Appunti di Algebra Computazionale A
Prof.ssa Gianni

Carlo Sircana

Indice

Capitolo 1

Estensioni di campi

In questo capitolo vogliamo occuparci di un metodo per l'implementazione delle estensioni di campi e del calcolo del campo di spezzamento di un polinomio.

1.1 Estensioni Semplici

Il primo problema da affrontare è capire come rappresentare gli elementi in una estensione. Sia K un campo e sia α un elemento algebrico su K. Sappiamo allora che α ha un polinomio minimo $p_\alpha = \sum a_i x^i$, l'unico polinomio monico e irriducibile che si annulla in α. Allora $K(\alpha)$ è isomorfo a $K[x]/(p_\alpha(x))$ e una base di questo campo come K-spazio vettoriale è data da $1, x, x^2, x^3, \ldots, x^{n-1}$, dove $n = \deg(p_\alpha)$. Dato comunque $\beta \in K(\alpha)$, possiamo allora rappresentarlo in questo modo:

$$\beta = b_0 + b_1\alpha + a_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}$$

dove ogni $b_i \in K$. Nelle implementazioni possiamo allora rappresentare un elemento $\beta \in K(\alpha)$ come un vettore $(b_0, \ldots, b_{n-1})$ o equivalentemente un polinomio.

Esiste anche un'altra rappresentazione, più comoda in alcuni casi. Consideriamo l'applicazione

$$\begin{array}{rccc} \varphi_\beta\colon & K(\alpha) & \longrightarrow & K(\alpha) \\ & \gamma & \longmapsto & \gamma\beta \end{array}$$

Questa è un omomorfismo di K-spazi vettoriali; poichè abbiamo fissato una base, tale applicazione è rappresentata in modo unico da una matrice M_β. La prima colonna conterrà i coefficienti della rappresentazione vettoriale di β; per trovare la seconda colonna, basta moltiplicare la relazione data dalla prima colonna per α

$$\begin{aligned} \alpha\beta &= \alpha(b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}) \\ &= \alpha b_0 + \alpha^2 b_1 + \cdots + \alpha^n b_{n-1} \\ &= \alpha b_0 + \alpha^2 b_1 + \cdots + \alpha^{n-1} b_{n-2} + (-a_{n-1}\alpha^{n-1} - a_{n-2}\alpha_{n-2} + \cdots + a_0) \\ &= a_0 + \alpha(b_0 - a_1) + \alpha^2(b_1 - a_2) + \cdots + \alpha^{n-1}(b_{n-2} - a_{n-1}) \end{aligned}$$

Dunque, per calcolare ogni colonna della matrice, data la rappresentazione di β in forma vettoriale, è sufficiente fare n somme per ogni colonna, e quindi il

passaggio dalla forma vettoriale alla forma matriciale richiede $O(n^2)$ operazioni. Passare invece dalla forma matriciale a quella vettoriale ha invece complessità costante: basta infatti prendere la prima colonna della matrice. Riportiamo ora in tabella i costi delle principali operazioni nelle due rappresentazioni riportate

	Vettore	**Matrice**
Somma	$O(n)$	$O(n^2)$
Prodotto	$O(n^2)$	$O(n^2)$
Inverso	$O(n^3)$	$O(n^3)$

Nel caso matriciale, si passa in forma vettoriale, si svolgono le operazioni e si ritorna in forma matriciale; eseguire direttamente le operazioni avrebbe infatti ordine maggiore.

1.2 Norma e Traccia

Supponiamo d'ora in poi di lavorare con estensioni separabili. Sia p_α polinomio minimo di α, consideriamo le sue radici (disstinte) $\alpha_1, \dots, \alpha_n$ e supponiamo $\alpha = \alpha_1$. Abbiamo visto che dato $\beta \in K(\alpha)$, β ammette una rappresentazione $\beta = q_\beta(\alpha)$. Definiamo rispettivamente norma e traccia di β come

$$\mathrm{N}(\beta) = \prod_{i=1}^{n} q_\beta(\alpha_i) \qquad\qquad \mathrm{Tr}(\beta) = \sum_{i=1}^{n} q_\beta(\alpha_i)$$

Notiamo che detto F il campo di spezzamento di p_α, si ha che ogni elemento del gruppo di Galois fissa sia $N(\beta)$ che $Tr(\beta)$ e dunque questi sono elementi di K. Notiamo che la norma è moltiplicativa, cioè $\mathrm{N}(\beta\gamma) = \mathrm{N}(\beta)\,\mathrm{N}(\gamma)$, mentre la traccia è lineare. Possiamo estendere la definizione ai polinomi: dato $f(x, \alpha) \in K(\alpha)[x]$, definiamo

$$\mathrm{N}(f(x,\alpha)) = \prod_{i=1}^{n} f(x, \alpha_i) \qquad\qquad \mathrm{Tr}(f(x,\alpha)) = \sum_{i=1}^{n} f(x, \alpha_i)$$

Osservazione 1.1. Notiamo che $f(x,\alpha) \mid N(f(x,\alpha))$ e che se $g \in K[x]$, allora $N(g(x)) = g(x)^n$. Inoltre, se $\beta \in K(\alpha)$, sia $\beta = q_\beta(\alpha)$. Allora $N(\beta) = \prod_{i=1}^{n} q_\beta(\alpha_i) = \mathrm{Ris}(p_\alpha, q_\beta) \in K$.

Per il calcolo della norma di un elemento, si può utilizzare la rappresentazione matriciale come spiegato nella seguente proposizione:

Proposizione 1.2. Sia α un elemento algebrico su K, $[K(\alpha) : K] = n$, e sia $\beta \in K(\alpha)$. Allora $\mathrm{N}(\beta) = \det(M_\beta)$.

Dimostrazione. È sufficiente notare che la norma come l'abbiamo definita è la potenza n/m-esima del termine noto del polinomio minimo di β (il termine noto è il prodotto di tutti i coniugati). Dunque, sia $1, \gamma_1, \dots, \gamma_{m/n-1}$ una base di $K(\alpha)/K(\beta)$. Allora la base

$$1, \beta, \dots, \beta^{m-1}, \gamma_1, \gamma_1\beta, \dots, \gamma_1\beta^{m-1}, \dots, \gamma_{m/n-1}, \dots, \gamma_{m/n-1}\beta^{m-1}$$

rende la matrice che rappresenta φ_β diagonale a blocchi, con blocchi uguali alla matrice compagna del polinomio minimo, come voluto.

□

Teorema 1.3. Sia $f(x,\alpha) \in K(\alpha)[x]$ un polinomio irriducibile. Allora la norma $N(f(x,\alpha)) = g(x)^k$, dove $g \in K[x]$ è un polinomio irriducibile, e $k \in \mathbb{N}$.

Dimostrazione. Supponiamo $N(f) = CD$ con $C, D \in K[x]$ e $(C,D) = 1$. Per definizione $N(f) = \prod f(x,\alpha_i)$; chiamiamo $f_i = f(x,\alpha_i)$. Poichè f è irriducibile e stiamo lavorando in un UFD, è anche primo e dunque vale $f \mid C \vee f \mid D$. Supponiamo senza perdità di generalità che $f \mid C$. Siano $\sigma_1, \ldots, \sigma_n$ le immersioni di $K(\alpha)$ in $\bar{K}$ e siano $\alpha_1 = \alpha, \ldots, \alpha_n$ le immagini di α tramite queste. Ogni immersione può essere estesa banalmente a $K(\alpha)[x]$

$$\begin{array}{rccc} \sigma_i\colon & K(\alpha)[x] & \longrightarrow & K(\alpha_i)[x] \\ & f(x,\alpha) & \longmapsto & f(x,\alpha_i) \end{array}$$

Poiché $C \in K[x]$, C viene fissato da ognuno di questi omomorfismi, mentre f_i viene mappato su f_j. Le relazioni di divisibilità devono essere conservate da ogni σ_i; poichè $f_1 = f \mid C$, allora $f_j \mid C$ per ogni j. Di conseguenza, $N(f) \mid C$ e dunque $D \in K^*$. Ciò vuol dire che $N(f)$ ha un solo fattore irriducibile, e dunque sarà la potenza di un irriducibile. □

1.3 Fattorizzazione

Sia $f(x,\alpha) \in K(\alpha)[x]$; ci poniamo ora il problema di fattorizzare f nell'estensione $K(\alpha)$. Questo sarà fondamentale nel calcolo del campo di spezzamento di un polinomio di $K[x]$; servirà infatti fattorizzare il polinomio nelle varie estensioni che troveremo. Sappiamo che

$$f(x,\alpha) \mid \mathrm{N}(f(x,\alpha)) = \prod_{i=1}^{n} F_i$$

dove F_i è una fattorizzazione in irriducibili in $K[x]$; allora vale il seguente

Teorema 1.4. Se $\mathrm{N}(f(x,\alpha))$ è libera da quadrati, allora

$$f(x,\alpha) = \prod_{i=1}^{n} (f(x,\alpha), F_i)$$

è la fattorizzazione in irriducibili di $f(x,\alpha)$.

Dimostrazione. Siano $v_1, \ldots, v_n \in K(\alpha)[x]$ gli irriducibili che dividono $f(x,\alpha)$. Allora $\mathrm{N}(v_i(x,\alpha)) \mid \mathrm{N}(f(x,\alpha))$; dato che per il teorema precedente $\mathrm{N}(v_i) = g^k$ con g irriducibile e la norma di f è libera da quadrati si ha che $k = 1$ ed esiste $j \in \{1, \ldots, n\}$ tale che $\mathrm{N}(v_i) = F_j$. Dato che g e F_j sono irriducibili, allora avremo $v \mid g = F_j$. Inoltre

$$\mathrm{N}(f) = \mathrm{N}\left(\prod v_i\right) = \prod \mathrm{N}(v_i) = \prod F_i$$

Abbiamo mostrato così che ogni fattore irriducibile di f divide almeno un F_i. Se v_i dividesse più di uno dei fattori, si negherebbe l'ipotesi che $(F_i, F_j) = 1$. Inoltre, dati due diversi v_i, non possono dividere lo stesso F_i, poiché altrimenti avrebbero la stessa norma, e quindi ci sarebbero due copie di F_i. Per ragioni di grado, infine, i v_i generano tutti gli F_i. Dunque $(f(x,\alpha), F_i)$ è irriducibile. □

Dunque, abbiamo trovato un algoritmo per il calcolo della fattorizzazione; basterà infatti calcolare la fattorizzazione della norma su $K[x]$ e calcolare i *gcd* tra f e i fattori ottenuti. Bisogna però mostrare che è sempre possibile supporre che la fattorizzazione della norma sia squarefree. Per questo, mostriamo ora che esistono solo un numero finito di elementi $s \in K$ tali che $\mathrm{N}(f(x + s\alpha))$ non sia libera da quadrati. Per questo, dobbiamo supporre che K sia infinito e perfetto, in quanto avremo bisogno della fattorizzazione squarefree di un polinomio.

Teorema 1.5. Sia $f \in K[x]$ un polinomio libero da quadrati. Allora esistono un numero finito di $s \in K$ tali che $\mathrm{N}(f(x - s\alpha))$ non sia libero da quadrati.

Dimostrazione. Siano $\beta_1, \ldots, \beta_m$ le radici distinte di f. Le radici di una sua traslazione $f(x - s\alpha)$ sono $\beta_1 + s\alpha, \ldots, \beta_m + s\alpha$. Dunque le radici di

$$\mathrm{N}(f(x - s\alpha)) = \prod f(x - s\alpha_j)$$

sono del tipo $\beta_i + s\alpha_j$. Se la norma non fosse libera da quadrati, avremmo $\beta_i + s\alpha_j = \beta_k + s\alpha_l$. Sicuramente $l \neq j$ perchè per ipotesi le β_i sono distinte. Di conseguenza,

$$s = \frac{\beta_i - \beta_k}{\alpha_l - \alpha_j}$$

e dunque $\mathrm{N}(f(x - s\alpha))$ non è squarefree per un numero finite di scelte di s. □

Lemma 1.6. Sia $f(x, \alpha) \in K(\alpha)[x]$ un polinomio libero da quadrati. Allora esiste $g \in K[x]$ libero da quadrati tale che $f \mid g$.

Dimostrazione. Consideriamo la decomposizione in fattori liberi da quadrati della norma $\mathrm{N}(f(x, \alpha))$, cioè $\mathrm{N}(f(x, \alpha)) = \prod G_i^i$. Chiaramente, $f \mid \prod G_i^i$ ma f è libero da quadrati, dunque $f \mid \prod G_i = g$. □

Proposizione 1.7. Sia $f \in K(\alpha)[x]$ un polinomio libero da quadrati. Allora esistono solo un numero finito di $s \in K$ tali che $N(f(x - s\alpha, \alpha))$ non sia libero da quadrati.

Dimostrazione. Per il lemma, esiste $g \in K[x]$ tale che $f \mid g$ e g è libero da quadrati. Di conseguenza,

$$f(x - s\alpha) \mid g(x - s\alpha) \Rightarrow N(f(x - s\alpha)) \mid N(g(x - s\alpha))$$

ma quest'ultima non è libera da quadrati solo per un numero finito di valori. □

Diamo ora lo pseudocodice di un algoritmo per il calcolo della fattorizzazione.

NormSq L'algoritmo NormSq 1.3 prende in input un polinomio $f \in K(\alpha)[x]$ libero da quadrati e il polinomio minimo p_α di α e restituisce $s \in K$, $g(x, \alpha) \coloneqq f(x - s\alpha)$ e $R(x) = N(g(x, \alpha))$ libera da quadrati.

Algoritmo 1.1 Norma Squarefree

1: $s = 0$
2: $g(x, \alpha) = f(x, \alpha)$
3: $check = false$
4: **while** $check == false$ **do**
5: $R(x) = \mathrm{Ris}_y(g(x, y), p_\alpha(y))$ $(= N(g))$
6: **if** $\deg(R, R')! = 0$ **then**
7: $check = true$
8: **else**
9: $s = s + 1$
10: $g(x, \alpha) = g(x - \alpha, \alpha)$
11: **end if**
12: **end while**
13: **return** (s, g, R)

Fattorizzazione Supponiamo di avere in input $f \in K(\alpha)[x]$ libero da quadrati. L'algoritmo restituisce in output la lista dei fattori irriducibili di f su $K(\alpha)$. L'algoritmo **fatt** è l'algoritmo di fattorizzazione di polinomi in $K[x]$.

Algoritmo 1.2 Fattorizzazione in estensioni semplici

1: $(s, g, R) = \mathbf{NormSq}(f(x, \alpha))$
2: $lfatt = [\,]$
3: $l = \mathbf{fatt}(R)$ in $K[x]$
4: **if** $Length(l) = 1$ **then**
5: $lfatt = [f]$
6: **else**
7: **for** $i = 1; i \leq Lenght(l); i = i + 1$ **do**
8: $h_i(x, \alpha) = (g(x, \alpha), l[i])$ in $K(\alpha)$
9: $g(x, \alpha) = g/h_i$ in $K(\alpha)$
10: $h_i(x, \alpha) = h_i(x + s\alpha, \alpha)$
11: $lfatt = [h_i, lfatt]$
12: **end for**
13: **end if**
14: **return** $lfatt$

1.4 Teorema dell'elemento primitivo

Ci poniamo ora il problema di determinare il campo di spezzamento di un polinomio in $K[x]$, nel caso in cui la caratteristica del campo sia 0. Agiremo aggiungendo le radici una ad una e avremo bisogno di lavorare ad ogni passo con estensioni semplici, in quanto l'algoritmo trattato nella sezione precedente ha necessità di queste ipotesi. Utilizzeremo allora la seguente forma del teorema dell'elemento primitivo

Teorema 1.8 (dell'elemento primitivo)**.** Sia K un campo infinito e siano α, β elementi separabili su K. Allora esiste $\gamma \in K(\alpha, \beta)$ tali che $K(\alpha, \beta) = K(\gamma)$.

Il problema è realizzare questo teorema dal punto di vista algoritmico. Dimostriamo un po' di risultati che ci porteranno alla dimostrazione:

Proposizione 1.9. Sia K un campo, sia α algebrico su K e consideriamo l'estensione $K(\alpha)$, con p_α polinomio minimo di α. Sia β algebrico su K e sia $Q_\beta(x,\alpha) \in K(\alpha)[x]$ tale che $Q(\beta,\alpha) = 0$. Supponiamo che $\mathrm{N}(Q_\beta(x,\alpha))$ sia libera da quadrati. Allora $\alpha \in K(\beta)$ e in $K(\beta)$ si ha

$$(p_\alpha(x), Q_\beta(\beta,x)) = x - \alpha$$

Dimostrazione. Siano $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ le radici di p_α. Per definizione, la norma $N(Q_\beta(x,\alpha_i)) = \prod_{i=1}^{n} Q_\beta(x,\alpha_i)$. Di conseguenza, α è radice sia di p_α che $Q_\beta(\beta,x)$, ma α_i non è radice di $Q_\beta(\beta,x)$ per $i \geq 2$. In caso contrario, infatti, avremmo $Q(\beta,\alpha) = Q(\beta,\alpha_i) = 0$ e dunque la norma avrebbe radici multiple, contro le ipotesi. Di conseguenza, $x - \alpha = (p_\alpha, Q_\beta(\beta,x))$. □

Proposizione 1.10. Sia $Q_\beta(x,\alpha)$ il polinomio minimo di β su $K(\alpha)$. Se $\mathrm{N}(Q_\beta(x,\alpha))$ è libero da quadrati, allora è il polinomio minimo di β su K.

Dimostrazione. Dato che $Q_\beta(x,\alpha)$ è irriducibile, allora $\mathrm{N}(Q_\beta(x,\alpha)) = g(x)^k$ è potenza di un irriducibile. Per ipotesi, la norma è libera da quadrati e dunque è irriducibile. Visto che si annulla su β, allora è il suo polinomio minimo su K. □

Sia ora β algebrico su K e sia $Q_\beta(x,\alpha) \in K(\alpha)[x]$ il suo polinomio minimo su $K(\alpha)$. In generale, $N(Q_\beta(x,\alpha))$ non è libera da quadrati, ma sappiamo che esiste $s \in K$ tale che $N(Q_\beta(x - s\alpha, \alpha))$ sia libero da quadrati. In tal caso, coincide con il polinomio minimo di $\beta + s\alpha = \gamma$. Abbiamo allora, per quanto dimostrato, che $K(\gamma) = K(\alpha,\gamma)$. Notiamo però che $\beta \in K(\alpha,\gamma)$, dunque otteniamo $K(\gamma) = K(\alpha,\beta)$. Abbiamo così trovato una dimostrazione costruttiva del teorema dell'elemento primitivo. Inoltre, poichè $\gamma = \beta + s\alpha$, abbiamo sia la rappresentazione di α che quella di β.

Diamo ora lo pseudocodice dell'algoritmo per l'elemento primitivo. In input supponiamo di avere p_α il polinomio minimo di α e $Q_\beta(x,\alpha)$ il polinomio minimo di β su $K(\alpha)$. In output restituiremo $R(x)$ il polinomio minimo dell'elemento primitivo γ su K, le rappresentazioni $A(\gamma)$ e $B(\gamma)$ rispettivamente di α e β in $K(\gamma)$.

Algoritmo 1.3 Elemento Primitivo

1: $(s, g, R) = \mathbf{NormSq}(Q_\beta) \quad (g(x,\alpha) = Q_\beta(x - s\alpha, \alpha))$
2: $\alpha = \mathbf{linsolve}(gcd(g(\gamma,x), p_\alpha(x)))$
3: $\beta = \gamma - s\alpha \in K(\gamma)$
4: **return** $(R(x), \gamma, \alpha, \beta)$

dove l'algoritmo **linsolve** risolve semplicemente le equazioni di primo grado. Grazie all'elemento primitivo, possiamo ora calcolare il campo di spezzamento di un polinomio $f \in K[x]$ separabile. Diamo ora lo pseudocodice dell'algoritmo: in input, supponiamo di avere un polinomio $p(x) \in K[x]$ irriducibile. In output forniremo le radici di $p(x)$ in $K(\gamma)$ e il polinomio $R(x)$ che definisce il campo di spezzamento.

Algoritmo 1.4 Campo di spezzamento di un polinomio

1: $roots = [\,]$
2: $polys = [p(x)]$
3: $minpoly = p(x)$
4: $newminpoly = p(x)$
5: $index = 1$
6: $\beta = \gamma$ radice di $minpoly$
7: $polys[index] = \frac{polys[index]}{x-\beta}$ $\star$
8: $new\_s = 0$
9: $Bpoly = x - \gamma$
10: $roots = [\beta, roots]$
11: $newfactor = [\,]$
12: $k = 1$
13: **for** P_i in $polys$ **do**
14: $(s, g, R) =$ **NormSq**$(P_i, minpoly)$
15: $L =$ **fatt**(R)
16: **for** F in L **do**
17: $f(x, \gamma) = (g(x, \gamma), F)$
18: **if** $deg(F) > deg(newminpoly)$ **then**
19: $newminpoly = F$
20: $index = k$
21: $new\_s = s$
22: $Bpoly(x, \gamma) = f(x, \gamma)$
23: **end if**
24: $g(x, \gamma) = g(x, \gamma) \big/ f(x, \gamma)$
25: $f(x, \gamma) = f(x + s\gamma, \gamma)$
26: **if** $deg(f(x, \gamma)) == 1$ **then**
27: $roots =$ [**linsolve**$(f(x, \gamma)), roots]$
28: **else**
29: $newfactors = [f, newfactors]$
30: $k = k + 1$
31: **end if**
32: **end for**
33: **end for**
34: new_γ radice di $newminpoly$
35: $\alpha =$ **linsolve**$(gcd(minpoly, Bpoly(new\_\gamma, x)))$
36: $\beta = new\_\gamma - new\_s\ \alpha$
37: sostituiamo α a γ in $roots$
38: **if** $newfactors == [\,]$ **then return** $(newminpoly, roots)$
39: **end if**
40: sostituiamo α a γ in $newfactors$
41: $polys = newfactors$
42: $minpoly = newminpoly$
43: $\gamma = new\_\gamma$
44: vai a $\star$

Spiegazione dell'algoritmo Significato delle variabili:

γ e new_γ: è l'elemento primitivo: alla fine dell'algoritmo indicherà un generatore del campo di spezzamento $K(\gamma)$

roots: Lista delle radici di f, espresse secondo la base data da γ

polys e $newfactor$: Fattori del polinomio f nelle varie estensioni intermedie.

