Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea Triennale in Matematica

Tesi di Laurea Triennale

Il calcolo del radicale reale per anelli di polinomi

Candidato:
Agnese Gini

Relatore:
Prof.ssa Patrizia Gianni

Anno Accademico 2014/2015

Indice

Introduzione

La geometria algebrica si occupa dello studio di particolari oggetti geometrici: le varietà algebriche. Se k è un campo e L/k un'estensione di k, la varietà (affine) in L^n definita da un ideale $I \subseteq k[X_1, \ldots, X_n]$ è l'insieme degli zeri comuni ai polinomi in I:

$$\mathcal{V}_L(I) \coloneqq \{x \in L^n \mid \forall f \in I \ f(x) = 0\}.$$

Allo studio di una varietà $V = \mathcal{V}_k(I)$ è associato lo studio dell'ideale di cui è il luogo di zeri:

$$\mathcal{I}_k(V) \coloneqq \{f \in k[X_1, \ldots, X_n] \mid f(x) = 0 \ \forall x \in V\}.$$

Se k è un campo algebricamente chiuso, il teorema degli zeri di Hilbert determina una corrispondenza biunivoca tra le varietà e gli ideali radicali, data da

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

Se il campo base è non è algebricamente chiuso questo non è più vero: lo scopo della nostra tesi è provare che, se il campo k è un *campo reale*, è possibile stabilire una corrispondenza biunivoca fra varietà affini e particolari ideali, gli ideali radicali reali e costruire esplicitamente il radicale reale di un ideale. Un campo k è detto reale se è ordinabile, ossia se è possibile trovare almeno un sottoinsieme, detto *preordine*, $\tau \subset k$ che gode delle seguenti proprietà: $\tau + \tau \subseteq \tau$, $\tau \cdot \tau \subseteq \tau$, $k^2 \subseteq \tau$, $-1 \notin \tau$. Vale che a partire da un preordine è sempre possibile costruire un ordinamento su k ($\alpha \subset k$ è un ordinamento se $\alpha + \alpha \subseteq \alpha$, $\alpha \cdot \alpha \subseteq \alpha$, $\alpha \cap (-\alpha) = \{0\}$ e $\alpha \cup (-\alpha) = k$).

In questo contesto allora più che di chiusura algebrica ha senso parlare di chiusura reale R: una chiusura reale di (k, τ) è un elemento massimale, rispetto all'inclusione, nell'insieme $\{(L, \beta)\}$, dove L è un'estensione algebrica di k e β un ordinamento ottenuto estendendo τ. A priori però, a partire da un preordine si possono trovare più ordinamenti α, i quali danno origine a diverse chiusure reali R_α. Il teorema di *Artin-Lang*[1] , mostra tuttavia che tutte queste chiusure sono coniugate. Noi, visti i nostri scopi, ci occuperemo di un particolare preordine, cioè

$$re \coloneqq \left\{ \sum_{finite} a_i^2 \mid a_i \in k \right\}.$$

[1] Teorema 1.3 di [Bec81]

Si ha infatti che re è il più piccolo dei preordini di ogni campo k reale e vale anzi che un campo è reale se e solo se re è un preordine. Chiameremo allora punti *reali* gli elementi di

$$\mathcal{V}_{re}(I) \coloneqq \bigcup_{\alpha \in \chi(k)} \mathcal{V}_\alpha(I).$$

con $\chi(k)$ la famiglia degli ordinamenti di k.
Non vero che le varietà reali sono in corrispondenza con gli ideali radicali, ma grazie all'esistenza di re è possibile definire un oggetto algebrico che svolge un ruolo analogo al radicale. Sia k campo reale e A una k-algebra, il *radicale reale* di un ideale $I \subseteq A$ è l'insieme

$$\sqrt[re]{I} \coloneqq \left\{ f \in A \mid f^{2r} + \sum_{i=1}^{N} a_i g_i^2 \in I \ a_i \in re, g_i \in A, \ r \in \mathbb{N}, N \in \mathbb{N}_0 \right\},$$

In particolare, se un ideale è tale che $\sqrt[re]{I} = I$ diremo che I è *reale*.
In maniera equivalente si può dire quindi che gli ideali reali sono gli ideali tali che se contengono una somma di quadrati $\sum a_i^2$ allora contengono tutti gli elementi a_i.
Krivine, Dubois e Risler ([Kri64], [Dub69] e [Ris70]) tra il 1964 e il 1970 provarono indipendentemente un risultato analogo al teorema degli Zeri di Hilbert ma per i campi reali, il Nullstellensatz Reale: se k è un campo reale e $I \subseteq k[X_1, \ldots, X_n]$ un ideale, allora vale che

$$\mathcal{I}_k(\mathcal{V}_{re}(I)) = \sqrt[re]{I}.$$

Il radicale reale si dimostra quindi un importante strumento per la geometria algebrica reale. Eberhard Becker e Rolf Neuhaus in un lavoro del 1993 [BN93] , ripreso poi da Neuhaus nel 1998 [Neu98], proposero un primo metodo per calcolare il radicali reale.
In effetti, a patto di supporre di disporre per l'algebra di polinomi sia di un metodo per fattorizzare i polinomi univariati sia di una funzione di valutazione è possibile dimostrare l'esistenza di un algoritmo per il calcolo di questo oggetto algebrico.
Presenteremo perciò, partendo da questo lavoro, un algoritmo per il calcolo del radicale reale per ideali di polinomi a coefficienti in $\mathbb{Q}$ o nel campo delle funzioni razionali $\mathbb{Q}(T_1, \ldots, T_m)$. Studieremo a tal fine la *parte reale* di un polinomio univariato $f \in k[X]$, ossia un polinomio che genera il radicale reale dell'ideale principale (f), e spiegheremo come trovarla. Una volta fatto questo, proveremo che partendo da ideali in $k[X_1, \ldots, X_n]$ è sempre possibile ridursi al caso univariato e descriveremo un algoritmo effettivo che, preso in input un ideale, restituisce il suo radicale reale.
Inizieremo con la descrizione di una procedura dedicata ai singoli polinomi.

Un polinomio è detto reale se coincide con la sua parte reale. Determinare se un polinomio è reale o meno non è tuttavia immediato, dovremo trattare per casi i due diversi tipi di campi: se il polinomio è a coefficienti in $\mathbb{Q}$ basta ricorrere al *Teorema di Sturm*; se invece i coefficienti sono in $\mathbb{Q}(T_1, \ldots, T_m)$ c'è bisogno di un algoritmo più complicato che si riduce a sua volta a costruire un *insieme isolante* per un polinomio univariato a coefficienti razionali per poter utilizzare il *Teorema di Zeng-Zeng*, pubblicato nell'articolo "*An effective decision method for semidefinite polynomials.* "[ZZ04]. Seguendo la costruzione proposta da Becker e Neuhaus mostreremo che per ideali la cui dimensione di Krull è zero, a meno di un cambio di coordinate, trovare il radicale reale è equivalente a calcolare la parte reale di un polinomio univariato. Sfruttando poi il fatto che l'operatore radicale reale commuta con l'immersione nell'anello delle frazioni, descriveremo un metodo per ricondursi ad ideali zero-dimensionali. Vedremo tuttavia che rendere invertibili alcune della variabili, sebbene ci permetta di calcolare una parte delle componenti del radicale reale, banalizza l'intersezione delle componenti di dimensione zero. Per determinarle, presenteremo allora due possibili procedure basate su proprietà più legate alle proprietà geometriche del radicale reale.

Capitolo 1

Radicale Reale e Varietà Reali

La geometria algebrica si occupa dello studio di particolari oggetti geometrici: le varietà algebriche. Se k è un campo e L/k un'estensione di k, la varietà (affine) in L^n definita da un ideale $I \subseteq k[X_1, \ldots, X_n]$ è l'insieme degli zeri comuni ai polinomi in I:

$$\mathcal{V}_L(I) \coloneqq \{x \in L^n \mid \forall f \in I \ f(x) = 0\}.$$

Allo studio di una varietà $V = \mathcal{V}_k(I)$ è associato lo studio dell'ideale di cui è il luogo di zeri:

$$\mathcal{I}_k(V) \coloneqq \{f \in k[X_1, \ldots, X_n] \mid f(x) = 0 \ \forall x \in V\}.$$

Se k è un campo algebricamente chiuso, il teorema degli zeri di Hilbert determina una corrispondenza biunivoca tra le varietà e gli ideali radicali, data da

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

Questo teorema instaura in maniera naturale anche le seguenti corrispondenze:

$$\begin{aligned}
\left\{\mathcal{V}_k(I) \subseteq k^n \mid I \subseteq k[X_1, \ldots, X_n]\right\} &\longleftrightarrow \left\{J \subseteq k[X_1, \ldots, X_n] \mid J = \sqrt{J}\right\} \\
\left\{\mathcal{V}_k(I) \mid \text{varietà irriducibile}\right\} &\longleftrightarrow \left\{P \mid P \text{ ideale primo}\right\} \\
\left\{(c_1, \ldots, c_n) \subseteq k^n\right\} &\longleftrightarrow \left\{M \mid M \text{ ideale massimale}\right\}
\end{aligned}$$

Esempio 1.1.

1. Prendiamo $I = (x^2 - 3, y^2 + 4) \subseteq \mathbb{C}[x, y]$, I è un ideale radicale e dunque è l'unico ideale radicale associato a

$$\mathcal{V}_{\mathbb{C}}(I) = \left\{\left(\sqrt{3}, 2i\right), \left(-\sqrt{3}, 2i\right), \left(\sqrt{3}, -2i\right), \left(-\sqrt{3}, -2i\right)\right\}.$$

2. Prendiamo $I = (x^2 - 3, y^2 - 4) \subseteq \mathbb{C}[x, y]$, I è l'unico ideale radicale associato a
$$\mathcal{V}_{\mathbb{C}}(I) = \left\{ \left(\sqrt{3}, 2\right), \left(-\sqrt{3}, 2\right), \left(\sqrt{3}, -2\right), \left(-\sqrt{3}, -2\right) \right\}.$$
In questo caso $\mathcal{V}_{\mathbb{C}}(I) = \mathcal{V}_{\mathbb{Q}(\sqrt{3})}(I)$.

3. $I = (x^2 + y^2 - 1) \subseteq \mathbb{C}[x, y]$ ha come varietà associata i punti della circonferenza di cento zero e raggio uno in $\mathbb{R}^2$ e dunque $\mathcal{V}_{\mathbb{C}}(I) \cap \mathbb{R}^2 \neq \varnothing$, mentre $J = (x^2 + y^2 + 1) \subseteq \mathbb{C}[x, y]$ dà una varietà che non ha alcun punto reale e dunque $\mathcal{V}_{\mathbb{R}}(J) = \varnothing$.

Dall'esempio osserviamo facilmente che preso un ideale non banale, generato da un polinomio a coefficienti reali, può succedere che i suoi elementi non si annullino in alcun punto di $\mathbb{R}^n$. È da qui che scaturisce la nostra riflessione: possiamo trovare, se il campo non è algebricamente chiuso, una relazione di qualche tipo tra ideali e varietà? Valgono le corrispondenze suddette oppure ne valgono diverse?
Se il campo base gode di particolari proprietà è possibile. Pensiamo per un attimo ai numeri reali, calcolando gli zeri sul campo complesso e restringendoci abbiamo l'insieme che stiamo cercando. La caratteristica di questi campi che vogliamo sfruttare per i nostri scopi è il fatto che siano *campi ordinati*.
Krivine, Dubois e Risler tra il 1964 e il 1970 provarono indipendentemente un risultato analogo al Teorema degli zeri di Hilbert, ma che vale proprio per i campi ordinati, il Nullstellensatz Reale. Anche per questi i campi infatti è possibile definire un oggetto algebrico in corrispondenza con le varietà affini: il radicale reale. Il nostro scopo è dimostrare che è possibile calcolare effettivamente questo oggetto, anzi esibiremo un possibile algoritmo.

Prima di trattare nel dettaglio tale costruzione è bene fissare le strutture, le proprietà e i concetti matematici di cui ci serviremo. Dedichiamo perciò questo primo capitolo a enunciare fatti su campi, ideali e varietà fondamentali per comprendere la costruzione fatta nei prossimi capitoli.

1.1 Campi reali

Per definire il radicale reale e le sue proprietà è necessario definire che cosa vuol dire che un campo è ordinato e alcune proprietà di questi campi. Per le dimostrazioni o uno studio più approfondito di quanto detto in questo paragrafo rimandiamo ai testi [Pre84] e [Bec81].

Definizione 1.2. Sia F un campo, allora un ordinamento totale $\leq$ è una relazione binaria tale che

(i) $a \leq a$

(ii) $a \leq b$, $b \leq c$ allora $a \leq c$

(iii) $a \leq b$, $b \leq a$ allora $a = b$

(iv) $a \leq b$ o $b \leq a$
Se valgono anche le seguenti proprietà, allora diremo che F è un *campo ordinato*

(v) $a \leq b$ allora $a + c \leq b + c$

(vi) $0 \leq a$, $0 \leq b$ allora $0 \leq ab$

Definiamo adesso una particolare classe di sottoinsiemi, i coni positivi, grazie ai quali è possibile definire degli ordinamenti sui campi.

Definizione 1.3. Sia F campo, diremo che $\tau \subset F$ è un cono positivo di F se valgono le seguenti proprietà:

1. $\tau + \tau \subseteq \tau$
2. $\tau \cdot \tau \subseteq \tau$
3. $F^2 \subseteq \tau$
4. $-1 \notin \tau$
5. $\tau \cup (-\tau) = F$

È facile osservare che $\tau = \{a \in F |\ 0 \leq a\}$ è un cono positivo, viceversa ad ogni cono sarà immediato associare una relazione binaria come seguenti

$$a \leq b \iff b - a \in \tau$$

Risulta così naturale identificare questi due concetti.

Definizione 1.4. Un campo F su cui è possibile definire un ordinamento è detto *campo reale*.

Osservazione.

- Nel seguito ci riferiremo quindi a τ come ad un ordinamento (totale) e una volta fissato per il campo in questione un cono positivo, intenderemo fissata anche la relazione d'ordine. Vale dunque che un campo che contiene un cono positivo è reale.
- In generale non vale l'unicità: coni positivi diversi sullo stesso campo possono indurre ordinamenti diversi

Esempio 1.5. Se $\mathbb{Q} \subseteq k \subseteq \mathbb{R}$ esiste banalmente un cono positivo: l'insieme delle somme finite di quadrati

$$\sum k^2 = \left\{ \sum_{\text{finite}} a^2 \mid a \in k \right\},$$

e dunque k è un campo reale.

Consideriamo adesso un altro tipo di sottoinsieme, definito però sugli anelli in generale:

Definizione 1.6. Sia A un anello commutativo con identità, diremo che $\sigma \subset A$ è un *preordine* o un *precono positivo* se valgono le seguenti proprietà:

1. $\sigma + \sigma \subseteq \sigma$
2. $\sigma \cdot \sigma \subseteq \sigma$
3. $A^2 \subseteq \sigma$
4. $-1 \notin \sigma$

Osservazione.

- Assumendo le altre proprietà si ha che *3.* equivale a $\sigma \cap (-\sigma) = \{0\}$.
- Ogni ordinamento è un preordine su F campo, infatti per ogni $x \in F$ si ha $x \in \tau$ e dunque $x^2 \in \tau$ o $-x \in \tau$ e $x^2 = (-x)(-x) \in \tau$. In particolare $1^2 = 1 \in \tau$ ci dà che $-1 \notin \tau$.
- Un preordine σ determina un ordinamento parziale su A tale che

$$a \leq b \iff b - a \in \sigma$$

Come risulta chiaro dalla definizione coni positivi e prordini sono legati. Fissato un $\sigma \subset F$ ci sarà utile definire

$$\Gamma_\sigma \coloneqq \{\sigma_0 | \sigma_0 \textit{ preordine di } F \textit{ tale che } \sigma \subseteq \sigma_0\}$$

$$\chi_\sigma \coloneqq \{\tau | \tau \textit{ ordinamento di } F \textit{ tale che } \sigma \subseteq \tau\}$$

Vale il seguente fatto:

Proposizione 1.7. *Preso un qualsiasi preordine σ di un campo F , abbiamo che*

(i) se $-x \notin \sigma$ allora $\sigma[a] \coloneqq \{x + ay |\ x, y \in \sigma\} \in \Gamma_\sigma$,

(ii) esiste $\tau \in \chi_\sigma$

Una condizione necessaria e sufficiente affinchè un campo sia reale è quindi che contenga un preordine.

L'insieme delle somme finite di quadrati, come abbiamo visto nell'esempio, è un buon candidato a preordine su qualsiasi campo. Da qui in poi, fissato un campo F, useremo la notazione

$$re \coloneqq \sum F^2 = \left\{ \sum_{finite} a^2 \mid a \in F \right\}$$

Proposizione 1.8. *Valgono i seguenti fatti:*

i. re *è contenuto in ogni preordine di* F*,*

ii. re *è chiuso per somma,*

iii. re *è un sottogruppo moltiplicativo di* F*.*

Dimostrazione. Le prime due sono ovvie. La terza deriva da

$$\sum x_i^2 \neq 0 \;\Rightarrow\; \left(\sum x_i^2\right)^{-1} = \sum \left(\frac{x_i}{\sum x_i^2}\right)^2$$

□

Corollario 1.9. re *è il più piccolo preordine di* $F \iff -1 \notin re$

Il seguente teorema mostra che è possibile caratterizzare i campi reali proprio grazie a re:

Teorema 1.10 (E.Artin)**.** *Sia* F *un campo, i seguenti fatti sono equivalenti:*

i. F *reale*

ii. $-1 \notin re$

iii. $\sum x_i^2 = 0 \Rightarrow \; x_i = 0 \; \forall i$

iv. $re \subsetneq F$

Dimostrazione. Evidentemente $ii \Leftrightarrow iii$ e $i \Rightarrow iv$.
$iv \Rightarrow ii$ Se $-1 \in re$ dalla relazione

$$a = \left(\frac{a+1}{2}\right)^2 + (-1)\left(\frac{a-1}{2}\right)^2$$

otteniamo che $re = F$.
$ii \Rightarrow i$ Se $-1 \notin re$ abbiamo che re è un preordine di F e dunque può essere esteso ad un ordinamento. □

Corollario 1.11. *Se F è un campo reale*

$$re = \bigcap \{\tau \mid \tau \text{ è un cono positivo di } F\}$$

Osservazione. Un campo reale ha caratteristica zero e dunque possiede un sottocampo isomorfo a $\mathbb{Q}$.

Esempio 1.12. re è un preordine per $\mathbb{Q}(T_1, \ldots, T_m)$, ma non è un cono positivo.

Per semplicità chiameremo $\chi(F) = \chi_{re}(F)$ l'insieme degli ordinamenti di un campo reale F. Dal teorema derivano due fatti che sono di fondamentale importanza.

