio che lega $\operatorname{Der}(A)$ e il gruppo $\operatorname{Aut}_{\mathbb{K}}(A)$. Per semplicità dato $D \in \operatorname{Der}(A)$ e $F \in \operatorname{Aut}_{\mathbb{K}}(A)$ denoteremo $D^F := F \circ D \circ F^{-1}$.

Lemma 2.32. La mappa ρ : $\operatorname{Aut}_{\mathbb{K}}(A) \times \operatorname{Der}(A) \to \operatorname{Der}(A)$, tale che $\rho(F, D) = D^F$ è un' azione di $\operatorname{Aut}_{\mathbb{K}}(A)$ su $\operatorname{Der}(A)$.

Dimostrazione. Verifichiamo innanzitutto che D^F è sempre una derivazione: l'additività segue dall'additività di F e D; per dimostrare la regola di Leibniz sfruttiamo che F e F^{-1} sono omomorfismi di anelli. Se $f,g\in A$,

$$\begin{split} D^F(f\cdot g) &= F\circ D(F^{-1}(f)\cdot F^{-1}(g)) = \\ &= f\cdot (F\circ D\circ F^{-1}(g)) + (F\circ D\circ F^{-1}(f))\cdot g = \\ &= f\cdot D^F(g) + D^F(f)\cdot g. \end{split}$$

Vale anche $D^{\mathrm{id}}=D$ e $(D^F)^G=\left(F\circ D\circ F^{-1}\right)^G=G\circ F\circ D\circ F^{-1}\circ G^{-1}=D^{G\circ F}$

Lemma 2.33. Siano D, E derivazioni, sia F un automorfismo di A e sia $g \in A$, allora valgono i seguenti fatti:

- (i) $(D+E)^F = D^F + E^F$;
- (ii) $(gD)^F = F(g)D^F$;
- (iii) $\operatorname{Ker} D^F = F(\operatorname{Ker} D);$
- (iv) Se $D \in LND(A)$, allora $D^F \in LND(A)$.

In particolare $D \mapsto D^F$ è un isomorfismo di K-spazi vettoriali.

Dimostrazione. Le prime due sono facili verifiche. Per la (3) basta notare che se $f \in A$ e $D^F(f) = 0$, allora $DF^{-1}(f) = 0$, in quanto la controimmagine di zero di un automorfismo è zero. Se $g := F^{-1}(f)$, allora $g \in (\text{Ker}(D))$ e quindi $f \in F(\text{Ker}(D))$. Allo stesso tempo se g è una costante, allora $DF^{-1}(F(g)) = 0$, quindi $D^F(F(g)) = 0$.

La (4) segue invece da $(D^F)^n = (D^n)^F$, infatti

$$\underbrace{F \circ D \circ F^{-1} \circ \cdots \circ F \circ D \circ F^{-1}}_{n \text{ volte}} = F \circ D^n \circ F^{-1}.$$

Come conseguenza della (1) e della (2) abbiamo che la mappa $D \mapsto D^F$ è lineare. Poiché la mappa è anche biiettiva, allora è un isomorfismo lineare.

Esempio 2.34. Possiamo definire per ogni automorfismo F di $A := \mathbb{K}[x_1, \dots, x_n]$ e per ogni i,

$$\frac{\mathrm{d}}{\mathrm{d}F_i} := \partial_{x_i}^F.$$

Queste derivazioni sono localmente nilpotenti poiché sono ottenute tramite coniugazione di derivazioni localmente nilpotenti e sono anche \mathbb{K} -lineari perché F lo è. Inoltre $\left\{\frac{d}{dF_i}\right\}_{1\leq i\leq n}$ sono una base di $\mathrm{Der}_{\mathbb{K}}(A)$, perché lo sono $\{\partial_{x_i}\}_{1\leq i\leq n}$ ed il coniugio è un isomorfismo di \mathbb{K} -spazi vettoriali per il lemma 2.33.

Poiché so calcolare $\text{Ker}(\partial_{x_i})$ posso anche calcolare le costanti di queste nuove applicazioni, sempre grazie al lemma 2.33. Otteniamo:

$$\operatorname{Ker} \frac{\mathrm{d}}{\mathrm{d}F_i} = F(\mathbb{K}[x_1, \dots, \hat{x}_i, \dots, x_n]) = \mathbb{K}[F_1, \dots, \hat{F}_i, \dots F_n].$$

2.7 Automorfismi esponenziali

Vediamo quindi come ottenere degli automorfismi di $A := \mathbb{K}[x_1, \dots, x_n]$ a partire da una derivazione D localmente nilpotente. Ci servirà supporre che la caratteristica del campo sia zero.

Definizione 2.35. Sia $\exp(D): A \to A$, tale che per ogni $f \in A$,

$$\exp(D)(f) = \sum_{i=0}^{+\infty} \frac{1}{i!} D^i f.$$

Dove $D^0 = I$, la derivazione identica. Notiamo che i termini della serie sono definitivamente nulli per l'ipotesi su D.

Lemma 2.36. La funzione $\exp(D)$ è un automorfismo di \mathbb{K} -algebre.

Dimostrazione. Siano $a \in \mathbb{K}$ e $f, g \in A$, allora $\exp(D)(af+g) = a \exp(D)(f) + \exp(D)(g)$, poiché somma di funzioni \mathbb{K} -lineari. Inoltre

$$\begin{split} (D)(fg) &= \sum_{i=0}^{+\infty} \frac{1}{i!} D^i(fg) = \sum_{i=0}^{+\infty} \frac{1}{i!} \sum_{s+t=i} \binom{s+t}{s} D^s(f) D^t(g) \\ &= \sum_{s,t} \frac{1}{s!} D^s(f) \frac{1}{t!} D^t(g) \\ &= \exp(D)(f) \exp(D)(g). \end{split}$$

Si verifica ora espandendo in modo analogo che se E è una derivazione localmente nilpotente che commuta con D, allora $\exp(D+E)=\exp(D)\circ\exp(E)$. Perciò $I=\exp(D-D)=\exp(D)\circ\exp(-D)$, quindi $\exp(D)$ è invertibile.

Lemma 2.37. Sia F un automorfismo, allora $\exp(D^F) = \exp(D)^F$.

Dimostrazione. La proposizione è una conseguenza del lemma 2.33, vale difatti che per ogni $f \in A$,

$$\exp(D^F)(f) = \sum_{i=0}^{+\infty} \frac{1}{i!} (D^F)^i(f) = \sum_{i=0}^{+\infty} \frac{1}{i!} (D^i)^F(f) =$$

$$= \left(\sum_{i=0}^{+\infty} \frac{1}{i!} D^i(f)\right)^F =$$

$$= \exp(D)^F(f) .$$

Capitolo 3

Il problema dei generatori moderati

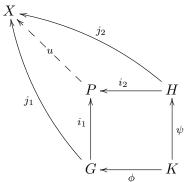
In questo capitolo dimostreremo innanzitutto che se R è un dominio allora il gruppo degli automorfismi moderati è il prodotto amalgamato sull'intersezione del gruppo delle affinità e quello degli automorfismi triangolari. Per ottenere questo risultato dimostreremo l'esistenza di una fattorizzazione unica di un certo tipo.

Successivamente dimostreremo il teorema di Rentschler, la dimostrazione è molto lunga ed utilizza molti lemmi già presentati nel capitolo due sulle derivazioni.

Nella parte finale parleremo del controesempio di Nagata, Shestakov, Umirbaev e del risultato di Martha Smith. Daremo inoltre qualche accenno al problema dei generatori stabilmente moderati.

3.1 Prodotto amalgamato

Definizione 3.1. Siano G, H e K gruppi e siano $\phi: K \to G$ e $\psi: K \to H$ due omomorfismi di gruppi. Sia P un gruppo tale che esistano $i_1: G \to P$ e $i_2: H \to P$ per cui per ogni gruppo X e per ogni coppia di omomorfismi $j_1: G \to X$ e $j_2: H \to X$ esiste un unica u che faccia commutare il diagramma:



Definiamo P un prodotto amalgamato di G e H rispetto ϕ e ψ .

Grazie all'unicità della mappa u si dimostra che il prodotto amalgamato è unico a meno di isomorfismi. Nel caso $(\phi, \psi) = (\iota_1, \iota_2)$ con ι_1, ι_2 gli omomorfismi di inclusione di K in G e H denotiamo il prodotto amalgamato $G *_K H$. Vediamo come si può costruire un tale gruppo.

Definiamo una parola in G e H una successione finita di elementi $s_1 ldots s_n$ dove ciascun s_i è un elemento di G oppure di H. Gli s_i saranno le lettere di una parola. Una parola può essere modificata con le seguenti quattro mosse:

- (i) Rimozione della lettera e_G oppure e_H ;
- (ii) Aggiunzione della lettera e_G oppure e_H ;
- (iii) Sostituzione di una coppia di lettere adiacenti s_i, s_{i+1} appartenenti entrambi a G, ad H o a K, con la lettera $s_i \cdot s_{i+1}$, dove \cdot indica l'operazione nel gruppo;
- (iv) Sostituzione di una lettera s_i con due lettere adiacenti s_i', s_{i+1}' appartenenti ad uno dei tre gruppi tali che $s_i = s_i' \cdot s_{i+1}'$.

Diciamo che due parole sono equivalenti se si possono ottenere l'una dall'altra con un numero finito di mosse. Si dimostra che questo gruppo è isomorfo canonicamente a $G *_K H$.