β: ultima radice di f aggiunta all'estensione.

Bpoly: Polinomio minimo di new_γ su $\mathbb{K}(\gamma)$.

L'algoritmo prende in input un polinomio irriducibile $p(x)$, e denomina come γ e β una sua radice, che mette in *roots*. Mettendosi in $\mathbb{K}(\gamma)[x]$, divide il $p(x)$ per $x - \beta$, ottenendo un polinomio $Q(x, \gamma)$ le cui radici sono gli elementi che deve aggiungere alla sua estensione per ottenere il campo di spezzamento. Mette $k = 1$ poiché è la posizione di Q in *polys*.

Preso Q, ne fa la **NormSq**, ottenendo un polinomio $g(x, \gamma) = Q(x + s\gamma, \gamma)$ la cui norma R è libera da quadrati e quindi fattorizza R. Se $Q = \prod Q_i$ è la sua fattorizzazione, allora R sarà il prodotto di R_i, che sono norme libere da quadrati di $g_i(x, \gamma) = Q_i(x + s\gamma, \gamma)$. Notiamo che Q_i, essendo irriducibili, saranno polinomi minimi su $\mathbb{K}(\gamma)$ delle sue radici. Inoltre, gli R_i saranno polinomi minimi delle radici di g_i su K, e queste sono gli elementi primitivi dell'estensione di $K(\gamma)$ con la rispettiva radice di Q_i. Preso dunque un R_i, che chiama F, ricava il g_i corrispondente, e lo chiama f. L'estensione di K con una radice di F comprende γ, dunque il grado di F è maggiore o uguale a quello di p; l'unico caso in cui è uguale, è quando tutte le radici del Q_i corrispondente sono già dentro $\mathbb{K}(\gamma)$, ma dato che Q_i sono irriducibili, allora sono in particolare lineari. In questo caso il blocco If non viene eseguito, e si ricava la radice di Q_i in relazione a γ. Infatti si ricava $Q_i = f(x + s\gamma, \gamma)$, calcola la radice e la aggiunge a *roots*. Quando invece il grado di F è maggiore del polinomio minimo, allora una qualsiasi radice di F è un elemento primitivo per γ e una radice di Q_i. Dunque segniamo F come il nuovo polinomio minimo, e diciamo che nel vettore (inizialmente vuoto) $newfactors$ il polinomio $Q_i = f(x+s\gamma, \gamma)$ si trova nella posizione $index = k$. Infatti dopo il blocco If, dato che f non è lineare, lo aggiungiamo all'array $newfactors$, e aumentiamo k di 1. Inoltre ci segniamo s in new_s, come segno che dobbiamo cambiare elemento primitivo, e in *Bpoly* segniamo f, che è il polinomio minimo del nuovo elemento primitivo su $\mathbb{K}(\gamma)$. Uscendo da tutti i For, diciamo che new_γ è il nuovo elemento primitivo, e calcoliamo γ in relazione a new_γ e lo salviamo in α. Questo funziona poiché *minpoly* è il polinomio minimo di γ su $\mathbb{K}$, *Bpoly* di new_γ su $\mathbb{K}(\gamma)$, ed inoltre la norma di *Bpoly* è la norma di f, cioè F, che era libero da quadrati; dunque il loro gcd è esattamente la funzione voluta. Inoltre la radice di $p(x)$ corrispondente sarà $new\_\gamma - new\_s\ \alpha$, che sarà un'espressione in new_γ, che salviamo in β (che aggiungeremo a *roots* solo se abbiamo ancora termini da fattorizzare, poiché altrimenti tutti i termini erano già lineari, e dunque β è già stato aggiunto). Aggiorniamo tutte le radici in relazione al nuovo elemento primitivo new_γ, semplicemente sostituendo α a γ in *roots*. Se non abbiamo più termini da fattorizzare, il programma è terminato, poiché allora nell'attuale estensione abbiamo già fattorizzato tutto. Altrimenti, aggiorniamo i $newfactors$ al nuovo elemento primitivo, e rilanciamo il programma da *star*, con il nuovo elemento primitivo, il

nuovo polinomio minimo, i nuovi termini da fattorizzare $polys = newfactors$, il nuovo $\gamma = new\_\gamma$ e il nuovo β. Nel caso in cui con il γ corrente si fattorizzasse tutto a termini lineari, l'inizializzazione di $Bpoly = x - \gamma$ e $new\_s = 0$ fa sì che $\alpha = \gamma = new\_\gamma$, garantendo così l'esattezza dell'algoritmo.

Capitolo 2

Decomposizione primaria

In questo capitolo siamo interessati a trovare la decomposizione primaria di un ideale di $K[x_1, \ldots, x_n] = K[x]$. Dapprima, vedremo gli algoritmi base per manipolare gli ideali, come l'intersezione e l'ideale divisione. Ci occuperemo poi di trovare la decomposizione primaria di ideali 0-dimensionali e la generalizzeremo poi a ideali qualunque. Termineremo il capitolo mostrando che la stessa tecnica può essere applicata ad altri problemi, come il calcolo del radicale.

2.1 Operazioni elementari

Intersezione di ideali

Lemma 2.1. Siano I, J ideali di $k[x]$. Allora $I \cap J = (tI + (1-t)J) \cap K[x]$.

Dimostrazione. Mostriamo che vale il doppio contenimento. Sia $p \in I \cap J$. Allora $p = tp + (1-t)p \in tI + (1-t)J$. Viceversa, sia $p \in (tI + (1-t)J) \cap K[x]$. Allora $p(x) = (1-t)f(x) + tg(x)$, dove $f \in I$ e $g \in J$. Dato che p non dipende da t, possiamo valutare p per $t = 0$ e $t = 1$. Dunque $g(x) = f(x) = p(x)$ da cui $p \in I \cap J$. □

Quoziente di ideali

Lemma 2.2. Siano I, J ideali di $k[x]$ e supponiamo $J = (h_1, \ldots, h_s)$. Sia $f \in K[x]$.

1. $(I \colon J) = \cap_{i=1}^{s} (I : (h_i))$
2. $(I : f) = \frac{1}{f}(I \cap (f))$

Dimostrazione.

1. Sia $x \in (I : J)$. Allora per ogni $j \in J$ vale $jx \in I$; questo vale in particolare per ogni generatore da cui un contenimento. Viceversa, sia $x \in \cap_{i=1}^{s} (I : (h_i))$. sia $j \in J$; allora $j = \sum a_i h_i$ e dunque

$$xj = x \sum a_i h_i = \sum a_i \underbrace{(xh_i)}_{\in I} \in I$$

da cui l'altro contenimento.

2. Sia $x \in (I : f)$; per definizione $fx \in I$ e quindi $fx \in I \cap (f)$. Di conseguenza $x \in \frac{1}{f}(I \cap (f))$ da cui un contenimento. Viceversa, sia $x \in \frac{1}{f}(I \cap (f))$. Allora $xf \in I \cap (f)$, da cui $x \in (I : f)$.

□

Iniettività e surgettività di una mappa polinomiale Consideriamo una mappa polinomiale

$$\begin{array}{rccc} f\colon & K[x_1,\dots,x_n] & \longrightarrow & K[y_1,\dots,y_m] \\ & x_i & \longmapsto & f_i(y) \end{array}$$

Vogliamo determinare il nucleo di tale mappa. Possiamo vedere f come la composizione

$$\begin{array}{ccccc} K[x] & \xrightarrow{i} & K[x,y] & \xrightarrow{g} & K[y] \\ & & y_i & \longmapsto & y_i \\ & & x_i & \longmapsto & f_i(y) \end{array}$$

e dunque è sufficiente studiare il nucleo di g dato che i è iniettiva. Notiamo che l'ideale $I = (x_1 - f_1(y), \dots, x_n - f_n(y))$ è contenuto nel nucleo di g. Viceversa, sia $h \in \mathrm{Ker}(g)$; dividendo h per $x_1 - f_1(y), \dots, x_n - f_n(y)$ con l'ordinamento lex otteniamo

$$h(x,y) = \sum_{i=1}^{m} c_i(x,y)(x_i - f_i(y)) + r(y)$$

Quindi $0 = g(h) = r(y)$ da cui l'altro contenimento. Per trovare il nucleo basta quindi calcolare l'ideale di eliminazione.

Osservazione 2.3. Possiamo adattare questo algoritmo nel caso che la mappa sia a valori in un quoziente $K[y]/J$. In questo caso basta infatti considerare $I = (x_1 - f_1(y), \dots, x_n - f_n(y), J)$.

Per quanto riguarda la surgettività, basta verificare che $y_i \in (f_1(y), \dots, f_n(y))$ in quanto l'immagine di f non è altro che la K-algebra generata da $f_1, \dots, f_n$.

2.2 Lemma di Normalizzazione

Vogliamo ora studiare un algoritmo costruttivo per il calcolo della normalizzazione di Noether. Per prima cosa abbiamo quindi necessità di un test di interezza:

Test di Interezza Siano $f_1, \dots, f_n \in K[x]$ e sia $A = K[f_1, \dots, f_n]$ la K-algebra da essi generata. Sia $I \subseteq K[x]$ un ideale e sia $B = K[x]/I$. Possiamo allora identificare A con la sua immagine $\tilde{A}$ in B. Vogliamo studiare un metodo per determinare se, dato $b \in B$, questo sia intero su A.

Proposizione 2.4 (Criterio di dipendenza intera)**.** Siano $t, y_1, \dots, y_k$ indeterminate. Consideriamo l'ideale

$$J = (t - b, y_1 - f_1, \dots, y_k - f_k, I) \subseteq K[x,t,y]$$

Sia G la base di Gröbner di J rispetto all'ordinamento lex $X > T > Y$. Allora

$$b \text{ è intero su } A \iff \text{esiste } g \in G \text{ tale che } \mathrm{lt}(g) = t^p \text{ con } p \geq 0$$

In tal caso, $g(T, f_1, \ldots, f_k)$ è una relazione di interezza per b.

Dimostrazione.

$\Longrightarrow$ Supponiamo che b sia intero e sia $p(t, f_1, \ldots, f_k)$ una relazione di interezza. Dato che $t - b \in J$ e $t - b \mid p(t, f_1, \ldots, f_k)$, necessariamente p riduce a zero se diviso per una qualsiasi base di Gröbner di J. Per come abbiamo scelto J, possiamo sostituire a ogni f_i che compare in $p(t, x)$ l'indeterminata y_i e quindi possiamo supporre che p dipenda solo da t e dalle y_i. Per l'ordinamento scelto, vale allora $\mathrm{lt}(p) = t^k$ e dunque esiste $g \in G$ tale che $\mathrm{lt}(g) \mid \mathrm{lt}(p) = t^k$, da cui la tesi.

$\Longleftarrow$ Sia $g \in G$ tale che $\mathrm{lt}(g) = t^p$. Allora, dato l'ordinamento scelto,

$$g(t, y) = t^p + \sum_{i=0}^{p-1} a_i(y) t^i$$

in g non compaiono le variabili x_i. Dato che $g \in J$, si ha $g(b, f_1, \ldots, f_k) \in J \cap K[x] = I$ e dunque $g(b, f_1, \ldots, f_k) \equiv 0 \pmod{I}$, da cui la tesi.

□

Teorema 2.5 (Lemma di Normalizzazione di Noether)**.** Sia K un campo e sia I un ideale di $K[x_1, \ldots, x_n]$. Allora esiste $s \leq n$ e un isomorfismo

$$\varphi \colon K[x_1, \ldots, x_n] \longrightarrow K[y_1, \ldots, y_n] = A$$

tale che

- la mappa $K[y_{s+1}, \ldots, y_n] \longrightarrow A/\varphi(I)$ sia iniettiva e finita
- Per ogni $j = 1, \ldots, s$ esista $g_j \in \varphi(I)$ della forma

  $$g_j = y_j^{e_j} + \sum_{k=0}^{e_j - 1} a_{j,k}(y_{j+1}, \ldots, y_n) y_j^k$$

  con $e_j > \deg(a_{j,k}) + k$
- Se I è omogeneo, i g_j siano omogenei
- Se I è primo, i g_j siano irriducibili
- Se K è perfetto e I è primo, l'estensione

  $$Q\Big(A \big/ \varphi(I)\Big) \supseteq Q\Big(K[y_{s+1}, \ldots, y_n]\Big)$$

  sia separabile
- Se K è infinito, φ sia lineare

  $$\varphi(x_i) = \sum m_{ij} y_j$$

Il lemma di normalizzazione di Noether ha importanza per quanto riguarda la teoria della dimensione per quanto concerne le K-algebre.

Definizione 2.6. Sia I un ideale di $K[x_1, \ldots, x_n]$ e sia U un sottoinsieme delle indeterminate. Diciamo che U è indipendente modulo I se $K[U] \cap I = (0)$. Diciamo che U è indipendente massimale modulo I se $\dim K[x]/I = \#U$.

Corollario 2.7. Sia I un ideale di $A = K[x_1, \ldots, x_n]$ e sia U un sottoinsieme indipendente modulo I. Allora $\dim A/I \geq \#U$. Inoltre, esiste un sottoinsieme $\tilde{U}$ che è indipendente massimale modulo I.

Dimostrazione. Se I è 0-dimensionale, necessariamente $U = \emptyset$. Infatti, $K[x_i] \cap I \neq (0)$ per ogni i, in quanto esiste un polinomio univariato in ogni variabile. Notiamo che quest'ultima è una caratterizzazione degli ideali 0-dimensionali. Supponiamo allora che $\dim K[x]/I > 0$; sia U un sottoinsieme delle coordinate indipendente modulo I. Dato che $K[U] \cap I = (0)$, si ha $K[U] \cap \sqrt{I} = (0)$. Allora esiste p primo minimale associato a I tale che $K[U] \cap p = (0)$ (perché (0) è primo in $K[U]$) e dunque

$$\#U = \operatorname{trdeg}(K[U]) \leq \operatorname{trdeg}\left(K[X]/P\right) = \dim K[X]/p \leq \dim K[X]/I$$

Per trovare il sottoinsieme $\tilde{U}$, basta scegliere un primo p associato a I tale che $\dim K[x]/I = \dim K[x]/p$ e scegliere un sottoinsieme massimale di indeterminate algebricamente indipendenti in $K[x]/p$. □

In particolare, il lemma di Normalizzazione può essere usato per il calcolo della dimensione di un ideale:

Algoritmo 2.1 Dimensione di un ideale tramite normalizzazione

1: $I = (f_1, \ldots, f_s)$
2: Cambiamento di coordinate

$$\varphi(x_i) = x_i \ \forall i < n \quad \varphi(x_n) = x_n + \sum_{i=1}^{n} a_i x_i$$

3: Calcolare una base di Gröbner G di $\varphi(I)$ con l'ordinamento lex
4: Ordinare $G = (g_1, \ldots, g_k)$ in modo tale che $lmf_r > \cdots > lmf_1$
5: Scegliere s minimo tale che $(g_1, \ldots, g_k) \cap K[x_{s+1}, \ldots, x_n] = (0)$
6: **if** $\exists g \in G$ tale che $lm(g) = x_j^{k_j}$ per ogni $j = s+1, \ldots, n$ **then**
7: **return** s
8: **else**
9: Scegliere un altro cambio di coordinate e ripetere.
10: **end if**

Ovviamente questo algoritmo risulta essere pesante, in quanto richiede il calcolo di una base di Gröbner lessicografica e il calcolo del cambio di coordinate.

Notiamo che, fissato un ordinamento monomiale su $K[x]$ di eliminazione per un sottoinsieme delle indeterminate U e un ideale I di $K[x]$, se U è indipendente modulo $(\operatorname{lt} I)$, allora è indipendente modulo I. Infatti $\operatorname{lt}(I) \cap K[U] = (0)$ implica $I \cap K[U] = (0)$. Dunque conoscere la dimensione di $\operatorname{lt}(I)$ è utile per conoscere quella di I.

Per gli ideali monomiali, calcolare la dimensione è molto più semplice.

Definizione 2.8. Sia $I = (m_1, \dots, m_s)$ un ideale monomiale di $K[x_1, \dots, x_n]$. Definiamo ricorsivamente

$$d(I, K[x_1, \dots, x_n]) \coloneqq \max \left\{ d(I|_{x_i=0}, K[x_1, \dots, \hat{x}_i, \dots, x_n]) \middle|^{x_i \text{ compare}}_{\text{in un } m_j} \right\}$$

e

$$d(0, K[x_1, \dots, x_s]) = s$$

Proposizione 2.9. Sia I un ideale monomiale di $K[x_1, \dots, x_n]$. Allora

$$d(I, K[x_1, \dots, x_n]) = \dim {}^{K[x_1, \dots, x_n]}\!/_{I}$$

Dimostrazione. Sia $I = (m_1, \dots, m_s)$. Notiamo che ogni primo che contiene I contiene necessariamente una variabile che compare in un dato m_i. Dunque per ogni primo minimale p di I esiste x_r tale che $x_r \mid m_i$ e $x_r \in p$. Allora $I|_{x_r=0} \subseteq p|_{x_r=0}$ e dunque per ipotesi induttiva

$$d(I|_{x_r=0}, K[X \setminus \{x_r\}]) = \dim {}^{K[X \setminus \{x_r\}]}\!/_{I|_{x_r=0}}$$

D'altronde

$$\dim {}^{K[X \setminus \{x_r\}]}\!/_{I|_{x_r=0}} \geq \dim {}^{K[X \setminus \{x_r\}]}\!/_{p|_{x_r=0}} = \dim {}^{K[X]}\!/_{p}$$

Da cui segue una disuguaglianza. Se valesse la disuguaglianza stretta, esisterebbe un x_i tale che

$$\begin{aligned}
\dim {}^{K[X]}\!/_{I} &< d(I, K[X]) \\
&= d(I|_{x_i=0}, K[X \setminus \{x_i\}]) \\
&= \dim {}^{K[X \setminus \{x_i\}]}\!/_{I|_{x_i=0}} && \text{ipotesi induttiva} \\
&= \dim {}^{K[x]}\!/_{(I, x_i)} \\
&\leq \dim {}^{K[x]}\!/_{I}
\end{aligned}$$

da cui un assurdo.

□

2.3 Ideali 0-dimensionali

Definizione 2.10. Sia A un anello noetheriano e sia $I \subseteq A$ un ideale. Chiamiamo i primi associati di I

$$\mathrm{Ass}(I) = \{p \in \mathrm{Spec}(A) \mid \exists b \in A \text{ t.c. } p = (I : b)\}$$

Chiamiamo primi associati di A i primi di $\mathrm{Ass}(0)$.
Un primo $p \in \mathrm{Ass}(I)$ si dice immerso se esiste $q \in \mathrm{Ass}(I)$ tale che $q \subseteq p$, minimale altrimenti.
Sia $p \in \mathrm{Spec}(A)$ e $I \subseteq A$. Chiamiamo gli associati a I relativamente a p

$$\mathrm{Ass}(I, p) = \{q \in \mathrm{Ass}(I) \mid q \subseteq p\}$$

Proposizione 2.11.

1. Se q è p-primario, allora p è primo.
2. Se q, q' sono p-primari, $q \cap q'$ è p-primario.
3. Se q è p-primario e $b \in A \setminus q$, allora $(q : b)$ è p-primario. Inoltre $(q : b) \supsetneq q$ se e solo se $b \in p$.
4. Se $p' \supseteq q$ e q è un ideale primario, allora $q^{ec} = q$ rispetto alla mappa $A \to A_{p'}$
5. Se A è un anello noetheriano e q è p-primario, esiste $d \in A$ tale che $p = (q : d)$. In particolare, se q è p-primario, $p \in \mathrm{Ass}(q)$.

Dimostrazione.

3. Mostriamo che $(q : b)$ è p-primario. Sia $\alpha\beta \in (q : b)$ e supponiamo che $\alpha \notin p = \sqrt{(q : b)}$. Dalla relazione $\alpha\beta b \in q$, otteniamo allora $\beta b \in q$, da cui $\beta \in (q : b)$. Se $b \in p \setminus q$, esiste $n \geq 2$ tale che $b^n \in q$. Sia m il minimo di tali n. Allora $b^{m-1}b \in q$ e dunque $b^{m-1} \in (q : b) \setminus q$. Se invece $(q : b) \supsetneq q$, esiste $a \in (q : b) \setminus q$ tale che $ab \in q$. Dato che $a \notin q$, deve valere $b \in p$, da cui la tesi.
4. È sufficiente notare che dato un qualsiasi ideale I, $I^{ec} = \cup_{s \in S}(I : s)$. Dato che q è primario, per ogni $x \in A$ la relazione $sx \in q$ implica $x \in q$, da cui la tesi.
5. Se $q = p$, è sufficiente considerare $d = 1$. Supponiamo allora $q \subsetneq p$ e sia $g_1 \in p \setminus q$. Allora $(q : g_1) \supsetneq q$. Se $(q : g_1) = p$ abbiamo terminato, altrimenti possiamo iterare il ragionamento scegliendo $g_2 \in p \setminus (q : g_1)$. Quindi
$$((q : g_1) : g_2) = (q : g_1 g_2) \supsetneq (q : g_1)$$
e così via. Per noetherianità, la catena deve essere stazionaria e dunque la tesi.

□

Teorema 2.12. Sia A un anello noetheriano e sia I un ideale di A. Sia $I = \cap_{i=1}^{s} Q_i$ una decomposizione primaria minimale. Allora
$$\mathrm{Ass}(I) = \{\sqrt{Q}_1, \ldots, \sqrt{Q}_s\}$$
Se $\mathrm{Ass}(I, p) = \{\sqrt{Q_{i_1}}, \ldots, \sqrt{Q_{i_s}}\}$ con $p \in \mathrm{Ass}(I)$, allora $Q_{i_1} \cap \cdots \cap Q_{i_s}$ è indipendente dalla decomposizione.