Proposizione 1.13. *$\tau_1, \tau_2 \in \chi(F)$, allora $\tau_1 \subseteq \tau_2$ implica $\tau_1 = \tau_2$*

Proposizione 1.14. *re è un ordinamento se e solo se $\chi(F) = \{re\}$*

Esempio 1.15. Abbiamo detto che re è un ordinamento per i campi $\mathbb{Q} \subseteq k \subseteq \mathbb{R}$ e dunque si ha che su tutti questi campi esiste un unico ordinamento.

Preso un campo F se L è una sua estensione algebrica, come nel caso di $\mathbb{Q}$, ha senso parlare di estendere l'ordinamento. Gli insiemi massimali di questa catena di inclusioni assumono un ruolo particolare.

Definizione 1.16. Un campo F è detto *reale chiuso* se è reale e non ha estensioni reali algebriche proprie.

Esempio 1.17.

- $\mathbb{R}$ è una campo reale chiuso.
- $\mathbb{R}_{\text{alg}}$, l'insieme dei numeri reali algebrici su $\mathbb{Q}$, è un campo reale chiuso.

Preso un qualsiasi campo F con un ordine $\leq$ questo è detto ordinato massimamente se e solo se non ha un estensione algebrica ordinata il cui ordine è un'estensione di $\leq$. Si può dimostrare che ogni elemento positivo di un campo massimamente ordinato è un quadrato e che dunque esso ammette un ordinamento unico. Vale inoltre la seguente caratterizzazione:

Lemma 1.18. *Un campo F è reale chiuso se e solo se è massimamente ordinato e ha un unico ordine .*

Enunciamo adesso il teorema di Artin-Schreier che ci dà tre criteri equivalenti per determinare se un campo reale è chiuso:

Teorema 1.19 (**Artin-Schreier**)**.** *Sia F un campo, i seguenti fatti sono equivalenti:*

a. F reale chiuso.

b. $re = \sum F^2$ *è un cono positivo di* F *e ogni polinomio in* $F[X]$ *di grado dispari ha una radice in* F*.*

c. $F(\sqrt{-1})$ *è algebricamente chiuso e* $F \neq F(\sqrt{-1})$*.*

Sottolineiamo che se F è un campo reale chiuso ha un unico ordinamento che quindi è proprio re.

Come nel caso di campi algebricamente chiusi, possiamo definire per un campo il più piccolo campo reale chiuso che lo contiene:

Definizione 1.20. Un estensione algebrica R di (F, τ) è detta *chiusura reale* se R è un campo reale chiuso e il suo unico cono positivo estende τ.

Enunciamo infine alcuni importanti risultati sulla chiusura reale.

Teorema 1.21. *Ogni* (F, τ) *campo reale ammette una chiusura reale* R *che è unica a meno di* F*-isomorfismo.*

Consideriamo adesso la definizione di segno e il seguente principio logico:

Definizione 1.22. Sia F un campo reale chiuso, la funzione $sign : F \longrightarrow \{-1, 0, 1\}$ è così definita:

$$sign(a) = \begin{cases} 1 \; se \; a > 0 \\ 0 \; se \; a = 0 \\ -1 \; se \; a < 0 \end{cases}$$

Teorema 1.23 (**Principio di Tarski-Seidenberg**)**.** *Se* F' *campo reale chiuso contenente* F *campo reale chiuso. Se* Φ *è una affermazione nel linguaggio dei campi ordinati su* F*, proposizione costruita mediante* $>$*,* $<$ *,* $=$*, sign. Allora* Φ *è vera in* F' *se e solo se è vera in* F*.*

Questo fatto ha due importati conseguenze. La prima è che permette di dimostrare un risultato sulla chiusura reale in un certo senso analogo all'unicità della chiusura algebrica:

Teorema 1.24 (**Artin-Lang [Bec81]**)**.** *Sia* F *un campo reale e* A *un dominio finitamente generato su* F *con campo delle frazioni* k*. Dati* $a_1, \ldots, a_n \in A \setminus \{0\}$ *, elementi qualsiasi, i seguenti fatti sono equivalenti:*

- *Esiste una chiusura reale* R *di* F *e un* F*-omomorfismo* $\varphi : A \longrightarrow R$ *tale che:*
  - $\varphi(a_i) > 0, i = 1, \ldots, n$*;*
  - $\mathfrak{M} = \ker \varphi$ *è un ideale massimale regolare, ossia* $A_{\mathfrak{M}}$ *è regolare*[1]*.*

[1]Vedi Definizione 1.56

- *esiste un ordinamento σ di k tale per cui $a_1, \dots, a_n \in \sigma$.*

Corollario 1.25. *Sia R un campo reale chiuso e A una R-algebra di tipo finito. Se esiste un omomorfismo di R-algebre $\varphi : A \longrightarrow R_1$ in un'estensione reale chiusa di R, allora esiste un omomorfismo di R-algebre $\Phi : R \longrightarrow R_1$.*

Corollario 1.26. *Le chiusure reali di un di un campo reale F sono tutte coniugate e l'unico F-automorfismo è l'identità.*

Esempio 1.27. Gli anelli di funzioni razionali su $\mathbb{Q}$ sono campi reali ma re è solo un preordine, immergendoli in $\mathbb{R}$ si ottengono diversi possibili ordinamenti.

La seconda conseguenza del Principio di Tarski-Seidenberg è che, sebbene la chiusura reale di $\mathbb{Q}$ e delle sue estensioni algebriche sia $\mathbb{R}_{\text{alg}}$, ogni asserto che vale per $\mathbb{R}_{\text{alg}}$ vale anche per $\mathbb{R}$ e quindi nel seguito potremmo riferirci direttamente al campo dei numeri reali dove dovremmo riferirci alla chiusura algebrica di questi campi.

1.2 Il radicale reale

Se k è un campo reale possiamo definire il radicale reale per le k-algebre.

Definizione 1.28. Sia k campo reale e A una k-algebra, il *radicale reale* di un ideale $I \subseteq A$ è l'insieme

$$\sqrt[re]{I} \coloneqq \Big\{ f \in A \mid f^{2r} + \sum_{i=1}^{N} a_i g_i^2 \in I \ a_i \in re, g_i \in A, \ r \in \mathbb{N}, N \in \mathbb{N}_0 \Big\},$$

In particolare, se un ideale è tale che $\sqrt[re]{I} = I$ diremo che I è *reale*.

Osserviamo che se A è una k-algebra, allora re genera un preordine che è proprio $\sigma = \{\sum_{finite} x_i^2 z_i \mid x_i \in A, z_i \in re\}$. In maniera equivalente si può dire quindi che gli ideali reali sono ideali tali che se contengono una somma di quadrati $\sum a_i^2$ allora contengono tutti gli elementi a_i.

Si definisce più in generale su un anello dotato di un preordine σ il σ-radicale:

Definizione 1.29. Sia $I \subseteq A$ un ideale, il σ-radicale di I è l'insieme

$$\sqrt[\sigma]{I} \coloneqq \{ f \in A \mid f^{2r} + s \in I, \text{ con } s \in \sigma, r \in \mathbb{N} \}$$

Se $\sqrt[\sigma]{I} = I$, allora I è detto σ-reale.

Allora per una quasiasi k-algebra, come prima, possiamo costruire al variare di $\sigma \in \Gamma(k)$ diversi σ-radicali, ma

$$\sqrt[re]{I} \subseteq \sqrt[\sigma]{I}$$

per ogni $\sigma \in \Gamma(k)$.

Anche per il σ-radicale reale valgono alcune proprietà del radicale ordinario.

Lemma 1.30. *Siano I, J ideali di (A, σ) e S sottoinsieme moltiplicativo di A allora vale che*

- $\sqrt[\sigma]{I \cap J} = \sqrt[\sigma]{I} \cap \sqrt[\sigma]{J} = \sqrt[\sigma]{I \cdot J}$
- *Se A è un dominio* $\sqrt[\sigma]{S^{-1}I} = S^{-1}(\sqrt[\sigma]{I})$.

Consideriamo adesso il seguente insieme:

Definizione 1.31. Sia $P \subseteq A$, consideriamo $k(P) = \mathrm{Q}(A/P)$ il *campo residuo* e le sue classi $\overline{a} := a + P \in k(P)$.

$$\overline{\sigma} \coloneqq \left\{ \sum_{finite} x_i^2 \overline{s}_i \mid x_i \in k(P),\ s_i \in \sigma \right\}$$

Un'altra possibile scrittura è

$$\overline{\sigma} = \left\{ \frac{\overline{s}}{\overline{a}^2} \mid a \in A \smallsetminus P, s \in \sigma \right\}$$

Da qui in poi noi scegliamo di usare sempre re come preordine e quindi enunceremo le proposizioni intendendo fissato (k, re) un campo reale (re preordine) e A una k-algebra con l'ordinamento indotto da re.
Vale allora un proprietà utile per la caratterizzazione dei primi reali:

Lemma 1.32. *Sono equivalenti:*

1. *$\overline{\sigma}$ è un preordine per $k(P)$*
2. *$-1 \notin \overline{\sigma}$*
3. *$\sqrt[re]{P} = P$*

Dimostrazione. Chiaramente i primi due fatti sono equivalenti essendo σ un preordine su A. Supponiamo $-1 \in \overline{\sigma}$ allora esisterebbero $a \in A/P$ e $s \in \sigma$ tali che

$$-1 = \frac{\overline{s}}{\overline{a}^2}$$

allora $s + a^2 \in P$ ma $a \notin P$, e dunque $P \subsetneq \sqrt[re]{P}$. Supponendo di avere un elemento nel radicale non in P si dimostra facilmente che possiamo ottenere una scrittura di -1 in $\overline{\sigma}$ □

Possiamo enunciare adesso alcune proprietà molto utili del radicale reale:

Proposizione 1.33.

1. *$\sqrt[re]{I}$ è un ideale e ogni suo primo minimale P è reale.*
2. *$\sqrt[re]{I} = \bigcap_{\mathcal{P}(I)} P$ con $\mathcal{P}(I) = \{P \mid \text{primi reali su } I\}$.*
3. *Un ideale P primo in A è reale se e solo se $\overline{\sigma}$ è un preordine su $k(P)$.*

Dimostrazione.

1. Dalla definizione non è chiaro che $\sqrt[re]{I}$ sia un ideale, in particolare è da dimostrare la chiusura additiva di questo insieme. Allora $p \in \sqrt[re]{I}$ se esistono $r' \in \mathbb{N}$ e $s \in \sigma$ tali per cui $p^{2r} + s \in I$. Prendiamo quindi $f, g \in \sqrt[re]{I}$, allora per definizione esistono $r, r' \in \mathbb{N}$ e $s, t \in \sigma$ tali per cui $f^{2r} + s \in I$ e $g^{2r'} + t \in I$. Possiamo supporre, a meno di moltiplicare per una potenza,$r = r'$. Consideriamo adesso l'elemento $(f+g)^{4r} + (f-g)^{4r}$, vogliamo mostrare che esiste un elemento $u \in \sigma$ tale per cui $(f+g)^{4r} + (f-g)^{4r} + u \in I$.

$$\begin{aligned}(f+g)^{4r} + (f-g)^{4r} &= \sum_{i=0}^{4r} \binom{4r}{i} f^i g^{4r-i} + \sum_{i=0}^{4r} \binom{4r}{i} f^i (-g)^{4r-i} \\ &= \sum_{i=0}^{4r} \binom{4r}{2i} f^{2i} g^{2(2r-i)}\end{aligned}$$

   Basterà allora prendere

$$u = \sum_{i=1}^{r} f^{2i} \cdot g^{2(r-i)} s + \sum_{i=1}^{r} f^{2(i-r)} \cdot g^{2(r-i)} t \in \sigma$$

   e dunque $f + g \in \sqrt[re]{I}$.
   Dimostriamo adesso la seconda parte dell'asserto. Sia P primo minimale di $\sqrt[re]{I}$ e a un suo elemento. Allora $a^r + s \in P$ per r, s opportuni. Grazie al teorema di unicità della decomposizione primaria abbiamo che, grazie alla minimalità di P, esiste un elemento $x \notin P$ e $l \in \mathbb{N}$ tali che $(a^r + s)^l x \in \sqrt[re]{I}$. Ossia:

$$(a^r + s)^{lm} x^m + t \in I$$

   per qualche $m \in \mathbb{N}$ e $t \in \sigma$. A meno di moltiplicare per potenze pari di x, abbiamo che esistono y e u tali che

$$(ay)^{2r} + u \in I,$$

   che equivale a dire che $ay \in \sqrt[re]{I}$ e che quindi $ay \in P$. Per ipotesi $y \notin P$ e dunque $a \in P$, che implica evidentemente che $P = \sqrt[re]{P}$.

2. $\sqrt[re]{I}$ è un ideale radicale e quindi la sua decomposizione primaria minimale è fatta di ideali primi, allora per il punto precedente

$$\sqrt[re]{I} = \bigcap\{P \mid P \text{ primo minimale su } \sqrt[re]{I}\}.$$

Osservando che $I \subseteq P$ implica $\sqrt[re]{I} \subseteq \sqrt[re]{P} = P$ si ha la tesi.

3. È proprio l'enunciato del Lemma 1.32.

□

Proposizione 1.34. *Vale inoltre che:*

i. $\sqrt[re]{I} = \bigcap\{\sqrt[\alpha]{I} \mid \alpha \in \chi(k)\}$ *dove* $\chi(k)$ *è l'insieme degli ordinamenti su* k.

ii. Un ideale primo è reale se solo se qualche $\alpha \in \chi(k)$ *è estendibile a* $k(P)$ *se solo se* P *è* α*-reale per qualche* $\alpha \in \chi(k)$.

Dimostrazione. Consideriamo dapprima *ii.* : $\sqrt[re]{P} = P$ se e solo se $\overline{\sigma}$ si estende a un preordine di $k(P)$. Per il Corollario 1.7 questo equivale a dire che esiste α che estende re a $k(P)$, con questo argomento $\sqrt[\alpha]{P} = P$. La dimostrazione si conclude osservando che ogni $\beta \supseteq re$. *i.* discende dalla Proposizione 1.33 e da *ii.* . □

Concludiamo questo paragrafo con un proposizione che ci sarà utile nel momento in cui parleremo della corrispondenza varietà ideali.

Proposizione 1.35. *Sia* k *campo reale e* A *una* k*-algebra. Assumendo che* P *sia un ideale reale di* A *allora* $P = \bigcap M$*, intersezione infinita di ideali massimali reali su* P.

Dimostrazione. Dobbiamo mostrare che per ogni $f \notin P$ possiamo trovare un ideale massimale $M \supseteq P$ tale che $f \notin M$, $\sqrt[re]{M} = M$. In effetti possiamo considerare la k-algebra affine $B \coloneqq (A/P)\left[\frac{1}{f}\right] \subseteq k(P)$, per quanto visto esiste un ordine $\widetilde{\alpha}$ di $k(P)$ tale che α ordinamento di k. Indicando con R_α la chiusura reale di (k, α), il Teorema 1.24 da l'esistenza di un omomorfismo

$$\varphi : B \longrightarrow R_\alpha$$

$$\Phi : A \xrightarrow{\pi} A/P \xrightarrow{i} B \xrightarrow{\varphi} R_\alpha$$

e si verifica che $\ker \Phi$ è il massimale cercato. □

In realtà la Proposizione 1.35 congiunta col secondo punto della Proposizione 1.33 da che per un qualsiasi ideale $I \subseteq A$ vale

$$\sqrt[re]{I} = \bigcap M \tag{1.1}$$

al variare di M tra gli ideali reali massimali che contengono I.

1.3 Nullstellensatz Reale

Sappiamo che re è un ordinamento per $\mathbb{R}$ e per tutti i suoi sottocampi e, grazie ad Artin sappiamo che l'ordinamento su $\mathbb{Q}$ si estende fino alla sua chiusura reale un maniera unica. Consideriamo adesso l'anello dei polinomi $\mathbb{Q}[X_1, \dots, X_n]$ oppure $\mathbb{Q}(T_1, \dots, T_m)[X_1, \dots, X_n]$, su questi insieme in quanto $\mathbb{Q}$-algebre è generato un preordine σ come visto sopra, e questo preordine è proprio l'insieme delle somme finite di quadrati. Questo è però anche un ordine e quindi è l'unico sempre per il teorema di Artin.
Se invece consideriamo $\mathbb{Q}(T_1, \dots, T_m)[X_1, \dots, X_n]$ come $\mathbb{Q}(T_1, \dots, T_m)$ algebra questo fatto non è più vero, infatti in generale su un campo k abbiamo definito semplicemente un preordine esistono più possibilità per estenderlo, le diverse estensioni danno origine a diverse chiusure reali. Queste chiusure sono sì coniugate, ma le diverse immersioni complicano la situazione al momento in cui si va a considerare la varietà associata ad un ideale. Ogni $\alpha \in \chi(k)$ dà origine ad una diversa chiusura reale R_α, unica a meno di k-coniugazione. Poiché due chiusure reali R_α e R'_α sono coniugate , dato $I \subseteq k[X_1, \dots, X_n]$ un ideale, abbiamo una bigezione $\mathcal{V}_{R_\alpha}(I) \to \mathcal{V}_{R'_\alpha}(I)$ e dunque è ben definito

$$\mathcal{V}_\alpha(I) \coloneqq \bigcup_{R \text{ chiusura reale di } \alpha} \mathcal{V}_R(I).$$

Definiamo quindi cos'è una varietà su un campo reale nelle ipotesi assunte nel paragrafo precedente

Definizione 1.36. Sia k un campo reale e $I \subseteq k[X_1, \dots, X_n]$ ideale,

$$\mathcal{V}_{re}(I) \coloneqq \bigcup_{\alpha \in \chi(k)} \mathcal{V}_\alpha(I)$$

è l'insieme dei *punti reali* su I.

Esempio 1.37. Se $\mathbb{Q} \subseteq k \subseteq \mathbb{R}$, si ha semplicemente che

$$\mathcal{V}_{re}(I) = \mathcal{V}_{\mathbb{R}}(I)$$

Ricordiamo che grazie al principio di Tarski-Seidenberg possiamo usare $\mathbb{R}$ invece della chiusura reale per ogni $\mathbb{Q} \subseteq k \subseteq \mathbb{R}$.

Possiamo adesso enunciare il Nullstellensatz Reale, che come nel caso dei campi algebricamente chiusi, dà la corrispondenza tra ideali e luoghi di zeri.