3.2 Teorema di struttura

Studiamo il gruppo degli automorfismi moderati in dimensione due. In virtù del lemma 1.7 sappiamo che è generato da $Af_2(R)$ e da $J_2(R)$.

$$Af_2(R) = \{(a_1x + b_1y + c_1, a_2x + b_2y + c_2) \mid a_i, b_i, c_i \in R; a_1b_2 - a_2b_1 \in R^*\}.$$

Invece gli automorfismi triangolari, in virtù del lemma 1.6 si possono scrivere

$$J_2(R) = \{(a_1x + c_1, b_2y + f(x)) \mid a_1, b_2 \in R^*; c_1 \in R; f(x) \in R[x]\}.$$

Definiamo ora $Bf_2(R) := Af_2(R) \cap J_2(R)$, allora

$$Bf_2(R) = \{(a_1x + c_1, a_2x + b_2y + c_2) \mid a_1, b_2 \in R^*; c_1, b_2, c_2 \in R\}.$$

Dimostriamo che esiste un insieme \mathcal{A} di rappresentanti di tutte le classi destre di $Af_2(R)$ rispetto $Bf_2(R)$ meno la classe dell'identità tale che tutte le classi vengono prese una sola volta e se $\alpha \in \mathcal{A}$, allora esiste $t \in R$ tale per cui

$$\alpha = (tx + y, x).$$

Se $\mu_1 \in Af_2(R) - Bf_2(R)$, allora $\mu_1 = (a_1x + b_1y + c_1, a_2x + b_2y + c_2)$ con $a_i, b_i, c_i \in R$, $a_1b_2 - a_2b_1 \in R^*$ e $b_1 \neq 0$.

$$\mu_1 = (b_1x + c_1, b_2x + (a_2b_1 - b_2a_1)b_1^{-1}y + c_2) \circ (a_1b_1^{-1}x + y, x)$$

Passiamo ora agli automorfismi triangolari. Dimostriamo che esiste un insieme \mathcal{B} di rappresentanti di tutte le classi destre di $J_2(R)$ rispetto $Bf_2(R)$ meno la classe dell'identità e appartenenti a classi distinte e tali che se $\beta \in \mathcal{B}$, allora esiste $f(x) \in R[x], f(x) \neq 0$ per cui

$$\beta = (x, y + x^2 f(x)).$$

Preso $\mu_2 \in J_2(R) - Bf_2(R)$, $\mu_2 = (a_1x + b_1, a_2y + f(x))$ con $a_1, a_2 \in R^*$, $b_1 \in R$ e $f(x) \in R[x]$ della forma $r + sx + x^2g(x)$ per qualche $r, s \in R$ e $g(x) \in R[x]$ non nulla tale che. Riusciamo allora a scomporlo come

$$\mu_2 = (a_1x + b_1, a_2y + r + sx) \circ (x, y + x^2a_2^{-1}g(x))$$

Fissiamo due insieme di rappresentanti \mathcal{A} e \mathcal{B} .

Lemma 3.2. Se $\varphi \in TA_2(R) - Bf_2(R)$, esiste $m \ge 1$ ed esistono $\{\mu_i\}_{1 \le i \le m}$ alternativamente in \mathcal{A} e \mathcal{B} e $\gamma \in Bf_2(R)$ tali che

$$\varphi = \gamma \circ \mu_1 \circ \dots \circ \mu_m. \tag{3.1}$$

Dimostrazione. Per definizione di automorfismo moderato $\varphi = \lambda_1 \circ \cdots \circ \lambda_\ell$ con λ_i alternativamente affinità e automorfismi triangolari. Sostituiamo coppie di automorfismi adiacenti in modo ottenere una riscrittura con un unico automorfismo di $\mathrm{Bf}_2(R)$ a sinistra.

Prendiamo la coppia $(\lambda_i, \lambda_{i+1})$ tale che $\lambda_{i+1} \in \mathrm{Bf}_2(R)$ e $\lambda_i \notin \mathrm{Bf}_2(R)$ con indice più grande e la sostituiamo con $(\lambda'_i, \lambda'_{i+1})$ in modo che $\lambda'_i \in \mathrm{Bf}(R)$, $\lambda'_{i+1} \in \mathcal{A} \cup \mathcal{B}$ e $\lambda_i \circ \lambda_{i+1} = \lambda'_i \circ \lambda'_{i+1}$. Dopo al più $\ell - 1$ mosse di questo tipo otteniamo la scrittura voluta.

Dimostriamo ora che è unica.

Lemma 3.3. Siano $\alpha_1, \ldots, \alpha_{m-1} \in \mathcal{A}$ $e \beta_1, \ldots, \beta_m \in \mathcal{B}$ con $m \geq 1$ e sia $\varphi := \beta_m \circ \alpha_{m-1} \circ \cdots \circ \alpha_1 \circ \beta_1$, allora

$$\operatorname{mdeg}(\varphi) = \left(\prod_{j=1}^{m-1} \operatorname{deg}(\beta_j), \prod_{j=1}^{m} \operatorname{deg}(\beta_j)\right).$$

Dove la prima produttoria va intesa uguale a 1 se m=1. Inoltre detti $\tilde{\varphi}_1$ e $\tilde{\varphi}_2$ le componenti omogenee dei due polinomi coordinati di φ , allora $\tilde{\varphi}_1^{\deg(\beta_m)} \mid \tilde{\varphi}_2$ su R.

Dimostrazione. La dimostrazione procede per induzione. Notiamo prima di tutto che la tesi vale se m=1 per definizione degli elementi di \mathcal{B} .

Inoltre se $\varphi = (\varphi_1, \varphi_2)$ è un automorfismo tale che $\deg(\varphi_1) < \deg(\varphi_2)$, allora se $\alpha = (tx + y, x)$ con $t \in R$, $\operatorname{mdeg}(\alpha \circ \varphi) = (\deg(t\varphi_1 + \varphi_2), \deg(\varphi_1)) = (\deg(\varphi_2), \deg(\varphi_1))$. Mentre se $\deg(\varphi_1) > \deg(\varphi_2)$, allora se $\beta = (x, y + x^2 f(x))$ con $f(x) \in R[x]$, $f(x) \neq 0$ mdeg $(\beta \varphi) = (\deg(\varphi_1), \deg(\varphi_1) \deg(\beta))$. Vale anche che la componente omogenea di grado massimo del secondo polinomio coordinato è uguale ad una potenza della prima per il coefficiente del monomio di grado massimo di f. Perciò se

$$\operatorname{mdeg}(\beta_m \circ \alpha_{m-1} \circ \cdots \circ \alpha_1 \circ \beta_1) = \left(\prod_{j=1}^{m-1} \operatorname{deg}(\beta_j), \prod_{j=1}^m \operatorname{deg}(\beta_j) \right),$$

allora se compongo per α_m a sinistra

$$\operatorname{mdeg}(\alpha_m \circ \beta_m \circ \alpha_{m-1} \circ \cdots \circ \alpha_1 \circ \beta_1) = \left(\prod_{j=1}^m \operatorname{deg}(\beta_j), \prod_{j=1}^{m-1} \operatorname{deg}(\beta_j) \right),$$

componendo poi per β_{m+1}

$$\operatorname{mdeg}(\beta_{m+1} \circ \alpha_m \circ \beta_m \circ \alpha_m \circ \cdots \circ \alpha_1 \circ \beta_1) = \left(\prod_{j=1}^m \operatorname{deg}(\beta_j), \prod_{j=1}^{m+1} \operatorname{deg}(\beta_j) \right).$$

Dove questi due passaggi posso farli poiché sono soddisfatte le ipotesi sul multigrado. La seconda parte del lemma segue dal fatto che l'ultimo automorfismo per cui compongo a sinistra è un elemento di \mathcal{B} .

Corollario 3.4. Gli elementi di $Af_2(R) - Bf_2(R)$ possono essere scritti in modo unico con una fattorizzazione del tipo (3.1).

Dimostrazione. Supponiamo

$$\varphi = \gamma \circ \mu_1 \circ \cdots \circ \mu_m \in Af_2(R) - Bf_2(R),$$

con $\gamma \in \mathrm{Bf}_2(R)$ e i μ_i alternativamente in \mathcal{A} e \mathcal{B} . Un'affinità ha come multigrado (1,1), perciò, per il lemma precedente, non può esistere una sottosequenza $\beta_m \alpha_{m-1} \dots \alpha_1 \beta_1$ con $\alpha_i \in \mathcal{A}$ e $\beta_i \in \mathcal{B}$. Dunque m=1 e μ_1 è l'unico elemento di \mathcal{A} che rappresenta la classe destra di φ modulo $\mathrm{Bf}_2(R)$.

Corollario 3.5. Sia $\varphi = (\varphi_1, \varphi_2) \in TA_2(R)$ tale che $mdeg(\varphi) = (d_1, d_2)$. Se $\tilde{\varphi_1}$ e $\tilde{\varphi_2}$ sono le componenti omogenee di grado massimo. Allora

- a) $d_1|d_2$ oppure $d_2|d_1$.
- b) Se $\deg \varphi > 1$, allora
 - (i) Se $d_1 < d_2$, allora $\tilde{\varphi}_2 = c\tilde{\varphi}_1^{d_2/d_1}$, per qualche $c \in R$.
 - (ii) Se $d_2 < d_1$, allora $\tilde{\varphi_1} = c\tilde{\varphi_2}^{d_1/d_2}$, per qualche $c \in R$.
 - (iii) Se $d_1 = d_2$, allora esiste $\lambda \in Af_2(R)$ tale che $\deg \varphi_1' < \deg \varphi_2'$ dove $(\varphi_1', \varphi_2') := \lambda \circ \varphi$.

Lemma 3.6. Gli elementi di $TA_2(R) - Bf_2(R)$ possono essere scritti in modo unico con una fattorizzazione del tipo (3.1).

Per le affinità lo abbiamo già dimostrato. Supponiamo ora che un automorfismo moderato φ che non sia un'affinità abbia due scritture del tipo (3.1), ovvero esistono $m, m' \geq 1$ tali che $\varphi = \gamma \circ \mu_1 \circ \cdots \circ \mu_m = \gamma' \circ \mu'_1 \circ \cdots \circ \mu'_{m'}$. Allora

$$\gamma \circ \mu_1 \circ \cdots \circ \mu_m \circ (\mu'_{m'})^{-1} \circ \cdots \circ (\mu'_1)^{-1} \circ (\gamma')^{-1} = (x, y)$$

che si riscrive

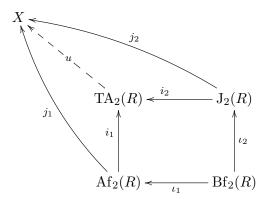
$$(\gamma')^{-1} \circ \gamma \circ \mu_1 \circ \cdots \circ \mu_m \circ (\mu'_{m'})^{-1} \circ \cdots \circ (\mu'_1)^{-1} = (x, y).$$

Gli elementi μ_m e $\mu_{m'}$ devono essere tutti e due in \mathcal{A} oppure \mathcal{B} , altrimenti otterrei una fattorizzazione non banale dell'identità. Inoltre $\mu_m \circ \mu_{m'}^{-1}$ deve essere un elemento di Bf₂(R) sempre perché altrimenti si otterrebbe una fattorizzazione non banale dell'identità del tipo (3.1). Perciò $\mu_m = \mu_{m'}$ per unicità dei rappresentanti.