Dimostrazione. Sia $p \in \mathrm{Ass}(I)$. Allora esiste $b \in A$ tale che $p = (I : b)$. Di conseguenza,
$$(I : b) = \cap(Q_i : b) = p$$
La stessa relazione deve valere quindi passando ai radicali, da cui esiste i tale che $p = \sqrt{Q_i}$ per irriducibilità degli ideali primi. Di conseguenza, $\mathrm{Ass}(I) \subseteq$

$\{\sqrt{Q}_1, \ldots, \sqrt{Q}_s\}$.
Mostriamo l'altra inclusione. Fissato un indice i, sia

$$J = \bigcap_{\substack{j=1 \\ j \neq i}}^{s} Q_j$$

Per minimalità della decomposizione, $J \not\subseteq Q_i$. Sia allora $d \in J \setminus Q_i$. Otteniamo

$$(I : d) = \cap(Q_j : d) = (Q_i : d)$$

Per il punto 5 della precedente proposizione, $\sqrt{Q}_i$ è allora un primo associato, da cui la tesi.
Per il secondo punto, è sufficiente sfruttare la proprietà dimostrata sulla localizzazione. □

Occupiamoci ora di trovare effettivamente una decomposizione. Notiamo che per anelli euclidei e PID, la decomposizione si riduce alla fattorizzazione. In più variabili, è necessario basarsi sulla dimensione. Supponiamo inizialmente $I = \sqrt{I}$ e che K sia un campo algebricamente chiuso. Allora I è intersezione di massimali

$$I = \cap \mathfrak{M}_i$$

con $\mathfrak{M}_i = (x_1 - a_1^i, \ldots, x_n - a_n^i)$. Vale il seguente:

Proposizione 2.13. Siano $I, J \subseteq K[y]$ ideali comassimali e siano

$$I_1 = (x - a, I) \qquad\qquad J_1 = (x - b, J)$$

ideali di $K[x, y]$. Allora esiste $c \in K[y]$ tale che $I_1 \cap J_1 = (x - c, IJ)$.

Di conseguenza, applicando ripetutamente il teorema e supponendo $a_n^i \neq a_n^j$, si ha

$$\sqrt{I} = (x_1 - g_1(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n))$$

Definizione 2.14. Sia p un ideale massimale di $K[x]$. p è in posizione generale se esistono $g_1, \ldots, g_n \in K[x_n]$ tali che

$$p = (x_1 - g_1(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n))$$

Diciamo che un ideale zero dimensionale è in posizione generale se ogni primo associato lo è e $p_i \cap K[x_n] \neq p_j \cap K[x_n]$ per ogni $i \neq j$ e per ogni $p_i \in \mathrm{Ass}(I)$.

Proposizione 2.15. Sia K un campo a caratteristica zero e sia I un ideale 0-dimensionale di $K[x]$. Allora esiste un aperto di Zariski U di K^{n-1} non vuoto tale che per ogni $a = (a_1, \ldots, a_{n-1}) \in U$ il cambio di coordinate

$$\begin{array}{rccc} \varphi_a\colon & K[x] & \longrightarrow & K[x] \\ & x_i & \longmapsto & x_i \qquad\qquad i = 1, \ldots, n-1 \\ & x_n & \longmapsto & x_n + \sum_{i=1}^{n-1} a_i x_i \end{array}$$

porti I in posizione generale.

Dimostrazione. Supponiamo dapprima che I sia un massimale. Allora $K[x]/I$ è un'estensione finita di K (Nullstellensatz) e vista l'ipotesi sulla caratteristica vale $K[x]/I = K(\alpha)$ per il teorema dell'elemento primitivo. In particolare, dalla dimostrazione di tale teorema discende che possiamo scegliere $\alpha = x_n + \sum_{i=1}^{n-1} a_i x_i$. Consideriamo allora l'isomorfismo

$$\begin{array}{ccc} K[x_1,\dots,x_n] & \longrightarrow & K[x_1,\dots,x_n] \\ x_i & \longmapsto & x_i \\ x_n & \longmapsto & x_n + \sum_{i=1}^{n-1} a_i x_i \end{array}$$

Dopo questo cambio di coordinate, vale

$$K(\alpha) = {}^{K[x_n]}\!\diagup_{g_n(x_n)}$$

e per ogni altra indeterminata x_i, si ha che $x_i = g_i(x_n)$. Di conseguenza $x_i - g_i(x_n) \in I$. Supponiamo ora che I sia un qualunque ideale 0-dimensionale. Consideriamo la decomposizione primaria minimale

$$I = \bigcap_{i=1}^{s} q_i$$

con primi associati p_i. Dato che intersezione finita di aperti di Zariski non vuoti è non vuota, esiste un cambiamento di coordinate che porta ogni p_i in posizione generale. Dunque possiamo supporre che ogni primo associato sia già in posizione generale. Vogliamo allora trovare un nuovo cambio di coordinate che separi gli zeri degli ideali di eliminazione di ogni p_i. Sia $a \in K^{n-1}$ e sia φ_a il corrispettivo cambio di coordinate e supponiamo che $\varphi_a(p_i)$ sia ancora in posizione generale per ogni i. Fissiamo $p = p_i = (x_1 - g_1(x_n), \dots, x_{n-1} - g_{n-1}(x_n), g_n(x_n))$ e sia $h_n(x_n)$ il generatore di $\varphi_a(p) \cap K[x_n]$. Notiamo che g_n e h_n devono avere lo stesso grado, in quanto φ_a è un isomorfismo. Inoltre, dette $\alpha_1, \dots, \alpha_s$ le radici di g_n in $\bar{K}$, si ha che le radici di h_n sono $\alpha_i + \sum a_j g_j(\alpha_i)$. Infatti,

$$p\bar{K}[x] = \bigcap_{i=1}^{l} (x_1 - g_1(\alpha_i), \dots, x_{n-1} - g_{n-1}(\alpha_i), x_n - \alpha_i)$$

e dunque

$$\begin{aligned} \varphi_a(p)\bar{K}[x] &= \bigcap_{i=1}^{s} \varphi_a(x_1 - g_1(\alpha_i), \dots, x_{n-1} - g_{n-1}(\alpha_i), x_n - \alpha_i) \\ &= \bigcap_{i=1}^{s} (x_1 - g_1(\alpha_i), \dots, x_{n-1} - g_{n-1}(\alpha_i), x_n - \alpha_i + \sum_j a_j x_j) \\ &= \bigcap_{i=1}^{s} (x_1 - g_1(\alpha_i), \dots, x_{n-1} - g_{n-1}(\alpha_i), x_n - \alpha_i + \sum_j a_j g_j(\alpha_i)) \end{aligned}$$

Dunque la condizione che le radici siano coincidenti (ossia che gli ideali di eliminazione siano uguali) è un chiuso di Zariski di K^{n-1} (le cui equazioni sono date dalle uguaglianze delle varie radici), da cui la tesi. □

Abbiamo necessità ora di trovare un test per capire se un ideale è in posizione generale. Infatti, non troviamo davvero un $a \in K^{n-1}$ che porti l'ideale in posizione generale, perché probabilisticamente ogni cambio di coordinate va bene.

Proposizione 2.16. I seguenti fatti sono equivalenti:

1. I è un ideale 0-dimensionale primario e in posizione generale rispetto a $x_1 > x_2 > \cdots > x_n$.
2. Detta G la base di Gröbner ridotta di I rispetto all'ordinamento lessicografico, esistono $g_1, \ldots, g_n \in K[x_n]$ e naturali $r_1, \ldots, r_n$ tali che
   - $g_n^{r_n} \in G$ e g_n è irriducibile
   - $(x_j + g_j)^{r_j}$ è uguale a un elemento di $G \cap K[x_j, \ldots, x_n]$ modulo $(x_{j+1} + g_{j+1}, \ldots, x_{n-1} + g_{n-1}, g_n)$.
3. Esistono $g_1, \ldots, g_n \in K[x_n]$ e $r_1, \ldots, r_n \in \mathbb{N}$ tali che
   - $I \cap K[x_n] = (g_n^{r_n})$ con g_n irriducibile.
   - Per ogni $j < n$ vale $(x_j + g_j)^{r_j} \in I$

Dimostrazione.

(1) $\Rightarrow$ (2) Sia $J = \sqrt{I}$; dato che I è 0-dimensionale, primario e in posizione generale, vale

$$J = (x_1 - g_1(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n))$$

con g_n irriducibile. Per la proprietà di eliminazione dell'ordinamento lessicografico, esiste $g \in G$ tale che $K[x_n] \cap I = (g)$; di conseguenza, $g = g_n^{r_n}$ (a meno di scegliere i polinomi monici). Sia ora $1 \leq j \leq n-1$. Dato che I è 0-dimensionale e G è ridotta, esiste un unico $h \in G$ tale che $lm(h) = x_j^{m_j}$. Consideriamo l'ideale di eliminazione $J' = J \cap K[x_{j+1}, \ldots, x_n]$ e il campo $K' = K[x_{j+1}, \ldots, x_n]/J' = K[x_n]/(g_n)$. Abbiamo la proiezione

$$\phi \colon K[x_1, \ldots, x_n] \longrightarrow K'[x_1, \ldots, x_j]$$

Mostriamo che $\phi(G \cap K[x_j, \ldots, x_n]) = \{\phi(h), 0\}$. Ci basta mostrare che per ogni $f \in G \cap K[x_j, \ldots, x_n]$ vale $\phi(f) = 0$. Sia $f \neq h$. Possiamo scrivere f come

$$f = \sum_{i=0}^{s} f_i x_j^i$$

Dato che S è ridotta e $lm(h) = x_j^m$, deve essere necessariamente $s < m$. Consideriamo allora l'ideale

$$L = (f_s \in K[x_{j+1}, \ldots, x_n] \mid \exists f_0, \ldots, f_{s-1}, s < m, \text{ tali che } \sum_{i=0}^{s} f_i x_j^i \in I)$$

Notiamo che L è un ideale proprio; se infatti $1 \in L$, potremmo trovare un polinomio $p \in I$ tale che $lm(p) = x^r$ con $r < s$, e questo è assurdo dato che avevamo supposto che la base fosse ridotta. Inoltre, $L \supseteq I \cap K[x_{j+1}, \ldots, x_n]$. Se infatti $g \in I \cap K[x_{j+1}, \ldots, x_n]$, allora g si scrive

come combinazione degli elementi di S nei quali non compaiono le variabili $x_1, \ldots, x_j$ nei leading monomial e questi appartengono singolarmente a L, da cui il contenimento voluto. Dato che I è primario e 0-dimensionale, lo stesso vale per $I \cap K[x_{j+1}, \ldots, x_n]$ e dunque $\sqrt{I} \cap K[x_{j+1}, \ldots, x_n]$ è l'unico ideale primo associato a L, ossia $L \subseteq \sqrt{I} \cap K[x_{j+1}, \ldots, x_n]$. Ora, possiamo cambiare f nel seguente modo

$$f' = x^{m-s} f - h f_s \in I$$

Possiamo scrivere $f' = \sum_{i=0}^{m-1} f'_i x_j^i$, da cui $f'_{m-1} \in L$. Ma $f'_i \equiv f_{i+s-m} \pmod{L}$ e dunque $f_{s-1} \in L$. Induttivamente $f_i \in L$ per ogni i, da cui $f \in J'$.

Allora, $\sqrt{\phi(I)} = \phi(J)$ e dunque

$$\sqrt{\phi(I)} \cap K'[x_j] = x_j + \bar{g}_j$$

dove $\bar{g}_j \equiv g_j \pmod{J'}$. Di conseguenza, $\phi(I) \cap K'[x_j] = (x_j + \bar{g}_j)^l$, da cui la tesi.

(2) $\Rightarrow$ (3) Notiamo che $g_n \in \sqrt{I}$ e, applicando l'ipotesi, induttivamente si ottiene $g_j + x_j \in \sqrt{I}$. Di conseguenza $\sqrt{I} = (x_1 + g_1(x_n), \ldots, x_{n-1} + g_{n-1}(x_n), g_n(x_n))$ per massimalità e dunque I soddisfa la tesi.

(3) $\Rightarrow$ (1) Ovvio, perché

$$J = (x_1 + g_1(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)) \subseteq \sqrt{I}$$

è un ideale massimale e dunque deve valere l'uguaglianza. D'altronde, J è in posizione generale da cui la tesi.

□

Dunque, possiamo supporre di lavorare con ideali in posizione generale. In questo caso, il problema ha una soluzione particolarmente semplice:

Proposizione 2.17. Sia I un ideale 0-dimensionale in posizione generale e sia g il generatore di $I \cap K[x_n]$. Consideriamo la fattorizzazione di $g = \prod g_i^{e_i}$ in fattori irriducibili. Allora

$$I = \bigcap_{i=1}^{s} (I, g_i^{e_i})$$

è una decomposizione primaria di I.

Dimostrazione. Mostriamo intanto che $(I, g_i^{e_i})$ è primario. Notiamo che tale ideale è proprio. Supponiamo infatti che esista $f \in I$ tale che $f + a \cdot g_i^{e_i} = 1$. Detto $g^i = g/g_i^{e_i}$, si ha allora $g^i = f g^i + a g$, da cui $g^i \in (f, g) \subseteq I$. Allora $g^i \in I \cap K[x_n] = (g)$ da cui un assurdo, in quanto $\deg(g^i) < \deg(g)$.
Siano ora $p_1, \ldots, p_l$ i primi associati a I e sia $(f_i) = p_i \cap K[x_n]$. Allora

$$\cap p_i \cap K[x_n] = \cap (f_i) = \left(\prod f_i \right)$$

D'altronde, $\cap p_i \cap K[x_n] = \sqrt{I} \cap K[x_n]$ e dato che $I \cap K[x_n] = (g)$ si ha necessariamente che

$$\prod_{i=1}^{l} f_i \mid g \qquad\qquad g \mid \prod_{i=1}^{l} f_i^k$$

per qualche k. Di conseguenza il numero di fattori di g coincide con il numero di primi associati a I e possiamo quindi supporre che $g_i = f_i$ a meno di riordinare i fattori. Di conseguenza ogni p_i contiene solo uno dei fattori di g e dunque $(I, g_i^{e_i})$ ha radicale massimale, dunque è primario.
Mostriamo ora che quella trovata è effettivamente una decomposizione primaria. Sicuramente vale

$$I \subseteq \bigcap_{i=1}^{s} (I, g_i^{e_i})$$

Mostriamo l'altro contenimento. Come in precedenza, sia

$$g^i = \frac{g}{g_i^{e_i}}$$

Notiamo che tali g^i sono coprimi e dunque esistono $a_i \in K[x]$ tali che $\sum a_i g^i = 1$. Sia allora $f \in \cap(I, g_i^{e_i})$. Esistono quindi $f_i \in I$ e $\xi_i \in K[x]$ tali che

$$f = f_i + \xi_i g_i^{e_i} \quad i = 1, \ldots, s$$

Di conseguenza,

$$f = f \cdot 1 = f \sum a_i g^i = \sum a_i g^i f = \sum a_i g^i (f_i + \xi_i g_i^{e_i}) = \underbrace{\sum a_i g_i f_i}_{\in I} + \underbrace{\sum a_i \xi_i g}_{\in I}$$

da cui la tesi. □

Possiamo ora scrivere lo pseudocodice dell'algoritmo per la decomposizione primaria di un ideale 0-dimensionale in posizione generale:

Algoritmo 2.2 Decomposizione primaria di un ideale 0-dimensionale

1: Input: I
2: Calcolare una base di Gröbner di I rispetto all'ordinamento $x_1 > \cdots > x_n$
3: Porre $g_n = G \cap K[x_n]$
4: Fattorizzare $g = \prod g_i^{e_i}$
5: Porre $q_i = (I, g_i^{e_i})$
6: **return** $[q_1, \ldots, q_k]$

2.4 Ideali di dimensione maggiore

Nel caso che l'ideale abbia dimensione positiva, vogliamo ricondurci tramite localizzazione al caso 0-dimensionale. In particolare useremo il seguente lemma:

Lemma 2.18. Sia A un anello e S un sottoinsieme moltiplicativamente chiuso. Sia I un ideale di A. Allora se $s \in S$ è tale che $I^{ec} = (I : s)$, allora

$$I = (I : s) \cap (I, s)$$

Dimostrazione. Dato che $(I : s) \supseteq I$ (è sempre vero), vale $I \subseteq (I : s) \cap (I, s)$. Mostriamo il viceversa. Sia $x \in (I : s) \cap (I, s)$; x si scrive allora come $x = as + i$, con $i \in I$. Basta mostrare allora che $as \in I$. Dato che $x \in (I : s)$, vale $sx = as^2 + si \in I$, da cui $as^2 \in I$. Dunque

$$\frac{as^2}{1} \in I^e \Longrightarrow \frac{as^2}{s^2} = \frac{a}{1} \in I^e \Longrightarrow a \in I^{ec} = (I : s)$$

Dunque $as \in I$ e dunque $x \in I$. □

Vogliamo sfruttare il lemma per costruire un sottoinsieme moltiplicativamente chiuso S tale che I^e sia 0-dimensionale. In questo modo, per i primi associati che non intersecano S possiamo utilizzare la corrispondenza biunivoca. Per gli altri, bisogna calcolare la decomposizione primaria di (I, s), che avrà dimensione maggiore di I. L'idea è quella di utilizzare come sottoinsieme S quello generato dalle variabili che non intersecano I.

Proposizione 2.19. Sia I un ideale di $K[X]$ e sia U un insieme massimale di variabili algebricamente indipendenti di $K[X]/I$.

1. I esteso in $K(U)[X \setminus U]$ è zero-dimensionale.
2. Sia $G = (g_1, \ldots, g_s) \subseteq K[X]$ è una base di Gröbner ridotta di I^e e consideriamo i g_i in $K[U][X \setminus U]$. Detto $h = lcm(lc(g_1), \ldots, lc(g_s)) \in K[U]$, si ha che
$$I^{ec} = I \stackrel{\infty}{:} h = I : h^m$$
con m tale che $(I : h^m) = (I : h^{m+1})$.
3. Se $I^e = Q_1 \cap \cdots \cap Q_s$ è una decomposizione primaria irridondante di I^e, allora $I^{ec} = Q_1^c \cap \cdots \cap Q_s^c$ è una decomposizione primaria irridondante di I^{ec}.

Dimostrazione.

1. Segue dalla teoria della dimensione sulle k-algebre.
2. Chiaramente vale l'inclusione $I^{ec} \supseteq I \stackrel{\infty}{:} h$. Mostriamo il viceversa. Sia $f \in I^{ec}$. Notiamo che f riduce a 0 se diviso per G in $K(U)[X \setminus U]$ e dunque
$$f = \sum_{i=1}^{s} a_i g_i$$
L'algoritmo di divisione richiede al massimo di dividere per i leading coefficient dei g_i e dunque $a_i \in K[x]_h$, da cui segue l'altro contenimento.
3. Notiamo preliminarmente che la contrazione di un ideale primario è primario e che $(I \cap J)^c = I^c \cap J^c$. Di conseguenza $I^{ec} = Q_1^c \cap \cdots \cap Q_s^c$ è una decomposizione primaria di I. Mostriamo allora l'irridondanza.
   - Supponiamo per assurdo che $\sqrt{Q_i^c} = \sqrt{Q_j^c}$ e mostriamo che questo implica che $\sqrt{Q_i} = \sqrt{Q_j}$. Se $f \in \sqrt{Q_i}$, allora $f^m \in Q_i$. Preso $h \in K[U]$ tale che $hf^m \in Q_i^c$, si ha $hf \in \sqrt{Q_i^c} = \sqrt{Q_j^c}$. Di conseguenza $f \in \sqrt{Q_j}$, da cui un assurdo per l'irridondanza.

- Supponiamo per assurdo che $Q_i^c \supseteq \cap_{j\neq i} Q_j^c$. Sia $f \in \cap_{j\neq i} Q_j^c$. Allora esiste $h \in K[U]$ tale che $hf \in \cap_{j\neq i} Q_j^c \subseteq Q_i^c$. Dunque $f \in Q_i$, da cui un assurdo per l'irridondanza della decomposizione.

□

Abbiamo quindi un algoritmo per la riduzione al caso 0-dimensionale.

Algoritmo 2.3 Riduzione al caso 0-dimensionale

1: Trovare un insieme massimale di variabili algebricamente indipendenti
2: Calcolare una base di Gröbner $\tilde{G}$ con $X \setminus U > U$
3: Se $\tilde{G} = \{g_1, \ldots, g_s\} \subseteq K[U][X \setminus U]$, porre $f = lcm(lc(g_i)) \in K[U]$.
4: Calcolare $m \in \mathbb{N}$ tale che $(I : f^m) = (I : f^{m+1})$ e porre $h = f^m$.
5: **return** $(U, \tilde{G}, h)$

Calcolo del radicale La stessa idea utilizzata per il calcolo della decomposizione primaria si può utilizzare per il calcolo del radicale di un ideale. Infatti, sappiamo calcolare il radicale nel caso 0-dimensionale; basta infatti calcolare dei polinomi univariati g_i in ogni variabile (che esistono perché $K[X]/I$ è uno spazio vettoriale di dimensione finita) e calcolare la loro fattorizzazione squarefree $\tilde{g}_i$. Nel caso di un ideale di dimensione positiva, possiamo calcolare un insieme di variabili U algebricamente indipendenti su $K[X]/I$ e considerare la mappa $K[X] \to K(U)[X \setminus U] = S^{-1}K[X]$. Preso $h \in S$ tale che $I^{ec} = (I : h)$, si ha

$$\sqrt{I} = \sqrt{(I:h)} \cap \sqrt{(I,h)} = \sqrt{I^{ec}} \cap \sqrt{(I,h)} = \sqrt{I^e}^c \cap \sqrt{(I,h)}$$

Sappiamo calcolare il radicale di I^e perché è 0-dimensionale; basta allora trovare il radicale di (I, h), che ha dimensione minore di I.