Teorema 1.38 (**Real Nullstellensatz**). *Sia k un campo reale e $I \subseteq k[X_1, \dots, X_n]$ un ideale, allora vale che*

$$\mathcal{I}_k(\mathcal{V}_{re}(I)) = \sqrt[re]{I}.$$

Dimostrazione. $\supseteq$ Se $f \in \sqrt[re]{I}$ per definizione $\exists m \in \mathbb{N}, a_i \in re, g_i \in k[X_1, \ldots, X_n]$ con $i = 1 \ldots s$ tali che $f^{2m} + \sum_{i=1}^{s} a_i g_i^2 \in I$. Se $\mathcal{V}_{re}(I) = \varnothing$ chiaramente $\sqrt[re]{I} \subseteq \mathcal{I}_k(\mathcal{V}_{re}(I)) = A$. Sia dunque $x \in \mathcal{V}_{re}(I)$, x sarà elemento di una certa $\mathcal{V}_{R_\alpha}(I)$, con R_α chiusura reale, e di conseguenza valutando

$$\Big(f^{2m} + \sum_{i=1}^{s} a_i g_i^2\Big)(x) = 0$$

$$f^{2m}(x) + \sum_{i=1}^{s} a_i g_i^2(x) = 0$$

Entrambi gli addendi, essendo quadrati, stanno in α e dunque sono positivi, ma allora $f^{2m}(x) = 0$ ed essendo in campo $f(x) = 0$.
$\subseteq$ Vogliamo mostrare che se $f \in k[X_1, \ldots, X_n] \setminus \sqrt[re]{I}$ allora esiste $x \in \mathcal{V}_{re}(I)$ tale che $f(x) \neq 0$.
L'equazione (1.1) mostra che esiste un massimale M radicale che contiene I e $f \notin M$ cosicché data una qualsiasi chiusura R di (k, α), con $\alpha \in \chi(k)$, esiste l'immersione

$$i : k(M) \hookrightarrow R$$

per la Proposizione 1.33. Adesso, se $\pi : k[X_1, \ldots, X_n] \longrightarrow k(M)$ è la proiezione canonica sul quoziente, allora il punto $\bar{x} = (\bar{X_1} \ldots \bar{X_n}) \in k(M)^n \subseteq R^n \subseteq \bar{k}^n$ punto cercato ($\bar{k}$ chiusa algebrica). □

Esempio 1.39. Inoltre se $\mathbb{Q} \subseteq k \subseteq \mathbb{R}$ un campo e $I \subseteq k[X_1, \ldots, X_n]$ un ideale, allora vale che

$$\mathcal{I}_k(\mathcal{V}_{\mathbb{R}}(I)) = \sqrt[re]{I}.$$

E abbiamo che se $k = \mathbb{R}$ allora sono ripristinate anche le corrispondenze:

$$\big\{\mathcal{V}_{\mathbb{R}}(I) \subseteq \mathbb{R}^n \mid I \subseteq k[X_1, \ldots, X_n]\big\} \longleftrightarrow \big\{J \subseteq \mathbb{R}[X_1, \ldots, X_n] \mid J = \sqrt[re]{J}\big\}$$
$$\big\{\mathcal{V}_{\mathbb{R}}(I) \mid \text{varietà irriducibile}\big\} \longleftrightarrow \big\{P \mid P \text{ ideale primo reale}\big\}$$
$$\big\{\mathcal{V}_{\mathbb{R}}(I) \mid \text{varietà irriducibile zero dimensionale}\big\} \longleftrightarrow \big\{M \mid M \text{ ideale massimale reale}\big\}$$

Vediamo qualche esempio di applicazione e poi alcune conseguenze:

Esempio 1.40.

1. Sia $I = (x^2 + 1) \subseteq \mathbb{R}[x]$, chiaramente $1 \in \sqrt[re]{I}$ allora in accordo col teorema $\mathcal{V}_{\mathbb{R}}(I) = \varnothing$.

2. Riprendiamo l'esempio iniziale, sia $I = (x^2 - 3, y^2 - 4) \subseteq \mathbb{Q}[x, y]$ allora $\sqrt[re]{I} = I = \mathcal{I}_{\mathbb{Q}}(\mathcal{V}_{\mathbb{R}}(I))$.

3. Riprendiamo l'esempio iniziale, sia $I = (x^3 - 5, y^2 - 4) \subseteq \mathbb{Q}[x, y]$ allora $\sqrt[re]{I} = I = \mathcal{I}_{\mathbb{Q}}(\mathcal{V}_{\mathbb{R}}(I))$ e dunque è reale su $\mathbb{Q}[x, y]$, ma ad esempio $\sqrt[re]{I} = \big(x - \sqrt[3]{5}, y^2 - 4\big) = \mathcal{I}_{\mathbb{Q}(\sqrt[3]{5})}(\mathcal{V}_{\mathbb{R}}(I)) \neq I$.

4. Riprendiamo l'esempio iniziale, sia $I = (x^2 - 3, y^2 + 4) \subseteq \mathbb{Q}[x, y]$ allora $\sqrt[re]{I} = (1) = \mathcal{I}_{\mathbb{Q}}(\mathcal{V}_{\mathbb{R}}(I))$.

Corollario 1.41.

i. $\mathcal{I}_k(\mathcal{V}_{R_\alpha}(I)) = \sqrt[\alpha]{I}$

ii. $\sqrt[re]{I\mathbb{R}_\alpha} \cap k[X_1, \ldots, X_n] = \sqrt[\alpha]{I}$

Dimostrazione. i. $\mathcal{I}_k(\mathcal{V}_{R_\alpha}(I)) = \mathcal{I}_k(\mathcal{V}_\alpha(I))$.
ii. $\mathcal{I}_k(\mathcal{V}_{R_\alpha}(I)) = \mathcal{I}_{R_\alpha}(\mathcal{V}_{R_\alpha}(I)) \cap k[X_1, \ldots, X_n]$ ed inoltre $\mathcal{I}_{R_\alpha}(\mathcal{V}_{R_\alpha}(I)) = \mathcal{I}_{R_\alpha}(\mathcal{V}_{R_\alpha}(I\mathbb{R}_\alpha)) = \sqrt[re]{I\ R_\alpha}$ □

Diamo infine un'altra condizione necessaria e sufficiente per caratterizzare i primi reali, che specifica le proposizioni date sin ora.

Lemma. *Se P è un ideale primo reale allora $P\ \mathbb{R}_\alpha$ è primo (reale).*

Dimostrazione. Vedere [BN93] pag.7 Proposizione 7. □

Proposizione 1.42. *Un ideale primo $P \subset k[X_1, \ldots, X_n]$ è reale se e solo se P si estende a Q ideale primo reale di $\mathbb{R}_\alpha[X_1, \ldots, X_n]$.*

Dimostrazione. Se $Q = P^e$ allora $P = Q \cap k[X_1, \ldots, X_n]$ e dunque $P \subseteq \sqrt[re]{P} \subseteq \sqrt[\alpha]{P} \subseteq \sqrt[re]{Q} \cap k[X_1, \ldots, X_n]$ ci da $P = \sqrt[re]{P}$. Viceversa se P è reale esiste un ordine $\alpha \in \chi(k)$ tale per cui $\sqrt[\alpha]{P} = P$. Se quindi R è la chiusura reale di (k, α) per il Nullstellensatz si ha che

$$P = \sqrt[\alpha]{P} = \sqrt[re]{P\ R_\alpha} \cap k[X_1, \ldots, X_n] = (\sqrt[re]{PR_\alpha})^c$$

Abbiamo però che per la Proposizione 1.33 $\sqrt[re]{PR_\alpha}$ reale, rimane da dimostrare che è primo, ma per il lemma vale la tesi.

□

Osservazione. Questo ed altri fatti, come la proposizione sopra, valgono più in generale e anche il Nullstellensatz appena enunciato è solo un caso particolare. Abbiamo visto che a partire da un preordine è sempre possibile costruire un ordinamento su k) e che in questo contesto allora più che di chiusura algebrica ha senso parlare di chiusura reale R, che è la più piccola estensione reale chiusa di (k, τ).
Il radicale reale in questo contesto diventa *τ-radicale*

$$\sqrt[\tau]{I} = \left\{ f \in k[X_1, \ldots, X_n] \mid f^{2r} + \sum_{i=1}^{N} a_i g_i^2 \in I \text{ per } a_i \in \tau, g_i \in k[X_1, \ldots, X_n] \right\}.$$

Allora l'insieme dei punti τ-reali su I è

$$\mathcal{V}_\tau(I) \coloneqq \bigcup_{\alpha \in \chi_\tau(k)} \mathcal{V}_\alpha(I)$$

e il teorema afferma che per ogni ideale $I \in k[X_1, \ldots, X_n]$

$$\mathcal{I}_k(\mathcal{V}_\tau(I)) = \sqrt[\tau]{I}.$$

1.4 Ideali zero-dimensionali

Il concetto di dimensione è molto importante nella geometria algebrica e sarà centrale per la nostra trattazione, raccogliamo quindi in questa sezione le definizioni e risultati che useremo per la costruzione dell'algoritmo per il calcolo del radicale reale di un ideale in un anello di polinomi.

Come prima cosa definiamo cosa si intende per dimensione di un anello e di un ideale:

Definizione 1.43. La dimensione di Krull di un anello A è l'estremo superiore delle lunghezze delle catene di primi strettamente crescenti in esso contenute (anche infinite). In particolare, data una catena

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$$

questa ha lunghezza n. Indicheremo la dimensione di Krull di A come $\dim(A)$.

Definizione 1.44. Dato un anello A e un suo ideale I, allora la dimensione dell'ideale I è la dimensione di Krull del quoziente.

$$\dim I := \dim \left({}^{A}\!/_{I} \right)$$

Per un ideale primo si definisce anche il concetto complementare a quello di dimensione, cioè l'altezza:

Definizione 1.45. Dato un anello A e un suo ideale primo P, allora l'*altezza* dell'ideale P, $ht(P)$, è l'estremo superiore dell'insieme di tutti gli interi per i quali esiste una catena di inclusioni di ideali primi distinti di A tali che

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_s = P.$$

In questi termini la dimensione di Krull di un anello non è altro che l'estremo superiore delle altezze di tutti i suoi ideali primi.

Lemma 1.46. *Dato I ideale di un anello di polinomi su un campo algebricamente chiuso, allora sono equivalenti*

i. $\#\mathcal{V}(I)$ *è finita*

ii. $\dim_k (k[X_1, \ldots, X_n]/I)$ *come k-spazio vettoriale è finita*

iii. $\dim I = 0$

ed in questo caso,

$$I = \sqrt{I} \iff \dim_k (k[X_1, \ldots, X_n]/I) = \#\mathcal{V}(I)$$

In realtà togliendo l'ipotesi algebricamente chiuso le implicazioni continuano a valere eccetto $i. \Rightarrow ii.$.

Sono di particolare rilievo per noi gli ideali di dimensione zero, vediamo adesso la generalizzazione di un risultato di algebra classica che ci servirà per dimostrare una proprietà molto utile degli ideale zero-dimensionali:

Teorema 1.47 (Teorema cinese del resto generalizzato)**.** *Siano I_1, I_2 ideali della forma*

$$I_1 = (X_1 - p_1(X_2, \ldots, X_n), J_1) \qquad I_2 = (X_1 - p_2(X_2, \ldots, X_n), J_2)$$

e supponiamo che

- $(J_1, J_2) = 1$
- $J_i = I_i \cap k[X_2, \ldots, X_n]$

Allora esiste $q \in k[X_1, \ldots, X_n]$ tale che $I_1 \cap I_2 = (X_1 - q(X_2, \ldots, X_n), J_1 J_2)$.

Dimostrazione. Chiaramente possiamo lavorare sul quoziente per l'ideale per X_1. Per il teorema cinese del resto, esiste un unico $q(X_2, \ldots, X_n)$ tale che

$$\begin{aligned} q \equiv p_1 \pmod{J_1}, \quad q \equiv p_2 \pmod{J_2} &\implies q - p_1 \in J_1, \quad q - p_2 \in J_2 \\ &\implies X_1 - q(X_2, \ldots, X_n) \in I_1 \cap I_2 \end{aligned}$$

e dunque abbiamo

$$I_1 \cap I_2 = (X_1 - q(X_2, \ldots, X_n), J_1 J_2)$$

□

Trattando anelli di polinomi ci serviranno anche la basi di Gröbner, ricordiamo perciò le definizioni principali:

Definizione 1.48. Un ordinamento monomiale è una relazione d'ordine su $\mathbb{N}^n$ tale che

a) è un buon ordine

b) $\forall \alpha, \beta, \gamma \in \mathbb{N}^n \ \alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma$

Gli ordinamenti monomiali a cui faremo riferimento sono

- Ordinamento lessicografco (lex):

  $\alpha \geq \beta \iff$ in $\alpha - \beta$ il primo termine non nullo da sinistra è positivo

- Ordinamento revlex:

  $\alpha \geq \beta \iff$ in $\alpha - \beta$ il primo termine non nullo da destra è positivo

- Ordinamento degrevlex:

  $\alpha \geq \beta \iff |\alpha| \geq |\beta|$ e il primo termine da destra non nullo di

  $\alpha - \beta$ è negativo

Fissato un qualsiasi ordinamento monomiale, allora il *multigrado* di un polinomio $f = \sum c_\alpha X^\alpha \in k[X_1, \ldots, X_n]$, $\deg f$, è il massimo degli δ tale che c_δ è non nullo e il *termine di testa o leading term* di f è proprio $lt(f) := c_\delta X^\delta$. Si definisce per ogni ideale I l'insieme $\mathrm{Lt}(I) := \{lt(f) \mid f \in I\}$, l'ideale monomiale $(\mathrm{Lt}(I))$ è detto ideale dei leading term di I.

Definizione 1.49. Sia I un ideale di $A := k[X_1, \ldots, X_n]$, fissato un ordinamento monomiale, una base di Gröbner di I è un insieme $\{f_1, \ldots, f_k\} \subseteq I$ tale che

$$(\mathrm{Lt}(G)) := (lt(f_1), \ldots, lt(f_k)) = (\mathrm{Lt}(I))$$

Inoltre:

Definizione 1.50. Un base di Gröbner $G = \{f_1, \ldots, f_k\}$ di I si dice ridotta se

i) $\{lt(f_1), \ldots, lt(f_k))\}$ è un insieme di generatori di cardinalità minimale di $(\mathrm{Lt}(I))$,

ii) il coefficiente c_δ di ogni termine di testa, *leading coefficient*, è 1,

iii) per ognuno dei f_i, nessun dei monomi di f_i appartiene all'ideale $\big(\mathrm{Lt}(G \setminus \{f_i\})\big)$.

Le basi di Gröbner ridotte sono molto speciali perché sono univocamente determinate (per i dettagli rimandiamo a [CLO07]) :

Teorema 1.51. *Sia I un ideale di $k[X_1, \ldots, X_n]$. Allora I ammette un'unica base di Gröbner ridotta.*

Possiamo a questo punto concentrarci su fatti più strettamente legati alla trattazione. Come prima cosa diamo la definizione di *posizione generale*, vedremo più avanti che per gli ideali in posizione generale è abbastanza semplice calcolare radicale reale.

Definizione 1.52. Un ideale zero-dimensionale primo $P \subseteq k[X_1, \ldots, X_n]$ si dice *in posizione generale* se nella base di Gröbner ridotta rispetto all'ordinamento revlex è della forma

$$P = (X_n - p_n(X_1), \ldots, X_{n-1} - p_{n-1}(X_1), p_1(X_1))$$

con p_1 irriducibile.

Definizione 1.53. Un ideale zero-dimensionale $I \subseteq k[X_1, \ldots, X_n]$ si dice *in posizione generale* se i suoi primi minimali associati sono in posizione generale.

Grazie al Teorema cinese del resto generalizzato otteniamo che un ideale radicale zero-dimensionale in posizione generale scritto nella base di Gröbner ridotta revlex è della forma

$$I = (X_n - p_n(X_1), \ldots, X_{n-1} - p_{n-1}(X_1), h_1 h_2 \ldots h_k(X_1))$$

con $(h_i, h_j) = 1$ e h_i irriducibile per ogni $i = 1, \ldots, k$.

Teorema 1.54 (Shape-Lemma)**.** *Sia I un ideale radicale zero-dimensionale. Allora per quasi ogni cambio di coordinate lineare φ_c di $k[X_1, \ldots, X_n]$ indotto da $c \in k^{n-1}$, eccetto un'unione finita di sottospazi lineari affini di k^{n-1}, l'immagine $\varphi_c(I)$ è in posizione generale.*

Dimostrazione. Sia $\mathcal{V}(I) = \{\alpha_1, \ldots, \alpha_m\}$. Cerchiamo $L\colon k^n \to k$ lineare tale che $L(\alpha_i) \neq L(\alpha_j)$. Sia C il vettore che rappresenta tale funzionale. Basta allora che C non appartenga all'ortogonale dei vettori $\alpha_i - \alpha_j$ al variare di i, j. Poiché vi sono $\binom{m}{2}$ scelte di i, j, abbiamo che le scelte di C che non soddisfano la tesi sono corrispondenti all'unione di $\binom{m}{2}$ iperpiani di k^n, da cui la tesi[2]. □

Introduciamo adesso un'applicazione dello *Shape Lemma* che ci servirà nel terzo capitolo:

Proposizione 1.55. *Se k è un campo qualsiasi con chiusura algebrica $\bar{k}$, $I \subseteq k[X_1, \ldots, X_n]$ e valgono le seguenti ipotesi:*

1. *$\{X_1, \ldots, X_m\}$ è un sottoinsieme massimale di $\{X_1 \ldots X_n\}$ indipendente[3] modulo I con $m \leq n - 2$,*

2. *l'ideale esteso $I^e := Ik(X_1, \ldots, X_m)[X_{m+1}, \ldots, X_n]$ è in posizione generale rispetto X_{m+1}.*

[2] serve che il campo k sia infinito e i campi reali lo sono.
[3] ossia $k[X_1, \ldots, X_m] \cap I = 0$.