Teorema 3.7 (Teorema di struttura). Sia R dominio e sia $Bf_2(R) := Af_2(R) \cap J_2(R)$, allora

$$TA_2(R) = Af_2(R) *_{Bf_2(R)} J_2(R).$$

Dimostrazione. Verifichiamo la proprietà universale del prodotto amalgamato. Siano i_1, i_2 le immersioni di $Af_2(R)$ e $J_2(R)$ in $TA_2(R)$ e ι_1, ι_2 le immersioni di $Bf_2(R)$ in $Af_2(R)$ e $J_2(R)$. Allora per ogni j_1, j_2 omomorfismi e X gruppo deve esistere un unico u, omomorfismo tale che:



Dimostriamo l'esistenza di u. Fisso \mathcal{A} e \mathcal{B} insiemi di rappresentanti come quelli dei lemmi precedenti. Su \mathcal{A} e su \mathcal{B} definiamo u come la restrizione di j_1 e j_2 rispettivamente. Gli omomorfismi j_1 e j_2 coincidano su $\mathrm{Bf}_2(R)$, perciò posso definire u su $\mathrm{Bf}_2(R)$. Si estende poi u utilizzando la fattorizzazione unica del tipo (3.1) per gli elementi di $\mathrm{TA}_2(R) - \mathrm{Bf}_2(R)$.

L'unicità di u segue semplicemente dal fatto che $\mathrm{TA}_2(R) = \langle \mathrm{Af}_2(R), \mathrm{J}_2(R) \rangle$. \square

3.3 Teoremi di Rentschler e di Jung, van der Kulk

Daremo ora una dimostrazione del teorema di Jung, van der Kulk in caratteristica zero, tramite il teorema di Rentschler. La dimostrazione originaria, data da Rentschler nel 1968 [1] utilizza i poligoni di Newton delle derivazioni localmente nilpotenti, rispetto alla gradazione standard di $\mathbb{K}[x,y]$. La dimostrazione è una rielaborazione della dimostrazione scritta nel 1998 da Makar-Limanov e reperibile in [12].

Sia \mathbb{K} di caratteristica zero e $A := \mathbb{K}[x, y]$. Vediamo alcuni lemmi necessari per dimostrare il teorema di Rentschler.

Lemma 3.8. Sia $D \in LND(A)$, allora $Ker(D) \supseteq \mathbb{K}$.

Dimostrazione. Supponiamo per assurdo $\operatorname{Ker}(D) = \mathbb{K}$. Iniziamo con il dimostrare l'esistenza di un elemento fondamentale. La derivazione D è localmente nilpotente, posso perciò prendere $v_D(\cdot)$ grado indotto. Se $f \in A - \mathbb{K}$ e $n := v_D(f) > 0$, $D^n(f) = a \in \operatorname{Ker}(D) - \{0\}$. Perciò per ipotesi a è invertibile in A. Sia ora $g := D^{n-1}(a^{-1}f)$, D(g) = 1. Il polinomio g è proprio il nostro elemento fondamentale. La derivazione D induce quindi un omomorfismo suriettivo $D|_{\mathbb{K}[q]} : \mathbb{K}[g] \to \mathbb{K}[g]$ per il corollario 2.13.

Prendiamo ora $h \in A$ tale che $D(h) \in \mathbb{K}[g]$. Per la suriettività di $D|_{\mathbb{K}[g]}$, esiste $h' \in \mathbb{K}[g]$ tale che D(h) = D(h'). Allora $h - h' \in \text{Ker}(D) = \mathbb{K}$, da cui $h \in \mathbb{K}[g]$. Tuttavia per ogni elemento $p \in A$ esiste il $n \in \mathbb{N}$ il più piccolo naturale tale che $D^n(p) \in \mathbb{K}[g]$. Un tale n esiste per la nilpotenza di D rispetto a ogni elemento di A. Ma se n > 0, allora $D^{n-1}(p) \in \mathbb{K}[g]$ per quanto visto in precedenza. Allora n = 0, ovvero $\mathbb{K}[x, y] = \mathbb{K}[g]$. Ma questo è assurdo, poiché l'anello di destra è PID, mentre quello di sinistra no.

Lemma 3.9. Sia $\omega := (\omega_1, \omega_2) \in \mathbb{N}^2$, tale che $gcd(\omega_1, \omega_2) = 1$. Preso $f \in A$, ω -omogeneo, con $deg_{\omega} f \in \omega_1 \omega_2 \mathbb{N}$, allora esiste un polinomio $g \in A$, standard-omogeneo, tale che $f = g(x^{\omega_2}, y^{\omega_1})$.

Dimostrazione. Sia $f_1 = ax^{s_1}y^{s_2}$ un monomio di f, con $s_1, s_2 \in \mathbb{N}$ e $a \in \mathbb{K}$. Poiché f è ω -omogeneo, $s_1\omega_1 + s_2\omega_2 = \deg_{\omega}(f) \in \omega_1\omega_2\mathbb{N}$ e per coprimalità di ω_1 e ω_2 , esistono $t_1, t_2 \in \mathbb{N}$ tali che $s_1 = t_1\omega_2$ e $s_2 = t_2\omega_1$.

Siano $u := x^{\omega_2}$ e $v := y^{\omega_1}$, allora $f_1 = au^{t_1}v^{t_2}$, perciò il grado rispetto alle variabili u e v, ovvero la somma di t_1 e t_2 , è uguale a $s_1/\omega_2 + s_2/\omega_1 = \deg_{\omega} f/(\omega_1\omega_2)$. Poiché questo grado non dipende da s_1 e s_2 , posso trovare $g(u,v) \in \mathbb{K}[u,v]$ standard-omogeneo di grado standard $\deg_{\omega}/(\omega_1\omega_2)$, tale che $f = g(x^{\omega_2}, y^{\omega_1})$.

Teorema 3.10 (Rentschler). Sia D_0 una derivazione non nulla, localmente nilpotente di A, allora esiste $G \in TA_2(\mathbb{K})$ e $h(x) \in \mathbb{K}[x]$ tali che

$$D_0^G = h(x)\partial_y.$$

Dimostrazione. Iniziamo con il notare che le funzioni localmente nilpotenti che annullano y sono derivazioni triangolari della forma $\mathbb{K}[x]\partial_y$. La dimostrazione di questo fatto l'abbiamo già data nel lemma 2.25. Perciò la tesi è equivalente a dimostrare che esiste un certo automorfismo G moderato tale che $x \in \text{Ker}(D_0^G)$, che a sua volta coincide con il dimostrare che per un certo G moderato $x \in G(\text{Ker}(D_0))$ per il 2.33. Possiamo riscriverla ancora in un altro modo: sia

$$\mathcal{S} := \bigcup_{G \in \mathrm{TA}_2(\mathbb{K})} G(\mathrm{Ker}(D_0)),$$

allora $x \in \mathcal{S}$. L'insieme \mathcal{S} è $\mathrm{TA}_2(\mathbb{K})$ -invariante, ovvero è unione delle orbite dei suoi elementi rispetto all'azione di $\mathrm{TA}_2(\mathbb{K})$.

Supponiamo per assurdo $x \notin \mathcal{S}$. Allora tutta l'orbita di x non è contenuta in \mathcal{S} ed in particolare $y \notin \mathcal{S}$, in quanto x = L(y) con L := (y, x).

L'insieme $\operatorname{Ker}(D_0) - \mathbb{K}$ è non vuoto per il lemma 3.8, perciò anche $\mathcal{S} - \mathbb{K}$ è non vuoto. Posso perciò prendere tra tutti gli elementi di $\mathcal{S} - \mathbb{K}$ l'elemento f che minimizza $\deg_x(\cdot) + \deg_y(\cdot)$. Sia $G \in \operatorname{TA}_2(\mathbb{K})$ tale che $f \in \operatorname{Ker}(D_0^G) - \mathbb{K}$, allora chiamiamo D la derivazione D_0^G . Notiamo che possiamo supporre $f \in (x, y)$ poiché possiamo sottrarre da f la costante f(0, 0), rimanendo in $\operatorname{Ker}(D) - \mathbb{K}$ e mantenendo costante $\deg_x(\cdot) + \deg_y(\cdot)$.

Vogliamo ora dimostrare il punto fondamentale del teorema, ovvero che esiste una ω -graduazione di A tale che l'addendo omogeneo di ω -grado massimo \tilde{f} di f, a meno di scambiare x con y, abbia una forma $\tilde{f} = a(x+by^t)^m$, con $a, b \in \mathbb{K}$ e $m, t \in \mathbb{N}$.

Scriviamo f = p(x) + q(y) + xyg(x, y) con $p(x) \in x\mathbb{K}[x]$ e $q(y) \in y\mathbb{K}[y]$. Notiamo subito che $p(x) \neq 0$ e $q(y) \neq 0$ perché altrimenti $f \in yA$ oppure $f \in xA$, ma Ker(D) è fattorialmente chiuso, f non è nullo e $x, y \notin \text{Ker}(D)$. Se $m = \deg_x p(x)$ e $n = \deg_y q(y)$ sia $e := \gcd(m, n)$, $\omega_1 = n/e$ e $\omega_2 = m/e$. Poniamo $\omega := (\omega_1, \omega_2)$, allora $\deg_\omega p(x) = m\omega_1 = (mn)/e = n\omega_2 = \deg_\omega q(y)$ e segue $\deg_\omega f \geq m\omega_1$.