Decomposizione Equidimensionale

Definizione 2.20. Sia A un anello noetheriano e sia I un ideale di A con decomposizione primaria irridondante $I = \cap_{i=1}^s Q_i$. Sia Σ l'insieme degli ideali della decomposizione tali che $\dim A/I = \dim A/Q_i$ e definiamo $E(I) = \cap_{Q_i \in \Sigma} Q_i$. Diciamo che I è equidimensionale se $E(I) = I$. Un anello A è equidimensionale se (0) è equidimensionale.

Esempio. L'ideale $I = (x^2, xy) \subseteq K[x, y]$ non è equidimensionale perchè

$$I = (x) \cap (x^2, y)$$

e I ha dimensione 1, mentre (x^2, y) ha dimensione 0.

Calcolare la decomposizione equidimensionale è semplice a partire da una decomposizione primaria, perché basta conoscere la dimensione degli ideali della decomposizione primaria.

Definizione 2.21. Sia I un ideale di $K[X]$ senza componenti immerse e sia $I = \cap Q_j$ una decomposizione primaria irridondante. Chiamiamo

$$E_r(I) = \bigcap_{\substack{i=1 \\ \dim Q_i = r}}^{x} Q_i$$

la componente r-dimensionale di I.

Lemma 2.22. Sia $I = \cap_{i=1}^{s} Q_i$ una decomposizione primaria irridondante di un ideale I di $K[X]$. Sia $E(I)$ la decomposizione equidimensionale di I. Allora

$$I = E(I) \cap (I : E(I))$$

e $\dim A/(I : E(I)) < \dim A/I$.

Dimostrazione. Sia $E(I) = \cap_{i=1}^{k} Q_i$. Calcoliamo $I : E(I)$:

$$\begin{aligned} I : E(I) &= \Big(\bigcap_{i=1}^{s} Q_i : \bigcap_{j=1}^{k} Q_j \Big) \\ &= \Big(\bigcap_{i=1}^{k} Q_i : \bigcap_{j=1}^{k} Q_j \Big) \cap \Big(\bigcap_{i=k+1}^{s} Q_i : \bigcap_{j=1}^{k} Q_j \Big) \\ &= \Big(\bigcap_{i=k+1}^{s} Q_i : \bigcap_{j=1}^{k} Q_j \Big) \\ &= \bigcap_{i=k+1}^{s} (Q_i : E(I)) \end{aligned}$$

Per irridondanza della decomposizione, $E(I) \not\subseteq p_i = \sqrt{Q_i}$ per ogni $i = k+1, \ldots, s$ e quindi $(Q_i : E(I)) = Q_i$ per il lemma 2.11. Si ha quindi la tesi. □

Capitolo 3

Normalizzazione

3.1 Conduttore e ideali test

Ci poniamo ora il problema di trovare la chiusura integrale di un anello in un campo. La teoria fornisce i seguenti risultati:

Teorema 3.1. Sia A un dominio noetheriano integralmente chiuso e sia $K = Q(R)$. Sia E un'estensione finita e separabile di K. Allora $\overline{A}^E$ è finita su A.

Dimostrazione. Sia $\beta_1, \ldots, \beta_n$ una base di E su K intera su A e sia $\gamma_1, \ldots, \gamma_n$ la base duale tramite il prodotto scalare definito da $\mathrm{Tr}_{E/K}$. Sia $x \in \overline{A}$. Allora x si scrive in termini della base duale

$$x = \sum_{i=1}^{n} a_i \gamma_i$$

con $a_i \in K$ per ogni i. Mostriamo che $a_i \in A$. In tal modo $\bar{A} \subseteq A[\gamma_1, \ldots, \gamma_n]$, da cui la tesi per noetherianità. Calcoliamo $\mathrm{Tr}(x\beta_j)$:

$$\mathrm{Tr}(x\beta_j) = \sum_{i=1}^{n} a_i \,\mathrm{Tr}(\beta_j \gamma_i) = a_i$$

Dato che $x\beta_j$ è intero su A, si ha $\mathrm{Tr}(x\beta_j) \in A$ da cui la tesi. □

Corollario 3.2. Sia A una K-algebra finitamente generata che sia un dominio e supponiamo $\mathrm{char}\, K = 0$. Allora la chiusura integrale $\overline{A}$ di A in $Q(A)$ è finita su A.

Dimostrazione. Per il lemma di normalizzazione di Noether, esistono $x_1, \ldots, x_n$ in A algebricamente indipendenti tali che A sia finito su $B = K[x_1, \ldots, x_n]$. Per il teorema precedente, la chiusura integrale di B in $Q(A)$ è finita su $K[x_1, \ldots, x_n]$ ($K[x_1, \ldots, x_n]$ è integralmente chiuso e noetheriano) e dunque lo è anche la chiusura integrale di A. □

Proposizione 3.3. Sia A un dominio. Sono equivalenti:

1. A è integralmente chiuso

2. A_p è integralmente chiuso per ogni $p \in \mathrm{Spec}(A)$
3. A_m è integralmente chiuso per ogni $m \in \mathrm{Spec}\, M(A)$

Definizione 3.4. Sia A un dominio noetheriano. Definiamo il non-normal locus di A come

$$N(A) = \{p \in \mathrm{Spec}(A) \mid A_p \neq \overline{A}_p\}$$

Definiamo il conduttore di A in $\overline{A}$ come

$$C = \{b \in Q(A) \mid b\overline{A} \subseteq A\} = (A :_{Q(A)} \overline{A})$$

In realtà il conduttore poteva anche essere definito come $(A :_A \overline{A})$. Chiaramente vale il contenimento $\supseteq$; per l'altro, basta notare che se $x \in (A :_{Q(A)} \overline{A})$, allora $x \cdot 1 \in A$ dato che $1 \in \overline{A}$ e dunque $x \in A$. Quindi il conduttore è un ideale di A e può essere caratterizzato come il più grande ideale di A che è anche un ideale di $\overline{A}$, cioè se J è un ideale di A e di $\overline{A}$, allora $J \subseteq C$. Infatti, $J\overline{A} = J \subseteq A$ e dunque $J \subseteq C$.

Lemma 3.5. Sia A un dominio noetheriano. Allora $\overline{A}$ è una A-algebra finita se e solo se $C \neq 0$.

Dimostrazione.

$\Longrightarrow$ Supponiamo che $\overline{A}$ sia finita su A e siano $x_1, \ldots, x_k$ dei generatori. Dato che $x_i \in Q(A)$, allora $x_i = a_i/b_i$, con $a_i, b_i \in A$. Detto $b = \prod b_i$, si ha $b\overline{A} \subseteq A$, da cui $C \neq 0$.

$\Longleftarrow$ Sia $c \in C$. Allora $c\overline{A} \subseteq A$ e dunque è un sottomodulo di un modulo noetheriano, dunque finito. Dato che A è un dominio, $c\overline{A} \simeq \overline{A}$ da cui la tesi.

□

Proposizione 3.6. Sia A un dominio noetheriano e supponiamo che $\overline{A}$ sia una A-algebra finita. Allora $N(A) = V(C) = \{p \in \mathrm{Spec}(A) \mid p \supseteq C\}$.

Dimostrazione.

$\subseteq$ Mostriamo che se $p \notin V(C)$, allora $p \notin N(A)$. Sia $p \notin V(C)$ e sia $s \in C \setminus p$. Vogliamo mostrare che $\overline{A}_p = A_p$. Sia $x \in \overline{A}_p$; allora $x = a/t$ con $a \in \overline{A}$ e $t \in A \setminus p$. Dunque

$$x = \frac{as}{ts} \in A_p$$

$\supseteq$ Siano $x_1, \ldots, x_n$ dei generatori di $\overline{A}$ su A. Allora

$$C = (A :_A \overline{A}) = \bigcap_{i=1}^{m} (A :_A x_i)$$

Di conseguenza

$$V(C) = V\Big(\bigcap_{i=1}^{m} (A :_A x_i)\Big) = \bigcup_{i=1}^{m} V(A :_A x_i)$$

Basta allora mostrare che $V(A : x) \subseteq N(A)$ per ogni $x \in \overline{A}$. Sia $x \in \overline{A}$ e supponiamo che $p \notin N(A)$. Sappiamo che $A_p = \overline{A}_p$ e $x \in \overline{A} \subseteq \overline{A}_p = A_p$. Dunque $x = a/s$ con $a \in A$ e $s \in A \setminus p$. Dunque $sx \in A$ e $s \in (A : x)$. Dato che $s \notin p$, $p \not\supseteq (A : x)$.

□

Lemma 3.7. Sia A un dominio noetheriano e supponiamo che $\overline{A}$ sia finita su A. Sia J un ideale non nullo di A. Allora

$$A \subseteq (J :_{Q(A)} J) \subseteq \overline{A}$$

Dimostrazione. Intanto, notiamo che $(J :_{Q(A)} J)$ è una A-algebra. Ci basta mostrare che se $x \in (J :_{Q(A)} J)$, allora x è intero su A. Sia $\varphi_x \colon J \to J$ la mappa di moltiplicazione per x. Per noetherianità di A, J è finitamente generato e possiamo utilizzare il teorema di Hamilton-Cayley. Dunque esistono $a_i \in A$ tali che $\varphi_x^n + \sum a_i \varphi_x^i = 0$. Dato che A è un dominio, $x^n + \sum a_i x^i = 0$ e dunque x è intero su A. □

Teorema 3.8 (Criterio di normalità)**.** Sia A un dominio noetheriano e supponiamo che $\overline{A}$ sia finita su A. Sia J un ideale radicale non nullo tale che $N(A) \subseteq V(J)$. Allora A è integralmente chiuso se e solo se $A = (J :_{Q(A)} J)$.

Dimostrazione.

$\Longrightarrow$ Segue banalmente dal lemma precedente.

$\Longleftarrow$ Basta mostrare che $\overline{A} \subseteq (J :_{Q(A)} J)$.

- Per prima cosa, mostriamo che $(J :_{Q(A)} J) = \overline{A} \cap (A :_{Q(A)} J)$. Chiaramente vale l'inclusione $\subseteq$. Sia allora $x \in \overline{A}$ tale che $xJ \subseteq A$. x induce per moltiplicazione un endomorfismo φ_x di $\overline{A}$, che è finito su A. Per il teorema di Hamilton-Cayley, esistono $a_i \in A$ tali che

  $$\varphi_x^n + \sum a_i \varphi_x^i = 0$$

  Dunque per $j \in J$ vale

  $$x^n j^n + j \sum a_i x^i j^{n-1} = 0$$

  cioè $x^n j^n \in J$. Dato che J è radicale, $xj \in J$.
- Mostriamo ora che $\overline{A} \subseteq (A :_{Q(A)} J)$. Sia $x \in \overline{A}$ e $I = (A : x)$. Per quanto visto precedentemente, $V(I) \subseteq N(A) \subseteq V(J)$ e dunque $\sqrt{I} \supseteq \sqrt{J}$. Per noetherianità, esiste $n \in \mathbb{N}$ tale che $J^n \subseteq I$. Sia m il minimo di questi e supponiamo per assurdo che $m > 1$. Notiamo che $J^m \subseteq I$ se e solo se $xJ^m \subseteq A$. Dunque esiste $j \in J^{m-1}$ tale che $xj \notin A$. D'altronde $xjJ \subseteq xJ^m \subseteq A$ e $xj \in \overline{A}$, da cui $xj \in \overline{A} \cap (A :_{Q(A)} J) = (J :_{Q(A)} J)$. Per ipotesi quest'ultimo è uguale a A e dunque $xj \in A$, da cui un assurdo. Di conseguenza $J \subseteq I$, ossia $xJ \subseteq A$ e $x \in (A : J)$, come voluto.

□

Definizione 3.9. Sia I un ideale non nullo di $K[X]$. I è un ideale test se è radicale e $N(A) \subseteq V(J)$.

Proposizione 3.10. Sia A un dominio noetheriano e supponiamo che $\overline{A}$ sia finita su A. Allora esiste un ideale test.

Dimostrazione. Per quanto dimostrato precedentemente, l'ideale conduttore C è non nullo. Sia allora $c \in C$ un elemento non nullo. Allora $J = \sqrt{c}$ è un ideale test. □

Scriviamo allora lo pseudocodice dell'algoritmo:

Algoritmo 3.1 Chiusura integrale

```
Trovare J ideale test.
Calcolare A_1 = (J :_{Q(A)} J)
if A = A_1 then
    return A
else
    A = A_1 e ripetere
end if
```

L'algoritmo è corretto per quanto visto in precedenza e termina per noetherianità. Il problema è che, per quanto visto fino ad ora, è necessario cambiare ad ogni iterazione l'anello su cui si lavora; cerchiamo un metodo per ridurre tutto a operazioni sull'anello A.

Proposizione 3.11. Sia A un dominio e sia $J \subseteq A$ un ideale non nullo. Se $p \in J$ è un elemento non nullo, $(J :_{Q(A)} J) = \frac{1}{p}(pJ :_A J)$.

Dimostrazione. Notiamo che

$$(J :_{Q(A)} J) = \frac{1}{p}(pJ :_{Q(A)} J)$$

e dunque basta mostrare che $(pJ :_{Q(A)} J) = (pJ :_A J)$. Chiaramente $(pJ :_{Q(A)} J) \supseteq (pJ :_A J)$. Sia allora $x \in Q(A)$ tale che $xJ \subseteq pJ$. In particolare $xp = pj$ con $j \in J$. Dato che A è un dominio e $p \neq 0$ si ha $x = j$. □

Proposizione 3.12. Sia A un dominio noetheriano e supponiamo che $\overline{A}$ sia finita su A. Sia $A \subseteq A' \subseteq \overline{A}$ un'estensione intermedia e sia J un ideale test per A. Allora $J' = \sqrt{J^e}$ è un ideale test per A'.

Dimostrazione. Chiaramente $J' \neq (0)$, $J' \neq A'$ per il lying over e J' è radicale per definizione. Siano C e C' gli ideali conduttori rispettivamente di A e di A'. Basta mostrare che $V_{A'}(J') \supseteq V_{A'}(C')$. Notiamo che $C \subseteq C'$ e dunque

$$V(C') \subseteq V(C)$$

Inoltre, dato che $V_A(C) \subseteq V_A(J)$, deve anche valere $V_{A'}(C) \subseteq V_{A'}(J^e) = V_{A'}(J')$, da cui la tesi. □

Abbiamo ora il problema della rappresentazione di A_1 come R-algebra:

Proposizione 3.13. Sia R un dominio noetheriano, sia $J \subseteq R$ un ideale test. Sia $d \in J$ e consideriamo dei generatori $d, u_1, \ldots, u_r$ di $(dJ :_R J)$ come R-modulo. Consideriamo l'omomorfismo di R-algebre

$$\begin{array}{rccc} \pi\colon & R[x_1,\ldots,x_n] & \longrightarrow & \frac{1}{d}(dJ :_A J) \\ & x_i & \longmapsto & \frac{u_i}{d} \end{array}$$

Allora:

1. per ogni $i \leq j$ esistono $\xi_k^{(ij)} \in R$ tali che

$$u_i u_j = \sum_{k=0}^{r} d\xi_k^{(ij)} u_k$$

2. presi dei generatori delle sizigie $Syz(u_1, \ldots, u_r) = \langle \eta^0, \ldots, \eta^s \rangle_R \subseteq R^r$ e detto

$$I = \Big(x_i x_j - \sum_{k=0}^{r} d\xi_k^{(ij)} x_k \mid 1 \leq i \leq j \leq r \Big) + \Big(\sum_i \eta_i^h x_i \mid h = 1, \ldots, s \Big)$$

allora $I = \mathrm{Ker}(\pi)$.

Dimostrazione.

1. Dato che $1/d(dJ : J)$ è un anello generato da $1, u_1/d, \ldots, u_r/d$ come R-modulo, si ha che il prodotto di due elementi appartiene ancora all'anello e dunque esistono $\xi_k^{(ij)}$ tali che

$$\frac{u_i}{d}\frac{u_j}{d} = \sum_{k=0}^{r} \xi_k^{(ij)} \frac{u_k}{d}$$

da cui il primo punto.

2. Chiaramente vale un'inclusione. Sia allora $h \in \mathrm{Ker}(\pi)$. Allora, utilizzando le relazioni di I, possiamo scrivere

$$h \equiv h_0 + \sum_{i=0}^{r} h_i x_i \pmod{I}$$

Applicando ϕ, otteniamo $h_0 + \sum_{i=0}^{r} h_i u_i/d = 0$, dunque h è una sizigia da cui il contenimento voluto.

□

In questo modo abbiamo trovato una rappresentazione in termini di elementi di R di ogni anello A_i che compare nel corso dell'algoritmo. Rimane il problema di determinare un ideale test. Se $\mathrm{char}\, K = 0$ e $A = K[x_1, \ldots, x_n]/I$, con $I = (f_1, \ldots, f_n)$, possiamo considerare la matrice Jacobiana $\mathcal{J}_f(x) = (\partial f_i/\partial x_j)_{i,j}$. Il criterio Jacobiano ci dice che la localizzazione in un massimale è regolare se il rango della matrice Jacobiana calcolata nel massimale è $n - r$, dove $r = \dim A$. Dato che un anello locale regolare è integralmente chiuso, questo ci fornisce un metodo per trovare un ideale contenuto nel conduttore. Detto infatti J l'ideale generato dai determinanti dei minori $(n - r)$ di $\mathcal{J}_f$, si ha $J \subseteq C$. In realtà, si può mostrare che se α è un elemento primitivo intero per l'estensione e f è il suo polinomio minimo (che supponiamo separabile), allora $f'(\alpha)$ appartiene al conduttore. Vale infatti il seguente

Proposizione 3.14. Sia α un elemento primitivo di L/K intero su A e supponiamo che L/K sia separabile. Sia $f \in A[x]$ il polinomio minimo di α e consideriamo

$$\frac{f}{x - \alpha} = \sum_{i=0}^{n-1} \beta_i x^i \in L[x]$$

Allora la base duale di $1, \alpha, \ldots, \alpha^{n-1}$ rispetto al prodotto scalare indotto dalla traccia è

$$\frac{\beta_0}{f'(\alpha)}, \ldots, \frac{\beta_{n-1}}{f'(\alpha)}$$

Da questo, dato che il generato dalla base duale contiene $\bar{A}$ e i β_i sono interi su A, si ha che $f'(\alpha) \in C$.

3.2 Anelli a ideali principali e basi intere

Supponiamo ora che R sia un PID e proviamo a specializzare l'algoritmo a questo caso. Chiamiamo allora $A = R[\alpha]$, dove α è un elemento primitivo intero di L su K con polinomio minimo $p_\alpha \in R[x]$ (supponiamo sempre che L/K sia separabile). Chiaramente allora l'anello $R[\alpha]$ è un'estensione intera di R che ha come campo dei quozienti L; purtroppo, raramente questo coincide con la chiusura integrale di R in L. Abbiamo comunque un buon punto di partenza per l'algoritmo. In queste ipotesi, siamo in grado di definire il discriminante $\mathrm{disc}(\alpha)$ (come il risultante tra p_α e p'_α dato che p_α è monico) e di fattorizzarlo:

$$\mathrm{disc}(\alpha) = \prod_{i=1}^{n} p_i^{e_i}$$

Questo fornisce un metodo semplice per trovare un ideale test:

Proposizione 3.15. Sia R un PID e sia K il suo campo dei quozienti. Sia $L = K(\alpha)$ un'estensione separabile di campi e supponiamo che α sia intero su R. Allora $\mathrm{disc}(\alpha)\overline{R} \subseteq R[\alpha]$.

Dimostrazione. Sia F il campo di spezzamento del polinomio minimo f di α e siano $\alpha = \alpha_1, \ldots, \alpha_n$ le sue radici. Sia S la chiusura intera di R in F e notiamo che per interezza ogni α_i appartiene a S. Consideriamo la matrice

$$M = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \cdots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

e sia $d = \det M = \prod(\alpha_i - \alpha_j)$. Notiamo che $d^2 = \mathrm{disc}(\alpha) \in Q(A)$. Sia $G = \mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_l\}$ e sia $b = \sum c_i \alpha^i$ un elemento di $\overline{R} = \overline{R}^L$. Ci basta mostrare che $d^2 c_i \in R$. Notiamo che

$$M \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} \sigma_{i_1}(b) \\ \sigma_{i_2}(b) \\ \vdots \\ \sigma_{i_n}(b) \end{pmatrix} \in S^n$$

Per la formula del metodo di Cramer,

$$c_i = \frac{\det M_i}{\det M}$$

dove M_i è la matrice ottenuta sostituendo alla i-esima colonna di M il termine noto del sistema lineare. Notiamo che $\det M_i \in S$ perché ogni $\sigma_j(b) \in S$ e dunque $\det(M)c_i \in S$. Dunque $d^2 c_i \in Q(A) \cap S = R$ da cui la tesi. □

Con questo teorema, possiamo applicare la teoria della sezione precedente e concludere. Possiamo però arrivare a questo risultato mediante la teoria sugli anelli di Dedekind.

Definizione 3.16. Sia $J \subseteq A$ un ideale. Definiamo idealizzatore di J l'anello

$$Id(J) = (J : J) = \{u \in Q(A) \mid uJ \subseteq J\}$$

Definiamo inverso di J come

$$J^{-1} = (A :_{Q(A)} J)$$

J è invertibile se $JJ^{-1} = A$.

Sappiamo che un anello è di Dedekind se e solo se ogni ideale non nullo è invertibile. Sfruttiamo questa proprietà e il fatto che il discriminante è invariante per localizzazione:

Lemma 3.17. Sia R un PID, sia $K = Q(R)$ e sia L un'estensione finita e separabile di K. Sia A un anello intero su R e sia $p \in \mathrm{Spec}(A)$. Sia $v_1, \ldots, v_n$ una base di L/K di elementi di A e sia $\Delta = \mathrm{disc}(v_1, \ldots, v_n)$. Se p non è invertibile allora $p \supseteq \Delta$.