Allora possiamo costruire $s \in k[X_1, \dots, X_m] \backslash 0$, $r_{m+2}, \dots, r_n \in k[X_1, \dots, X_{m+1}]$ *e* $J \in k[X_1, \dots, X_{m+1}]$ *tale che per ogni* $x \in \overline{k}^n$ *con* $s(x_1, \dots, x_m) \neq 0$ *vale il seguente fatto:*

$$x \in \mathcal{V}_{\overline{k}}(I) \iff (x_1, \dots, x_{m+1}) \in \mathcal{V}_{\overline{k}}(J),\ x_i = \frac{r_i(x_1, \dots, x_{m+1})}{s(x_1, \dots, x_m)} \text{ per } i = m+2, \dots, n$$

Dimostrazione. Possiamo ridurci al caso I radicale. Sia G la base di Gröbner di I rispetto l'ordine lessicografico con $X_1 < \cdots < X_n$ e sia $S \coloneqq k[X_1, \dots, X_m] \backslash 0$. Detta $A = k[X_1, \dots, X_n]$, consideriamo il monomorifsmo:

$$\mu \colon A \longrightarrow S^{-1}A$$

Allora $\mu(G) = G$, per le ipotesi[4] , è anche la base di Gröbner dell'ideale I^e rispetto all'ordine lessicografico puro $X_{m+1} < \cdots < X_n$. Grazie al Teorema 1.54 ci sono $g_{m+2}, \dots, g_n \in G$ della forma $g_i = h_i \cdot X_i + r_i$ con $h_i \in S$ e $r_i \in k[X_1, \dots, X_{i-1}]$ per $i = m+2, \dots, n$. Definiamo $s \coloneqq \prod_{j=m+2}^{n} h_j \in S$. Pseudoriducendo G moltiplicando per $h_{m+2}, \dots, h_n$ si ha un insieme finito

$$G' = \{g'_{m+2}, \dots, g'_n, g'_{n+1}, \dots\} \subseteq k[X_1, \dots, X_n]$$

che soddisfa le seguenti condizioni:

- $g'_i = h_{m+2}^{n_{i,m+2}} \cdots h_{i-1}^{n_{i,i-1}} \cdot X_i + r'_i$ dove $n_{i,m+2}, \dots, n_{i,i-1} \in \mathbb{N}_0$ e $r'_i \in k[X_1, \dots, X_{m+1}]$ per $i = m+2, \dots, n$.
- $g'_i \in k[X_1, \dots, X_{m+1}]$ per $i > n$.
- $\mathcal{V}_{\overline{k}}(G') \cap \{s \neq 0\} = \mathcal{V}_{\overline{k}}(I) \cap \{s \neq 0\}$

Definendo $J \coloneqq (g'_i \colon i > n)k[X_1, \dots, X_{m+1}]$ otteniamo per tutti $x \in \overline{k}^n$ tali che $s(x_1\, dots, x_m) \neq 0$ che $x \in \mathcal{V}_{\overline{k}}(I)$ se e solo se $(x_1, \dots, x_{m+1}) \in \mathcal{V}_{\overline{k}}(J)$ e

$$h_{m+2}^{n_{i,m+2}} \cdots h_{i-1}^{n_{i,i-1}} h_i(x_1, \dots, x_m) \cdot x_i + r'_i(x_1, \dots, x_{m+1}) = 0$$

per $i = m+2 \dots n$. □

Osservazione. Sia k un campo infinito, ad esempio un campo reale, $I \subseteq k[X_1, \dots, X_n]$, $m \coloneqq \dim I \leq n-2$ e senza perdita di generalità $\{X_1, \dots, X_m\}$ un sottoinsieme massimale di $\{X_1, \dots, X_n\}$ indipendente[5] modulo I. Per $c = (c_{m+2}, \dots, c_n) \in k^{n-m-1}$ definiamo l'automorfismo

$$\begin{array}{rccc} \varphi_c \colon & k[X_1, \dots, X_n] & \longrightarrow & k[X_1, \dots, X_n] \\ & f(X_1, \dots, X_n) & \longmapsto & f(X_1, \dots, X_{m+1} + \sum_{i=m+2}^{n} c_i X_i, \dots X_n). \end{array}$$

Allora per quasi tutti i vettori $c = (c_{m+2}, \dots, c_n) \in k^{n-m-1}$, ossia tutti eccetto un'unione finita di sottospazi lineari affini di k^{n-m-1}, $\varphi_c(I)$ soddisfa le ipotesi della Proposizione 1.55. Vettori di questa sorta sono comunque determinabili deterministicamente.

[4] $G \subseteq k[X_{m+1}, \dots, X_n]$

[5] ossia $k\,[X_1, \dots, X_m] \cap I = 0$

1.5 Anelli regolari

Così come per la dimensione anche gli anelli regolari ricorreranno più volte, riportiamo quindi la definizioni e alcune proprietà che ci serviranno.

Definizione 1.56. Se A è un anello noetheriano locale, con $\mathfrak{M}$ ideale massimale e $k = A/\mathfrak{M}$ il campo residuo, allora A è detto *regolare* se $\dim A = \dim_k \mathfrak{M}/\mathfrak{M}^2$, dove $\mathfrak{M}/\mathfrak{M}^2$ è visto come k-spazio vettoriale.
Un anello noetheriano è regolare se ogni sua localizzazione $A_{\mathfrak{M}}$ (dove $\mathfrak{M}$ è un suo ideale massimale) è un anello locale regolare.

Osservazione. Una definizione equivalente di anello regolare può essere che il numero di generatori del suo ideale massimale è uguale alla sua dimensione di Krull.

Gli anelli regolari godono di alcune particolari proprietà:

Proposizione 1.57. *Sia A è un anello regolare locale, con $\mathfrak{M}$ ideale massimale e $k = A/\mathfrak{M}$ il campo residuo, di dimensione d. Allora:*

1. *A è un dominio integralmente chiuso.*
2. *Un sistema di d elementi genera $\mathfrak{M}$ se e solo se le loro classi modulo $\mathfrak{M}^2$ sono una base di $\mathfrak{M}/\mathfrak{M}^2$ sul k. E in tal caso si dicono sistema regolare di parametri.*
3. *Se Q è un ideale di A, A/Q è regolare se e solo se Q è generato da elementi di $\mathfrak{M}$ le cui classi modulo $\mathfrak{M}^2$ sono indipendenti su k. In tal caso* $\dim A - \dim A/Q$ *è il numero di generatori.*

Capitolo 2

Polinomi Reali

Prima di iniziare a parlare di calcolo del radicale reale è utile dedicare la nostra attenzione al caso di un singolo polinomio. In questo capitolo vedremo dunque che cosa vuol dire che un polinomio è reale. Nel prossimo capitolo infatti mostreremo che è possibile ricondurre il calcolo del radicale reale per un qualsiasi I alla capacità di decidere se un polinomio irriducibile in una sola variabile abbia zeri reali o meno.

2.1 Polinomi univariati

Consideriamo per adesso solamente polinomi a coefficienti in k, un campo reale con re preordine, che dipendono solo dalla variabile X.

Osservazione. La prima osservazione da fare è che, dato un campo F, l'anello dei polinomi $F[X]$ è sempre un dominio ad ideali principali. Otteniamo che in questo speciale caso ogni ideale I può essere scritto nella forma $I = (f)$. Ma allora il suo radicale reale sarà generato dà un unico polinomio.

Definizione 2.1. Sia k un campo reale. Se $f \in F[X]$ allora f è detto *reale* se $\sqrt[re]{(f)} = (f)$.

Definizione 2.2. Sia k un campo reale. Se $f \in F[X]$, allora la *parte reale* di f è un polinomio $\widetilde{f} \in F[X]$ tale che

$$\sqrt[re]{(f)} = (\widetilde{f})$$

Notiamo che questa è una buona definizione perché due generatori di un'ideale principale in $k[X]$ differiscono per la moltiplicazione per un invertibile.
Osserviamo che dalla definizione è già chiaro che trovare la parte reale di un polinomio in questo contesto equivale a trovare il radicale reale. In termini di parte reale si ha anche che vale la seguente equivalenza:

Proposizione 2.3. *Sia k un campo reale e $f \in k[X]$. Allora un f è reale se e solo se coincide con la sua parte reale.*

Esempio 2.4. I sottocampi di $\mathbb{R}$, nel primo capitolo abbiamo visto che godono di particolari proprietà. In questo caso le definizioni di parte reale e polinomio reale diventano:

Definizione 2.5. Sia $F/\mathbb{Q}$ un'estensione di campi con $F \subset \mathbb{R}$, se $f \in F[X]$ allora f è detto *reale* se $\sqrt[re]{(f)} = (f)$.

Definizione 2.6. Sia $F/\mathbb{Q}$ un'estensione di campi con $F \subset \mathbb{R}$, se $f \in F[X]$, allora la *parte reale* di f è un polinomio $\widetilde{f} \in F[X]$ tale che

$$\sqrt[re]{(f)} = (\widetilde{f})$$

In questo particolare caso vale un fatto banale ma di fondamentale importanza:

Corollario 2.7. *Sia $p \in k[X]$ un polinomio irriducibile. Allora p è reale se e solo se esiste $a \in \mathbb{R}$ tale che $p(a) = 0$.*

In questo caso per capire se un polinomio irriducibile, a coefficienti in un tale k, è reale ci basta contarne le radici. Vedremo nel prossimo capitolo una possibile strategia, effettivamente implementabile, se $F = \mathbb{Q}$.

Diamo adesso qualche esempio per capire meglio quello che abbiamo detto sin ora:

Esempio 2.8.

1. Sia $p(x) = x^5 - 3x^4 + 6x + 1 \in \mathbb{Q}[x]$ è un polinomio irriducibile di grado dispari e dunque ha una radice reale, allora p è reale. Mentre se $g = x^7 - 3x^6 + 6x^5 - 18x^4 + 6x^3 + x^2 + 36x + 6 = p \cdot (x^2 + 6)$ allora si calcola che $\widetilde{g} = \widetilde{p}$, e quindi g non è reale.

2. Sia $p(x) = x^2 + 2\alpha x + \alpha^2 \in \mathbb{Q}(\alpha)[x]$ con $\alpha \in \mathbb{R}$ allora $\widetilde{p} = x + \alpha$.

3. Sia $p = x^4y^4 - 2x^5y^3z^2 + x^6y^2z^4 + 2x^2y^3z - 4x^3y^2z^3 + 2x^4yz^5 + z^2y^2 - 2z^4yx + z^6x^2 \in \mathbb{Q}[x, y, z]$ allora $\widetilde{p} = x^3yz^2 - x^2y^2 + xz^3 - yz$, mentre se $g = p \cdot (x^2 + y^2 + 1)$ allora $\widetilde{g} = \widetilde{p}$.

Consideriamo adesso un polinomio in $F := \mathbb{Q}(T_1, \ldots, T_m)$ e che cosa comporta dire che un polinomio è reale anche in questo caso. Abbiamo detto che re è un preordine anche per F, e dunque la definzione si estende in maniera ovvia. In questo contesto, a differenza dell'esempio, è però più difficile capire che cosa vuol dire che un polinomio $f \in F[X]$ è reale.

In generale sia k un campo reale. Allora vale il seguente criterio che ci aiuta, se il polinomio in oggetto è irriducibile, a capire se è reale o meno.

Proposizione 2.9. *Sia $p \in k[T_1, \ldots, T_m, X]$ polinomio irriducibile in $F[X]$ con $F \coloneqq k(T_1, \ldots, T_m)$. Allora i seguenti fatti sono equivalenti:*

i. $\sqrt[re]{p} = (p)$*, ossia p è reale su F.*

ii. Esiste un ordinamento $\alpha \supseteq re$ tale che il polinomio $-lc_X(p) \cdot p$, valutato nella chiusura R_α di k, assume almeno in un punto un valore strettamente positivo ($lc_X(p)$ è il leading coefficient di p rispetto alla variabile X).

Dimostrazione.

i. $\Rightarrow$ *ii.*Per la Proposizione 1.34, *ii.* abbiamo che esiste $\alpha' \in \chi(F)$ il quale si estende a un ordinamento $\bar{\alpha}$ del campo $L \coloneqq F[X]/(p)$. Consideriamo la valutazione p-adica su $F(X)$ e $\pi \coloneqq -lc_X(p) \cdot p$ come parametro uniformante.
Ogni elemento $f \in F(X)^*$ ha un'unica rappresentazione $f = \pi^r \cdot g(X)$ con $g \in F[X]$ e $\pi \nmid g(X)$. Poniamo

$$\tilde{\alpha} \coloneqq \{0\} \cup \{\pi^r \cdot g(X) \mid r \in \mathbb{Z}, g \in F[X], \pi \nmid g(X), g(u) \in \bar{\alpha}\}$$

dove $u = X + (p(X)) \in L$. $\tilde{\alpha}$ è un altro ordinamento su $F(X)$ e $\pi = -lc_X(p) \cdot p \in \tilde{\alpha}$. Usando il teorema di Artin-Lang (Teorema 1.24) si dimostra che π in effetti assume valore strettamente positivo in R_α, con $\alpha = \tilde{\alpha} \cap k$.
ii. $\Rightarrow$ *i.* Per ipotesi $\pi(u_1, \ldots, u_m, v) > 0$ in una appropriata R_α, $\alpha \supseteq re$. Il nucleo dell'omomorfismo

$$\begin{array}{rccc} \varphi\colon & k[T_1, \ldots, T_m, X] & \longrightarrow & R_\alpha \\ & (T_1, \ldots, T_m, X) & \longmapsto & (u_1, \ldots, u_m, v) \end{array}$$

è un ideale regolare[1], in quanto $k[T_1, \ldots, T_m, X]$ è un anello regolare. Per il teorema di Artin-Lang, nella forma di Becker, allora esiste un ordinamento $\tilde{\alpha}$ su $k(T_1, \ldots, T_m, X)$ che estende α tale per cui si ha che $\pi = -lc_X(p) \cdot p \in \tilde{\alpha}$. Poniamo adesso $\tilde{\alpha_0} \coloneqq \tilde{\alpha} \cap k(T_1, \ldots, T_m)$. Applicando nuovamente Artin-Lang a $k(T_1, \ldots, T_m)$ e $\tilde{\alpha_0}$ otteniamo l'esistenza di una chiusura reale $R_{\tilde{\alpha_0}}$ in cui $\pi(T_1, \ldots, T_m, \tilde{v}) > 0$, per qualche $\tilde{v} \in R_{\tilde{\alpha_0}}$. Chiaramente esisterà un punto su cui π assume valore negativo e dunque per il Teorema dei Valori Intermedi per campi reali (vedere [BCR98]) possiamo trovare uno zero di π in $R_{\tilde{\alpha_0}}$ e quindi anche di $p(T_1, \ldots, T_m, X)$.
Questo significa che $F[X]/(p)$[2] ammette un ordinamento $\bar{\alpha_0}$ che si estende a $\tilde{\alpha_0}$. E dunque per la Proposizione 1.34 $\sqrt[\bar{\alpha_0}]{(p)} = (p)$. Ma per ipotesi $re \subseteq \tilde{\alpha_0}$ e dunque $\sqrt[re]{(p)} = (p)$. □

[1] ossia $k[T_1, \ldots, T_m, X]_{\ker \varphi}$

[2] $F[X]/(p)$ è un campo in quanto PID e (p) primo, dunque massimale. E quindi il suo campo delle frazioni è lui stesso.

Esplicitiamo adesso una conseguenza del teorema precedente se $k = \mathbb{Q}$:

Corollario 2.10. *Sia $p \in \mathbb{Q}[T_1, \ldots, T_m, X]$ polinomio irriducibile non costante rispetto alla variabile X. Allora i seguenti fatti sono equivalenti:*

i. (p) *è reale su* $\mathbb{Q}(T_1, \ldots, T_m)[X]$.

ii. (p) *è reale su* $\mathbb{Q}[T_1, \ldots, T_m, X]$.

iii. Esistono due punti $x, x' \in \mathbb{R}^{m+1}$ *tali che* $p(x) \cdot p(x') < 0$ *in* $\mathbb{R}$.

Dimostrazione. L'equivalenza tra le prime due e la terza è una conseguenza che risulta immediatamente dalla dimostrazione della proposizione precedente e dal fatto che $\mathbb{Q}(T_1, \ldots, T_m)$ si immerge in $\mathbb{R}$.
Detto $S = \mathbb{Q}[T_1, \ldots, T_m] \setminus 0$, definiamo l'applicazione:

$$\begin{array}{rccc} \mu\colon & \mathbb{Q}[T_1, \ldots, T_m, X] & \longrightarrow & \mathbb{Q}(T_1, \ldots, T_m)[X] \\ & I & \longmapsto & \mu(I) = S^{-1}I \end{array}$$

ii. $\Rightarrow$ *i.* è chiaramente una conseguenza della Proposizione 1.33 e il Lemma 1.30.
i. $\Rightarrow$ *ii.* Per le ipotesi su p, allora l'ideale $(p)^e$ in $\mathbb{Q}(T_1, \ldots, T_m)[X]$ è proprio e dunque per corrispondenza $(p)^{ec} = (p) \subseteq \sqrt[re]{(p)}$.
Per ipotesi inoltre p è reale e quindi, per il Lemma 1.30, vale che $(p)^e = S^{-1}(p) = \sqrt[re]{S^{-1}(p)} = S^{-1}\sqrt[re]{(p)} = (\sqrt[re]{(p)})^e$. Osservando che in generale si ha che $I^{ec} \supseteq I$ allora $\sqrt[re]{(p)} \subseteq (\sqrt[re]{(p)})^{ec} = (p)^{ec} = (p)$.

□

La Proposizione 2.9 fornisce un criterio per capire quando un polinomio univariato è reale. Tuttavia sfruttando le altre proprietà del radicale reale è possibile calcolare effettivamente la parte reale di un polinomio.
Vale quindi il seguente teorema:

Teorema 2.11. *Sia k, un campo reale e detto $F \coloneqq k(T_1, \ldots, T_m)$ tale che*

- *esiste un algoritmo per la fattorizzazione di polinomi univariati,*
- *esiste un algoritmo per decidere se un polinomio multivariato su k è indefinito fissata una qualsiasi chiusura reale R_α di k.*

Allora esiste un algoritmo per calcolare la parte reale di ogni polinomio $f \in F[X]$.

Dimostrazione. Usando un algoritmo per il calcolo della fattorizzazione squarefree di f in $F[X]$, come [Sei74] p.289, otteniamo $f = \prod_{i=1}^{s} p_i$ dove i p_i sono irriducibili.
Per la Proposizione 2.9 allora possiamo calcolare la parte reale di p_i per

ogni $i = 1, \ldots, s$. Usando il Lemma 1.30 e la Proposizione 2.7 abbiamo dunque

$$\sqrt[re]{(f)} = \left(\prod_{p_i \text{ reale}} p_i \right).$$

□

Il problema di questo teorema e del calcolo del radicale reale in generale è che le due ipotesi assunte sono molto forti. Non sempre è possibile trovare due algoritmi, uno di valutazione e uno di fattorizzazione, e anche se troviamo due algoritmi teorici non è detto che siano implementabili.
Per questo da qui in poi specializzaremo la nostra trattazione ai polinomi a coefficienti in $\mathbb{Q}$. Nella seguente sezione mostreremo due algoritmi per decidere se polinomio irriducibile è reale e un algoritmo effettivo per il calcolo della parte reale.

2.2 Due algoritmi di Decisione

Vogliamo mostrare, per $F = \mathbb{Q}$ o $F = \mathbb{Q}(T_1, \ldots, T_m)$, che è possibile decidere se un polinomio univato è reale, ma è bene trattare i due campi separatamente. Se per $\mathbb{Q}$ infatti è abbastanza semplice trovare un algoritmo efficace, per gli altri $F = \mathbb{Q}(T_1, \ldots, T_m)$ è più laborioso.