Siano f, \tilde{F} e \tilde{D} gli addendi omogenei di ω -grado massimo di f, F e D rispettivamente. Per quanto visto nel lemma 2.30 \tilde{D} è localmente nilpotente e $\tilde{D}(\tilde{f})=0$. In più x e y, poiché non sono contenute in $\operatorname{Ker}(D)$ non sono contenute neanche in $\operatorname{Ker}(\tilde{D})$. Se $\deg_{\omega} f$ fosse diverso da $m\omega_1$, allora $\tilde{f}=xy\tilde{F}$, ma questo è assurdo per il fatto che $\operatorname{Ker}(\tilde{D})$ è fattorialmente chiuso, \tilde{f} è non nulla e $x,y\not\in\operatorname{Ker}(\tilde{D})$. Per il lemma 3.9, poiché \tilde{f} è ω -omogeneo con grado multiplo di ω_1 e ω_2 , con ω_1 e ω_2 coprimi allora esiste g standardomogeneo tale che $\tilde{f}(x,y)=g(x^{\omega_2},y^{\omega_1})$.

Sia ora $\overline{\mathbb{K}}$ la chiusura algebrica di \mathbb{K} e sia $\overline{D}: \overline{\mathbb{K}}[x,y] \to \overline{\mathbb{K}}[x,y]$ la derivazione $\overline{\mathbb{K}}$ -lineare uguale a \widetilde{D} sui generatori x,y. In particolare \overline{D} è non nulla, poiché \widetilde{D} è non nulla. Per di più \overline{D} è localmente nilpotente, perché è $\overline{\mathbb{K}}$ -lineare e nilpotente rispetto ai generatori. Su $\overline{\mathbb{K}}$, esiste $n \geq 1$ e $(c_i, d_i) \in \overline{\mathbb{K}}^2 - (0,0)$ tale che $g(x^{\omega_2},y^{\omega_1}) = \prod_{i=1}^e (c_i x^{\omega_2} + d_i y^{\omega_1})$. Per costruzione $\overline{D}(g(x^{\omega_2},y^{\omega_1})) = 0$ e poiché le costanti sono fattorialmente chiuse, allora tutti i $(c_i x^{\omega_2} + d_i y^{\omega_1})$ sono costanti rispetto a \overline{D} . Se esistessero due vettori (c_i,d_i) e (c_j,d_j) linearmente indipendenti, allora $\overline{D}(x^{\omega_2}) = 0$ e $\overline{D}(y^{\omega_1}) = 0$, assurdo. Per lo stesso motivo tutti i c_i e i d_i devono essere tutti non nulli. Allora esistono $a,b \in \overline{\mathbb{K}}^*$ tali che $\widetilde{f} = a(x^{\omega_2} + by^{\omega_1})^e$.

Lavoriamo sull'identità dedotta da $\bar{D}(\tilde{f}) = 0$, ovvero $\bar{D}(x^{\omega_2} + by^{\omega_1}) = 0$. Per l'identità di Leibniz diventa

$$\omega_2 x^{\omega_2 - 1} \bar{D}(y) + b\omega_1 y^{\omega_1 - 1} \bar{D}(x) = 0.$$

Questo ci dice due cose: la prima è che $b \in \mathbb{K}^*$, in quanto in $\overline{\mathbb{K}}(x,y)$ posso scrivere

$$b = -\frac{\omega_2 x^{\omega_2 - 1} \bar{D}(x)}{\omega_1 y^{\omega_1 - 1} \bar{D}(y)},$$

perciò $b \in \mathbb{K}(x,y) \cap \overline{\mathbb{K}}^* = \mathbb{K}^*$. La seconda è che $\omega_1 = 1$ oppure $\omega_2 = 1$, infatti se fosse $\omega_1 > 1$ e $\omega_2 > 1$ avremmo che che $\overline{D}(x) \in y\overline{\mathbb{K}}[x,y]$ e $\overline{D}(y) \in x\overline{\mathbb{K}}[x,y]$.

Queste sono proprio le condizioni con cui poter applicare il lemma 2.24, quindi $\bar{D}(x) = 0$ oppure $\bar{D}(y) = 0$. Assurdo. Perciò, a meno di scambiare x con y, possiamo supporre $\omega_2 = 1$. Segue e = m e $n = m\omega_1$ e soprattutto

$$\tilde{f} = a(x + by^{\omega_1})^e.$$

Scriviamo f in componenti omogenee, $f:=\sum_{j=0}^m f_j$ e prendiamo $G:=(x-by^{\omega_1},y)$. Notiamo che $\deg_{\omega}\left(G(f_j)\right)=j$ perché $x-by^{\omega_1}$ e y sono ω -omogenei di grado ω_1 , perciò $\deg_{\omega}(G(f))=e\omega_1$.

Vediamo come variano i gradi rispetto ad x e ad y passando da f in G(f). Innanzitutto $G(\tilde{f}) = ax^e$, perciò $\deg_x(f) = \deg_x(G(f)) = e$. Per il grado rispetto alla y sappiamo che $\deg_y(f) = n$. Limitiamo $\deg_y(G(f))$ notando che, poiché $\deg_\omega(y) = 1$, $\deg_y(G(f)) < \deg_\omega(G(f)) = e\omega_1 = n$. Perciò $G(f) \in \mathcal{S} - \mathbb{K}$ e $\deg_x(G(f)) + \deg_y(G(f)) < \deg_x(f) + \deg_y(f)$. Assurdo.

Teorema 3.11 (Jung). Gli automorfismi di \mathbb{K} algebra di $\mathbb{K}[x,y]$ sono moderati.

Dimostrazione. La derivazione $\frac{\mathrm{d}}{\mathrm{d}F_2}$, come abbiamo visto, è localmente nilpotente. Per il teorema di Rentschler esistono G moderato ed $f(x) \in \mathbb{K}[x]$ tali che

$$\left(\frac{\mathrm{d}}{\mathrm{d}F_2}\right)^G = f(x)\partial_y.$$

Detto H l'inverso di G,

$$\frac{\mathrm{d}}{\mathrm{d}F_2} = H(f(x)) \cdot \frac{\mathrm{d}}{\mathrm{d}H_2}.$$

Valutando in F_2 a sinistra ottengo 1 e a destra ottengo $H(f(x)) \cdot \frac{\mathrm{d}}{\mathrm{d}H_2}(F_2)$ dunque $f(x) \in \mathbb{K}[x]^*$, quindi $f(x) = c \in \mathbb{K}^*$.

Allora $\frac{d}{dF_2}$ e $\frac{d}{dH_2}$ differiscono per la moltiplicazione di uno scalare. Passando agli anelli delle costanti si ottiene

$$\mathbb{K}[F_1] = \mathbb{K}[H_1].$$

Per il corollario 1.5 esistono $a \in \mathbb{K}^*$ e $b \in \mathbb{K}$, tali che $F_1 = aH_1 + b$.

Allo stesso tempo $\frac{d}{dH_2}(F_2) = k^{-1}$ implica $F_2 = k^{-1}H_2 + g(H_1)$, con $g(t) \in \mathbb{K}[t]$. Perciò $(F_1, F_2) = (ax + b, c^{-1}y + g(x)) \circ (H_1, H_2)$, quindi F si scrive come composizione di due automorfismi moderati, il primo perché triangolare.

Enunciamo il risultato completo da noi dimostrato.

Teorema 3.12 (Jung, van der Kulk). Sia K un campo di caratteristica zero, allora

$$GA_2(\mathbb{K}) = Af_2(\mathbb{K}) *_{Bf_2(\mathbb{K})} J_2(\mathbb{K}).$$

3.4 Controesempio di Nagata, Shestakov, Umirbaev

Vediamo che il teorema di Jung, van der Kulk è falso se R è un dominio che non è un campo.

Supponiamo che a sia un elemento di R non zero che non sia un'unità. Sia $D := 2y\partial_x + a\partial_y$, allora $f := ax - y^2$ è una costante della derivazione. Sia $\sigma := \exp(fD)$, si verifica che

$$\sigma = (x + 2yf + af^2, y + af).$$

Le componenti omogenee di grado massimo sono ay^4 e $-ay^2$. Ma $(-ay^2)^2$ non divide ay^4 e questo va contro il corollario 3.5, perciò σ non è moderato. In particolare la sua fattorizzazione in $R[a^{-1}]$ è

$$\sigma = (y, x) \circ (x, y + a^{-1}x^2) \circ (y, x) \circ (x, y + a^2x) \circ (y, x) \circ (x, y - a^{-1}x^2) \circ (y, x).$$

Per $R = \mathbb{K}[z]$, a = z, questo è l'esempio dato da Nagata nel 1972 di un automorfismo non moderato. Poiché il gruppo $GA_2(\mathbb{K}[z])$ si immerge in $GA_3(\mathbb{K})$ tramite la mappa che manda $(f_1, f_2) \mapsto (f_1, f_2, z)$, Nagata congetturò che σ fosse selvaggio anche in $GA_3(\mathbb{K})$.

Nel 2002 i matematici Ualbai U. Umirbaev e Ivan P. Shestakov [5], [6] hanno dimostrato:

Teorema 3.13. Sia \mathbb{K} un campo di caratteristica zero e siano $GA_2(\mathbb{K}[z])$ e $TA_2(\mathbb{K}[z])$ in $GA_3(\mathbb{K})$, allora

$$GA_2(\mathbb{K}[z]) \cap TA_3(\mathbb{K}) = TA_2(\mathbb{K}[z]).$$

Questo fatto dà una risposta affermativa alla congettura di Nagata nel caso char $\mathbb{K}=0$. Perciò il problema dei generatori moderati ha una risposta negativa nel caso n=3 e la caratteristica è zero. La domanda è ancora aperta per $n\geq 4$.

Definizione 3.14. Diremo che un automorfismo $F \in \mathbb{K}[x_1, \dots, x_n]$ è *stabil*mente moderato se esiste un certo intero positivo m e un automorfismo moderato \bar{F} di $\mathbb{K}[x_1, \dots, x_{n+m}]$, tali che $\bar{F} = (F(x_1, \dots, x_n), x_{n+1}, \dots, x_{n+m})$.

Teorema 3.15 (Martha Smith). Sia $\bar{\sigma}: \mathbb{K}[x,y,z,t] \to \mathbb{K}[x,y,z,t]$ che estende σ , allora $\bar{\sigma}$ è moderato, ovvero l'automorfismo di Nagata è stabilmente moderato.