Dimostrazione. Notiamo che i primi che non contengono Δ sono tali che A_p è normale. Infatti Δ è invertibile nel localizzato e il discriminante appartiene al conduttore, da cui $A_p = \overline{A}_p$ Sia allora p un ideale che non contiene Δ. Dato che essere invertibile è una proprietà locale, basta verificare che pA_q è invertibile per ogni $q \in \mathrm{Spec}(A)$. Dato che A ha dimensione 1, è sufficiente dimostrare che pA_p è invertibile. Ma A_p è integralmente chiuso e quindi è un dominio di Dedekind. Di conseguenza ogni ideale non nullo è invertibile e in particolare lo è pA_p, da cui la tesi. □

In base al lemma basta quindi verificare solo i primi che contengono il discriminante.

Corollario 3.18. Supponiamo che $A \neq \overline{A}$ e sia $A = \langle \alpha_1, \ldots, \alpha_n \rangle$. Allora esiste $p \in \mathrm{Spec}(A)$ tale che $p \supseteq \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ e p non è invertibile.

Dimostrazione. Se A non è integralmente chiuso in L, allora A non è un dominio di Dedekind. Di conseguenza esiste $p \in \mathrm{Spec}(A)$ non invertibile da cui la tesi. □

Abbiamo già mostrato nel lemma 3.7 che l'idealizer di un ideale è intero su A e dunque

Proposizione 3.19. A è integralmente chiuso se e solo se l'idealizzatore di ogni ideale primo che contiene il discriminante è uguale ad A.

Dimostrazione. Se A è integralmente chiuso, per ogni ideale J vale $(J : J) = A$ dal lemma 3.7, da cui la tesi. Se A non è integralmente chiuso, allora esiste un ideale massimale m di A non invertibile (che dunque contiene il discriminante). Dunque $m \subseteq m^{-1}m \subsetneq A$ e per massimalità deve valere $m = m^{-1}m$. Allora per definizione $Id(m) \supseteq m^{-1} \supsetneq A$ da cui la tesi. □

Lemma 3.20. Siano I, J ideali di A. Allora

$$Id(IJ) \supseteq Id(J) \qquad\qquad Id(IJ) \supseteq Id(I)$$

Dimostrazione. Sia $x \in Id(I) = (I : I)$. Allora $xI \subseteq I$ e dunque $xIJ \subseteq IJ$, ossia $x \in Id(IJ)$. □

Corollario 3.21. A è integralmente chiuso se e solo se $Id(\sqrt{\Delta}) = A$

Dimostrazione. Se A è integralmente chiuso, allora $Id(\sqrt{\Delta}) = A$ in quanto per il lemma 3.7 è un sovranello intero su A. Viceversa, se $Id(\sqrt{\Delta}) = A$, detti $p_1, \ldots, p_n$ i primi che contengono il discriminante, si ha

$$A = Id(\sqrt{\Delta}) \supseteq Id(p_i)$$

e dunque $Id(p_i) = A$ per ogni i. □

Possiamo allora fornire l'outline dell'algoritmo di normalizzazione su un PID, partendo da $A = R[\alpha]$ con α elemento primitivo di L su $K = Q(R)$ intero su R:

Algoritmo 3.2 Normalizzazione su PID

1: Calcolare Δ di A su R
2: Porre $J = \sqrt{\Delta}$
3: Calcolare $Id(J) = (J :_{Q(A)} J)$
4: **if** $Id(J) \neq A$ **then**
5: $\quad A = Id(J)$ e ripetere
6: **else**
7: $\quad$ **return** A
8: **end if**

In realtà l'algoritmo è uguale a quello dato in precedenza; ci siamo però arrivati utilizzando strumenti diversi. Inoltre disponiamo di un metodo efficace per il calcolo di un ideale test. Infatti il discriminante di α può essere calcolato come $\mathrm{Ris}(f, f')$, dove f è il polinomio minimo di α. In questo caso, possiamo anche utilizzare la forma normale di Hermite per il calcolo dell'idealizer e del radicale. Sia infatti $J \subseteq A$ un ideale e consideriamone un insieme di generatori $J = (m_1, \ldots, m_n)$ come modulo su A. Sia $x \in Id(J)$. Allora $xm_i \in J$ e dunque

$$xm_i = \sum_{i=1}^{n} a_{ij} m_i$$

con gli a_{ij} in R. Consideriamo allora l'applicazione

$$\begin{array}{rccc} \psi_{m_i}: & A & \longrightarrow & A \\ & a & \longmapsto & am_i \end{array}$$

e sia M_i la matrice che rappresenta tale mappa. Possiamo estendere tale mappa al campo dei quozienti; dato $u \in Q(A)$, abbiamo allora che $u \in Id(J)$ se e solo se um_i appartiene al sottospazio generato da $m_1, \ldots, m_k$ su R per ogni i. Detta allora M la matrice $n^2 \times n$

$$M = \begin{bmatrix} M_1 \\ \vdots \\ M_k \end{bmatrix}$$

si ha che questo equivale a trovare i vettori $v \in Q(A)^n$ tali che $Mv \in Span(m_1, \dots, m_k)$. Dunque siamo interessati a risolvere i k sistemi

$$M \cdot x = \begin{bmatrix} [m_i] \\ [m_i] \\ \vdots \\ [m_i] \end{bmatrix}$$

dove con $[m_i]$ abbiamo indicato il vettore delle coordinate di $[m_i]$.
Occupiamoci ora del calcolo del radicale. Ci interessa trovare il radicale dell'estensione di un primo, cioè $J = \sqrt{p^e} \subseteq A$ con $p \subseteq R$. Notiamo che se $u \in J$, preso $f(x) = x^m + \sum a_i x^i$ il suo polinomio minimo, si ha $a_i \in p$.

Definizione 3.22. Definiamo l'ideale p-traccia come

$$(p - tr) \coloneqq \{u \in A \mid \forall w \in A \; p \mid \mathrm{Tr}(uw)\}$$

Notiamo che la traccia di un elemento $x \in J$ coincide con $-\frac{m}{n} a_{m-1}$, dove a_i sono i coefficienti del polinomio minimo di x e $n = [Q(A) : Q(R)]$. Di conseguenza se $u \in J$ allora $u \in (p - tr)$. Infatti per ogni $x \in A$ si ha $ux \in J$ e dunque la sua traccia appartiene a J e dunque $u \in (p - tr)$. In realtà sotto certe condizioni vale il viceversa:

Teorema 3.23. Sia q la caratteristica di R/p. Se $q > n$ o $q = 0$, allora $\sqrt{p^e} = (p - tr)$.

Dimostrazione. Sia $w \in (p - tr)$ e consideriamo $E = Q(R[w])$. Consideriamo la traccia E/K; allora $\mathrm{Tr}(w^k)$ appartiene a p per ogni $k > 0$. Detto $s_k = \mathrm{Tr}(w^k)$, vale per $1 \leq k \leq n$ (identità di Newton)

$$a_{m-k} s_1 + \cdots + (-1)^{k-2} a_{m-1} s_{k-1} + (-1)^{k-1} s_k = k a_{m-k}$$

Di conseguenza induttivamente $a_i \in p$ e dunque $w \in \sqrt{p^e}$. □

Utilizzando la forma normale di Hermite, possiamo allora calcolare facilmente il radicale nei casi come sopra. Sia infatti $(w_1, \dots, w_n)$ una base di A su R. Allora

$$\begin{aligned} (p - tr) &= \{u \in A \mid \forall w \in A \; p \mid \mathrm{Tr}(uw)\} \\ &= \{u \in A \mid \mathrm{Tr}(uw_i) \equiv 0 \pmod{p} \; \forall i\} \\ &= \{u = \sum u_j w_j \in A \mid \sum_j u_j \, \mathrm{Tr}(w_i w_j) \equiv 0 \pmod{p} \; \forall i\} \end{aligned}$$

Di conseguenza $u \in (p - tr)$ se e solo se, detta $M = (m_{ij})$ con $m_{ij} = \mathrm{Tr}(w_i w_j)$ la matrice delle tracce, si ha

$$M \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \in pR^n$$

La riduzione in forma di Hermite può far perdere informazioni sull'appartenenza di u a R^n. Notiamo però che

$$u \in R^n \iff pI_n u \in pR^n$$

e dunque basta considerare la matrice

$$\begin{pmatrix} M \\ pI_n \end{pmatrix}$$

e ridurla in forma di Hermite. Dato che la matrice M ha rango n, la forma di Hermite corrispondente ha le prime n righe linearmente indipendenti e le altre sono nulle. Sia quindi N il minore $n \times n$ dato dalle prime n righe e chiamiamo $\tilde{N}_i$ le colonne di N^{-1}. Abbiamo allora che $p\tilde{N}_1, \ldots, p\tilde{N}_n$ è una base di $(p - tr)$. Ci manca ora da considerare il caso in cui la caratteristica del quoziente q sia maggiore di n. Sia allora $k \in \mathbb{N}$ tale che $q^k > n$ e consideriamo l'endomorfismo di Frobenius

$$\begin{array}{rccc} \varphi\colon & A/p^e & \longrightarrow & A/p^e \\ & a & \longmapsto & a^{q^k} \end{array}$$

Lemma 3.24. $\mathrm{Ker}(\varphi) = \mathfrak{N}(A/p^e)$.

Dimostrazione. Chiaramente, un elemento nel nucleo appartiene al nilradicale, in quanto $x^{q^k} = 0$. Viceversa, sia $x \in \mathfrak{N}(A/p^e)$. x induce per moltiplicazione un endomorfismo φ_x di R/p-spazi vettoriali su A/p^e che necessariamente è nilpotente. Dunque tutti gli autovalori di φ_x sono nulli e il suo polinomio caratteristico è $p(t) = t^n$. Di conseguenza, $x^n = 0$ e dunque, visto che $q^k > n$, $x^{q^k} = 0$. □

Il lemma permette allora di ricondurre il problema al calcolo del nucleo dell'endomorfismo di Frobenius. Dunque basta scrivere la matrice che rappresenta tale applicazione e trovare il nucleo; anche per questo è necessario il calcolo di una forma normale di Hermite.

Capitolo 4

Decomposizione di un anello artiniano

In questo capitolo, ci occupiamo di fornire un metodo costruttivo per fornire la decomposizione data dal teorema di struttura degli anelli artiniani:

Teorema 4.1. Sia A un anello artiniano. Allora A si decompone come prodotto diretto di anelli artiniani locali.

Dimostrazione. Dato che A è artiniano, il nilradicale è nilpotente e dunque esiste $n \in \mathbb{N}$ tale che $\mathfrak{N}(A)^n = 0$. Dato che $\mathfrak{N}(A) = \prod \mathfrak{M}_i$ è prodotto di tutti i massimali, si ha $\mathfrak{M}_1^n \dots \mathfrak{M}_k^n = 0$. Per il teorema cinese del resto,

$$A = {}^{A}\!\diagup_{\mathfrak{N}(A)^n} \simeq \prod {}^{A}\!\diagup_{\mathfrak{M}_i^n}$$

e ogni fattore è artiniano locale. □

Trovare la decomposizione è equivalente a trovare gli idempotenti che generano ogni fattore.

Proposizione 4.2. Sia A una B algebra finita. Le seguenti sono equivalenti:

1. Esistono $A_1, \dots, A_n$ B-algebre finite tali che $A \simeq \prod A_i$
2. Esistono $u_1, \dots, u_n \in A$ idempotenti tali che $\sum u_i = 1$ e $u_i u_j = 0$.

Dimostrazione.

(1) ⇒ (2) È sufficiente considerare $u_i = (0, \dots, 0, 1, 0, \dots, 0)$.

(2) ⇒ (1) Sia $a \in A$. Allora

$$a = \sum_{i=1}^{n} u_i a$$

e dunque gli $A \simeq \sum \langle u_i \rangle$. Mostriamo che tale somma è diretta per induzione sul numero di elementi idempotenti. Se $n = 2$,sia $d \in \langle u_1 \rangle + \langle u_2 \rangle$. Mostriamo che $d \neq 0$.

$$d = au_1 = bu_2 \Longrightarrow du_1 = au_1^2 = au_1 = bu_1 u_2 = 0 \Longrightarrow au_1 = 0$$

Induttivamente, si conclude che la somma è diretta.

□

Troviamo quindi un metodo per individuare una famiglia di idempotenti.

Definizione 4.3. Sia B una $\mathbb{Q}$-algebra artiniana e sia $b \in B \setminus \{0,1\}$. Due idempotenti a, b sono ortogonali se $ab = 0$. Diciamo che a contiene b se $ab = b$. Un idempotente a si dice primitivo se non contiene propriamente un altro idempotente.

4.1 Algebre artiniane su campi finiti

La strategia che adotteremo per trovare gli idempotenti della decomposizione sarà quella di trovare gli idempotenti di una opportuna algebra su $\mathbb{F}_p$ e sollevare tali idempotenti sui razionali. Occupiamoci allora di un metodo per individuarli nel primo caso.

Proposizione 4.4. Sia A una $\mathbb{F}_q$-algebra artiniana e sia $\varphi\colon A \to A$ l'endomorfismo di Frobenius. Detto $A^\varphi = \mathrm{Fix}(\varphi)$, valgono i seguenti:

- $\dim_{\mathbb{F}_q} A^\varphi = \#\operatorname{Spec} M(A)$
- A^φ è generato dagli idempotenti di A

Dimostrazione. Per il teorema di struttura degli anelli artiniani, possiamo supporre che A sia locale. Vogliamo mostrare allora che A^φ ha dimensione 1 come $\mathbb{F}_q$-spazio vettoriale. L'idea della dimostrazione è quella di mostrare che A^φ è un anello locale artiniano e ridotto. Infatti, un anello artiniano locale e ridotto è un campo e quindi A^φ sarebbe isomorfo a $\mathbb{F}_{q^r}$ per un qualche $r \in \mathbb{N}$. Dato che per definizione A^φ è fissato dal Frobenius, avremmo $r = 1$ da cui seguirebbe la tesi.

- A^φ ha dimensione finita come $\mathbb{F}_q$-spazio vettoriale in quanto sottospazio di A e dunque A^φ è artiniano.
- A^φ non contiene nilpotenti. Supponiamo infatti che $a^n = 0$; possiamo distinguere due casi:

  $$\begin{cases} m \geq q & 0 = a^m = a^{m-q}a^q = a^{m-q+1} & \Rightarrow q = 1 \text{ per minimalità} \\ m < q & a = a^q = 0 & \Rightarrow a = 0 \end{cases}$$

  e dunque si ha un assurdo.
- A^φ è locale. Per il teorema di struttura degli anelli artiniani, basta mostrare che non contiene idempotenti non banali. Questo è però ovvio, in quanto l'operazione su A^φ è la restrizione dell'operazione su A e A non contiene idempotenti non banali.

□

Lemma 4.5. Sia A una $\mathbb{F}_q$-algebra locale e finita. Per ogni $a \in A$ il polinomio caratteristico dell'applicazione lineare

$$\begin{array}{rccc} \varphi_a\colon & A & \longrightarrow & A \\ & x & \longmapsto & ax \end{array}$$

è potenza di un irriducibile di $\mathbb{F}_q[x]$.

Dimostrazione. Sia $a \in A$ e sia μ il polinomio minimo di φ_a. Supponiamo per assurdo che $\mu = q(x)r(x)$ con $(q, r) = 1$. Dato che μ è il generatore dell'ideale, è il polinomio monico di grado minimo che si annulla in a.

Per Bezout, sappiamo che esistono $s, t \in \mathbb{F}_q[x]$ tali che $qs+rt = 1$. Mostriamo che $q(a)s(a)$ e $t(a)r(a)$ sono idempotenti.

$$\begin{aligned} q(a)^2 s(a)^2 &= q(a)s(a)(1 - t(a)r(a)) \\ &= q(a)s(a) - \underbrace{q(a)r(a)}_{=\mu(a)=0} s(a)t(a) \\ &= q(a)s(a) \end{aligned}$$

Considerato che A è locale, questi devono essere idempotenti banali e dunque possiamo supporre senza perdita di generalità che $q(a)s(a) = 1$ e $t(a)r(a) = 0$. Questo implica che $q(a)$ è invertibile e dunque dalla relazione

$$0 = \mu(a) = q(a)r(a)$$

otteniamo $r(a) = 0$, da cui un assurdo in quanto avevamo supposto che μ fosse il polinomio di grado minimo che si annulla in a. □

Osservazione 4.6. Grazie a questa proposizione, possiamo scegliere in maniera casuale $a \in A$ e considerare l'omomorfismo di moltiplicazione φ_a. Dalla fattorizzazione del polinomio caratteristico, possiamo allora isolare qualche componente della decomposizione.

Per trovare gli idempotenti, in base a quanto visto è necessario intanto conoscere A^φ, in modo da poter trovare poi gli idempotenti. Questa può essere trovata come il nucleo di $\varphi - \mathrm{Id}$, dove φ è l'endomorfismo di Frobenius. Dai generatori trovati di A^φ, possiamo trovare gli idempotenti. Sia $d = \dim A^\varphi$. Se $d = 1$, A è locale e non ci sono idempotenti non banali. Supponiamo quindi $d > 1$. Allora $A^\varphi \simeq \prod_{i=1}^{d} \mathbb{F}_q$; distinguiamo due casi:

$q = 2^m$ Se $m = 1$, la base trovata è composta proprio dagli elementi idempotenti cercati. Se $m > 0$, sia $v \in A^\varphi$ uno degli elementi della base trovata. Allora $u = \sum_{i=0}^{m-1} v^{2^i}$ è un idempotente. Infatti

$$u^2 = \sum_{i=0}^{m-1} v^{2^{i+1}} = u$$

in quanto $v^{2^m} = v$. Ragionando per componente, la probabilità che $u_i = 1$ o $u_i = 0$ è uguale a $1/2$ in entrambi i casi. Infatti la mappa

$$\begin{array}{rccc} \psi\colon & \mathbb{F}_q & \longrightarrow & \mathbb{F}_2 \\ & x & \longmapsto & \sum_{i=0}^{m-1} x^{2^{i+1}} \end{array}$$

è un omomorfismo surgettivo di gruppi e dunque la metà delle classi ha immagine 1 e l'altra metà 0.

$q = p^m$, $p \neq 2$ Sia $v \in A^\varphi$. Detto $t = v^{(q-1)/2}$, si ha che uno tra

$$e_1 = \frac{t(t+1)}{2} \qquad\qquad e_2 = \frac{t(t-1)}{2}$$

è un idempotente non banale, purchè $t \neq 0, \pm 1$. Infatti, lavorando su una singola componente t_i del prodotto, si ha che t_i può essere solo 0,± 1. Quindi, dopo la moltiplicazione per $t \pm 1$, e_i potrà essere solo 0, 1 e dunque e_1 ed e_2 sono idempotenti. In particolare, uno dei due è necessariamente non banale. Per vedere questo, ragioniamo per casi.

- Supponiamo dapprima che vi sia una componente nulla 0. Se tutte le altre componenti sono 1, allora e_1 è non banale, mentre se sono -1 e_2 è non banale. Se invece esiste una componente 1, una -1 e una nulla entrambi sono non banali.
- Supponiamo che non vi siano componenti nulle: allora esiste almeno una componente t_i uguale a -1 (perché t è non banale). In questo caso, moltiplicando per $t + 1$ otteniamo $(e_1)_i = 0$ e quindi e_1 è un idempotente non banale oppure 0. Ma se $e_1 = 0$, allora ogni t_i doveva essere uguale a -1, contro le ipotesi.

4.2 Sollevamento degli idempotenti

Sfruttiamo allora la facilità di lavorare sui campi finiti per sollevare gli idempotenti su $\mathbb{Q}$. Intanto, per ridurci a un campo finito abbiamo necessità di lavorare con algebre libere su $\mathbb{Z}$. Notiamo che presa una base $\mathcal{B} = (\alpha_1, \ldots, \alpha_n)$ su $\mathbb{Q}$, possiamo esprimere i prodotti come combinazione degli elementi della base

$$\alpha_i \alpha_j = \sum_{k=1}^{n} c_{ijk} \alpha_k$$

e $c_{ijk} \in \mathbb{Q}$ vengono dette *costanti di struttura*.

Proposizione 4.7. Sia A una $\mathbb{Q}$-algebra finita. Allora esiste una $\mathbb{Z}$-algebra libera e finita $A_\mathbb{Z}$ tale che $A \simeq A_\mathbb{Z} \otimes_\mathbb{Z} \mathbb{Q}$.

Dimostrazione. Sia $\mathcal{B} = (\alpha_1, \ldots, \alpha_n)$ una base di A su $\mathbb{Q}$ e sia d il minimo comune multiplo dei denominatori delle costanti di struttura. Allora

$$\alpha_i \alpha_j = \sum_{k=1}^{n} c_{i,j,k} \alpha_k = \sum_{k=1}^{n} \frac{b_{i,j,k}}{d} \alpha_k$$

con $b_{i,j,k} \in \mathbb{Z}$. Dunque, detto $\beta_i = d\alpha_i$, si ha che $\mathcal{B}' = (\beta_1, \ldots, \beta_n)$ è ancora una $\mathbb{Q}$-base di A con costanti di struttura in $\mathbb{Z}$ e dunque genera una $\mathbb{Z}$-algebra $A_\mathbb{Z}$. Dato che per costruzione $A_\mathbb{Z} \otimes_\mathbb{Z} \mathbb{Q} \simeq A$, si ha la tesi. □

Ci serve ora capire quali denominatori compaiono nella scrittura di un elemento idempotente di A, per scegliere in modo appropriato il primo da scegliere.