2.2.1 Metodo di Sturm

Per decidere se un polinomio irriducibile $p \in \mathbb{Q}[X]$ è reale o meno basta 'contarne 'le radici reali. Ricordiamo che, grazie al teorema fondamentale dell'algebra, se il polinomio è di grado dispari ha almeno una radice in $\mathbb{R}$. Nel caso in cui il polinomio abbia grado pari useremo invece un metodo che impiega il criterio di Sturm, il quale trova il numero delle radici reali distinte in un intervallo $[a, b]$ con $a < b$. Per rendere più efficace il calcolo, visto che computazionalmente il metodo di Sturm non è molto accurato, utilizzeremo anche la continuità delle mappe polinomiali su $\mathbb{R}$.
Vale infatti che:

Teorema 2.12 (Valori intermedi)**.**

- *$p \in \mathbb{R}[X]$, $a, b \in \mathbb{R}$ con $a < b$, se $p(a)p(b) < 0$ allora esiste $x \in]a, b[$ tale che $p(x) = 0$.*
- *$p \in \mathbb{R}[X]$, $a, b \in \mathbb{R}$ con $a < b$, se la derivata p' è positiva su $]a, b[$ allora p è strettamente crescente su $[a, b]$.*

Definiamo la sequenza di Sturm:

Definizione 2.13. Siano $p, g \in \mathbb{R}[X]$. Definiamo *sequenza di Sturm* di p e g i polinomi $(p_0, \ldots, p_k)$ tali che

$$\begin{cases} p_0 = p,\ p_1 = p'g \\ p_i = p_{i-1}g_i - p_{i-2} \end{cases}$$

con $g_i \in \mathbb{R}[X]$ e $deg(p_i) < deg(p_{i-1})$ per $i = 1 \ldots k$ e $p_k = \gcd(p, p'g)$.
Presa inoltre $a \in \mathbb{R}$, elemento non radice di p, indichiamo con $v(p, g; a)$ il *numero di cambi di segno della sequenza di Sturm* di p e g valutata in a.

Teorema 2.14 (**Teorema di Sturm**). *Siano $p \in \mathbb{R}[X]$, $a, b \in \mathbb{R}$ con $a < b$ che non siano radici di p, allora il numero di radici di p in $]a, b[$ è uguale a $v(p, 1; b) - v(p, 1; a)$.*

Per sfruttare il teorema ci serve però un intervallo, il seguente lemma ci fornisce una possibile scelta:

Lemma 2.15. *Sia $f = a_0t^n + \cdots + a_{n-1}t + a_n \in \mathbb{R}[x]$ un polinomio di grado n. Allora tutte le radici reali di f sono nell'intervallo $[-M, M]$, dove M è detto $C(f)$* estremo di Cauchy *di f*

$$M \coloneqq \max\left\{1, \frac{|a_1|, \ldots, |a_n|}{|a_0|}\right\}.$$

Dimostrazione. Possiamo assumere senza perdita di generalità che a_0 sia 1. Consideriamo un elemento $\alpha \in \mathbb{R} \setminus \{0\}$ tale che $f(\alpha) = 0$ si ha che

$$\alpha = -(a_1 + a_2\alpha^{-1} + \cdots + a_n\alpha^{1-n}).$$

Ma allora

$$|\alpha| = |a_1 + a_2\alpha^{-1} + \cdots + a_n\alpha^{1-n}| \leq |a_1| + |a_2| \cdot |\alpha^{-1}| + \cdots + |a_n| \cdot |\alpha^{1-n}|,$$

e dunque $|\alpha| \leq 1$ o $|\alpha| \leq |a_1| + |a_2| + \cdots + |a_n|$. □

Ma allora si ha che:

Corollario 2.16. *Nelle notazioni del Lemma precedente, il numero di radici reali distinte di f è esattamente $v(f, 1; M) - v(f, 1; -M)$.*

Prima di dare quindi un algoritmo di decisione per i polinomi di $\mathbb{Q}[x]$ diamo un'ultima definizione:

Definizione 2.17. Sia $f = \sum_{i=0}^{n-1} a_{n-i}x^i + x^n$ un polinomio monico di $\mathbb{Q}[x]$ la *lunghezza di f* è

$$length(f) \coloneqq 1 + |a_1| + \cdots + |a_n|.$$

Si ha che allora, poiché $length(f) \geq M + 1$ (nella notazione del Lemma), le radici reali di f sono tutte nell'intervallo $[-length(f), length(f)]$.

Per decidere quindi se un polinomio irriducibile p è reale la stategia è sostanzialmente la seguente: se il polinomio ha grado dispari è certmente reale; altrimenti, a meno di dividere per il coefficiente direttivo, possiamo considerare il polinomio monico e calcolare $length(p)$, come visto sopra; provare ad usare poi il teorema dei valori del segno, ed eventualmente ricorrere a Sturm. Più precisamente, l'algoritmo è il seguente:

Algoritmo 2.1. ***IsReal_ Q***

Input*: p polinomio irriducibile su* $\mathbb{Q}[x]$
Output*: 0 se p non è reale e 1 se p è reale*

```
1  inizializzazione;
   // se il polinomio è un costante allora è reale
2  if deg p = 0 then
3  |  return 1;
4  end
5  if deg p = 1 mod 2 then
6  |  return 1;
7  else
8  |  L := length(p);
9  |  if (p(−L) · p(L) < 0) then
10 |  |  return 1;
11 |  else
12 |  |  n := v(p, 1; L) − v(p, 1; −L);
13 |  |  if n > 0 then
14 |  |  |  return 1;
15 |  |  else
16 |  |  |  return 0;
17 |  |  end
18 |  end
19 end
```

2.2.2 Metodo Zeng-Zeng

Per i polinomi a coefficienti in $\mathbb{Q}(T_1, \ldots, T_m)$ determinare se un polinomio è reale, oppure no, è un po' più complicato. Grazie al Corollario della Proposizione 2.9 sappiamo che quello che in realtà ci basta è un criterio per capire se un polinomio irriducibile $p \in \mathbb{Q}[T_1, \ldots, T_m, X]$, non costante rispetto alla variabile X, è indefinito.
Chiariamo che cose intendiamo con indefinito:

Definizione 2.18. Diremo che un polinomio non nullo $f \in \mathbb{Q}[x_1, \ldots, x_n]$ è *semidefinito positivo* se $f(a_1, \ldots, a_n) \geq 0$ per ogni $a = (a_1, \ldots, a_n) \in \mathbb{R}^n$. Diremo invece che è *indefinito* se esistono due punti $a, b \in \mathbb{R}^n$ tali che $f(a) \cdot f(b) < 0$ in $\mathbb{R}$.

Il teorema fondamentale su cui si basa questo metodo, per i cui dettagli e le dimostrazioni rimandiamo a [ZZ04], afferma che l'essere semidefinito positivo o meno di un polinomio dipende da un insieme minimale (vedremo poi in che senso) di zeri reali isolati di un polinomio univariato. Definiamo quindi, innanzi tutto, questo insieme:

Definizione 2.19. Sia $f \in \mathbb{Q}[X] \setminus \{0\}$ un polinomio. Allora un insieme finito $\Lambda \coloneqq \{a_1, \ldots, a_m\} \subseteq \mathbb{R}$ è detto *insieme isolante* di f se

1. $\forall a \in \Lambda$ vale $f(a) \neq 0$;

2. Se consideriamo gli a_i ordinati in maniera crescente, allora f ha al più una radice in ogni intervallo della forma (a_i, a_{i+1}) a per ognuna delle radici di f, però, esiste uno di questi intervalli che lo contiene.

3. Un insieme isolante è detto *minimale* se la sua cardinalità è esattamente uguale il numero delle radici distinte di f.

Se $\deg f = 0$ allora poniamo $\Lambda \coloneqq \{0\}$.

Vale dunque che

Teorema 2.20 (**Criterio di Zeng-Zeng**). *Sia f un polinomio in $\mathbb{Q}[T_1, \ldots, T_m, X]$ con $n \geq 2$. Allora è possibile calcolare, effettivamente, un polinomio $p \in \mathbb{Q}[X]$ tale che preso un qualsiasi insieme isolante Λ di p, allora*

$$f(T_1, \ldots, T_m, X) \geq 0 \text{ in } \mathbb{R}^{m+1} \iff f(T_1, \ldots, T_m, a) \geq 0 \text{ per ogni } a \in \Lambda.$$

Quello di cui perciò abbiamo bisogno per costruire un algoritmo è come prima cosa una funzione che trovi un insieme isolante per polinomi in $\mathbb{Q}[X]$. A questo scopo introduciamo i *Polinomi di Bernstein*, che sono un base, alternativa a quella canonica, per i polinomi di grado minore o uguale a n, $\mathbb{Q}[X]_{\leq n}$ per ogni $n \in \mathbb{N}$.

Definizione 2.21. I *polinomi di Bernstein di grado n sull'intervallo* (l, r) sono

$$Bern_{n,i}(l, r)(x) = \binom{n}{i} \frac{(x-l)^i \cdot (r-x)^{n-i}}{(r-l)^n}$$

con $i = 1 \ldots n$.

Non è nostro interesse studiare questi polinomi, diamo per assunto quindi che per ogni $f \in \mathbb{R}[X]$ di grado al più n sia possibile computare il vettore delle coordinate $b = (b_1 \dots b_n)$ di f nella base $\{Bern_{n,i}(l,r) : i = 1 \dots n\}$, per (l,r) fissati; i b_i sono anche detti *coefficienti di Bernstein.* Per i dettagli e le dimostrazioni relativi a questi polinomi rimandiamo al capitolo 10.2 di [BPR06].
L'utilità di questi polinomi è legata alla seguente proprietà:

Proposizione 2.22. *Sia $f \in \mathbb{R}[X]$ un polinomio di grando n e b il vettore dei suoi coefficienti di Bernstein su (l,r). Detto* $\mathrm{num}(f,(l,r))$ *il numero delle radici di f in (l,r) contate con molteplicità e* $\mathrm{Var}(b)$ *il numero di cambi di segno in b, allora*

- $\mathrm{Var}(b) \geq \mathrm{num}(f,(l,r))$
- $\mathrm{Var}(b) - \mathrm{num}(f,(l,r))$ *è pari.*

Da cui si ha anche

Corollario 2.23. *Se* $\mathrm{Var}(b) = 1$ *f ha esattamente una radice in (l,r).*

Alla luce di ciò possiamo descrivere un algoritmo per isolare le radici reali di un polinomio $\mathbb{Q}[x]$, l'idea è quella di rimpicciolire via via gli intervalli (a,b), fino che contengano una sola radice.

Algoritmo 2.2. ***RealRootIsolating***

Input: *f polinomio in $\mathbb{Q}[x]$*
Output: *Un insieme L di intervalli (a, b) con $a, b \in \mathbb{Q}$ tali che ognuno contiene esattamente una radice di f*

inizializzazione;
$M \coloneqq length(g)$;
calcola $b(g, -M, M)$ il vettore dei coefficienti di Bernstein su $(-M, M)$;
$POS \coloneqq \{b(g, -M, M)\}$ *e* $L \coloneqq \varnothing$;
while $POS \neq \varnothing$ **do**
  seleziona un elemento $b(g, l, r) \in POS$;
  if $Var(b(g, l, r)) > 1$ **then**
    $L \leftarrow L \cup \{(l, r)\}$;
  end
  calcola[a] $b(g, l, m)$ *e* $b(g, m, r)$ *per* $m = (l + r)/2$;
  if $g(m) = 0$ **then**
    trova $\epsilon > 0$ tale che $(m - \varepsilon, m + \varepsilon)$ contenga una sola radice;
    $L \leftarrow L \cup \{(m - \epsilon, m + \varepsilon)\}$;
    calcola $b(g, l, m - \varepsilon)$ e $b(g, m + \varepsilon, r)$;
    $POS \leftarrow POS \cup \{b(g, l, m - \varepsilon), b(g, m + \varepsilon, r)\}$;
  else
    $POS \leftarrow POS \cup \{b(g, l, m), b(g, m, r)\}$;
  end
end

[a] vedi, ad esempio, Algoritmo 10.2 a pag.365 di [BPR06]

La corretta e la terminazione di **RealRootIsolating** derivano dal Corollario 2.23 e dal seguente lemma:

Lemma. *Siano b, b_1, b_2 i vettori dei coefficienti di Bernstein di un polinomio $f \in \mathbb{R}[X]$ rispettivamente su $(l, r), (l, m)$ e (m, r). Se $l < m < r$, allora*

$$Var(b_1) + Var(b_2) \leq Var(b).$$

Inoltre, se $f(m) \neq 0$ allora $Var(b) - Var(b_2) - Var(b_1)$ è pari.

Possiamo concentrarci ora sulla procedura principale, quello che dobbiamo fare in sostanza è costruire un polinomio a coefficienti razionali a partire dal $p \in \mathbb{Q}(T_1, \ldots, T_m)[X]$ in modo da poter applicare il *Criterio di Zeng-Zeng*.

Se f è un polinomio di $\mathbb{Q}[T_1, \ldots, T_m, X]$ e indichiamo con

$$\mathcal{S}(f, X) \coloneqq \{b \in \mathbb{R} \mid \exists a_1, \ldots, a_m \in \mathbb{R} \ : \ f(a_1, \ldots, a_m, b) < 0\},$$

allora $\mathcal{S}(f, X)$ è unione di intervalli aperti disgiunti se f è indefinito. Vale inoltre che se $\mathcal{S}(f, X) \neq \mathbb{R}$ allora esiste almeno un estremo di a di questi intervalli che è diverso da più e meno infinito. Si ha che è possibile trovare effettivamente un sottoinsieme finito di $\mathbb{R}$ che contiene tutti questi punti, in particolare vale che:

Teorema 2.24. *Sia $f \in \mathbb{Q}[T_1, \ldots, T_m, X] \setminus 0$. Allora può essere computato effettivamente un polinomio $p(X)$ tale che $p(a) = 0$ per ogni punto estremo finito di $\mathcal{S}(f, X)$.*

Dimostrazione. Dimostrazione Teorema 2 pag.92 [ZZ04]. □

Possiamo quindi dimostrare il teorema di Zeng-Zeng:

Dimostrazione Teorema 2.20. Per il Teorema precedente esiste un polinomio $p(X)$ tale che $p(a) = 0$ per ogni punto estremo finito di $\mathcal{S}(f, X)$; sia adesso Λ un suo insieme isolante (che sappiamo calcolare).
Chiaramente f non è semidefinito positivo se $f(T_1, \ldots, T_m, a)$ non è semidefinito positivo per ogni $a \in \Lambda$. Assumiamo ora che $f(T_1, \ldots, T_m, X)$ non sia semidefinito positivo. Allora $\mathcal{S}(f, X) \neq \varnothing$. Se $\mathcal{S}(f, X) = \mathbb{R}$, si ha che $f(T_1, \ldots, T_m, a)$ non è semidefinito positivo per ogni $a \in \Lambda$. Se $\mathcal{S}(f, X) \neq \mathbb{R}$, allora esiste almeno un estremo finito in $\mathcal{S}(f, X)$ e per costruzione $p(a) = 0$. Allora esistono due punti $b, c \in \Lambda$ tali che $b < c$ e (b, c) contiene solamente il punto a di $\mathcal{S}(f, X)$, ma in tal modo si ha che o $b \in \mathcal{S}(f, X)$ o $c \in \mathcal{S}(f, X)$, e dunque o $f(T_1, \ldots, T_m, b)$ o $f(T_1, \ldots, T_m, c)$ non è definito positivo. □

Osservazione $(*)$. Ricordiamo che un polinomio in $\mathbb{R}[x]$ è semidefinito positivo su $\mathbb{R}$ se ha leading coefficient positivo e se g, il polinomio ottenuto da f cancellando i fattori irriducibili pari, non ha radici reali.

L'algoritmo per decidere se un polinomio è semidefinito è dunque il seguente:

Algoritmo 2.3. ***Decision***

Input: *f polinomio in $\mathbb{Q}[T_1, \ldots, T_m, X]$, con leading coefficient positivo*

Output: *1 se f è semidefinita positiva altrimenti 0*

```
1  inizializzazione;
2  if n=1 then
3  |  ricorriamo all'Osservazione (*);
4  end
5  if n>1 then
6  |  calcola il polinomio p(X) del Teorema 2.24
   |  Λ := RealRootIsolating(p) ;
7  |  while Λ ≠ ∅ e controllo=1 do
8  |  |  seleziona a ∈ Λ;
9  |  |  controllo = Decision(f(T_1, ..., T_m, a));
10 |  end
11 |  if controllo=1 then
12 |  |  return 1;
13 |  else
14 |  |  return 0;
15 |  end
16 end
```

2.3 Calcolo della parte reale di un polinomio univariato

Gli algoritmi appena illustrati oltre che a capire se un polinomio irriducibile è reale permettono di calcolare la parte reale di un polinomio, come abbiamo visto dal Teorema 2.11. Vale allora che

Teorema 2.25. *Sia $f \in F[x]$ polinomio con $F = \mathbb{Q}(T_1, \ldots, T_m)$ o $F = \mathbb{Q}$. Allora esiste un algoritmo per calcolare la parte reale di f su $F[X]$.*

La dimostrazione è sostanzialmente la stessa. Riassumiamo dunque, usando lo psedocodice, l'algoritmo. Per chiarezza usiamo due procedure: una che preso in input un polinomi irriducibile in $F[X]$ determina se è reale o meno, discriminando in base al tipo di campo quale delle due funzioni di decisione utilizzare (nel caso si debba utilizzare la funzione ***Decision*** è necessario prima fare un oppurtuna cambio di anello, la funzione infatti prende in input polinomi in $\mathbb{Q}[T_1, \ldots, T_m, X]$); l'altra procedura invece prende in input un polinomio $f \in F[X]$, calcola i fattori irriducibili e calcola la parte reale di f come prodotto delle loro parti reali.

Algoritmo 2.4. ***IrridRealPart***

Input: *p polinomio irriducibile su* $F[X]$
Output: *0 se p non è reale e 1 se p è reale*

inizializzazione;
`// se il polinomio è un costante nella variabile X allora è reale`
if $\deg p = 0$ **then**
  return *1;*
end
`// distinguo se usare Sturm oppure Decision per decidere se il polinomio è reale o meno, discriminando in merito al campo base`
if $F = \mathbb{Q}$ **then**
  return ***IsReal_ Q***(p)*;*
else
  if $\deg p = 1 \mod 2$ **then**
    return *1;*
  else
    return $1-$***Decision***(p)*;*
  end
end

Algoritmo 2.5. ***RealPart***

Input: *f polinomio in* $F[x]$
Output: *g parte reale di f*

inizializzazione;
`// calcola i fattori irriducibili squarefree di f`
$J \coloneqq \{p_i\}$ *;*
`// per ognuno dei fattori irriducibili determino se è reale ed in tal caso lo impongo fattore della parte reale di f`
while $J \neq \varnothing$ **do**
  if ***IrridRealPart***(p_i) **then**
    $g \leftarrow g \cdot p_i$*;*
  end
end
return *g;*

Capitolo 3

Calcolo del radicale reale

Il nostro scopo è dimostrare che è possibile trovare un algoritmo per calcore il radicale reale. Seguendo quanto fatto nel capitolo precedente ci limeteremo a parlare di polinomi in $F[X_1, \ldots, X_n]$, con $F = \mathbb{Q}$ o $F = \mathbb{Q}(T_1, \ldots, T_m)$. Abbiamo visto infatti che in questo caso siamo in grado di costruire la parte reale di polinomi univariati. Vogliamo mostrare adesso che grazie alla proposizione 2.25, è possibile ridurci a trattare questi polinomi per calcolare il radicale reale di un ideale qualsiasi $I \subseteq F[X_1, \ldots, X_n]$.