Dimostrazione. Siano $\tau_1 = \exp(-f\partial_t)$ e $\tau_2 = \exp(-tD)$, si verifica che $\tau_1 = (x, y, z, t - f)$ e $\tau_2 = (x - 2yt - zt^2, y - zt, z, t)$. Entrambi gli automorfismi sono perciò moderati. Voglio dimostrare che

$$\bar{\sigma} = \tau_1 \circ \tau_2 \circ \tau_1^{-1} \circ \tau_2^{-1}$$

da cui seguirebbe $\bar{\sigma}$ moderato.

Poiché l'azione di coniugio commuta con l'esponenziale, $\tau_1 \circ \tau_2 \circ \tau_1^{-1} = (\exp(-tD))^{\tau_1} = \exp(-(tD)^{\tau_1}) = \exp((f-t)D^{\tau_1})$. Ma τ_1 fissa $\mathbb{K}[x,y,z]$, perciò commuta con D, allora $D^{\tau_1} = D$. Inoltre, visto che f e t sono costanti per D, allora fD commuta con -tD, perciò $\bar{\sigma}\tau_2 = \exp(fD) \circ \exp(-tD) = \exp((f-t)D)$. Avrò allora

$$\bar{\sigma} \circ \tau_2 = \tau_1 \circ \tau_2 \circ \tau_1^{-1}$$

quindi la tesi.

Problema (dei generatori stabilmente moderati). $Sia \mathbb{K}$ un campo di caratteristica zero. É vero che tutti gli automorfismi polinomiali di \mathbb{K}^n sono stabilmente moderati?

Questa domanda non ha ancora una risposta per ogni $n \geq 3$. Il problema è molto interessante in quanto non è ancora stata dimostrata l'esistenza di automorfismi non stabilmente moderati neanche a coefficienti in un dominio.

Nel 2012 i matematici Joost Berson, Arno van den Essen, e David Wright hanno pubblicato un articolo in cui mostrano che per ogni campo (anche di caratteristica positiva), gli automorfismi in $GA_3(\mathbb{K})$ che fissano una coordinata (come quello di Nagata), sono tutti stabilmente moderati e in particolare se il campo ha caratteristica zero diventano moderati con l'aggiunta di tre variabili [7].

Capitolo 4

Problema di linearizzazione

In questo capitolo presenteremo il problema di linearizzazione. Inizieremo con alcune definizioni e teoremi sulle varietà algebriche affini e i gruppi algebrici. Successivamente introdurremo alcuni concetti sulle rappresentazioni per arrivare a studiare le azioni regolari dello spazio affine. Alla fine parleremo del problema di linearizzazione, della congettura di Kambayashi e del teorema di Kambayashi.

4.1 Varietà e gruppi algebrici affini

In questa sezione richiameremo le definizioni base delle varietà algebriche affini. Faremo particolare attenzione al prodotto di varietà e la rispettiva K-algebra di funzioni regolari.

Sia \mathbb{K} un campo algebricamente chiuso di caratteristica zero e sia $A := \mathbb{K}[x_1, \ldots, x_n]$. Interpretiamo gli elementi di A come funzioni da \mathbb{K}^n in \mathbb{K} , definendo $f(P) = f(a_1, \ldots, a_n)$, dove $f \in A$ e $P \in \mathbb{K}^n$ con $P = (a_1, \ldots, a_n)$. Se $T \subseteq A$, possiamo parlare degli zeri comuni di tutti gli elementi di T, ovvero dell'insieme

$$Z(T) := \{ P \in \mathbb{K}^n | f(P) = 0 \text{ per tutti gli elementi } f \in T \}.$$

Definizione 4.1. Un sottoinsieme X di \mathbb{K}^n è detto *insieme algebrico* se esiste un sottoinsieme $T \subseteq A$ tale che X = Z(T).

Nel caso $T=\{f\}$ scriveremo per comodità Z(f). Si dimostra che gli insiemi algebrici sono i chiusi di una topologia su \mathbb{K}^n detta topologia di Zariski. Denoteremo con $\mathbb{A}^n_{\mathbb{K}}$ lo spazio topologico così ottenuto.

Definizione 4.2. Sia $f \in A$, chiameremo aperto principale e lo denoteremo U^f , il complementare del chiuso Z(f).

Definizione 4.3. Chiamiamo varietà algebrica quasi-affine (o semplicemente varietà quasi-affine) un sottospazio topologico di $\mathbb{A}^n_{\mathbb{K}}$ che è intersezione di un chiuso e di un aperto dello spazio ambiente.

Vediamo di definire delle mappe tra varietà quasi-affine. Sia X un varietà quasi-affine, iniziamo a prendere mappe "algebriche" da X in \mathbb{K} .

Definizione 4.4. Una funzione $f: X \to \mathbb{K}$ è regolare in un punto $P \in X$ se esiste un intorno aperto U di P e polinomi $g, h \in A$ tali che $P \in U^h$, e f = g/h su U. Nell'ultima uguaglianza i polinomi sono interpretati come funzioni a valori in \mathbb{K} .

Diremo inoltre che f è regolare in X se è regolare per ogni punto di X.

Si dimostra che una funzione regolare di X è una funzione continua da X a $\mathbb{A}^1_{\mathbb{K}}$ (se si pensa \mathbb{K} come $\mathbb{A}^1_{\mathbb{K}}$).

Esempio 4.5. Le funzioni costanti sono funzioni regolari. Altre funzioni regolari sono le funzione coordinate, ovvero le funzioni x_i che associano ad un elemento di \mathbb{K}^n la sua *i*-esima coordinata.

L'insieme di funzioni regolari ha una naturale struttura di \mathbb{K} -algebra, con \mathbb{K} immerso nelle funzioni costanti. Difatti la somma è il prodotto di funzioni continue rimane continuo nella topologia di Zariski. Anche la proprietà locale passa alla somma e al prodotto. Indicheremo con \mathcal{O}_X tale \mathbb{K} -algebra.

Definizione 4.6. Date due varietà quasi-affini X e Y, diremo che un *morfismo di varietà* è una mappa continua $\varphi: X \to Y$ tale che per ogni funzione regolare f di Y, la funzione $f \circ \varphi$ è ancora una funzione regolare di X.

Diremo che φ è un *isomorfismo* se esistono due morfismi ψ_1 e ψ_2 tali che $\psi_1 \circ \varphi = \mathrm{id}_X$ e $\varphi \circ \psi_2 = \mathrm{id}_Y$. Diremo inoltre che due varietà quasi-affini sono *isomorfe* se esiste un isomorfismo che va da una all'altra.

Notiamo che in particolare, per la definizione precedente, se ψ è un morfismo, le funzioni $\psi_i := x_i \circ \psi$ sono funzioni regolari al variare di i. Si dimostra che è vero anche il contrario: se le ψ_i sono funzioni regolari per ogni i, allora ψ è un morfismo.

Se ψ è un morfismo da X a Y, posso definire la mappa ψ^{\sharp} che va da \mathcal{O}_Y a \mathcal{O}_X e che manda $f \in \mathcal{O}_Y$ in $f \circ \psi$. Questa mappa è un omomorfismo di anelli e fissa le costanti, perciò è un omomorfismo di \mathbb{K} -algebre. In particolare se X e Y sono varietà quasi-affini isomorfe, allora le \mathbb{K} -algebre delle funzioni regolari sono isomorfe.

Definizione 4.7. Diremo che una varietà quasi-affine è un varietà affine se è isomorfa ad una varietà quasi-affine che è un chiuso di $\mathbb{A}^n_{\mathbb{K}}$.

Un esempio non banale di varietà affine è una qualsiasi varietà quasiaffine che è un aperto fondamentale di $\mathbb{A}^n_{\mathbb{K}}$.

Lemma 4.8. Se U^f è un aperto fondamentale di $\mathbb{A}^n_{\mathbb{K}}$, allora è isomorfo come varietà ad un insieme algebrico Y di $\mathbb{A}^{n+1}_{\mathbb{K}}$.

Dimostrazione. Prendiamo la mappa $\varphi: U^f \to \mathbb{A}^{n+1}_{\mathbb{K}}$ tale che $\varphi(a_1,\ldots,a_n) = (a_1,\ldots,a_n,1/f(a_1,\ldots,a_n))$. Poiché tutte le φ_i sono funzioni regolari, allora φ è un morfismo. L'immagine di φ è certamente contenuta in $Y:=Z(y_{n+1}f(y_1,\ldots,y_n)-1)$. Se ψ è la proiezione di Y in $\mathbb{A}^n_{\mathbb{K}}$ delle prime n coordinate, ovvero la mappa che manda (a_1,\ldots,a_{n+1}) in (a_1,\ldots,a_n) , innanzitutto possiamo comporre $\psi \circ \varphi$, ottenendo l'identità su U^f . Notiamo poi che l'immagine di ψ è contenuta in U^f , in quanto la prima n-upla di coordinate di Y non può annullare f, altrimenti $a_{n+1}f(a_1,\ldots,a_n)-1$ non avrebbe soluzioni. Allora posso comporre $\varphi \circ \psi$ e questa volta ottengo l'identità su Y. Perciò U^f e Y sono isomorfi, ovvero U^f è una varietà affine. \square

Vediamo come i sottoinsiemi di $\mathbb{A}^n_{\mathbb{K}}$ sono relazionati con gli ideali di $\mathbb{K}[x_1,\ldots,x_n]$. Sia $Y\subseteq\mathbb{K}^n$, definiamo l'ideale di Y, l'ideale

$$I(Y) := \{ f \in \mathbb{K}[x_1, \dots, x_n] \mid f(P) = 0 \text{ per ogni } P \in Y \}.$$

Poiché siamo nell'ipotesi di campo algebricamente chiuso possiamo sfruttare il seguente teorema:

Teorema 4.9 (Nullstellensatz). Sia \mathbb{K} un campo algebricamente chiuso e sia $n \geq 0$ un intero, sia T un sottoinsieme di $\mathbb{K}[x_1, \ldots, x_n]$ e sia I l'ideale generato da T. Allora $I(Z(T)) = \sqrt{I}$, in particolare se $V(E) = \emptyset$, allora I = (1).

Corollario 4.10. Vi è una corrispondenza biunivoca tra gli insiemi algebrici di $\mathbb{A}^n_{\mathbb{K}}$ e gli ideali radicali di $\mathbb{K}[x_1,\ldots,x_n]$ che rovescia le inclusioni che manda un insieme algebrico Y in I(Y) e \mathfrak{g} ideale di $\mathbb{K}[x_1,\ldots,x_n]$ in $Z(\mathfrak{g})$.