Lemma 4.8. Sia A una $\mathbb{Z}$-algebra libera, finita e ridotta e sia $A_\mathbb{Q} = A \otimes_\mathbb{Z} \mathbb{Q}$. Allora la chiusura intera di A in $A_\mathbb{Q}$ è contenuta in $(1/d)A$, dove

$$d = \max\{b \mid b^2 \mid \operatorname{disc}(A)\}$$

Dimostrazione. In queste ipotesi, la traccia è un prodotto scalare non degenere, quindi $\overline{A}$ è finita su A (basta ripetere la dimostrazione della finitezza della chiusura integrale sui PID) e come modulo è libero su $\mathbb{Z}$, con lo stesso rango di A. Notiamo che

$$\operatorname{disc}(A) = \left|{}^{\overline{A}}\!/_{A}\right|^2 \operatorname{disc}(\overline{A})$$

e dunque

$$\left|{}^{\overline{A}}\!/_{A}\right|^2 = \frac{\operatorname{disc}(A)}{\operatorname{disc}(\overline{A})}$$

Dato che il discriminante varia per quadrati, si ha la tesi. □

Ogni idempotente è intero perché soddisfa il polinomio $p(x) = x^2 - x$. Quindi, in base al lemma e alla proposizione precedente, dato un idempotente $u \in A$, possiamo scrivere

$$u = \frac{1}{d} \sum_i u_i \alpha_i$$

con $u_i \in \mathbb{Z}$. Se scegliamo $p \in \mathbb{Z}$ tale che $p \nmid d$, possiamo sollevare gli idempotenti senza problemi. Dunque ci siamo ridotti a lavorare su $\mathbb{Z}$-algebre. Vediamo ora di capire come sollevare degli idempotenti; in particolare vogliamo dimostrare il seguente:

Proposizione 4.9. Sia A un anello e sia $p \subseteq A$ un ideale. Per $k \geq 1$, definiamo

$$A_k = {}^{A}\!/_{p^k}$$

Se $u_k \in A_k$ è un idempotente non banale, esiste un unico $u \in A_{2k}$ idempotente tale che $u \equiv u_k \pmod{p^k}$.

Dimostreremo questa proposizione tramite alcuni lemmi. Intanto mostriamo l'unicità del sollevamento:

Lemma 4.10. Sia A un anello e sia $p \subseteq A$ un ideale. Siano u, v idempotenti $\pmod{p^2}$ e supponiamo $u \equiv v \pmod{p}$. Allora $u \equiv v \pmod{p^2}$.

Dimostrazione. Vale

$$v \equiv v^2 \equiv (u + (v-u))^2 \equiv u^2 + 2u(v-u) + (v-u)^2 \equiv u + 2u(v-u) \pmod{p^2}$$

Di conseguenza,

$$(1-2u)(v-u) \equiv 0 \pmod{p^2}$$

D'altronde,

$$(1-2u)^2 \equiv 1 + 4u^2 - 4u \equiv 1 \pmod{p^2}$$

e dunque è invertibile. Abbiamo allora ottenuto $u \equiv v \pmod{p^2}$, come voluto. □

Per quanto concerne l'esistenza, l'idea è quella di applicare il metodo di Newton per costruire una successione di idempotenti. Consideriamo quindi la funzione

$$f(x) = x^2 - x$$

Se u approssima uno zero di f, allora

$$\hat{u} = u - \frac{f(u)}{f'(u)}$$

è una approssimazione migliore. Nel nostro caso,

$$\hat{u} = u - \frac{u^2 - u}{2u - 1}$$

Dato che $(2u-1)^2 \equiv 1$, si ha

$$\hat{u} \equiv u + (1-2u)(u^2-u) = u^2(3-2u)$$

Ad ogni iterazione, $\hat{u}$ non è detto che sia idempotente, ma

$$\hat{u}^2 - \hat{u} = (u^2-u)^2(4(u^2-u)-3)$$

Sfruttando questa idea, possiamo allora dimostrare la proposizione:

Dimostrazione della proposizione 4.9. Basta definire $u = u_k^2(3-2u_k)$. Infatti, dalla formula sull'errore segue immediatamente che u è idempotente in A^{2k}. Inoltre, in A_k,

$$u \equiv u_k(3-2u_k) \equiv 3u_k - 2u_k = u_k$$

da cui la tesi. □

Dato che vorremmo applicare il metodo a famiglie di idempotenti, vorremmo che l'ortogonalità fosse mantenuta dall'algoritmo.

Lemma 4.11. Siano u, v idempotenti modulo p^2 e ortogonali modulo p. Allora u, v sono ortogonali modulo p^2.

Dimostrazione. Notiamo che

$$uv \equiv u^2v^2 \equiv (uv)^2 \pmod{p^2}$$

Dato che $uv \equiv 0 \pmod{p}$, si ha $(uv)^2 \equiv 0 \pmod{p^2}$, da cui la tesi. □

Corollario 4.12. Siano $u_1, \ldots, u_{n-1} \in A_k$ idempotenti ortogonali tali che $\sum u_i = 1$ e siano $w_1, \ldots, w_{n-1}$ sollevamenti in A_{2k}. Posto $w_n = 1 - \sum w_j$, allora $w_1, \ldots, w_n$ sono idempotenti ortogonali in A_{2k} e $\sum w_i = 1$.

Dimostrazione. Dai lemmi visti in precedenza, basta verificare che w_n sia idempotente e ortogonale agli altri. Verifichiamo prima l'idempotenza

$$\begin{aligned}
w_n^2 &= \Big(1 - \sum_{i=1}^{n-1} w_i\Big)^2 \\
&= 1 + \sum_{i=1}^{n-1} w_i^2 - 2\sum_{i=1}^{n-1} w_i^2 - 2\sum_{i\neq j} w_i w_j \\
&= 1 - \sum_{i=1}^{n-1} w_i^2 \\
&= 1 - \sum_{i=1}^{n-1} w_i \\
&= w_n
\end{aligned}$$

Verifichiamo ora l'ortogonalità:

$$w_i w_n = \Big(1 - \sum_{j=1}^{n-1} w_j\Big) w_i = w_i - \sum_{j=1}^{n-1} w_i w_j = w_i - w_i^2 = 0$$

□

Corollario 4.13. Ogni famiglia di idempotenti ortogonali $u_1, \dots, u_n$ a somma 1 di $A/\mathfrak{N}(A)$ si estende in modo unico a A.

Il corollario ci permette allora di considerare solo algebre ridotte, a patto di saper calcolare il nilradicale. D'altronde, vale il seguente:

Lemma 4.14. Sia A una $\mathbb{Q}$-algebra artiniana. Allora

$$\mathfrak{N}(A) = \{u \in A \mid \operatorname{Tr}(uv) = 0 \ \forall v \in A\}$$

Dimostrazione. Se $u \in \mathfrak{N}(A)$, allora l'applicazione di moltiplicazione

$$\begin{array}{rccc} \varphi_u \colon & A & \longrightarrow & A \\ & v & \longmapsto & uv \end{array}$$

è nilpotente e dunque $\operatorname{Tr}(u) = \operatorname{Tr}(\varphi_u) = 0$ (una mappa nilpotente ha tutti gli autovalori nulli e la traccia è la somma degli autovalori). Viceversa, sia $u \in A$ tale che $\operatorname{Tr}(uv) = 0$ per ogni $v \in A$. Allora $\operatorname{Tr}(u^k) = 0$ per ogni $k \in \mathbb{N}$. Detta A la matrice che rappresenta φ_u in una base qualsiasi, mostriamo per induzione che A è nilpotente. Per Hamilton-Cayley, si ha che esiste un polinomio $p(t)$ tale che

$$0 = p(A) = \sum_{i=0}^{n} a_i A^i$$

Di conseguenza,

$$\sum_{i=0}^{n} a_i \operatorname{Tr}(A^i) = \sum_{i=0}^{n} a_i \operatorname{Tr}(u^i) = n a_0 = 0$$

da cui $a_0 = 0$, ossia 0 è autovalore per A. Sia allora $v \in \operatorname{Ker}(A) \setminus \{0\}$ e completiamolo a base $\mathcal{B} = (v, v_2, \dots, v_n)$. La matrice che rappresenta φ_u in questa base è del tipo

$$\left(\begin{array}{c|ccc} 0 & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & A & \\ 0 & & & \end{array}\right)$$

Per induzione, si ha allora che il minore B ha traccia nulla, lo stesso vale per le sue potenze e dunque B è nilpotente. Allora A è nilpotente, da cui la tesi. □

Dunque possiamo supporre nel seguito che A sia una $\mathbb{Q}$-algebra artiniana ridotta. Troviamo un bound per capire quando possiamo fermare le iterazioni dell'algoritmo.

Proposizione 4.15. Sia A una $\mathbb{Q}$-algebra ridotta con base $\alpha_1, \dots, \alpha_n$ su $\mathbb{Q}$. Allora esistono n idempotenti primitivi $e_1, \dots, e_n$ di $A_{\mathbb{C}} = A \otimes_{\mathbb{Q}} \mathbb{C}$ con $n = \dim_{\mathbb{Q}} A$. Inoltre, detta $M = (m_{ij})$ la matrice tale che $\alpha_i = \sum m_{ij} e_j$, si ha

1. $\operatorname{disc}(\mathcal{B}) = \det M^2$
2. $|m_{ij}| \leq \max\{\sum_k |c_{ijk}|\}$

Dimostrazione. L'enunciato principale è ovvio in quanto su $\mathbb{C}$ vale il Nullstellensatz. Il punto 1 segue dal fatto che

$$\operatorname{disc}(\mathcal{B}) = \det(\operatorname{Tr}(\alpha_i\alpha_j)) = \det(M \operatorname{Tr}(e_ie_j)M^t) = \det(M)^2$$

Per il punto 2, notiamo che

$$\alpha_i e_j = \Big(\sum_k m_{ik}e_k\Big)e_j = m_{ij}e_j$$

dove nell'ultimo passaggio abbiamo utilizzato l'ortogonalità degli idempotenti e_i. Di conseguenza, detta φ_{α_i} la moltiplicazione per α_i, si ha che la matrice associata nella base $e_1, \dots, e_n$ è diagonale:

$$\begin{pmatrix} m_{i1} & & & \\ & m_{i2} & & \\ & & \ddots & \\ & & & m_{in} \end{pmatrix}$$

Nella base $\alpha_1, \dots, \alpha_n$, si ha invece la matrice

$$A = \begin{pmatrix} c_{i11} & c_{i21} & \cdots & c_{in1} \\ c_{i12} & c_{i22} & \cdots & c_{in2} \\ \vdots & \vdots & \ddots & \vdots \\ c_{i1n} & c_{i2n} & \cdots & c_{inn} \end{pmatrix}$$

Dato che il raggio spettrale di una matrice è minore della sua norma per ogni norma matriciale, si ha che

$$\max_j |m_{ij}| \leq \|A\|_1 = \max_j \sum_k |c_{ijk}|$$

Prendendo il massimo su i, si ha

$$\max_{ij} |m_{ij}| \leq \max_{i,j} \sum_k |c_{ijk}|$$

□

Proposizione 4.16 (Disuguaglianza di Hadamard)**.** Sia $M \in M(n, \mathbb{C})$ una matrice quadrata a coefficienti complessi tale che $|m_{ij}| \leq C$, con $C \in \mathbb{R}$. Allora

$$|\det(M)| \leq C^n n^{\frac{n}{2}}$$

Lemma 4.17. Sia A una $\mathbb{Q}$-algebra ridotta e artiniana con base $\mathcal{B} = (\alpha_1, \dots, \alpha_n)$. Sia $u = \sum u_i\alpha_i$ un idempotente e sia $C = \max\{\sum_k |c_{ijk}|\}$, dove c_{ijk} sono le costanti di struttura. Allora

$$|u_i| \leq \mathcal{U} = (n-1)\sqrt{\frac{(n-1)^{n-1}C^{2(n-1)}}{\operatorname{disc}(A)}}$$

Dimostrazione. Preliminarmente, consideriamo $e_1, \dots, e_n$ idempotenti primitivi su $\mathbb{C}$ e sia $\alpha_i = \sum m_{ij} e_j$. I coefficienti di M^{-1} sono gli u_{ij} tali che $e_i = \sum_j u_{ij}\alpha_j$.

Sia ora u un idempotente non banale; possiamo scriverlo come somma di al più $n-1$ idempotenti primitivi $u = \sum t_i e_i$. Per idempotenza, necessariamente $t_i = 0$ oppure $t_i = 1$. Dunque $u = \sum e_i = \sum_i \sum_j u_{ij}\alpha_j = \sum_j (\sum_i u_{ij})\alpha_j$. Per unicità della scrittura, vale $\sum_i u_{ij} = u_j$, ossia u_j coincide con la somma degli elementi della j-esima colonna. Dunque

$$\begin{aligned} |u_i| &\leq \sum_i |u_{ij}| \\ &\leq (n-1)\max\{|u_{ij}|\} \\ &\leq (n-1)\frac{\det M_{n-1}}{|\det M|} \end{aligned}$$

dove nell'ultimo passaggio abbiamo utilizzato la formula dell'aggiunta e abbiamo indicato con M_{n-1} il minore $n-1 \times n-1$ di M che corrisponde all'elemento di massimo modulo di M^{-1}. Applicando la disuguaglianza di Hadamard (gli elementi di M sono maggiorati da C per la proposizione precedente), otteniamo allora

$$\begin{aligned} |u_i| &\leq (n-1)\frac{C^{n-1}(n-1)^{\frac{n-1}{2}}}{\sqrt{\operatorname{disc}(A)}} \\ &= (n-1)\sqrt{\frac{C^{2(n-1)}(n-1)^{n-1}}{\operatorname{disc}(A)}} \end{aligned}$$

come voluto. □

Proposizione 4.18. Sia $\mathcal{U}$ la costante del lemma precedente e sia $N \in \mathbb{N}$ tale che

$$p^N > \mathcal{U} + n^2 C \mathcal{U}^2$$

Allora ogni idempotente modulo p^N con coefficienti $\leq \mathcal{U}$ è un idempotente razionale.

Dimostrazione. Sia e un idempotente modulo p^N come nelle ipotesi. Scriviamo $e = \sum u_i \alpha_i$; allora

$$\begin{aligned} e^2 - e &= \sum_{i,j} u_i u_j \alpha_i \alpha_j - \sum_k u_k \alpha_k \\ &= \sum_{i,j} u_i u_j \sum_k c_{ijk}\alpha_k - \sum_k u_k \alpha_k \\ &= \sum_k \alpha_k \Big(u_k - \sum_{i,j} u_i u_j c_{ijk} \Big) \end{aligned}$$

Notiamo che

$$\Big| u_k - \sum_{i,j} u_i u_j c_{ijk} \Big| \leq \mathcal{U} + n^2 C \mathcal{U}^2$$

e dato che questo deve essere 0 modulo p^N, deve essere 0 anche sui razionali, da cui la tesi. □

Prima di fornire lo pseudocodice per il sollevamento degli idempotenti, osseriviamo che se $p \in \mathbb{Z}$ è un primo che non divide il denominatore d del lemma 4.8 e $u \in A$ è un idempotente, allora proviene da un unico idempotente modulo p.

Algoritmo 4.1 Sollevamento degli idempotenti

1: Rendere A una $\mathbb{Q}$-algebra ridotta.
2: Prendere $p \in \mathbb{Z}$ un primo tale che $p \nmid d$, dove $d = \max\{b \mid b^2 \mid \mathrm{disc}(A)\}$.
3: Trovare idempotenti modulo p di $A_{\mathbb{Z}} \otimes \mathbb{F}_p$.
4: Calcolare il bound $\mathcal{U}$ e scegliere $N \in \mathbb{N}$ tale che $p^N > \mathcal{U} + n^2 C \mathcal{U}^2$.
5: Sollevare gli idempotenti.

Capitolo 5

Localizzazioni

Iniziamo la trattazione con due esempi naturali in cui si manifesta la necessità di lavorare su localizzazioni di anelli.

- Consideriamo l'ideale $I = (x^3+x^2, y^2)$ in $\mathbb{C}[x, y]$. Questo è 0-dimensionale, con luogo degli zeri $V(I) = \{(-1, 0), (0, 0)\}$. Questo è inaspettato, in quanto $\dim_{\mathbb{C}} \mathbb{C}[x, y]/I = 6$, e dunque ci aspettiamo che ci sia una sorta di molteplicità.
- Se consideriamo l'ideale $I = (y(x-1), z(x-1))$, la varietà associata è l'unione di un piano e una retta, la dimensione di Krull dell'anello $\mathbb{C}[x, y, z]/I$ è 2 ma c'è una componente di dimensione uno. In un intorno dello zero, infatti, localizzando l'anello per (x, y, z), si ottiene che la dimensione del localizzato è 1.

Definizione 5.1. Sia $p \in V$ e supponiamo che $I(V)$ sia 0-dimensionale. Definiamo molteplicità di p come la dimensione dell'anello

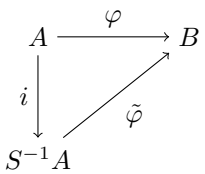
$$\left(K[x]/I(V)\right)_p$$

Un'altro caso in cui le localizzazioni si manifestano in maniera naturale è nel caso delle parametrizzazioni. Per esempio, per parametrizzare una circonferenza di raggio 1 centrata in $(-1, 0)$ si ha

$$\begin{cases} x = \frac{-2t^2}{1+t^2} \\ y = \frac{2t^2}{1+t^2} \end{cases}$$

e dunque stiamo identificando x, y come elementi di $K[t]_{(1+t^2)}$.

Richiamiamo ora la proprietà universale delle localizzazioni. Sia quindi A un anello e sia $S \subseteq A$ un sottoinsieme moltiplicativamente chiuso. Sia $\varphi\colon A \to B$ un omomorfismo di anelli tale che $f(S) \subseteq B^*$. Allora esiste un unico omomorfismo di anelli $\tilde{\varphi}\colon S^{-1}A \to B$ che faccia commutare il diagramma



Inoltre, valgono le seguenti proprietà sull'omomorfismo i:

- $j(s) \in (S^{-1}A)^*$ per ogni $s \in S$.
- Se $j(a) = 0$, allora esiste $s \in S$ tale che $as = 0$. In particolare, j è iniettiva se e solo se $S \cap \mathfrak{D}(A) = \emptyset$.
- j è biunivoca se e solo se $S \subseteq A^*$.

5.1 Ordinamenti Locali e Globali

Definizione 5.2. Sia $M = \{x^\alpha \mid \alpha \in \mathbb{N}^n\}$ l'insieme dei monomi di $K[x]$ e sia $>$ un ordinamento su M compatibile con il prodotto. Diciamo che

- $>$ è globale se per ogni $\alpha \neq 0$ vale $x^\alpha > 1$.
- $>$ è locale se per ogni $\alpha \neq 0$ vale $x^\alpha < 1$.
- $>$ è misto se non è né globale né locale.

Tra gli ordinamenti locali, i più usati sono

- il lessicografico negativo, rappresentato dalla matrice $-I$
- il graduato lessicografico inverso negativo (degrevneglex), in cui la matrice è uguale a quella del degrevlex eccetto per la prima riga, che è composta di -1.

Per esempio, nell'anello dei polinomi in una variabile $K[x]$, l'unico ordinamento monomiale locale è quello dato da $1 > x > x^2 > \cdots$.

Definizione 5.3. Sia $>$ un ordinamento monomiale (globale o locale). Chiamiamo

$$S_> = \{u \in K[x] \mid lm(u) = 1\}$$

Se l'ordinamento è globale, chiaramente vale $S_> = K^*$. Se invece l'ordinamento è locale, si ha che $S_> = K[x]/(x)$. Notiamo che $S_>$ è moltiplicativamente chiuso, in quanto $lm(fg) = lm(f)lm(g)$. Possiamo allora considerare l'anello delle frazioni

$$K[x]_> = S_>^{-1}K[x]$$

Osservazione 5.4. Valgono le seguenti:

- $K[x] \subseteq K[x]_> \subseteq K[x]_{(x)}$
- $K[x]_>^* = \{u/v \mid lm(u) = lm(v) = 1\}$ e inoltre $K[x]_>^* \cap K[x] = S_>$
- $K[x]_>$ è noetheriano

Esempio. Consideriamo $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ con un ordinamento prodotto $>= (>_1, >_2)$, ossia

$$x^\alpha y^\beta > x^\gamma y^\delta \iff (x^\alpha >_1 x^\gamma) \text{ oppure } x^\alpha = x^\gamma \text{ e } y^\beta >_2 y^\delta$$

Supponiamo che $>_1$ sia globale e $>_2$ sia locale. Allora $S_> = K^* \cup (Y)K[Y]$ e

$$K[x, y]_> = (K[y]_{(y)})[x] \simeq K[y]_{(y)} \otimes_K K[x]$$

Notiamo che questo ordinamento ha la proprietà di eliminazione rispetto alle y.

5.2 Forma Normale di Mora

Vogliamo ora capire in che modo generalizzare le basi di Gröbner al caso delle localizzazioni per questo tipo di sottoinsiemi moltiplicativi. Abbiamo intanto bisogno di ricreare tutta la notazione che avevamo nel caso di anelli di polinomi.

Definizione 5.5. Sia $f \in K[x]_>$ e sia $u \in K[x]$ tale che $lm(u) = 1$ e $uf \in K[x]$. Definiamo

- $lm(f) = lm(uf)$
- $lc(f) = lc(uf)$
- $lt(f) = lt(uf)$
- $tail(f) = f - lt(f)$

Definizione 5.6. Se $G \subseteq K[x]_>$, definiamo $lt(G) = \{lm(g) \mid g \in G \setminus \{0\}\}$ e il leading term ideal come l'ideale generato da $lt(G)$ in $K[x]$.

Ora, possiamo definire il concetto analogo alle basi di Gröbner:

Definizione 5.7. Sia $R = K[x]_>$ e sia I un ideale di R. Un insieme $G \subseteq I$ è una base standard per I se $(lt(I)) = (lt(G))$. Una base standard è minimale se $lm(g) \nmid lm(f)$ per ogni $f, g \in G$ distinti. Diciamo che $f \in G$ è ridotto da G se nessun elemento nello sviluppo di f (come serie formali) sta in $lt(G)$. G è ridotta se ogni $g \in G$ è ridotto da $G \setminus \{g\}$.