Mostreremo una possibile costruzione dell'algoritmo nello schema che segue. Partendo dal fatto che siamo in grado di trovare la parte reale di un polinomio, prenderemo un ideale qualsiasi $I \subseteq F[X_1, \ldots, X_n]$ e calcoleremo il radicale reale come intersezione di due insiemi particolari. In verità noi supporremo l'ideale in input radicale, nel caso infatti non lo sia possiamo, con una semplice operazione, renderlo tale e ci basta ora osservare che $\sqrt[re]{\sqrt{I}} = \sqrt[re]{I}$. Consideriamo la seguente scrittura della decomposizione in primi minimale del radicale reale di I

$$\sqrt[re]{I} = \bigcap_{i=1}^{s} P_i \cap \bigcap_{j=1}^{r} M_j$$

con P_i, M_j primi reali e $\dim P_i > 0$ e $\dim M_j = 0$. Gli insiemi in questione sono esattamente le intersezioni *zero-dimensionale* $I_0 = \cap_j M_j$ e *non zero-dimensionale* $I_1 = \cap_i P_i$, che troveremo appunto separatamente. Per quanto riguarda I_0 forniremo due possibili approcci che ricorrono uno alla decomposizione equidimensionale e al calcolo dei luoghi singolari l'altro ai punti isolati della varietà associata, mentre per calcolare I_1 sfrutteremo l'operatore radicale reale commuta con l'immersione nell'anello delle frazioni e ci ridurremo ad ideali di dimensione zero. Sappiamo appunto che gli ideali zero-dimensionali possono essere facilmente messi in posizione generale, ed in tal caso calcolare il radicale reale è equivalente a calcolare la parte reale

di un polinomio univariato. Discuteremo perciò prima il caso di un ideale di dimensione zero (caso base) e solo a quel punto il caso generale.

Riassumiamo tramite una procedura ricorsiva l'algoritmo che proponiamo:

Algoritmo 3.1. ***RealRad***
Input: $I \subseteq A$ *ideale*
Output: $J = \sqrt[re]{I}$
1 *inizializzazione;*
2 **if** $I = A$ **then**
3 | **return** (1)*;*
4 **end**
5 **if** $\dim I = 0$ **then**
6 | **return** ***RealRadZero***(I)*;*
7 **end**
8 $I_1 \leftarrow$ ***NonZeroIntersection***(I)*;*
9 $I_0 \leftarrow$ ***ZeroIntersection***(I)*;*
10 $J \leftarrow I_1 \cap I_0$*;*
11 **return** J*;*

3.1 Ideali zero-dimensionali

Il primo passo è il calcolo del radicale radicale per una particolare classe di ideali che saranno la base della ricorsione: quelli di dimensione zero. Come anticipato quello che vogliamo fare è in sostanza cercare di ridurci a calcolare la parte reale di un polinomio univariato. Per far ciò sfrutteremo lo Shape Lemma (Teorema 1.54) e l'unicità delle basi di Gröbner ridotte (Teorema 1.51).

Consideriamo un ideale zero-dimensionale $I \subseteq F[X_1, \ldots, X_n]$, dove F è $\mathbb{Q}$ o $\mathbb{Q}(T_1, \ldots, T_m)$. Abbiamo già detto che $\sqrt[re]{\sqrt{I}} = \sqrt[re]{I}$ e possiamo perciò supporre I radicale (eventualmente c'è da calcolare $\sqrt{I}$). Allora, abbiamo visto nella sezione sugli ideali zero-dimensionali, per quasi tutti i vettori $c = (c_2, \ldots, c_n) \in F^{n-1}$, ossia tutti eccetto un'unione finita di sottospazi lineari affini di F^{n-1}, l'automorfismo

$$\begin{array}{rccc} \varphi_c\colon & F[X_1, \ldots, X_n] & \longrightarrow & F[X_1, \ldots, X_n] \\ & f(X_1, \ldots, X_n) & \longmapsto & f(X_1 + \sum_{i=2}^{n} c_i X_i, X_2, \ldots, X_n) \end{array} \tag{3.1}$$

porta $\varphi_c(I)$ in posizione generale rispetto a X_1. Altrimenti è possibile trovare in maniera deterministica un vettore opportuno, anche se si verifica non essere necessario da un punto di vista pratico.
Lo Shape Lemma ci garantisce che la base di Gröbner ridotta G di $\varphi_c(I)$

rispetto l'ordinamento lessicografico $X_1 < \cdots < X_n$, che è unica, ha la forma

$$G = \{g_1(X_1),\ X_j - g_j(X_1)\ :\ j = 2, \ldots, n\}$$

con $g_1(X_1)$ un polinomio squarefree.

Esempio 3.1. Consideriamo in $\mathbb{Q}[x, y, z]$ gli ideali zero dimensionali $I_1 = (x - 1, y^2 - y, z - y)$, $I_2 = (xyz - 1, z - y, x - 3)$, $I_3 = (x, y, z^2 + 1)$ nessuno di questi ideali è in posizione generale. Se prendiamo il cambio di coordinate $\varphi(x, y, z) = (z + x/5, y, z)$ allora abbiamo che $\varphi(I_1) = (x^2 + 3x - 4, y + x/5 - 1/5, z + x/5 - 1/5)$, $\varphi(I_3) = (x^2 + 25, y, z + x/5)$, $\varphi(I_2) = (x^2 + 6x + 2/3, y + x/5 - 3/5, z + x/5 - 3/5)$ sono in posizione generale.

Se $g_1 = \prod p_i$, scomposizione in fattori primi su $F[X_1]$, allora

$$M_i \coloneqq (p_i(X_1),\ X_j - g_j(X_1)\ :\ j = 2, \ldots, n)$$

sono i massimali nella decomposizione primaria $\varphi_c(I) = \cap_i M_i$. In particolare abbiamo che $F[X_1, \ldots, X_n]/M_i \simeq F[X]/(p_i(X))$ tramite la mappa

$$f(X_1, \ldots, X_n) + M_i \mapsto f(X, g_2(X), \ldots, g_n(X)) + (p_i(X)).$$

Queste semplici osservazioni ci portano a una condizione necessaria e sufficiente per gli ideali massimali che in realtà, come nel caso della dimostrazione del Nullstellensatz, è il passo base per studiare gli ideali generici.

Proposizione 3.2. *M_i è reale come ideale di $F[X_1, \ldots, X_n]$ se e solo se $(p_i(X))$ è reale come ideale di $F[X]$.*

Corollario 3.3.

$$\sqrt[re]{\varphi_c(I)} = \bigcap_{M_i\ reale} M_i\ =\ (\widetilde{g}_1(X_1),\ X_j - g_j(X_1)\ :\ j = 2, \ldots, n)$$

dove $\widetilde{g}_1(X_1)$ è la parte reale di $g_1(X_1) \in F[X_1]$

Ma da questo, sfruttando che φ_c è un automorfismo, otteniamo

Teorema 3.4.

$$\sqrt[re]{I} = \varphi_c^{-1}\left(\sqrt[re]{\varphi_c(I)}\right).$$

I passaggi logici di questa sezione non solo ci mostrano che è possibile, riducendoci al caso univariato, calcolare il radicale reale per gli ideali zero dimensionali, ma ci danno anche un metodo.
A conclusione di questo paragrafo espliciteremo l'algoritmo, riprendiamo adesso invece l'ultimo esempio:

Esempio 3.5.

1. Sia $I_1 = (x-1, y^2-y, z-y)$. Abbiamo visto che esiste un cambio di coordinate tale che $\varphi(I_1) = (x^2+3x-4, y+x/5-1/5, z+x/5-1/5)$, ma x^2+3x-4 è un polinomio reale (ha una radice reale) e dunque $\sqrt[re]{\varphi(I_1)} = \varphi(I_1)$, applicando l'inversa $\sqrt[re]{I_1} = I_1$.

2. Sia $I_2 = (xyz-1, z-y, x-3)$, operando come sopra e osservando che $x^2+6x+2/3$ è reale si ottiene $\sqrt[re]{I_2} = I_2$.

3. $I_3 = (x, y, z^2+1)$, dopo il cambio di coordinate il polinomio univariato è x^2+25, chiaramente $\sqrt[re]{(x^2+25)} = (1)$. Così si ottiene che $\sqrt[re]{I_3} = \mathbb{Q}[x, y, z]$.

L'idea per la procedura che vorremmo realizzare è la seguente: se I non è radicale calcoliamo il radicale; controlliamo se è in posizione generale rispetto l'ultima variabile, altrimenti facciamo un cambio di coordinate; prendiamo dunque il polinomio univariato e con ***RealPart*** calcoliamo la parte reale ed eventualmente torniamo indietro.
Per formalizzare quanto appena detto ci serve innanzi tutto un algoritmo per determinare se I è in posizione generale.
Quello proposto è il più facile possibile, prende un ideale radicale di dimensione zero, calcola la base di Gröbner ridotta e controlla in prima istanza, usando le molteplicità del polinomio il cui leading term ha grado più piccolo possibile, che l'ideale sia radicale. Se poi è possibile ridurre tutti gli f_i, elementi della base di Gröbner ridotta, tramite potenze di opportuni polinomi di primo grado rispettivamente nelle x_i l'ideale è in posizione generale, altrimenti non lo è.
Nota: supponiamo che l'ordinamento monomiale sia già quello giusto.

Algoritmo 3.2. ***GeneralPosition***

Input: *$I \subseteq F[X_1, \ldots, X_n]$ radicale di dimensione zero con $\{f_1, \ldots, f_n\}$ base di groebner ridotta*

Output: *1 se I è in posizione generale, altrimenti 0*

```
1  inizializzazione;
2  L := {fattori di f_1(X_1)};
3  J ← (L);
4  controllo dimensione;
5  i ← n  while i > 1 do
6  |  i − −;
7  |  m ← deg f_i;
8  |  b ← il coefficienti x_i^{m−1} come polinomio in x_i;
9  |  q ← x_i + b/m;
10 |  if q^m ≡ f  mod J then
11 |  |  J ← (J, q) ;
12 |  else
13 |  |  return 0;
14 |  end
15 end
16 return 1 ;
```

Abbiamo dimostrato che se l'ideale è in posizione generale $I = (X_i - f_i(X_1), f_1(X_1))$, detta $\widetilde{f}(X_1)$ la parte reale di f_1,

$$\sqrt[re]{I} = (X_i - f_i(X_1), \widetilde{f}(X_1)).$$

Se non lo è, con un facile cambio di coordinate, possiamo portarlo in posizione generale, calcolare $\widetilde{f}(X_1)$, aggiungerla ai generatori e riportarlo nelle coordinate originali. L'algoritmo che segue fa esattamente ciò tramite una procedura ricorsiva:

Algoritmo 3.3. ***RealRadZero***

Input: *$I \subseteq F[X_1, \ldots, X_n]$ ideale radicale di dimensione zero*

Output: *J radicale reale di I*

```
1  inizializzazione;
2  if GeneralPosition(I) = 1 then
3  |  g ← RealPart(f_1(X_1));
4  |  J ← (I, g);
5  end
6  while notloop do
7  |  cambio coordinate random J ← φ_c(I);
8  |  J ← RealRadZero(J);
9  |  return φ_c^{−1}(J);
10 end
```

3.2 Caso generale

Fino ad ora abbiamo dimostrato che se siamo in grado di fattorizzare polinomi in una solo variabile e determinare se siano o meno definiti, possiamo in maniera molto semplice, al più facendo un cambio di coordinate, calcolare il radicale reale di ideali di dimensione zero e abbiamo mostrato anche che non bisogna far altro che ridurci al calcolo della parte reale di un polinomio univariato. Vogliamo fare la stessa cosa nel caso di un ideale $I \subseteq F[X_1, \ldots, X_n]$.
Vedremo che però non è così elementare, poiché nel tentare di 'abbassare' la dimensione dell'ideale, per poter usare le tecniche suddette, si rischia di banalizzare alcune componenti del radicale reale. Per ovviare a tale problema ricorreremo a criteri che richiamano la natura anche geometrica dell'oggetto che stiamo studiando.

L'idea che svilupperemo per dimostrare l'esistenza di un algoritmo è quella di ridurci in maniera ricorsiva al caso zero-dimensionale (che in sostanza è ridursi al calcolo della parte reale di un polinomio univariato). Per far ciò useremo due semplici osservazioni: la prima è che l'operatore radicale reale commuta con l'immersione nell'anello delle frazioni, la seconda è che l'intersezione delle componenti della decomposizione in primi del radicale sono fortemente legate con le singolarità e i punti isolati della varietà associata all'ideale.

Vale dunque che:

Proposizione 3.6. *Sia $I \subseteq F[X_1, \ldots, X_n]$ un ideale e sia $\sqrt[re]{I} = \bigcap_{i=1}^{s} P_i \cap \bigcap_{j=1}^{t} M_j$ la decomposizione in primi di $\sqrt[re]{I}$ dove P_i, M_j reali primi*[1] *e tali che $\dim P_i > 0$ e $\dim M_j = 0$.*
Allora se $S_h := F[X_h] \setminus 0$ abbiamo

$$\bigcap_{h=1}^{n} \left(\sqrt[re]{{S_h}^{-1} I} \cap F[X_1, \ldots, X_n] \right) = \bigcap_{i=1}^{s} P_i. \tag{3.2}$$

Con questa operazione, in un certo senso, volgiamo la nostra attenzione verso i primi su $\sqrt[re]{I}$ di cui non sappiamo calcore il radicale reale, immergendoli però in un algebra in cui è dipendono da un variabile in meno. Diventa perciò chiaro come tramite una procedura ricorsiva sia possibile riportarci al caso base.

Dimostrazione. Innanzi tutto osserviamo che

- se $\dim P_i > 0 \Rightarrow \exists h$ tale che $({S_h}^{-1} P_i)^c = P_i$

[1] ricorda Proposizione 1.33.

- se $\dim M_j = 0 \Rightarrow \ \forall h \ (S_h{}^{-1}M_j)^c = F[X_1, \ldots, X_n]$

Infatti, sia P_i un primo reale di dimensione positiva supponiamo per assurdo che non esista h tale che $(S_h{}^{-1}P_i)^c = P_i$, allora avremmo che P_i contiene un polinomio univariato per ogni X_h, il tal caso però avrebbe dimensione zero.
Sia invece M_j un primo reale di dimensione zero, supponiamo ad esempio, senza perdita di generalità, che $M_j \cap S_1 \neq 0$. Allora esisterebbe un polinomio $p(X_1) \in F[X_1]$ tale che $(M_j, p(X_1))$ sarebbe un ideale proprio di $F[X_1, \ldots, X_n]/M_j$, che è un campo.
Combinando questa osservazione con il Lemma 1.30 otteniamo:

$$\begin{aligned}\bigcap_{h=1}^{n}\left(\sqrt[re]{S_h{}^{-1}I} \cap F[X_1, \ldots, X_n]\right) &= \bigcap_{h=1}^{n} S_h{}^{-1}(\sqrt[re]{I}) \\ &= \bigcap_{i}\bigcap_{h=1}^{n} S_h{}^{-1}P_i \cap \bigcap_{j}\bigcap_{l=1}^{n} S_h{}^{-1}M_j \\ &= \bigcap_{i} P_i.\end{aligned}$$

□

Grazie alla Proposizione 3.6 pertanto, attivando come già detto il meccanismo ricorsivo, possiamo sfruttare il calcolo del radicale reale in $F(X_1)[X_2 \ldots X_n]$ e ottenere l'intersezione dei primi reali minimali di dimensione positiva su ogni ideale $I \subseteq F[X_1, \ldots, X_n]$.
Abbiamo visto dunque che preso un ideale qualsiasi (che possiamo supporre radicale): se l'ideale ha dimensione zero, a meno di poche operazioni, basta sostituire tra i generatori il polinomio univariato con la sua parte reale; se l'ideale ha dimensione positiva sfruttando la localizzazione possiamo, ragionando sulla dimensione delle immagini, trovare i primi su $\sqrt[re]{I}$ di dimensione positiva.
Se riuscissimo a identificare i primi di dimensione zero il nostro calcolo sarebbe completo.

Proponiamo qui un possibile schema ricorsivo, la cui terminazione è garantita grazie a semplici osservazioni sulla dimensione degli ideali coinvolti. Preso infatti I, la cui dimensione possiamo suppore essere strettamente positiva (altrimenti non c'è bisogno di ricorrere a questa funzione), ci basta calcolare $\sqrt[re]{S_h{}^{-1}I}$ otteniamo P poiché vale che per ognuno dei P_i $\exists h$ tale che la contrazione di $S_h{}^{-1}P_i \subseteq F(X_h)[X_1, \ldots, \check{X}_h, \ldots, X_n]$ è uguale a P_i .

Algoritmo 3.4. ***NonZeroIntersection***
Input*: $I \subset A$ ideale di dimensione strettamente positiva*
Output*: $I_1 = \cap_i P_i$*
1 *inizializzazione;*
2 **while** $h \leq n$ **do**
3 $\quad S_h = F[X_h] \setminus 0$*;*
4 $\quad I_1 \leftarrow I_1 \cap realrad({S_h}^{-1} I)$*;*
5 **end**
6 **return** I_1*;*

3.2.1 Componenti zero-dimensionali

L'equazione 3.2 mostra rendendo invertibili alcune variabili, sebbene ci permetta di calcolare $\cap_i P_i$, banalizza l'intersezione delle componenti zero-dimensionali del radicale. Attualmente non è noto se sia possibile trovare esplicitamente gli M_j a partire esclusivamente da I, tuttavia possiamo aggirare questo problema: presentiamo infatti due possibili metodi per determinare $\boldsymbol{ZeroIntersection}(I) = \cap_j M_j$, che è quello che strettamente ci serve per calcolare $\sqrt[re]{I}$, i quali si basano su proprietà più legate alla geometria del radicale reale.

Punti Reali Isolati

Il primo metodo si fonda sulla nozione di punto isolato, ne ricordiamo dunque la definizione e fissiamo la seguente notazione: parlando di un campo reale chiuso R lo intenderemo come spazio topologico e lo spazio affine R^n sarà inteso con la topologia prodotto.