Possiamo ora calcolare l'algebra delle funzioni regolari di un chiuso di Zariski:

Corollario 4.11. Sia X un insieme algebrico, allora

$$\mathcal{O}_X \simeq \mathbb{K}[x_1,\ldots,x_n]/I(X).$$

Quindi ad esempio la \mathbb{K} -algebra di funzioni regolari di $\mathbb{A}^n_{\mathbb{K}}$ è $\mathbb{K}[x_1,\ldots,x_n]$. In generale vale che per ogni insieme algebrico l'algebra è generata dalle funzioni coordinate.

Definiamo ora il prodotto di varietà quasi-affini. Siano $C_1:=Z(T_1)\subseteq \mathbb{A}^n_{\mathbb{K}}$ e $C_2:=Z(T_2)\subseteq \mathbb{A}^m_{\mathbb{K}}$ due chiusi di Zariski, allora l'insieme $C_1\times C_2$ è un chiuso di Zariski di $\mathbb{A}^{n+m}_{\mathbb{K}}$ e ottenuto come l'insieme degli zeri comuni di T_1 con variabili in x_1,\ldots,x_n e di T_2 con variabili x_{n+1},\ldots,x_{n+m} . Perciò $\mathbb{A}^{n+m}_{\mathbb{K}}$ ha una topologia più fine del prodotto topologico $\mathbb{A}^n_{\mathbb{K}}$ e $\mathbb{A}^m_{\mathbb{K}}$.

Definizione 4.12. Se $X = C_1 \cap U_1 \subseteq \mathbb{A}^n_{\mathbb{K}}$ e $Y = C_2 \cap U_2 \subseteq \mathbb{A}^m_{\mathbb{K}}$ sono varietà quasi-affini, con C_1 , C_2 chiusi e U_1 , U_2 aperti, possiamo definire allora la varietà quasi-affine prodotto $X \times Y$, la varietà ottenuta dall'intersezione di $C_1 \times C_2$ con $U_1 \times U_2$. I due insiemi sono infatti rispettivamente un chiuso e un aperto di $\mathbb{A}^{n+m}_{\mathbb{K}}$ per quanto abbiamo visto.

Osservazione. Se esiste un isomorfismo $\psi_1: X \to X'$ e un isomorfismo $\psi_2: Y \to Y'$, allora la mappa (ψ_1, ψ_2) è ancora un morfismo perché ogni coordinata è regolare ed in particolare sarà un isomorfismo.

Da questo segue ad esempio che se X e Y sono varietà affini, allora $X \times Y$ è ancora una varietà affine.

Lemma 4.13. Siano X e Y due varietà affini, allora $\mathcal{O}_X \otimes_k \mathcal{O}_Y \simeq \mathcal{O}_{X \times Y}$. Inoltre se X e Y sono chiusi di Zariski, allora l'isomorfismo è quello che manda $f(x) \otimes g(y)$ in f(x)g(y).

Dimostrazione. Possiamo dimostrare l'isomorfismo direttamente per insiemi algebrici, poiché varietà isomorfe hanno \mathbb{K} -algebre isomorfe. Se $\alpha: \mathcal{O}_X \otimes_k \mathcal{O}_Y \to \mathcal{O}_{X\times Y}$ che manda $f(x)\otimes g(y)$ in f(x)g(y). La mappa è suriettiva in quanto le funzioni coordinate sono contenute nell'immagine e abbiamo visto che queste funzioni generano tutto $\mathcal{O}_{X\times Y}$. Dimostriamo che è anche iniettiva, sia $\sum_{i\in I} f_i \otimes g_i \neq 0$ un elemento di $\mathcal{O}_X \otimes \mathcal{O}_Y$, dove possiamo supporre g_i linearmente indipendenti in \mathcal{O}_Y . Se l'immagine fosse zero, allora per ogni $x_0 \in X$, $\sum_{i\in I} f_i(x_0)g_i(y) = 0$ come funzione in \mathcal{O}_Y , perciò $f_i(x_0) = 0$ per ogni i. Allora, poiché questo vale per ogni $x_0 \in X$, le f_i sono tutte funzioni regolari nulle di X. Perciò l'elemento iniziale è zero, quindi la tesi.

Definizione 4.14. Un gruppo algebrico affine (o semplicemente gruppo algebrico) è una varietà affine G insieme ad un elemento $e \in G$ e a due morfismi di varietà quasi-affini $\mu: G \times G \to G$, $\iota: G \to G$ che danno a G una struttura di gruppo. Un morfismo $f: G \to H$ di gruppi algebrici è un morfismo di varietà quasi-affini che è anche un omomorfismo di gruppi.

Esempio 4.15. (i) Il gruppo additivo \mathbb{G}_a , ovvero lo spazio affine \mathbb{A}^1 con l'operazione di somma.

- (ii) Il gruppo moltiplicativo \mathbb{G}_m , ovvero la varietà affine $\mathbb{A}^1 \setminus \{0\}$ con l'operazione di prodotto è il gruppo moltiplicativo \mathbb{G}_m .
- (iii) Il gruppo $GL_n(\mathbb{K})$ è un aperto principale di \mathbb{A}^{n^2} , corrispondente al complementare del luogo degli zeri del polinomio $\det(\cdot)$. I coefficienti del prodotto di due matrici sono ottenuti da polinomi a valori nei coefficienti di ciascuna delle due. Anche l'inverso è un morfismo della varietà in quanto i coefficienti della matrice inversa si ottengono con polinomi diviso per il determinante. Ma $GL_n(\mathbb{K})$ è proprio l'aperto principale di $\det(\cdot)$.
- (iv) Il gruppo $SL_n(\mathbb{K})$ è un insieme algebrico, corrispondente agli zeri comuni di $det(\cdot) 1$ e l'operazione di gruppo e l'inverso sono morfismi per quanto visto in $GL_2(k)$.

4.2 Rappresentazioni

Iniziamo ad introdurre il concetto di rappresentazione di un gruppo G su uno spazio vettoriale V su \mathbb{K} . Per adesso non chiederemo che V sia di dimensione finita.

Definizione 4.16. Sia $\rho: G \mapsto \operatorname{GL}(V)$ un omomorfismo di gruppi, diremo che ρ agisce linearmente su V, che V è un $\mathbb{K}[G]$ -modulo e che la coppia (V, ρ) è una rappresentazione di G su V. Se W è un sottospazio vettoriale di V che è G-invariante, ovvero che è unione delle orbite dei sui elementi, allora diremo che W è un $\mathbb{K}[G]$ -sottomodulo.

Se V è un $\mathbb{K}[G]$ -modulo diremo che V è semplice se non ha $\mathbb{K}[G]$ -sottomoduli diversi da 0 e sè stesso. Inoltre diremo che se per ogni $\mathbb{K}[G]$ -sottomodulo W di V, esiste un completamento, ovvero un $\mathbb{K}[G]$ -sottomodulo W' tale che $V = W \oplus W'$, allora V è semisemplice. Chiameremo le rispettive rappresentazioni semplici e semisemplici.

Osservazione. La somma di $\mathbb{K}[G]$ -sottomoduli è ancora un $\mathbb{K}[G]$ -sottomodulo e lo stesso vale per l'intersezione.

Lemma 4.17. Ogni $\mathbb{K}[G]$ -sottomodulo di un modulo semisemplice è semi-semplice.

Dimostrazione. Sia V un $\mathbb{K}[G]$ -modulo semisemplice e sia V' un suo $\mathbb{K}[G]$ -sottomodulo. Se W è un $\mathbb{K}[G]$ -sottomodulo di V', allora esiste W' G-invariante tale che $V = W \oplus W'$. Quindi $V' = W \oplus (V' \cap W')$, ma $V' \cap W'$ è ancora G-invariante. Perciò W ha un completamento in V'. Visto che questo vale per tutti i $\mathbb{K}[G]$ -sottomoduli di V', abbiamo dimostrato che V' è semisemplice.

Lemma 4.18. Un $\mathbb{K}[G]$ -modulo V è semisemplice se e solo se è somma di $\mathbb{K}[G]$ -moduli semplici.

Dimostrazione. Iniziamo a dimostrare la " \Rightarrow ". Sia S la somma dei $\mathbb{K}[G]$ -sottomoduli semplici di V. Supponiamo che esista un elemento $v \in V$ che non appartiene a S. Sia S' la somma dei $\mathbb{K}[G]$ -moduli che non contengono v. Sia T' il complementare di S', vogliamo dimostrare che è un $\mathbb{K}[G]$ -modulo semplice. Notiamo che un $\mathbb{K}[G]$ -sottomodulo non nullo di T' contiene v, altrimenti sarebbe contenuto in S'. Supponiamo per assurdo che esista $U_1 \subsetneq T'$ un $\mathbb{K}[G]$ -modulo diverso da zero. Allora U_2 , il complementare di U_1 in T' (che esiste in quanto T' è semisemplice 4.17) è un $\mathbb{K}[G]$ -modulo disgiunto da U_1 e diverso da zero per costruzione. Ma U_1 e U_2 sono allora $\mathbb{K}[G]$ -moduli non nulli di T', perciò v appartiene ad entrambi. Assurdo.

Dimostriamo ora la "\(\infty\)". Supponiamo $V = \sum_{i \in I} V_i$, ove ogni V_i è un $\mathbb{K}[G]$ -modulo semplice. Sia W un $\mathbb{K}[G]$ -sottomodulo di V, dimostriamo che esiste un complementare. Sia W' il $\mathbb{K}[G]$ -modulo ottenuto dalla somma di

 $\mathbb{K}[G]$ -sottomoduli a intersazione banale con W. Lo spazio W' eredita la proprietà di avere intersezione banale con W. Se S := W + W', allora $S \cap V_i$ può essere uguale a V_i o a 0 per ogni i, poiché per ipotesi i V_i sono semplici. Se per assurdo, $S \cap V_j$ fosse banale per un qualche $j \in I$, allora V_j avrebbe intersezione banale anche con W. Quindi $V_j \subseteq W'$ per come abbiamo costruito W. Assurdo.