Definizione 5.8. Sia $\mathcal{G} = \{G \subseteq R \mid \#G < \infty\}$. Definiamo forma normale debole una funzione

$$\begin{array}{rccc} \mathrm{NF}\colon & R \times \mathcal{G} & \longrightarrow & R \\ & (f, G) & \longmapsto & \mathrm{NF}(f|G) \end{array}$$

tale che

- $\mathrm{NF}(0|G) = 0$ per ogni G
- Se $\mathrm{NF}(f|G) \neq 0$, allora $lm(\mathrm{NF}(f|G)) \notin (lt(G))$
- Se $G = \{g_1, \ldots, g_s\}$, esiste $u \in R^*$ tale che $uf - \mathrm{NF}(uf|G) = \sum a_i g_i$ con $lm(a_i g_i) \leq lm(\sum a_i g_i)$ (rappresentazione standard)

Se inoltre per ogni $f \in K[x]$ e per ogni $G \subseteq K[x]$ esiste $u \in R^* \cap K[x]$ tale che uf abbia una rapppresentazione standard con coefficienti in $K[x]$, la forma normale debole si dice polinomiale.

Esempio. Mostriamo un esempio del perché le cose non funzionano bene come nella teoria delle basi di Gröbner. Consideriamo i polinomi $f(x) = x$ e $g(x) = x - x^2$ e un ordinamento locale. Allora $s(f, g) = x^2$, che ridotto con g fornisce x^3, e così via. Andando avanti, otteniamo $f - (\sum x^i)g = 0$, ossia $(1 - x)f = g$, ma $1 - x$ è invertibile in $K[x]_>$.

Definizione 5.9. Sia $g = \sum c_\alpha x^\alpha$ e sia t una variabile ausiliaria. Definiamo omogeneizzato di g il polinomio

$$g^H = \sum c_\alpha t^{d-|\alpha|} x^\alpha$$

dove $d = \deg(g)$.

Definizione 5.10. Se $>$ è un ordinamento (locale, globale o misto) su $K[x]$, definiamo l'ordinamento $>'$ su $K[t,x]$ come segue

$$t^a x^\alpha >' t^b x^\beta \iff \begin{array}{l} a+|\alpha| > b+|\beta| \text{ oppure} \\ a+|\alpha| = b+|\beta| \text{ e } x^\alpha > x^\beta \end{array}$$

Indipendentemente dalla natura di $>$, $>'$ è sempre un ordinamento monomiale. Infatti la condizione sul grado dei termini garantisce che $>'$ sia un buon ordine.

Proposizione 5.11. Siano $F, F_1, \ldots, F_s \in K[t,x]$ polinomi omogenei e muniamo $K[t,x]$ con l'ordinamento $>'$. Allora esistono dei polinomi omogenei $U, A_1, \ldots, A_s, H \in K[t,x]$ tali che

- $UF = (\sum A_i F_i) + H$
- $lm(U) = t^a$ per un certo $a \in \mathbb{N}$
- $a + \deg F = \deg A_i + \deg F_i = \deg H$
- $lm(F_i) \nmid lm(t^b H)$ per ogni $b \geq 0$.

Dimostrazione. La dimostrazione è costruttiva e consiste nel seguente algoritmo che prende in input $F, F_1, \ldots, F_s$ e restituisce $H, A_1, \ldots, A_s, U$.

Algoritmo 5.1 Forma normale di Mora omogenea

```
1:  H = F
2:  A_i = 0 per ogni i
3:  U = 1
4:  L = {F_1, ..., F_s}
5:  M = {g ∈ L | lm(g) | lm(t^a H) per qualche a}
6:  while M ≠ ∅ do
7:      Scegliere g ∈ M tale che a sia minimo.
8:      if a > 0 then
9:          L = L ∪ {H}
10:     end if
11:     H = Riduci(t^a H, g)
12:     if t^b | H e t^{b+1} ∤ H then
13:         H = H / t^b
14:     end if
15:     M = {g ∈ L | lm(g) | lm(t^a H) per qualche a}
16: end while
```

Nello pseudocodice non abbiamo mai aggiornato gli A_i e U perché questo dipende dall'elemento di L scelto e discuteremo questo nella verifica della correttezza dell'algoritmo. L'algoritmo termina per noetherianità. Consideriamo infatti l'ideale $L_j = \{lm(g) \mid g \in L \text{ al passo } j\}$. Vale $L_j \subseteq L_{j+1}$, in quanto durante l'algoritmo vengono solo aggiunti elementi a L, da cui esiste $n \in \mathbb{N}$ tale che $L_n = L_{n+1}$ e dunque anche L si stabilizza. Di conseguenza, L non viene più aggiornata e continuano solo le riduzioni. Dato che $>'$ è un ordinamento monomiale e la successione dei $lm(H)$ è decrescente, le riduzioni terminano, da cui la terminazione dell'algoritmo.

Dimostriamo ora la correttezza per induzione sui passi.

Passo 1 Questo è banale, in quanto si ottiene $1 \cdot F = 0 + F$.

Passo $j+1$ Dal passo j-esimo, vale

$$U_j F = \sum_{i=1}^{s} A_{ij} F_i + H_j \tag{5.1}$$

Chiamiamo U_i il valore della variabile U al passo i e allo stesso modo denotiamo $A_{j,i}$ e H_i. Sia a_k l'esponente di t in $lm(U_k)$ al passo $k \leq j$. Per ipotesi induttiva vale $a_k \geq a_{k-1}$ in quanto ad ogni passo deve valere $a_k + \deg(F) = \deg(H_k)$ e il grado di H_k è crescente (la riduzione non altera il grado e la a scelta ad ogni passo è maggiore della b per la quale si divide H). Dunque si ha $\deg(H_k) \geq \deg(t^{a_k - a_{k-1}} H_{k-1})$ da cui segue $t^{a_k} lm(H_{k-1}) >' t^{a_{k-1}} lm(H_k)$. Questo è chiaro nel caso in cui $\deg(H_k) > \deg(t^{a_k - a_{k-1}} H_{k-1})$; nel caso valga l'uguaglianza in questa relazione, dato che è stato applicato un passo di riduzione, vale $lt(H_k) >' lt(H_{k-1})$ da cui la relazione. Iterando tale formula, otteniamo

$$t^{a_j} lm(H_k) >' t^{a_k} lm(H_j)$$

per ogni $k \leq j$.

Se non esiste F_i tale che $lm(F_i) \mid t^b lm(H_j)$ per ogni b, abbiamo finito. Supponiamo allora che esista $g \in L$ tale che $lm(g) \mid lm(t^a H_j)$ con a minimo. Se tale g coincide con un F_i per qualche $i = 1, \ldots, s$, allora da $lm(F_i) \mid lm(t^a H_j)$ esiste un monomio m_j tale che $lm(t^a H_j) = m_j lm(F_i)$. Possiamo allora modificare la relazione 5.1 ponendo

$$U_{j+1} \coloneqq t^a U_j \quad A_{l,j+1} \coloneqq \begin{cases} t^a A_{l,j} \text{ se } l \neq i \\ t^a A_{l,j} + m_j \text{ se } l = i \end{cases} \qquad H_{j+1} \coloneqq t^a H_j - m_j F_i$$

In questo caso, le varie proprietà elencate nell'enunciato seguono banalmente.

Se invece $g \neq F_i$ per ogni i, allora deve coincidere con uno degli H_k con $k \leq j$. Dunque esiste m_j tale che

$$t^a lm(H_j) = m_j lm(H_k)$$

Dalla relazione per il passo k, vale

$$m_j H_k = m_j U_k F - m_j \Big(\sum_{i=1}^{s} A_{ik} F_i \Big)$$

Basta allora porre

$$U_{j+1} \coloneqq t^a U_j - m_j U_k \quad A_{l,j+1} \coloneqq t^a A_{l,j} - m_j A_{l,k} \quad H_{j+1} \coloneqq t^a H_j - m_j H_k$$

Questa scelta rende anche la condizione sui gradi verificata. Infatti

$$t^{a+a_j} lm(H_k) >' t^{a+a_k} lm(H_j) = t^{a_k} lm(t^a H_j) = t^{a_k} m_j lm(H_k)$$

da cui $t^{a+a_j} > t^{a_k} m_j$. Dato che $lm(U_j) = t^{a_j}$, si ha

$$lm(U_{j+1}) = lm(t^a U_j - m_j U_k) = t^{a+a_j}$$

da cui segue la seconda proprietà richiesta nell'enunciato; allo stesso modo segue l'uguaglianza dei gradi.

□

Tutte le operazioni in questo caso sono state svolte nell'anello dei polinomi senza mai passare al localizzato. Deomogeneizzando, otteniamo il seguente:

Corollario 5.12. Siano $f, f_1, \ldots, f_s$ polinomi in $k[x_1, \ldots, x_n]$ e sia $>$ un ordinamento monomiale. Allora esistono $u, a_1, \ldots, a_s, h \in K[x]$ tali che

$$uf = \sum_{i=1}^{s} a_i f_i + h$$

e $lm(u) = 1$, $lm(a_i f_i) \leq lm(f)$ e $h = 0$ oppure $lm(h)$ non è divisibile per nessuno dei $lm(f_i)$.

Se $f \in K[x]_>$ e $f_1, \ldots, f_s \in K[x]$, possiamo applicare l'algoritmo anche in questo caso. Se infatti $f = f'/u'$, possiamo applicare l'algoritmo a f' e otteniamo

$$uf' = \sum a_i f_i + h$$

Dividendo la relazione per u e u' (che sono invertibili in quanto $lm(u) = lm(u') = 1$), otteniamo

$$f = \sum \frac{a_i}{uu'} f_i + \frac{h}{uu'}$$

Con questa forma normale generalizzata, possiamo adattare tutti gli algoritmi che già conoscevamo (utilizzando ordinamenti di eliminazione), in particolare

- l'ideal membership
- $I \cap J$
- $I : J$
- $I :^\infty J$
- $f \in \sqrt{I}$

Capitolo 6

Integrazione

Definizione 6.1. Sia R un anello commutativo con identità. Una derivazione su R è un'applicazione $\partial\colon R \to R$ tale che

- $\partial(a+b) = \partial(a) + \partial(b)$
- $\partial(ab) = a\partial(b) + b\partial(a)$

Ci poniamo ora il problema dell'integrazione: data $f \in A$, vogliamo trovare $g \in A$ tale che $\partial(g) = f$. Osserviamo prima di tutto che data una derivazione ∂ su un dominio R, è possibile estenderla al campo dei quozienti $Q(R)$. Dato infatti $a/b \in Q(A)$, notiamo che

$$\partial(a) = \partial\Big(\frac{a}{b}b\Big) = \bar{\partial}\Big(\frac{a}{b}\Big)b + \frac{a}{b}\bar{\partial}(b)$$

Ci limiteremo quindi a studiare campi. Il problema è capire dove lavorare. Intanto serve capire se un dato elemento di R è uguale a 0; questo si può fare solo lavorando con funzioni effettive.

Definizione 6.2. Sia (R, ∂) un anello con derivazione. Definiamo costanti dell'anello l'insieme

$$\mathrm{Const}(R) = \{a \in R \mid \partial(a) = 0\}$$

6.1 Funzioni razionali

Occupiamoci ora dell'integrazione di funzioni razionali su campi a caratteristica zero. Tramite divisione possiamo ridurci al caso di $f = q/r$, con $\deg(q) < \deg(r)$, in quanto integrare i polinomi è semplice. Consideriamo una fattorizzazione squarefree di r

$$r = \prod_{i=1}^{n} r_i^i \qquad\qquad (r_i, r_j) = 1$$

dove ogni r_i è quindi squarefree. Per coprimalità degli r_i, possiamo scrivere

$$\frac{q}{r} = \frac{q}{\prod_{i=1}^{n} r_i^i} = \sum_{i=1}^{n} \frac{q_i}{r_i^i}$$

Di conseguenza, ci siamo ridotti all'integrazione di ogni singolo addendo per additività dell'integrale. Dato che ogni r_i è squarefree, $(r_i, r_i') = 1$ e dunque per Bezout esistono a_i, b_i tali che $a_i r_i + b_i r_i' = 1$, da cui

$$\begin{aligned}\int \frac{q_i}{r_i^i} &= \int \frac{q_i(a_i r_i + b_i r_i')}{r_i^i} \\ &= \int \frac{q_i a_i}{r_i^{i-1}} + \int \frac{q_i b_i r_i'}{r_i^i} \\ &= \int \frac{q_i a_i}{r_i^{i-1}} - \frac{q_i b_i}{r_i^{i-1}} + \int \frac{(q_i b_i)'}{(i-1) r_i^{i-1}} \\ &= -\frac{q_i b_i}{r_i^{i-1}} + \int \frac{(q_i b_i)' + (i-1) a_i q_i}{(i-1) r_i^{i-1}}\end{aligned}$$

Possiamo allora iterare fino a trovare esponente 1; a quel punto si integra esattamente con il logaritmo. Questo algoritmo risulta però costoso, in quanto richiede il calcolo dei coefficienti di Bezout. Possiamo però sfruttarlo come base teorica e renderlo più efficiente. Infatti, dai calcoli effettuati si deduce che l'integrale di una funzione razionale si scrive come

$$\int \frac{q}{r} = \frac{q_1}{r_1} + \int \frac{q_2}{r_2}$$

con $r_1 = \gcd(r, r')$ e $r_2 = r/\gcd(r, r')$ (con questa scelta q_2/r_2 potrebbe non essere ridotta). Derivando questa relazione si ottiene

$$\frac{q}{r} = \left(\frac{q_1}{r_1}\right)' + \frac{q_2}{r_2}$$

da cui

$$\frac{q}{r} = \frac{q_1' r_2 - q_1 \frac{r_1' r_2}{r_1} + q_2 r_1}{r_1 r_2}$$

Notiamo che $r_1' r_2 / r_1$ è un polinomio, come si può verificare facilmente con una potenza di un irriducibile. Trovare la primitiva è allora equivalente alla risoluzione di un sistema lineare le cui incognite sono i coefficienti dei polinomi q_1 e q_2; dato che $\deg(q_1) < \deg(r_1)$ e $\deg(q_2) < \deg(r_2)$ si uguaglia grado per grado e si ricavano i coefficienti. Abbiamo ricondotto quindi il calcolo dell'integrale a un problema di algebra lineare.
Curiamo ora il calcolo della parte logaritmica. Supponiamo quindi

$$\int \frac{q}{r} = \sum c_i \ln(v_i)$$

con c_i costanti e v_i funzioni razionali. Per le proprietà del logaritmo, possiamo supporre che i v_i siano polinomi liberi da quadrati e coprimi a due a due. Derivando la relazione otteniamo allora

$$\frac{q}{r} = \sum c_i \frac{v_i}{v_i'} = \frac{\sum c_i v_i u_i}{\prod v_i}$$

dove $u_i = \prod_{i \neq j} v_j$. Di conseguenza $r = \prod v_i$ e $q = \sum c_i v_i' u_i$; notiamo inoltre che $r' = \sum v_i' u_i$, da cui

$$\begin{aligned} v_k &= \gcd(0, v_k) \\ &= \gcd(q - \sum c_i v_i' u_i, v_k) \\ &= \gcd(q - c_k v_k' u_k, v_k) \\ &= \gcd(q - c_k \sum v_i' u_i, v_k) \\ &= \gcd(q - c_k r', v_k) \end{aligned}$$

D'altra parte, se $l \neq k$, $\gcd(q - c_k r', v_l) = 1$ e quindi conoscendo i c_k possiamo trovare facilmente i v_k tramite il calcolo di un gcd. Per trovare questi, è sufficiente calcolare $\mathrm{Ris}_x(q(x) - yr'(x), r(x))$ e i c_k coincidono con gli zeri di questo polinomio.

6.2 Il teorema di Liouville e sue conseguenze

Per integrare le funzioni razionali, è servito utilizzare i logaritmi e dunque abbiamo avuto bisogno di ampliare la classe delle primitive ammissibili. Sviluppiamo ora una teoria più generale per estendere quanto visto sulle funzioni razionali.

Definizione 6.3. Sia K un campo di funzioni e sia L un'estensione di K. $\theta \in L$ è un generatore elementare se vale una delle seguenti:

- θ è algebrico su K
- θ è esponenziale su K, cioè esiste $\eta \in K$ tale che $\theta' = \eta'\theta$
- θ è logaritmo su K, cioè esiste $\eta \in K^*$ tale che $\theta' = \eta'/\eta$

Se $\theta_1, \ldots, \theta_k$ sono generatori elementari su K, chiamiamo il campo $K(\theta_1, \ldots, \theta_k)$ un campo di funzioni elementari.

Definizione 6.4. Sia K un campo di funzioni e sia $f \in K$. Diciamo che f ha un integrale elementare su K se $\int f$ appartiene a un'estensione elementare di K.

In questa sezione, vogliamo allora determinare un algoritmo per determinare, se esiste, una primitiva di un elemento $f \in K$ in una opportuna estensione elementare di K. Il teorema di Liouville (e la sua dimostrazione) è un risultato importante sia a livello teorico che algoritmico:

Teorema 6.5 (Liouville)**.** Sia K un campo di funzioni e sia $f \in K$. Supponiamo che f abbia un'integrale elementare su K e chiamiamo K' un campo tale che $\int f \in K'$. Allora

$$\int f = v_0 + \sum_{i=1}^{n} c_i \ln(v_i)$$

dove $v_0 \in K$, $v_i \in K'$ con un numero finito di costanti algebriche e c_i costanti in K'.

Dimostreremo una forma più debole di questo teorema. Intanto, cerchiamo di capire in che modo si estenda una derivazione su una estensione di K.

Teorema 6.6. Sia (K, ∂) un campo differenziale e siano $\theta_1, \ldots, \theta_n \in L$, dove L è un'estensione di K. Sia $I = \{p \in K[x_1, \ldots, x_n] \mid p(\theta_1, \ldots, \theta_n) = 0\}$ l'ideale delle relazioni polinomiali tra i θ_i e siano $f_1, \ldots, f_l$ dei generatori di I. Siano $u_1, \ldots, u_n \in K(\theta_1, \ldots, \theta_n)$ tali che

$$f_i^{\partial}(\theta_1, \ldots, \theta_n) + \sum_{i=1}^{n} \frac{\partial f_i}{\partial x_i}(\theta_1, \ldots, \theta_n) u_i = 0$$

dove f_i^{∂} è il polinomio ottenuto derivando i soli coefficienti di f_i. Allora esiste un'unica derivazione $\bar{\partial}$ su $K(\theta_1, \ldots, \theta_n)$ che estende ∂ e $\bar{\partial}(\theta_i) = u_i$.

Dimostrazione. Supponiamo intanto l'esistenza di $\bar{\partial}$. Per ogni $p \in I$ deve allora valere $\bar{\partial}(p(\theta)) = 0$. D'altronde, per la regola di Leibniz deve valere

$$0 = \bar{\partial}(p(\theta)) = p^{\partial}(\theta) + \sum \frac{\partial p}{\partial x_i}(\theta) \bar{\partial}(\theta_i)$$

da cui $\bar{\partial}(\theta_i) = u_i$. Chiaramente, ∂ si estende effettivamente a $\bar{\partial}$ con la regola

$$\bar{\partial}(g(\theta_1, \ldots, \theta_n)) = g^{\partial}(\theta_1, \ldots, \theta_n) + \sum_{i=1}^{n} \frac{\partial g}{\partial \theta_i}(\theta_1, \ldots, \theta_n) u_i$$

da cui la tesi. □

Esempio. Studiamo a parte il caso in cui l'estensione è generata da un unico elemento $K(\theta)$. Se θ è trascendente, l'ideale I del teorema è banale e dunque possiamo scegliere liberamente $u \in K(\theta)$. Supponiamo quindi che θ sia algebrico e sia p_θ il suo polinomio minimo. Allora

$$p_\theta^{\partial}(\theta) + p_\theta'(\theta) u = 0 \implies u = \frac{p_\theta^{\partial}(\theta)}{p_\theta'(\theta)}$$

e dunque esiste un'unica possibilità per definire una derivazione, a patto che p sia separabile. Se l'estensione è inseparabile, si ha invece che l'unica derivazione estendibile è quella banale.

Consideriamo ora il caso di un campo K di funzioni e di un estensione $F = K(\theta_1, \ldots, \theta_n)$ tale che θ_i sia elementare su $K(\theta_1, \ldots, \theta_{i-1})$ e trascendente.

Lemma 6.7. Sia $(K,')$ un campo differenziale, sia θ trascendente su K e sia $(K(\theta),')$ un'estensione di campi differenziali. Supponiamo che $Const(K) = Const(K(\theta))$. Allora

- Se θ è un logaritmo, ossia $\theta' = \eta'/\eta$ con $\eta \in K$ e $p(\theta) \in K[\theta]$ con $\deg_\theta(p) = n > 0$, si ha che
  - se $lc(p(\theta)) \notin Const(K)$, allora $\deg(p(\theta)') = \deg(p(\theta))$
  - se $lc(p(\theta)) \in Const(K)$, allora $\deg(p(\theta)') = \deg(p(\theta)) - 1$
- Se θ è esponenziale, ossia $\theta' = \eta'\theta$ con $\eta \in K$ e $p(\theta) \in K[\theta]$, allora $\deg(p(\theta)) = \deg(p(\theta)')$. Inoltre, per ogni $\alpha \in K^*$ e per ogni $n \in \mathbb{Z}$ esiste $h \in K^*$ tale che $(\alpha\theta^n)' = h\theta^n$ e $p(\theta) \mid p(\theta)'$ se e solo se $p(\theta)$ è un monomio.