In generale si ha che

Definizione 3.7. Un punto x appartenente ad un sottoinsieme Y di uno spazio topologico è un punto isolato di Y se esiste un intorno di x non contenente altri punti di Y.

Possiamo specializzare ai campi reali la definizione ricordando che ogni campo reale ammette almeno una chiusura:

Definizione 3.8. Sia k un campo reale con chiusura algebrica $\overline{k}$ e $I \subseteq k[X_1, \ldots, X_n]$ ideale. Un punto $x \in \mathcal{V}_{\overline{k}}(I)$ è detto punto reale (topologicamente) isolato se esiste una chiusura reale R tale che x è isolato nello spazio topologico $\mathcal{V}_R(I) \subseteq R^n$. Inoltre con $\mathcal{V}_{iso}(I)$ si indica l'insieme di tutti i punti isolati.

In altri termini

$$\mathcal{V}_{iso}(I) \coloneqq \bigcup_{R \text{ chiusura reale di } k} \{x \in \mathcal{V}_R(I) \mid x \text{ è un punto isolato}\}.$$

Definiamo poi

$$I^{iso} \coloneqq \mathcal{I}_k(\mathcal{V}_{iso}(I)) \subseteq k[X_1, \dots, X_n].$$

Osservazione. Se $k = \mathbb{Q}$ grazie a quanto visto nel primo capitolo $\mathcal{V}_{iso}(I)$ è il sottoinsieme di $\mathbb{R}^n$ che contiene tutti i punti isolati nel senso usuale del termine.

Quello che ci permetterà di calcolare quanto ci manca del radicale reale è il seguente criterio:

Proposizione 3.9. *Sia k campo reale e $I \subseteq k[X_1, \dots, X_n]$ un ideale. Allora valgono i seguenti fatti:*

i. $I^{iso} = k[X_1, \dots, X_n]$ oppure I^{iso} è un ideale reale zero-dimensionale.

ii. Se M è una componenti zero-dimensionale di $\sqrt[re]{I}$ allora $I^{iso} \subseteq M$ e dunque M è una componente anche si I^{iso}.

Dimostrazione. i. I^{iso} è reale, infatti per un certo $N \subseteq k[X_1, \dots, X_n]$

$$I^{iso} = \mathcal{I}_k(\mathcal{V}_{iso}(I)) = \mathcal{I}_k(\mathcal{V}_{re}(N)) \overset{Null}{=} \sqrt[re]{N}$$

Se $\dim I^{iso} \geq 1$ esisterà un punto isolato in qualche $\mathcal{V}_R(I)$ che è anche un punto regolare di $\mathcal{V}_{\overline{k}}(I^{iso})$ di dimensione locale al più uno. Il teorema delle funzioni implicite[2] su R mostra che x non può essere isolato sulla varietà più grande $\mathcal{V}_R(I)$.
ii. Sia M l'ideale nelle ipotesi, per il secondo punto della Proposizione 1.34 abbiamo che $\sqrt[re]{M} = M$. Inoltre grazie alla Proposizione 1.42 possiamo estendere M ad un massimale reale $\widetilde{M} \subseteq R_\alpha[X_1, \dots, X_n]$ per qualche $\alpha \in \chi(k)$. Il fatto che $\widetilde{M}$ sia reale da inoltre che esiste un punto $x \in R_\alpha^n$.
Sosteniamo adesso che $\widetilde{M}$ è una componente zero-dimensionale di $\sqrt[re]{IR_\alpha}$. Se non lo fosse infatti potremmo trovare un altro ideale primo $\widetilde{Q}$ tra $\sqrt[re]{IR_\alpha}$ e $\widetilde{M}$ tale che

$$\sqrt[re]{IR_\alpha} \subseteq \widetilde{Q} \subset \widetilde{M}.$$

Ma allora

$$I \subseteq \widetilde{Q} \cap k[X_1, \dots, X_n] =: Q \subset M$$

Inoltre essendo $\widetilde{Q}$ reale, per la scelta degli ordinamenti abbiamo $\sqrt[re]{Q} = Q$ e dunque $\sqrt[re]{I} \subseteq Q \subset M$: assurdo.
Perciò $\widetilde{M}$ è una componente zero-dimensionale di $\sqrt[re]{IR_\alpha}$, cosicché

$$\sqrt[re]{IR_\alpha} = \bigcap_i P_i \cap \widetilde{M}.$$

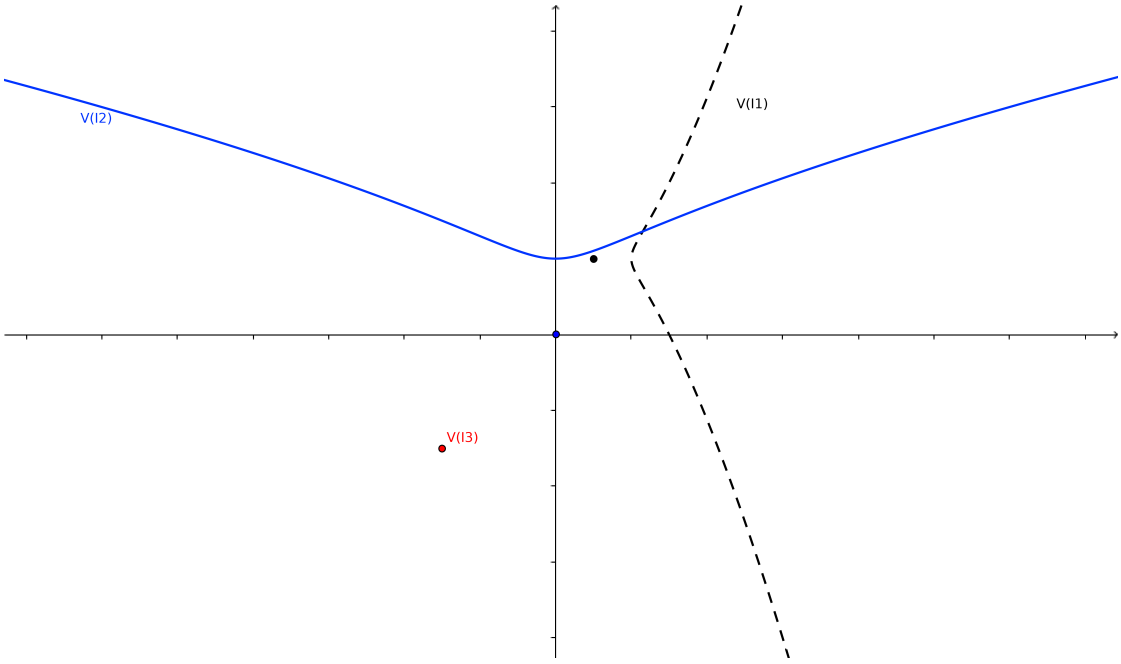
Sia adesso $f \in \bigcap_i P_i \setminus \widetilde{M}$, allora $\mathcal{V}_{R_\alpha}(I) \cap \{f \neq 0\} = \{x\}$, che equivale a dire che x è un punto isolato di $I^{iso} \subseteq M$. □

[2] [BCR98] 2.9.8

È evidente la rilevanza di questa proposizione per i nostri scopi: preso infatti un ideale I se $I^{iso} = \bigcap_i Q_i$, massimali di dimensione zero, abbiamo che ogni componente zero-dimensionale del radicale è uno dei Q_i.
Questo ci permette trovando un ideale $J \subseteq I^{iso}$ di dimensione zero, nella notazione della Proposizione 3.6, di scrivere $\sqrt[re]{I} = \bigcap_i P_i \cap \sqrt[re]{I+J}$.

È importante sottolineare che in generale ci sono più punti isolati che di quelli date dalle componenti del radicale reale.

Facciamo un esempio:



Esempio 3.10. Consideriamo l'ideale

$$\begin{aligned} I =& (x^3y^4 - x^5y + x^3y^3 - 4x^2y^4 - y^6 - 3x^5 + \\ & 4x4^y - 6x^3y^2 - 3x^2y^3 + 5xy^4 + 3y^5 + 12x^4 - \\ & 5x^3y + 23x^2y^2 + 5xy^3 + 4y^4 - 15x^3 - 6x^2y - 30xy^2 - \\ & 30y^3 + 18x^2 + 36y^2, x^4y^3 - x^6 - 2x^4y^2 - x^3y^3 - \\ & xy^5 + x^5 + 3x^3y^2 - 7x^2y^3 + 6xy^4 - 3y^5 + 7x^4 - 4x^3y + \\ & 17x^2y^2 + xy^3 + 18y^4 - 9x^3 - 12x^2y - 18xy^2 - 42y^3 + 18x^2 + 36y^2) \end{aligned}$$

che è l'intersezione degli ideali primi $I_1 = ((y-2)^2 - (x-1)^2 \cdot (x-2))$, $I_2 = (x^2 - y^2 \cdot (y-2))$ e $I_3 = (x+3, y+3)$. I primi due ideali rappresentano due cubiche irriducibili contenenti due punti isolati $(1,2)$ e $(0,0)$ rispettivamente. Si ha quindi che $\mathcal{V}_{\text{iso}}(I) = \{(-3,-3),(1,2),(0,0)\}$ e dunque che

$I^{\text{iso}} = (y^2 + 10x - 7y, xy + 8x - 5y, x^2 + 7x - 4y)$. Ma I è un ideale reale e ha un solo primo isolato $I_3 \supsetneq I^{\text{iso}}$.

Vogliamo provare che è possibile, a partire da un ideale $I \subseteq k[X_1, \ldots, X_n]$, costruire $J \subseteq I^{iso}$ di dimensione zero tramite delle proiezioni.
Vorremmo utilizzare qui la Proposizione 1.55, che fornisce un metodo per identificare i punti della varietà basandosi solo sulla proiezione su un sottospazio proprio. Dobbiamo mostrare, per usare questo fatto, che possiamo però restringerci al caso di ideali $I \subseteq k[X_1, \ldots, X_n]$ tali che $\dim I \leq n-2$. Usando il teorema delle funzioni implicite otteniamo che vale il seguente lemma:

Lemma 3.11. *Sia k un campo reale , $I = (f_1, \ldots, f_r) \subseteq k[X_1, \ldots, X_n]$ con $\dim I = n - 1$ e f la parte libera da quadrati di $\sum_{i=1}^{r} f_i^2$ in $k[X_1, \ldots, X_n]$. Se $R \subset \overline{k}$ è una chiusura reale di k allora ogni punto isolato di $\mathcal{V}_R(I)$ è uno zero dell'ideale*

$$L \coloneqq \left(I, \frac{\partial f}{\partial X_i} \colon i = 1, \ldots, n \right) k[X_1, \ldots, X_n],$$

dove $\dim L \leq n - 2$.

Si potrebbe riformulare il Lemma dicendo che $\mathcal{V}_{\text{iso}}(I) \subseteq \mathcal{V}(L)$: questo fatto per noi è importante perché prova che anche se l'ideale di partenza ha dimensione maggiore di $n-2$, per trovare i punti isolati possiamo comunque ridurci a a considerare un altro ideale L, al più $n-2$. Quindi possiamo in ogni caso trovare un sottoinsieme di variabili indipendenti modulo I (o L) e a meno di un cambio di variabili, per la proposizione 1.55, lavorare su un sottospazio di dimensione inferiore.
Grazie a queste osservazioni è possibile finalmente enunciare il teorema di esistenza dell'ideale J, che ricordiamo essere quello che ci serve per poter completare il calcolo del radicale reale:

Proposizione 3.12. *Sia k un campo reale, con $\bar{k}$ chiusura algebrica, e $I \subseteq k[X_1, \ldots, X_n]$. Allora è possibile costruire un ideale $J \subseteq k[X_1, \ldots, X_n]$ tale che*

i. $\dim J = 0$ *oppure* $J = k[X_1, \ldots, X_n]$,

ii. $J \subseteq I^{iso}$

Dimostrazione. Procederemo per induzione sul numero di variabili e poi una volta fissato n per induzione noetheriana su $k[X_1, \ldots, X_n]$. Se l'ideale ha dimensione zero la veridicità della tesi è evidente.
Chiamiamo $m \coloneqq \dim I$, per Lemma 3.11 $m \in \{1, \ldots, n-2\}$ e $n \geq 3$, possiamo supporre che $\{X_1, \ldots, X_m\}$ sia un sottoinsieme indipendente massimale di $\{X_1, \ldots, X_n\}$ modulo I. Per induzione assumiamo che l'asserto sia vero

per ogni $n' < n$ e per ideali di $k[X_1, \dots, X_n]$ propriamente contenuti in I. Scegliamo perciò $c = (c_{m+2}, \dots, c_n) \in k^{n-m-1}$ tale per cui possiamo applicare la Proposizione 1.55 a $\varphi_c(I)$: in questo modo otteniamo

$$s \in k[X_1, \dots, X_m] \setminus 0, r_{m+2} \dots r_n \in k[X_1, \dots, X_{m+1}]$$

e $\tilde{J} \in k[X_1, \dots, X_{m+1}]$ tali che per ogni $x \in \overline{k}^n$ con $s(x_1 \dots x_m) \neq 0$ allora $x \in \mathcal{V}_{\overline{k}}(I)$ sse

$$(x_1, \dots, x_{m+1}) \in \mathcal{V}_{\overline{k}}(\tilde{J}),\ x_i = \frac{r_i(x_1, \dots, x_{m+1})}{s(x_1 \dots x_m)} \text{ per } i = m+2 \dots n$$

Poiché $m + 1 < n$ per ipotesi induttiva esiste $J_1 \subseteq \tilde{J^{iso}}$ e $\dim J_1 = 0$ o $J_1 = k[X_1, \dots, X_{m+1}]$. Sia ora $J_2 \subseteq k[X_1, \dots, X_{m+1}]$ tale che $\mathcal{V}_{\overline{k}}(J_2) = \mathcal{V}_{\overline{k}}(J_2) \cap \{s \neq 0\}$.[3] Allora l'ideale

$$I_1 \coloneqq (J_2, s \cdot X_i - r_i \colon i = m+2 \dots n)k[X_1, \dots, X_n]$$

ha dimensione 0 o è tutto. Dal momento che I è un sottoideale proprio di (I, s) esiste un ideale $I_2 \subseteq k[X_1, \dots, X_n]$ con $\dim I_2 = 0$ o $I_2 = k[X_1, \dots, X_n]$ e $I_2 \in (\varphi_c(I), s)^{iso}$. E allora $\mathcal{V}_{iso}(I) \subseteq \mathcal{V}_{\overline{k}}(\varphi_c^{-1}(I_1 I_2))$ e $\dim \varphi_c^{-1}(I_1 I_2) \leq 0$, ossia $J = \varphi_c^{-1}(I_1 I_2)$ è l'ideale cercato. □

Possiamo quindi affermare che:

Teorema 3.13. *Sia $F = \mathbb{Q}(T_1, \dots, T_m)$ o $F = \mathbb{Q}$ e I un ideale di $F[X_1, \dots, X_n]$. Allora esiste un algoritmo per calcolare il radicale reale $\sqrt[re]{I}$.*

Dimostrazione 1. Procediamo per induzione su $m \coloneqq \dim I$.
Se $m = 0$ allora banalmente $\sqrt[re]{I} = \mathit{RealRadZero}(I)$.
Se $m > 0$, sia $\sqrt[re]{I} = \bigcap_{i=1}^{s} P_i \cap \bigcap_{j=1}^{t} M_j$ la decomposizione in primi minimale di I, dove P_i e M_j sono primi reali tali che $\dim P_i > 0$ e $\dim M_j = 0$. Sfruttando la proposizione precedente e la proposizione 3.9 possiamo costruire un ideale $J \in k[X_1, \dots, X_n]$ tale che $\dim J = 0$ o $J = (1)$ e $J \subseteq \bigcap_j M_j$. Allora

$$\sqrt[re]{I} \subseteq \bigcap_i P_i \cap \sqrt[re]{I + J} \subseteq \bigcap_i P_i \cap \bigcap_j M_j = \sqrt[re]{I},$$

cosicché $\sqrt[re]{I} = \bigcap_i P_i \cap \sqrt[re]{I + J}$. Per ipotesi induttiva infine possiamo sia costruire $\bigcap_i P_i$, usando la Proposizione 3.6, sia calcolare $\sqrt[re]{I + J}$, dato che $\dim(I + J) = 0$. □

Le proposizioni 3.12 e 1.55, danno tutti i dettagli e lo schema per un algoritmo per calcolare J, che chiameremo ***FoundIso***(I). Con questa notazione la funzione ***ZeroIntersection***(I) è semplicemente la seguente:

[3] Per esempio $J_2 = J_1^{ec}$ rispetto alla mappa $\Omega \colon k[X_1, \dots, X_{m+1}] \to k[X_1, \dots, X_{m+1}]_s$

Algoritmo 3.5. ***ZeroIntersection_Iso***

Input: $I \subset F[X_1, \ldots, X_n]$ *ideale di dimensione strettamente positiva*
Output: $I_0 = \cap_j Q_j$

```
1 inizializzazione;
2 J :=FoundIso(I);
3 I_0 ←RealRad(I, J);
4 return I_0;
```

Nell'impossibilità di computare effettivamente le componenti zero dimensionali abbiamo comunque esposto un metodo per trovarne l'intersezione che è quanto effettivamente serve. Nel seguito sfrutteremo invece, per il medesimo fine, la possibilità di decomporre equi-dimensionalmente l'ideale, dando così una seconda dimostrazione del Teorema 3.13.

Decomposizione Equi-dimensionale e punti singolari

Nel paragrafo precedente abbiamo proposto di calcolare $\sqrt[re]{I} = \bigcap_i P_i \cap \bigcap_j M_j$, trovando prima $\cap_i P_i$ col metodo discusso all'inizio del capitolo, poi costruendo un ideale J di dimensione al più zero in modo da poter scrivere $\sqrt[re]{I} = \bigcap_i P_i \cap \sqrt[re]{I + J}$. Presentiamo qui un altro possibile metodo per individuare $\bigcap_i M_i$. Invece di trattare $\mathcal{V}_R(I)$ in questo contesto è più appropriato concentrare la nostra attenzione su Spec $\left(F[X_1, \ldots, X_n]/\sqrt{I}\right)$, volgliamo infatti sfruttare alcuni risultati riguardanti gli ideali primi su I. Definiamo adesso i concetti di cui ci serviremo in questa sezione. Come prima cosa è utile dare un criterio per caratterizzare univocamente gli anelli regolari[4]:

Teorema 3.14 (**Criterio Jacobiano Generalizzato**). *Sia $I = (f_1, \ldots, f_m)$ un ideale di $k[X_1, \ldots, X_n]$ e Q un suo primo associato. Si poi $P \supset Q$ un ideale primo. Allora*

$$\mathrm{rk}\left(\frac{\partial f_i}{\partial X_j} \mod P\right) \leq \mathrm{ht}(Q),$$

e $k[X_1, \ldots, X_n]_P/I_P$ è anello locale regolare se e solo se

$$\mathrm{rk}\left(\frac{\partial f_i}{\partial X_j} \mod P\right) = \mathrm{ht}(Q),$$

Definiamo ora il luogo singolare di un anello A, che è lo strumento di cui ci avvarremo per caratterizzare una certa parte degli ideali primi zero-dimensionali sul radicale reale, che ricordiamo è quello che vogliamo calcolare.