Teorema 4.19 (Maschke). Sia \mathbb{K} un campo e G un gruppo finito tale che la caratteristica del campo non divide l'ordine del gruppo, allora ogni rappresentazione del gruppo è semisemplice.

Dimostrazione. Sia V un $\mathbb{K}[G]$ -modulo e W un $\mathbb{K}[G]$ -sottomodulo. Sia U un qualsiasi completamento di W (in generale non sarà un $\mathbb{K}[G]$ -modulo), allora chiamiamo $\varphi: W \oplus U \to W$ la proiezione sul primo addendo. Sia ora $\psi: V \to W$ tale che

$$\psi(v) := \frac{1}{|G|} \sum_{g \in G} g^{-1} \varphi(gv).$$

La mappa ψ è un $\mathbb{K}[G]$ -morfismo in quanto è \mathbb{K} -lineare e per ogni $h \in G$,

$$\psi(hv) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \varphi(ghv) = \frac{1}{|G|} \sum_{\bar{g} \in G} h\bar{g}^{-1} \varphi(\bar{g}v) = h \frac{1}{|G|} \sum_{\bar{g} \in G} \bar{g}^{-1} \varphi(\bar{g}v).$$

Inoltre ψ è l'identità su W, perciò $\operatorname{Im}(\psi) = W$ e ψ è idempotente. Allora $V = \operatorname{Im}(\psi) \oplus \ker(\psi) = W \oplus \ker(\psi)$ e $\ker(\psi)$ è un G-modulo poiché ψ è un $\mathbb{K}[G]$ -morfismo.

4.3 Rappresentazioni razionali e regolari

Sia G un gruppo algebrico e V un \mathbb{K} -spazio vettoriale finito dimensionale.

Definizione 4.20. Sia $\rho: G \to \operatorname{GL}(V)$ una rappresentazione che è anche un morfismo di varietà, diremo che ρ è una rappresentazione razionale di G in V e diremo che V è un G-modulo. Diremo inoltre che un sottospazio vettoriale W di V è un G-sottomodulo se è G-invariante. Utilizzeremo le espressioni di G-modulo semplice e semisemplice e di rappresentazione razionale semplice e semisemplice in analogia con la notazione usata per le rappresentazioni.

Definizione 4.21. Diremo che un gruppo algebrico G è linearmente riduttivo (o semplicemente riduttivo) se ogni G-modulo è semisemplice.

Esempio 4.22. Grazie al teorema di Maschke abbiamo dimostrato dimostrato che i gruppi finiti sono riduttivi. Con un po' più di fatica si può dimostrare che anche i gruppi G_m , $GL_n(\mathbb{K})$ e $SL_n(\mathbb{K})$ sono riduttivi ([10]). Vedremo in seguito che invece G_a non è riduttivo.

Un lemma che ci tornerà utile per dimostrare che un gruppo è riduttivo è il seguente.

Lemma 4.23. Se G è un gruppo riduttivo e H un gruppo algebrico e se esiste $f: G \to H$, morfismo di gruppi algebrici suriettivo, allora H è riduttivo.

Dimostrazione. Supponiamo per assurdo H non riduttivo, allora esiste una rappresentazione razionale (V, ρ) di H non semisemplice. Poiché f e ρ sono morfismi di gruppi algebrici, anche $\rho \circ f$ è un morfismo di gruppi algebrici. Perciò $(V, \rho \circ f)$ è una rappresentazione razionale di G. Ma l'immagine di ρ e di $f \circ \rho$ sono le stesse, perciò le orbite delle due azioni sono tutte uguali e quindi gli spazi G-invarianti e H-invarianti sono uguali. Questo vuol dire che anche $(V, \rho \circ f)$ non è una rappresentazione semisemplice. Assurdo. \square

Sia V un \mathbb{K} -spazio vettoriale (anche di dimensione infinita).

Definizione 4.24. Diremo che una rappresentazione $\rho: G \to \operatorname{GL}(V)$ è localmente finita se per ogni sottospazio W finito dimensionale, GW è di dimensione finita. Diremo inoltre che una rappresentazione localmente finita è localmente razionale se per ogni sottospazio W finito dimensionale, la rappresentazione indotta su GW è razionale.

Definizione 4.25. Sia X una varietà algebrica, e sia G un gruppo algebrico, dico che X è una G-varietà se esiste $\rho: G \times X \to X$ azione che è anche un morfismo di varietà. Chiameremo ρ azione algebrica.

Chiameremo rappresentazione regolare di G su \mathcal{O}_X , la rappresentazione $\sigma: G \times \mathcal{O}_X \to \mathcal{O}_X$ tale che $\sigma_g = \rho_{g-1}^{\sharp}$.

Lemma 4.26. La rappresentazione regolare σ di una G-varietà X è localmente razionale.

Dimostrazione. Facciamo vedere inizialmente che σ è localmente finita. Sia $\rho^{\sharp}: \mathcal{O}_X \to \mathcal{O}_G \otimes \mathcal{O}_X$ l'omomorfismo di K-algebre indotto da ρ . Ci basta dimostrare che per ogni elemento f di \mathcal{O}_X , lo spazio vettoriale dell'orbita di σ è di dimensione finita. Ma $\rho^{\sharp}(f) = \sum_{i=1}^m p_i \otimes f_i$, con $p_i \in \mathcal{O}_G$ e $f_i \in \mathcal{O}_X$, perciò per ogni $g \in G$, $\sigma_g(f)(\cdot) = \rho^{\sharp}(f)(g^{-1}, \cdot) = \sum_{i=1}^m p_i(g^{-1})f_i(\cdot)$, quindi $\sigma_g(f) \in \langle f_1, \ldots, f_m \rangle$. Per dimostrare che σ è localmente razionale procediamo in modo analogo. Sia $\{h_1, \ldots, h_\ell\}$ una base di GW, allora per ogni $h_i \rho^{\sharp}(h_i) = \sum_{j=1}^\ell r_j \otimes h_j$, con $r_j \in \mathcal{O}_G$, perciò $\sigma_g(h_i) = \sum_{j=1}^\ell r_j(g^{-1})h_j$.

Corollario 4.27. Se G è un gruppo riduttivo, allora

- (i) Ogni $\mathbb{K}[G]$ -modulo W finito dimensionale di \mathcal{O}_X è un G-modulo ;
- (ii) \mathcal{O}_X è un $\mathbb{K}[G]$ -modulo semisemplice.

Dimostrazione. La (i) segue direttamente dal teorema. Per la (ii), dimostriamo che \mathcal{O}_X è somma di $\mathbb{K}[G]$ -moduli semplici. Sia $f \in \mathcal{O}_X$, allora l'azione di G su $G\langle f \rangle$ è razionale. Ma G è riduttivo, perciò $G\langle f \rangle$ si scrive come somma di G-moduli semplici, ma per la (i) un G-modulo semplice è un $\mathbb{K}[G]$ -modulo semplice. Perciò ogni elemento di \mathcal{O}_X appartiene ad una somma finita di $\mathbb{K}[G]$ -moduli semplici, perciò \mathcal{O}_X è semisemplice per il lemma 4.18.

4.4 Problema di linearizzazione

Adesso abbiamo tutto quello che ci serve per studiare il problema di linearizzazione.

Problema. Sia ρ un'azione algebrica di un gruppo algebrico G su $\mathbb{A}^n_{\mathbb{K}}$. Esiste un automorfismo $F \in GA_n(\mathbb{K})$, tale che $F\rho_g^{\sharp}F^{-1} \in GL_n(\mathbb{K})$ per ogni $g \in G$

Chiamiamo $\rho^{\sharp}(G) < GA_n(\mathbb{K})$ il gruppo degli automorfismi ρ_g^{\sharp} al variare di $g \in G$.

Fissiamo n=2 e utilizziamo il teorema di Jung, van der Kulk, dunque $\rho^{\sharp}(G) < \mathrm{Af}_2(\mathbb{K}) *_{\mathrm{Bf}_2(\mathbb{K})} \mathrm{J}_2(\mathbb{K}).$

Ci viene ora in aiuto un importante teorema sui prodotti amalgamati.

Definizione 4.28. Siano G e H gruppi e sia K un sottogruppo di $G*_{G\cap H}H$, diciamo che K è *limitato* se esiste M naturale tale per cui in ogni classe di K esiste un rappresentante con un numero di lettere minore o uguale a M.

Teorema 4.29. Ogni sottogruppo limitato di $G *_{G \cap H} H$ è coniugato ad un sottogruppo di G oppure ad un sottogruppo di H.

Dimostrazione. La dimostrazione di questo fatto si può trovare su [9], sezione 1.4.3, Teorema 8.

Dimostriamo ora il lemma mancante.

Lemma 4.30. Il sottogruppo $\rho^{\sharp}(G) < \operatorname{Af}_{2}(\mathbb{K}) *_{\operatorname{Bf}_{2}(\mathbb{K})} J_{2}(\mathbb{K}) \ \dot{e} \ limitato.$

Dimostrazione. Nella sezione precedente abbiamo visto che le rappresentazioni regolari sono localmente finite. Perciò se W è un sottospazio vettoriale di $\mathcal{O}_{\mathcal{A}^n_{\mathbb{K}}} = \mathbb{K}[x,y]$, allora GW è finito dimensionale. Preso $W := \langle x,y \rangle$, GW finito dimensionale equivale a dire che il grado degli automorfismi di $\rho^{\sharp}(G)$

è limitato. Difatti ricordiamo che se $\rho_g^{\sharp} = (F_1, F_2)$, allora $\rho_g^{\sharp}(x) = F_1$ e $\rho_g^{\sharp}(y) = F_2$.

Fissiamo ora \mathcal{A} e \mathcal{B} come nella sezione 3.2.Prendiamo un automorfismo ρ_g^{\sharp} e supponiamo che soddisfi le ipotesi del Lemma 3.3, ovvero supponiamo che esistano $\alpha_1, \ldots, \alpha_{m-1} \in \mathcal{A}$ e $\beta_1, \ldots, \beta_m \in \mathcal{B}$ con $m \geq 1$ tali che $\varphi := \beta_m \circ \alpha_{m-1} \circ \cdots \circ \alpha_1 \circ \beta_1$, allora

$$\mathrm{mdeg}(\rho_g^{\sharp}) = \left(\prod_{j=1}^{m-1} \deg(\beta_j), \prod_{j=1}^{m} \deg(\beta_j)\right).$$

Ma $2 \leq \deg(\beta_j)$, perciò $2^m \leq \deg(\rho_g^{\sharp})$, da cui $m \leq \log_2(\deg(\rho_g^{\sharp}))$.