Dimostrazione. Supponiamo dapprima che θ sia un logaritmo e scriviamo $p(\theta) = \sum_{i=0}^{n} a_i\theta^i$. Allora

$$p(\theta)' = \sum_{i=0}^{n} a_i'\theta^i + \sum_{i=1}^{n} i a_i \frac{\eta'}{\eta}\theta^{i-1}$$

da cui $\deg(p(\theta)) = \deg(p(\theta)')$ se $a_n' \neq 0$ (ossia $a_n \notin Const(K)$) e $\deg(p(\theta)) = \deg(p(\theta)') + 1$ se $a_n' = 0$, ossia $a_n \in Const(K)$). Infatti, se $na_n\eta'/\eta + a_{n-1}' = 0$, allora integrando si ottiene $na_n\theta + a_{n-1} = c$ dove $c \in Const(K(\theta)) = Const(K)$. Questo è assurdo, in quanto θ è trascendente e $na_n \neq 0$.

Supponiamo ora che θ sia un esponenziale. Allora chiaramente $\deg(p(\theta)) = \deg(p(\theta)')$. Inoltre, $(\alpha\theta^n)' = \alpha'\theta^n + n\alpha\eta'\theta^n$ e dunque preso $h = \alpha' + n\alpha\eta' \in K$ si ha $(\alpha\theta^n)' = h\theta^n$. Inoltre $h \neq 0$; se fosse $h = 0$ avremmo $(\alpha\theta^n)' = 0$ e dunque $\alpha\theta^n \in Const(K(\theta)) = Const(K)$, da cui un assurdo per la trascendenza di θ. Per l'ultima parte, chiaramente se $p(\theta)$ è un monomio vale $p(\theta) \mid p(\theta)'$. Viceversa, supponiamo che $p(\theta)$ abbia due termini distinti a_nt^n e a_mt^m. Allora, detto $k \in K$ il fattore $p(\theta)'/p(\theta)$, si ha

$$\frac{a_n' + na_n\eta}{a_n} = k \qquad\qquad \frac{a_m' + ma_m\eta}{a_m} = k$$

Uguagliando, otteniamo

$$\frac{a_n' + na_n\eta'}{a_n} = \frac{a_m' + ma_m\eta'}{a_m}$$

da cui

$$\frac{a_n'}{a_n} + n\eta' = \frac{a_m'}{a_m} + m\eta'$$

Notiamo ora che

$$\begin{aligned}\left(\frac{a_n\theta^{n-m}}{a_m}\right) &= \frac{a_n'a_m - a_m'a_n}{a_m^2}\theta^{n-m} + \frac{a_n}{a_m}(n-m)\eta'\theta^{n-m} \\ &= \theta^{n-m}\frac{a_n}{a_m}\left(\frac{a_n'}{a_n} + \frac{a_m'}{a_m} + (n-m)\eta'\right) \\ &= 0\end{aligned}$$

Di conseguenza $\theta^{n-m}(a_n/a_m) \in Const(K)$, che è assurdo per la trascendenza di θ.

□

Lemma 6.8. Sia θ un generatore elementare trascendente su K tale che $Const(K) = Const(K(\theta))$ e sia $p(\theta) \in K[\theta]$. Se p è libero da quadrati, ossia $\gcd(p, \partial p/\partial\theta) = 1$, allora $\gcd(p, p') = 1$.

Dimostrazione. Supponiamo che θ sia logaritmo e quindi che $\theta' \in K$. A meno di estendere il campo $K(\theta)$, possiamo scrivere $p(\theta) = \prod_{i=1}^{n}(\theta - \alpha_i)$ per fattorizzazione unica. Dunque

$$p(\theta)' = \sum_{i=1}^{n}(\theta' - \alpha_i')\prod_{j\neq i}(\theta - \alpha_j)$$

Se $\theta' = \alpha_i'$ per qualche i, si avrebbe $(\theta - \alpha_i)' = 0$ ossia $\theta - \alpha_i \in Const(K(\theta)) = Const(K)$. Dato che θ è trascendente su K e $\theta - \alpha_i \in K$, si ottiene un assurdo.

Supponiamo ora che θ sia esponenziale, ossia $\theta' = \eta'\theta$ con $\eta \in K$. Allora

$$p(\theta)' = \sum_{i=1}^{n} (\eta'\theta - \alpha_i') \prod_{i \neq j} (\theta' - \alpha_j)$$

Se $(\theta - \alpha_i) \mid \gcd(p, p')$, allora $\theta - \alpha_i \mid \eta'\theta - \alpha_i'$. Dato che sono lineari in θ, si ha

$$\eta'\theta - \eta'\alpha_i = \eta'\theta - \alpha_i'$$

e dunque $\alpha_i' = \eta'\alpha_i$ e α_i è esponenziale. D'altronde

$$\begin{aligned} \left(\frac{\theta}{\alpha_i}\right)' &= \frac{\theta'\alpha_i - \theta\alpha_i'}{\alpha_i^2} \\ &= \frac{\theta(\eta'\alpha_i - \alpha_i')}{\alpha_i^2} = 0 \end{aligned}$$

Di conseguenza $\theta/\alpha_i \in Const(K(\theta)) = Const(K)$, dunque θ è algebrico su K da cui un assurdo. □

Teorema 6.9 (Liouville, forma debole - caso trascendente)**.** Sia $(K,')$ un campo differenziale di caratteristica zero. Sia F un'estensione elementare di K tale che $Const(K) = Const(F)$ e sia $f \in K$ un elemento che ammette un'integrale elementare in F. Supponiamo inoltre che $F = K(\theta_1, \ldots, \theta_s)$ e θ_i trascendente su $F_i = K(\theta_1, \ldots, \theta_{i-1})$. Allora esistono $v_0, \ldots, v_n \in K$ e $c_1, \ldots, c_n \in Const(K)$ tali che

$$f = v_0' + \sum_{i=1}^{n} c_i \frac{v_i'}{v_i}$$

Dimostrazione. Procediamo per induzione su s.

$s = 0$ Basta scegliere $v_0 = g$.

$s - 1 \Rightarrow s$ Chiamiamo $\theta = \theta_1$ e consideriamo le estensioni $K \subseteq K(\theta) \subseteq F$. Dato che $f \in K$, allora $f \in K(\theta)$; per ipotesi induttiva vale

$$f = v_0(\theta)' + \sum_{i=1}^{n} c_i \frac{v_i(\theta)'}{v_i(\theta)}$$

Per la fattorizzazione unica, possiamo supporre che $v_i \in F$ oppure v_i monico e irriducibile in $F[\theta]$. Inoltre possiamo supporre che siano tutti distinti. v_0 si può esprimere nella forma $a(\theta)/b(\theta)$ e possiamo fattorizzare $b(\theta) = \prod_{i=1}^{k} b_i(\theta)^{e_i}$. Quindi possiamo scrivere v_0 come

$$v_0 = a_0(\theta) + \sum_{i=1}^{k} \sum_{j=1}^{e_i} \frac{a_{ij}(\theta)}{b_i(\theta)^j}$$

Dunque, sostituendo nell'equazione per f,

$$f = a_0(\theta)' + \sum_{i=1}^{k} \sum_{j=1}^{e_k} \frac{a_{ij}(\theta)}{b_i(\theta)^j} + \sum c_i \frac{v_i(\theta)'}{v_i(\theta)}$$

Supponiamo che θ sia un logaritmo. Sia b_i uno dei polinomi che compare al denominatore dell'espressione di v_0 con $\deg(b_i) > 0$. Dato che θ è logaritmo, $b_i(\theta)' \in F[\theta]$. Inoltre, per motivi di grado, $b_i(\theta)$ non divide $b_i(\theta)'$ e dunque $b_i(\theta)$ compare nel denominatore di f, che invece è indipendente da θ, da cui un assurdo. La stessa contraddizione si ottiene per i $v(\theta)$ e dunque otteniamo

$$f = a_0(\theta)' + \sum c_i \frac{v_i'}{v_i}$$

e questo implica che $a_0(\theta)'$ deve essere indipendente da θ, perché f e i v_i lo sono. Dunque $a(\theta) = s + t\theta$, da cui la tesi nel caso logaritmico.

Supponiamo ora che θ sia esponenziale. Come prima, possiamo scrivere

$$f = a_0(\theta)' + \sum_{i=1}^{k} \sum_{j=1}^{e_k} \frac{a_{ij}(\theta)}{b_i(\theta)^j} + \sum c_i \frac{v_i(\theta)'}{v_i(\theta)}$$

Sia b_i uno dei denominatori. Se b_i non è un monomio, b_i non divide b_i' da cui un assurdo come nel caso logaritmico. Lo stesso deve valere per i v_i e dunque ci basta considerare il caso in cui $b = b_i$ sia un monomio. Per irriducibilità deve essere necessariamente $b_i = \theta$ e dunque

$$\int f = \sum_{-k \le i \le s} h_i \theta^i$$

Derivando,

$$f = \Big(\sum_{-k \le i \le s} h_i \theta^i \Big)' = \Big(\sum_{-k \le i \le s} \bar{h}_i \theta^i \Big)$$

in quanto la derivata di una potenza di un esponenziale non ne fa calare il grado. Dato che f è indipendente da θ, ne segue che $f = \bar{h}_0 = h_0'$, ossia

$$\int f = h_0 \in F$$

come voluto.

□

Teorema 6.10 (Liouville, forma forte)**.** Nelle ipotesi del precedente teorema, esistono $v \in K$, $c_1, \ldots, c_n \in \overline{Const(K)}$ e $u_1, \ldots, u_n \in K(c_1, \ldots, c_n)^*$ tali che

$$f = v' + \sum c_i \frac{u_i'}{u_i}$$

Teorema 6.11 (di struttura di Risch)**.** Sia K un campo di costanti, sia $F = K(\theta_1, \ldots, \theta_n)$ un'estensione di K e supponiamo che θ_i sia un generatore elementare su $F_i = K(\theta_1, \ldots, \theta_{i-1})$.

- Sia $g = \ln(f)$ con $f \notin K$. Supponiamo che $\theta_i = \ln(u_i)$ con $u_i \in F_{i-1}$. Allora g è trascendente se e solo se per ogni $k, h_j \in \mathbb{Z}$ l'elemento $f^k \prod_j u_j^{h_j}$ non appartiene a K.

- Sia $g = \exp(f)$ con $f \notin K$. Supponiamo che $\theta_i = \exp(w_i)$ con $w_i \in F_{i-1}$. Allora g è trascendente se e solo se per ogni $c_i \in \mathbb{Q}$ l'elemento $g + \prod_j c_j w_j$ non appartiene a K.

Occupiamoci ora di un algoritmo di integrazione nel caso di $K(\theta)$ in cui θ è un logaritmo, trascendente su K e $Const(K) = Const(K(\theta))$. Intanto abbiamo necessità di un lemma di divisione in parte polinomiale e parte frazionaria. Chiaramente questo è possibile in quanto $K[\theta]$ è un UFD, ma non è detto in generale che se i singoli elementi della decomposizione ammettano una primitiva.

Lemma 6.12. Sia $f \in K(\theta)$ con θ logaritmo. Sia $f = p + \frac{q}{r}$ con $p, q, r \in K[\theta]$ e $\deg(q) < \deg(r)$. Allora f è elementare se e solo se p e q/r sono elementari.

Dimostrazione. Per il teorema di Liouville,

$$f = p + \frac{q}{r} = v_0(\theta)' + \sum c_i \frac{v_i(\theta)'}{v_i(\theta)} = v_0' + \sum_{i=k+1}^{n} c_i \frac{v_i'}{v_i} + \sum_{i=1}^{k} c_i \frac{v_i(\theta)'}{v_i(\theta)}$$

dove nell'ultimo passaggio abbiamo separato i v_i dipendenti da θ da quelli indipendenti. Possiamo anche esplicitare $v_0 = \bar{p} + (\bar{q}/\bar{r})$, da cui

$$f = \underbrace{\bar{p}' + \sum_{i=k+1}^{n} c_i \frac{v_i'}{v_i}}_{\text{polinomiali in } \theta} + \underbrace{\sum_{i=1}^{k} c_i \frac{v_i(\theta)'}{v_i(\theta)} + \left(\frac{\bar{q}}{\bar{r}}\right)'}_{\text{razionale propria in } \theta}$$

Dato che $K[\theta]$ è un UFD, la decomposizione in parte polinomiale e parte razionale propria è unica, da cui

$$p = \bar{p}' + \sum_{i=k+1}^{n} c_i \frac{v_i'}{v_i} \qquad \frac{q}{r} = \sum_{i=1}^{k} c_i \frac{v_i(\theta)'}{v_i(\theta)} + \left(\frac{\bar{q}}{\bar{r}}\right)'$$

Ne segue che

$$\int p = \bar{p} + \sum_{i=k+1}^{n} c_i \log v_i \qquad \int \frac{q}{r} = \frac{\bar{q}}{\bar{r}} + \sum_{i=1}^{k} c_i \log v_i$$

da cui la tesi. □

Risolviamo prima la parte polinomiale. Sia $p = \sum_{i=0}^{m} a_i \theta^i$ e sia $\bar{p} = \sum b_i \theta^i$ come nella dimostrazione. Otteniamo allora

$$p(\theta) = \sum_{i=0}^{n} b_i' \theta^i + \theta' \sum_{i=1}^{n} i b_i \theta^{i-1} + \sum_{i=k+1}^{n} c_i \frac{v_i'}{v_i}$$

Per identità dei polinomi, deve valere $m = n$ o $n = m + 1$ e

$$\begin{cases} b_{m+1}' = 0 \\ a_i = (i+1) b_{i+1} \theta' + b_i' \\ a_0 = b_1 \theta' + \bar{b}_0' \end{cases}$$

con $\bar{b}_0 = b_0 + \sum c_i \log(v_i)$. Si ha che $b_{m+1} \in K$, in quanto costante di $K(\theta)$. Integrando la seconda relazione, otteniamo

$$\int a_i = (i+1)b_{i+1}\theta + b_i$$

Se questa non è risolubile, f non ha un integrale elementare. Se lo è, sappiamo trovare b_i a meno di una costante e a cascata possiamo determinare tutti gli altri coefficienti, sempre a meno di una costante. All'ultimo passo, possiamo scegliere liberamente tale costante (la primitiva è unica a meno di costante) e dunque terminare l'algoritmo.

Esempio. Vogliamo calcolare $\int \log x$. Consideriamo allora il campo $\mathbb{Q}(x, \theta)$ con θ tale che $\theta' = \frac{1}{x}$. Quindi

$$\int \theta = b_2\theta^2 + b_1\theta + b_0$$

Impostiamo le equazioni:

$$\begin{cases} 0 = b_2' \\ 1 = 2b_2\theta' + b_1' \\ 0 = b_1\theta' + b_0' \end{cases} \implies \begin{cases} 0 = b_2' \\ x + c_1 = 2b_2\theta + b_1 \\ 0 = b_1\theta' + b_0' \end{cases}$$

dove abbiamo solo integrato la seconda equazione. Dato che θ non compare a sinistra, $b_2 = 0$ e $b_1 = x + c_1$. Di conseguenza,

$$\begin{cases} b_2 = 0 \\ b_1 = x + c_1 \\ 0 = (x + c_1)\theta' + b_0' \end{cases}$$

Lavoriamo sulla terza equazione.

$$-x\theta' = c_1\theta' + \bar{b}_0' \Rightarrow -1 = (c_1\theta + \bar{b}_0)' \Rightarrow c_1\theta + \bar{b}_0' = -x$$

e dunque $c_1 = 0$. Ne segue che

$$\int \theta = x\theta - x$$

ossia

$$\int \log x = x \log x - x$$

Teorema 6.13 (Liouville-caso algebrico)**.** Sia K un campo di funzioni elementari e sia $q, r \in K[\theta]$ con $\deg q < \deg r$. Allora q/r è elementare se e solo se $R(y) = \mathrm{Ris}(q - yr', r)$ ha solo radici in K. In tal caso,

$$\int \frac{q}{r} = \sum c_i \log v_i$$

dove c_i sono le radici distinte di R e $v_i(\theta) = \gcd(q - c_i r', r)$.

Esempio. Proviamo a risolvere $\int 1/\log x$ in $\mathbb{Q}(x,\theta)$ con $\theta' = 1/x$. Questo è puramente razionale con $q(\theta) = 1$ e $r(\theta) = \theta$. Vale che

$$\mathrm{Ris}_\theta\left(1 - \frac{y}{x}, \theta\right) = 1 - \frac{y}{x} = \frac{1}{x}(x - y)$$

Dato che x è radice e $x \notin Const(\mathbb{Q}(x,\theta))$, tale funzione non è integrabile.

Esempio. Consideriamo l'integrale

$$\int \frac{1}{x \log x} = \int \frac{1/x}{\theta}$$

Dunque $q(\theta) = 1/x$ e $r(\theta) = \theta$.

$$\mathrm{Ris}_\theta\left(\frac{1}{x} - \frac{y}{x}, \theta\right) = \frac{1}{x}(y - 1)$$

che ha come radice $y = 1$. Dato che $v_1(\theta) = \gcd(1/x - 1/x, \theta) = \theta$, si ha

$$\int \frac{1}{x \log x} = c_1 \log(v_1(\theta)) = \log\log x$$

Consideriamo ora il caso esponenziale. Sia quindi $K(\theta)$ un'estensione elementare di K con θ esponenziale e supponiamo di saper risolvere in K l'equazione

$$y' + fy = g$$

Vale ancora $f = p + (q/r)$, ma

$$p(\theta) = \sum_{i=-m}^{n} a_i \theta^i$$

, $q, r \in K[\theta]$ e $\theta \nmid r$. Dal teorema di Liouville,

$$f = v_0' + \sum c_i \frac{v_i'}{v_i} = v_0' + \sum_{i=k+1}^{n} c_i \frac{v_i'}{v_i} + \sum_{i=1}^{k} c_i \frac{v_i(\theta)'}{v_i(\theta)}$$

Dato che $lt(v_i) = \theta^{m_i}$, si ha $lt(v_i') = m_i \eta' \theta^{m_i}$, dove η è tale che $\theta' = \eta\theta$. Dunque $lt(v_i') = m_i \eta' \theta^{m_i}$. Sottraendo $c_i m_i \eta' \in K$, otteniamo

$$c_i \frac{v_i'}{v_i} - c_i m_i \eta' = \frac{c_i v_i' - c_i m_i \eta' v_i}{v_i}$$

e il numeratore ha grado minore di $\deg v_i$. Dunque abbiamo la decomposizione

$$p + \frac{q}{r} = \underbrace{\bar{p}' + \sum_{i=k+1}^{n} c_i \frac{v_i'}{v_i} + \eta' \sum_{i=1}^{k} c_i m_i}_{\text{polinomio generalizzato in } \theta} + \underbrace{\left(\frac{\bar{q}}{\bar{r}}\right)' + \sum_{i=1}^{k} c_i \frac{v_i' - m_i \eta' v_i}{v_i}}_{\text{frazione razionale propria}}$$

e quindi possiamo fare tutto come sopra. Per la parte razionale propria, si utilizza il teorema come sopra

$\int \frac{q}{r}$ è elementare se e solo se $R(y) = \mathrm{Ris}(q - yr', r)$ ha solo radici in K

e in tal caso

$$\frac{q}{r} = -\Big(\sum c_i \deg v_i(\theta)\Big)\eta' + \sum c_i \frac{v_i'}{v_i}$$

con v_i, c_i come nel teorema sopra.

Per la parte del polinomio generalizzato, si integra termine a termine. Supponiamo quindi

$$\bar{p}(\theta) = \sum_{i=-\bar{m}}^{\bar{n}} v_i \theta^i$$

e sappiamo che $\bar{p}'$ ha lo stesso grado di $\bar{p}$. Inoltre,

$$(b_i\theta^i)' = (b_i' + i\eta' b_i)\theta^i$$

da cui deriva l'equazione differenziale $a_i = b_i' + i\eta' b_i$ che per ipotesi ha soluzione in K.

Esempio. Consideriamo l'integrale

$$\int e^{-x^2}$$

e cerchiamo di risolverlo in $\mathbb{Q}(x,\theta)$ con $\theta' = -2x\theta$. Allora

$$\int \theta = q\theta$$

con $q \in \mathbb{Q}(x)$, da cui segue $\theta = q'\theta + q\theta' = q'\theta - 2x\theta q$. Di conseguenza, cerchiamo $q \in \mathbb{Q}(x)$ tale che $q' - 2xq - 1 = 0$. Scriviamo $q = P/Q$ con $P, Q \in \mathbb{Q}[x]$ elementi coprimi; allora

$$q' = \frac{P'Q - PQ'}{Q^2}$$

da cui

$$\frac{P'Q - PQ'}{Q^2} - \frac{2xP}{Q} - 1 = 0 \Longrightarrow PQ' = P'Q - 2xPQ - Q^2$$

Dall'ultima relazione, segue che $Q \mid PQ'$ e questo è assurdo, dunque $q \in \mathbb{Q}[x]$. Ma nessun polinomio può risolvere quell'equazione differenziale per motivi di grado. Dunque il problema non ha soluzione.

Esempio. Consideriamo l'integrale $\int \cos x$ in $\mathbb{Q}(i,x,\theta)$ con $\theta = e^{ix}$. Dato che $\cos x = e^{ix} + e^{-ix}/2$, dobbiamo calcolare

$$\int \frac{1}{2}(\theta + \theta^{-1}) = a\theta + b\theta^{-1}$$

Derivando,

$$\frac{1}{2}(\theta + \theta^{-1}) = a'\theta + ai\theta + b'\theta - ib\theta$$

da cui il sistema

$$\begin{cases} a = \frac{1}{2i} \\ b = -\frac{1}{2i} \end{cases}$$

da cui si ottiene la soluzione $(\theta - \theta^{-1})/2i = \sin x$.

Esempio. Calcoliamo

$$\int \frac{1}{1+e^x}$$

in $\mathbb{Q}(x,\theta)$ con $\theta' = \theta$. Calcoliamo il risultante

$$R(y) = \mathrm{Ris}(1 - y\theta, \theta + 1) = -1 - y$$

da cui $c_1 = -1$. Dunque si ha $v_1(\theta) = \gcd(1+\theta, 1+\theta) = 1+\theta$. Dunque

$$\int \frac{1}{1+\theta} = -c_1 \deg v_1 x + c_1 \log v_1 = x - \log(e^x + 1)$$