Stime analoghe si ottengono anche cambiando l'ordine degli α_j e β_j oppure aggiungendo a sinistra un elemento $\gamma \in \mathrm{Bf}_2(\mathbb{K})$. Ma i gradi dei ρ_g^{\sharp} al variare di $g \in G$ sono limitati, perciò il numero di lettere prese da \mathcal{A} , \mathcal{B} oppure $Bf_2(\mathbb{K})$ è più piccolo di un naturale M.

Abbiamo così dimostrato il seguente teorema.

Teorema 4.31 (Kambayashi). Sia G un gruppo algebrico che agisce su $\mathbb{A}^2_{\mathbb{K}}$, allora esiste $F \in GA_2(\mathbb{K})$ tale che $F\rho^{\sharp}(G)F^{-1} < Af_2(\mathbb{K})$ oppure $F\rho^{\sharp}(G)F^{-1} < J_2(\mathbb{K})$.

Questo risultato semplifica molto lo studio delle azioni regolari su $\mathbb{K}[x,y]$. In particolare vale il seguente corollario.

Teorema 4.32. Sia \mathbb{K} un campo algebricamente chiuso di caratteristica zero e sia G un gruppo algebrico affine, linearmente riduttivo che agisce su $\mathbb{A}^2_{\mathbb{K}}$, allora esiste $F \in GA_2(\mathbb{K})$ tale che $F \rho^{\sharp}(G)F^{-1} < GL_2(\mathbb{K})$.

Impiegheremo il resto della sezione per dimostrare questo teorema. Per prima cosa un'azione linearizzabile ha almeno un punto fisso. Vediamo che questa condizione si verifica per i sottogruppi riduttivi del gruppo delle affinità.

Lemma 4.33. Sia G un sottogruppo di $Af_n(\mathbb{K})$ riduttivo, allora l'azione naturale in \mathbb{K}^n ha almeno un punto fisso.

Dimostrazione. Se g è un'affinità esiste $M_g \in \mathcal{M}_n(\mathbb{K})$ e $\underline{b}_q \in \mathbb{K}^n$ tale che

$$g \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = M_g \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \underline{b}_g.$$

Sia $\{e_1,\ldots,e_{n+1}\}$ la base canonica di \mathbb{K}^{n+1} e sia $\rho: G \to \mathrm{GL}_{n+1}(\mathbb{K})$ la rappresentazione tale che

$$\rho(g) = \begin{pmatrix} M_g & \underline{b}_g \\ \hline 0 & \cdots & 0 & 1 \end{pmatrix},$$

dove la matrice si intende nella base canonica. Si verifica che la mappa ρ è un morfismo di gruppi algebrici, perciò ρ è una rappresentazione razionale di G in \mathbb{K}^{n+1} .

Inoltre, per ogni $g \in G$, $\rho(g)\langle e_1, \ldots, e_n \rangle \subseteq \langle e_1, \ldots, e_n \rangle$, perciò $\langle e_1, \ldots, e_n \rangle$ è un G-sottomodulo di \mathbb{K}^{n+1} .

Poiché G è riduttivo, ρ è semisemplice, esiste un G-sottomodulo $\langle \underline{w} \rangle$, con $\underline{w} = a_1 e_1 + \cdots + a_n e_n + e_{n+1}$, $a_1, \ldots, a_n \in \mathbb{K}$. Allora per ogni $g \in G$, $\rho(g)\underline{w} = \lambda \underline{w}$ con $\lambda \in \mathbb{K}$. Guardando l'ultima coordinata dell'uguaglianza ci si accorge che $\lambda = 1$. Ma questo vuol dire in particolare che

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

è un punto fisso dell'azione di G in \mathbb{K}^n .

Corollario 4.34. Il gruppo additivo G_a non è linearmente riduttivo.

Lemma 4.35. Sia G un sottogruppo di $Af_n(\mathbb{K})$ che è anche un gruppo riduttivo, allora esiste una traslazione τ tale per cui $\tau \circ G \circ \tau^{-1} < GL_n(\mathbb{K})$.

Dimostrazione. Il gruppo G, agendo su \mathbb{K}^n deve avere almeno un punto fisso per il 4.33. Prendiamone uno a caso (a_1,\ldots,a_n) , con $a_1,\ldots,a_n \in \mathbb{K}$ e prendiamo come $\tau := (x_1 - a_1,\ldots,x_n - a_n)$. Allora $\tau \circ G \circ \tau^{-1}$ è un gruppo di affinità con punto fisso $(0,\ldots,0)$, perciò è un sottogruppo di $\mathrm{GL}_n(\mathbb{K})$. \square

Lemma 4.36. Sia G un gruppo riduttivo di $J_2(\mathbb{K})$, allora esiste $\sigma \in J_2(\mathbb{K})$ tale che $\sigma \circ G \circ \sigma^{-1} < GL_2(\mathbb{K}) \cap J_2(\mathbb{K})$.

Dimostrazione. Ricordiamo che gli automorfismi triangolari possono essere scritti nella forma

$$J_2(\mathbb{K}) = \{(a_1x + c_1, b_2y + f(x)) | a_1, b_1 \in \mathbb{K}^*; c_1 \in \mathbb{K}; f(x) \in \mathbb{K}[x]\}.$$

Dimostriamo che se G è un gruppo riduttivo allora possiamo coniugarlo per un elemento di $J_2(\mathbb{K})$ ed ottenere un gruppo G' tale che tutti i termini noti c_1 del primo polinomio coordinato siano uguali a zero.

La mappa $\pi_1: J_2(\mathbb{K}) \to \mathrm{Af}_1(\mathbb{K})$ che manda $(a_1x + c_1, b_2y + f(x))$ in $(a_1x + c_1)$ è un morfismo di gruppi algebrici. Abbiamo visto che i sottogruppi riduttivi di $\mathrm{Af}_1(\mathbb{K})$ sono coniugati tramite traslazione ad un gruppo di $\mathrm{GL}_1(\mathbb{K})$. Inoltre abbiamo visto che l'immagine di un gruppo riduttivo tramite un morfismo di gruppi algebrici è un gruppo riduttivo a sua volta. Dunque esiste τ_1 traslazione tale che $\tau_1 \circ \pi_1(G) \circ \tau_1^{-1} < \mathrm{GL}_1(\mathbb{K})$, perciò $G' := (\tau_1, y) \circ G \circ (\tau_1, y)^{-1}$ è il gruppo cercato.

Ora $\mathbb{A}^2_{\mathbb{K}}$ è una G'-varietà, quindi per il Corollario 4.27, $\mathbb{K}[x,y]$ è un $\mathbb{K}[G']$ modulo semisemplice. Lo spazio vettoriale $V' := \langle \mathbb{K}[x], y \rangle$ è G'-invariante

perché G' consta solo di elementi triangolari. Allora V' è un $\mathbb{K}[G']$ -modulo semisemplice. Lo spazio $W = \mathbb{K}[x]$ è a sua volta G'-invariante perciò deve esistere W' completamento G'-invariante di W in V'. Lo spazio W' deve essere generato da un elemento della forma y+h(x) con $h(x) \in \mathbb{K}[x]$. Imponiamo ora che W' sia G'-invariante. Prendiamo $g \in G'$, $g = (a_1x, b_1y + f(x))$ e imponiamo $g \cdot (y+h(x)) = \lambda(y+h(x))$. L'uguaglianza diviene $b_1y+f(x)+h(a_1x) = \lambda y + \lambda h(x)$. Perciò $\lambda = b_1$, quindi

$$f(x) + h(a_1 x) = b_1 h(x). (4.1)$$

Notiamo che questa uguaglianza deve valere per ogni $g \in G'$ e che h(x) è indipendente da g.

Se adesso prendiamo $G'' = (x, y + h(x)) \circ G' \circ (x, y - h(x))$ abbiamo $G'' < \operatorname{GL}_2(\mathbb{K})$. Difatti se $g \in G'$ e $g = (a_1x, b_1y + f(x)), (x, y + h(x)) \circ g \circ (x, y - h(x)) = (a_1x, b_1y - b_1h(x) + f(x) + h(a_1x))$.

Per l'identità 4.1 il membro di destra è uguale a (a_1x, b_1y) .

Bibliografia

- [1] Rudolf Rentshler, Opérations du groupe additif sur le plan, C. R. Acad. Sci. Paris, 1968
- [2] Tatsuji Kambayashi, Automorphism group of a polynomial ring and algebraic group actions on affine space, J. of Algebra, 60, 439-451, 1979
- [3] Hymann Bass, Edwin H. Connell, and David Wright, *The Jacobian conjecture: Reduction of degree and formal expansion of the inverse*, Bull. Amer. Math. Soc. (N.S.), Vol. 7, No. 2, 1982
- [4] Gerry Schwarz, Exotic algebraic group actions, C. R. Acad. Sci. Paris, 309, 89-94, 1989
- [5] Ivan P. Shestakov, and Ualbai U. Umirbaev, Poisson brackets and twogenerated subalgebras of rings of polynomials, J. Amer. Math. Soc. 17, 2004
- [6] Ivan P. Shestakov, and Ualbai U. Umirbaev, The tame and the wild automorphisms of polynomial rings in three variables, J. Amer. Math. Soc. 17, 2004
- [7] Joost Berson, Arno van den Essen, and David Wright, Stable Tameness of Two-Dimensional Polynomial Automorphisms Over a Regular Ring, arXiv:0707.3151v10 [math.AC], 2012
- [8] Robin Hartshorne, Algebraic Geometry, Springer, 1977
- [9] Jean-Pierre Serre, J. Stiwell, Trees, Springer, 1980
- [10] Armand Borel, Linear Algebraic Groups, Springer, 1991
- [11] Arno van den Essen, Polynomial Automorphisms and the Jacobian Conjecture, Birkhäuser, 2000
- [12] Gene Freudenburg, Algebraic Theory of Locally Nilpotent Derivations, Springer, 2006