[4]Vedi Definizione 1.56

Definizione 3.15. Sia A un anello, l'insieme

$$\mathrm{Sing}(A) \coloneqq \{P \in \mathrm{Spec}(A) \mid A_P \text{ non è regolare}\}$$

è detto il luogo singolare di A.
Inoltre $P \in \mathrm{Spec}(A)$ è detto singolare se e solo se $P \in \mathrm{Sing}(A)$.

Enunciamo ora un teorema che ci permette di determinare questo insieme come luogo di zeri di un certo ideale e che oltretutto ci dice anche che il luogo singolare di un anello è un chiuso della topologia di Zariski. Per fare ciò è necessario tuttavia definire il concetto di equidimensionale, che vedremo sarà anche fondamentale per la scrittura dell'algoritmo.

Definizione 3.16. Se A è un anello Noetheriano, I un suo ideale proprio è detto *equidimensionale* se tutti i suoi primi associati hanno la medesima dimensione.

Definizione 3.17. Sia I ideale di un anello Noetheriano, diremo che $I^{(t)}$, con $t = 0 \dots \dim I$ è la *componente di dimensione* t di I se $I^{(t)} = \bigcap Q$ con Q che varia tra i primi minimali di I di dimensione esattamente t.
Quando parleremo di *decomposizione equidimensionale* intenderemo la scrittura di I come intersezione delle sue componenti equidimensionali:

$$I = \bigcap_{t=0}^{d} I^{(t)}$$

con $d \coloneqq \dim I$.

Possiamo quindi enunciare il teorema:

Teorema 3.18. *Sia k un campo, $A = k[X_1, \dots, X_n]/(f_1, \dots, f_m)$ equidimensionale, con $\dim(A) = r$, e sia $J \subseteq A$ l'ideale generato dei minori $n-r$ della matrice Jacobiana $\mathcal{J}$. Allora*

$$\mathrm{Sing}(A) = \{Q \subset A \text{ primi } | J \subset Q\} = V(J)^5.$$

Esempio 3.19. Consideriamo l'ideale $I = (x^2 - y^2 \cdot (y+1)) \cap (xy - 1)$ il luogo singolare di $A \coloneqq \mathbb{Q}[x,y]/I$ è

$$\begin{aligned}\mathrm{Sing}(A) =& (xy^4 - x^3y + xy^3 - y^3 + x^2 - y^2,\\ & 4xy^3 - x^3 + 3xy^2 - 3y^2 - 2y,\\ & y^4 - 3x^2y + y^3 + 2x)\end{aligned}$$

[5] con la topologia dello spettro.

Torniamo al calcolo, come prima cosa facciamo la seguente osservazione: se $\sqrt{I} = \bigcap_i Q_i \cap \bigcap_j N_j$ è la decomposizione in primi con $\dim Q_i \geq 1$ e $\dim N_j = 0$, allora

$$\sqrt[re]{I} = \bigcap_i \sqrt[re]{Q_i} \cap \bigcap_j \sqrt[re]{N_j}.$$

Allora o $\sqrt[re]{N_j} = F[X_1, \ldots, X_n]$ o $\sqrt[re]{N_j} = N_j$[6] , da cui otteniamo che alcuni degli M_i sono componenti zero-dimensionali di $\sqrt{I}$.
Questi però non sono tutti, dobbiamo dunque elaborare un modo per trovare gli M_i mancanti. Se $\sqrt[re]{Q_i} = \bigcap_j Q_{ij} \cap \bigcap_k M_{ik}$ con $\dim Q_{ij} \geq 1$ e $\dim M_{ik} = 0$, allora gli altri M_i sono tra gli M_{ik}.

Quello che noi sosteniamo è che gli M_i che stiamo cercando sono quelli, tra gli M_{ik}, che occorrono come un ideale primo singolare di $F[X_1, \ldots, X_n]/\sqrt{I}$. In realtà questo infatti è solo un caso particolare del seguente lemma:

Lemma 3.20. *Sia $Q \subseteq F[X_1, \ldots, X_n]$ ideale primo e sia P un ideale primo minimale di $\sqrt[re]{Q}$ (e dunque P è -reale). Se $\dim P < \dim Q$ allora P/Q è ideale primo singolare di $F[X_1, \ldots, X_n]/Q$.*

Dimostrazione. Vedere [BN93] (Lemma 17, pag.15) e il Capito 7 [Pre84]. □

Si ha in verità nel nostro caso che quella del Lemma è un condizione necessaria e sufficiente. Abbiamo trovato dunque il modo di identificare, tramite ideali singolari, $\cap_i M_i$.

Osservazione. In questo capitolo stiamo trattando il caso in cui $\dim\sqrt{I} > 0$ e dunque presa una componente di dimensione almeno uno tra quelle del radicale reale di I, una qualsiasi dei primi zero-dimensionali minimali su essa soddisfano le ipotesi.

Riassumendo gli M_i compaiono tra:

a) le componenti zero-dimensionali di Spec $\left(F[X_1, \ldots, X_n]/\sqrt{I}\right)$, oppure

b) i punti singolari di una delle componenti di dimensione almeno uno di Spec $\left(F[X_1, \ldots, X_n]/\sqrt{I}\right)$.

Trovando quindi un ideale $J \supseteq I$ tale che Spec $\left(F[X_1, \ldots, X_n]/J\right)$ contiene tutti primi a) e b), nella notazione della Proposizione 3.6, avremmo

$$\sqrt[re]{I} = \bigcap_i P_i \cap \sqrt[re]{J}.$$

Dimostriamo che un ideale di tale sorta esiste e diamo anche un algoritmo per costruirlo:

[6] Visto che $\sqrt{I}$ è radicale gli N_j sono dei massimali.

1. calcolo del $\sqrt{I}$;
2. calcolo delle componenti equi-dimensionali $I^{(t)}$ con $t = 0, \ldots, \dim I$ di I: per far ciò useremo certi minori della matrice Jacobiana associata al radicale;
3. per $t \geq 1$ calcolo del luogo singolare $\mathrm{Sing}(A/I^{(t)}) = V(\widetilde{I^{(t)}})$, $\widetilde{I^{(t)}} \supseteq I^{(t)}$ usando il criterio Jacobiano (Teorema 3.14). Osserviamo che $\dim \widetilde{I^{(t)}} < \dim I^{(t)}$.

Otteniamo quindi:

Proposizione 3.21. *Sia I un ideale di $k[X_1, \ldots, X_n]$, con k campo reale. Allora è possibile costruire un ideale J tale che*

i. $\dim J < \dim I$, *se* $\dim I \geq 1$

ii. $\sqrt[re]{I} = \bigcap_i P_i \cap \sqrt[re]{J}$

Dimostrazione. Nella notazione sopra, basterà sceglire $J \coloneqq I^{(0)} \cap \widetilde{I^{(1)}} \cap \cdots \cap \widetilde{I^{(d)}}$ dove $d \coloneqq \dim I$. □

Esplicitiamo i dettagli dell'algoritmo. È utile osservare che nel calcolo della scomposizione equidimensionale del radicale, basato anch'esso sul criterio Jacobiano, viene determinata anche la dimensione dell'ideale.

Osservazione. Consideriamo l'algebra affine $A = F[X_1, \ldots, X_n]/I$ con $I = (f_1, \ldots, f_r)$. Siamo quindi nelle ipotesi del criterio Jacobiano per ideali primi (3.14) regolari e la proposizione 1.57. Allora, se $Q \supseteq I$ un primo qualsiasi, detta

$$\mathcal{J} \coloneqq \left(\frac{\partial f_j}{\partial X_i}\right)_{i=1,\ldots,n;i=1,\ldots,r}$$

la matrice Jacobiana di I e $\mathcal{J}(Q)$ l'immagine di $\mathcal{J}$ su $k(Q) = \mathrm{Q}\left(A/Q^e\right)$, dove $Q^e = Q/I$, vale che

Lemma. Q/I regolare in A se e solo se

$$\mathrm{rk}_{k(Q)}\, \mathcal{J}(Q) = \mathrm{ht}(IF[X_1, \ldots, X_n]_Q) = \mathrm{ht}(Q) - \dim A_{Q/I}.$$

Da qui in poi considereremo I ideale radicale nell'anello dei polinomi. Se ora Q è un primo minimale di I allora Q/I è un primo minimale dell'anello ridotto A, dunque $A_{Q/I}$ è un campo, in particolare è un anello regolare. Così

$$\mathrm{rk}_{k(Q)}\, \mathcal{J}(Q) = n - \dim Q. \tag{3.3}$$

Inoltre poniamo $I^{(t)} \coloneqq \bigcap Q$ con Q che varia tra i primi minimali di I di dimensione t, se non ci sono $I^{(t)} \coloneqq F[X_1, \ldots, X_n]$.
Chiaramente $I = \cap_{0 \leq t \leq d} I^{(t)}$, $d = \dim I$. Supponendo che $I = (f_1, \ldots, f_r)$, allora un primo minimale Q di dimensione t, se esiste,

$$\begin{cases} \operatorname{rk} \mathcal{J}(Q) = n - t \quad (3.3) \\ \operatorname{rk} \mathcal{J}(Q) \leq \min\{n, r\} \end{cases} \implies n - t \leq \min\{n, r\} \implies t \geq n - r$$

e quindi se $t < n - r$ $I^{(t)} = F[X_1, \ldots, X_n]$.
Perciò definiamo per ogni t l'ideale J_t:

- se $0 \leq n - t \leq \min\{n, r\}$

  $J_t \coloneqq$ ideale di $F[X_1, \ldots, X_n]$ generati dai minori$(n-t)\times(n-t)$ di $\mathcal{J}(f_1 \ldots f_r)$,

- se $\min\{n, r\} < n - t \leq n$ allora $J_t \coloneqq (0)$.

Lemma 3.22. *Se* $\min\{n, r\} \geq n - t$*, allora per ogni primo minimale* Q *di* I *vale che*

$$J_t \nsubseteq Q \iff \dim Q \leq t.$$

Dimostrazione. Sia Q come nelle ipotesi e supponiamo che $\dim Q \leq t$, l'equazione 3.3 ci dà direttamente che

$$\operatorname{rk}_{k(Q)} \mathcal{J}(Q) = n - \dim Q \geq n - t$$

che equivale a dire che i minori di dimensione fino $n - t$ del jacobiano sono invertibili in $k(Q)$ e dunque $J_t \nsubseteq Q$.
Viceversa se $\dim Q > t$ abbiamo che

$$\operatorname{rk}_{k(Q)} \mathcal{J}(Q) = n - \dim Q < n - t$$

e quindi ragionando nello stesso modo otteniamo che $J_t \subseteq Q$. □

In virtù di quanto appena detto, vale il seguente fatto che permette di individuare le componenti della scrittura equidimensionale tramite i J_t e quindi anche l'ideale J, il cui radicale reale ricordiamo è quello che stiamo cercando.

Proposizione 3.23. $I = (f_1, \ldots, f_r)$ *ideale radicale di* $F[X_1, \ldots, X_n]$ *e* $0 \leq t < n$*. Allora*

$$\begin{aligned} (I \colon J_t) &= I^{(t)} \cap I^{(t-1)} \cap \cdots \cap I^{(0)} \\ (I \colon (I \colon J_t)) &= I^{(d)} \cap I^{(d-1)} \cap \cdots \cap I^{(t+1)}. \end{aligned}$$

Dimostrazione. Se $\min\{n, r\} < n - t$ allore per definizione $J_t = (0)$, perciò $(I\colon J_t) = F[X_1, \ldots, X_n]$ $(I\colon (I\colon J_t)) = I$ (questo è conforme all'equazione 3.3).
Se invece $\min\{n, r\} \geq n - t$, grazie al lemma precedente $J_t \subseteq Q$ per ogni Q primo minimale di dimensione $f \in \{t+1, \ldots, d\}$, cosicché

$$J_t \subseteq I^{(d)} \cap I^{(d-1)} \cap \cdots \cap I^{(t+1)}$$

$$J_t \cdot \left(\bigcap_{f \leq t} I^{(f)} \right) \subseteq \bigcap_{f \leq d} I^{(f)} = I$$

e dunque $\bigcap_{f \leq t} I^{(f)} \subseteq (I\colon J_t)$.
Viceversa, se $g \in (I\colon J_t)$ allora $gJ_t \subseteq Q$ per tutti i primi minimali su I tali che $\dim Q \leq t$ (per $>$ lo sappiamo già). E dunque $g \in \bigcap_{f \leq t} I^{(f)}$, ossia $\bigcap_{f \leq t} I^{(f)} \supseteq (I\colon J_t)$.
Inoltre da quanto appena dimostrato otteniamo

$$(I\colon J_t) \cdot \left(\bigcap_{f > t} I^{(f)} \right) \subseteq (I\colon J_t) \cap \left(\bigcap_{f > t} I^{(f)} \right) = I.$$

Se $g \in (I\colon (I\colon J_t))$ allora $g(I\colon J_t) = g \cdot \bigcap_{f \leq t} I^{(f)}$, osservando che I è radicale e $(I\colon J_t) \nsubseteq Q$ per ogni primo minimale su I di dimensione al più $t+1$.

□

La Proposizione 3.23 permette di determinare ricorsivamente l'ideale $I^{(e)}$ tramite il calcolo di $I^{(0)}, \ldots, I^{(t-1)}$ e $\widehat{I^{(t)}} := \bigcap_{f \geq t} I^{(f)}$. Usando J_0 si ottiene $I^{(0)}, \widehat{I^{(1)}}$. Se $I^{(0)}, \ldots, I^{(t-1)}$ e $\widehat{I^{(t)}}$ sono stati calcolati, tramite l'ideale Jacobiano J_t di $\widehat{I^{(t)}}$ si può costruire $I^{(t)}$ e $\widehat{I^{(t+1)}}$. Il calcolo termina dal momento in cui si trova $\widehat{I^{(t+1)}} = F[X_1, \ldots, X_n]$.
A questo punto usando algoritmi standard per il calcolo del quoziente e usando la caratterizzazione di $\mathrm{Sing}(A)$ data, ancora una volta, dal Teorema dello Jacobiano Generalizzato si conclude il calcolo.

Sopra abbiamo dato i passaggi fondamentali per costruirle, supponiamo quindi di avere le due sottoprocedure ***EquiDim***(I) e ***SingLocus***$(I^{(t)})$, la prima che preso in input un ideale ne calcola la decomposizione equidimensionale, l'altra che dato un ideale equidimensionale ne calcola l'ideale associato al luogo singolare. La procedura ***ZeroIntersection*** diventa dunque:

Algoritmo 3.6. ***ZeroIntersection_Sing***

Input: $I \subset F[X_1, \ldots, X_n]$ *ideale di dimensione strettamente positiva*
Output: $I_0 = \cap_j Q_j$

```
1 inizializzazione;
2 E := {I^(t)} = EquiDim(I);
3 I_0 := I^(0);
4 while E ≠ ∅ do
5 |   I_0 ← I_0 ∩ SingLocus (I^(t));
6 |   E ← E \ I^(t);
7 end
8 return I_0;
```

Possiamo dare ora una dimostrazione alternativa del Teorema d'esistenza di un algoritmo per il calcolo radicale reale 3.13:

Dimostrazione 2. Procediamo per induzione su $m := \dim I$.
Se $m = 0$ allora banalmente $\sqrt[re]{I} = \mathit{RealRadZero}(I)$.
Se $m > 0$, sia $\sqrt[re]{I} = \bigcap_{i=1}^{s} P_i \cap \bigcap_{j=1}^{t} M_j$ la decomposizione in primi minimale di I, dove P_i e M_j sono primi reali tali che $\dim P_i > 0$ e $\dim M_j = 0$. Per ipotesi induttiva si può calcolare $\bigcap_i P_i$ a grazie alla proposizione 3.6; usando invece la costruzione degli $I^{(t)}$ appena mostrata, il criterio jacobiano 3.14 per trovare i luoghi singolari e intersecando al variare di t si ottiene l'ideale J della proposizione 3.21 la cui dimensione è minore di m . Ma allora sempre per ipotesi induttiva

$$\sqrt[re]{I} = \bigcap_i P_i \cap \sqrt[re]{J}.$$

□

Osservazione. La prima parte della dimostrazione è, come plausibile, la stessa della sezione precedente; la differenza tra le due chiaramente è relativa al calcolo della parte zero-dimensionale.

Non possiamo dire se un metodo sia migliore dell'altro: abbiamo visto in entrambi in casi considerati che nonostante non sia possibile individuare singolarmente le componenti zero dimensionali del radicale, quanto esposto però ci permette di trovarne l'intersezione, la quale è sufficiente per completare il calcolo.

In questo e nei capitoli precedenti abbiamo fornito tutti gli strumenti e le procedure che permettono di scrivere una funzione che calcoli effettivamente il radicale reale di un ideale. Concludiamo dunque con due esempi:

Esempio 3.24. Consideriamo l'ideale in $\mathbb{Q}[x,y]$

$$\begin{aligned} I =&(x^4y - 2x^3y + x^2y^2 - 2xy^2 - 2xy + 4y,\\ &x^6 - 2x^5 + x^4 - x^2y^2 - 4x^3 + x^2y + 2xy^2 + 4x^2 - 2x - 4y + 4,\\ &5x^3y^5 + 5xy^6 - 7x^5 - 10y^5 - 7x^3y - 7x^3 + 14x^2 - 7xy + 14) \end{aligned}$$

di dimensione $\dim I = 1$.

- $\sqrt{I} = I = (y^5-7, x-2)\cap(x^2+1, y)\cap(x^3+xy-2)$ è la decomposizione primaria minimale;
- calcoliamo le localizzazioni ${S_1}^{-1}I = ((x)y + (x^3 - 2))$ e ${S_2}^{-1}I = (x3 + (y)x - 2)$ e dunque $\cap_i P_i = (x^3 + xy - 2)$ ideale primo;
- calcoliamo infine l'intesezione delle componenti zero-dimensionali col secondo metodo, le decomposizione equidimensionale dà $I^{(0)} = (xy - 2y, x^3 - 2x^2 + x - 2, 5y^5 - 7x^2 - 7)$ e $I^{(1)} = (x^3 + xy - 2)$; allora una volta trovato $\widetilde{I^{(1)}} = (x^3 + xy - 2, x, 3x^2 + y)$ si ha che

  $$J = I^{(0)} \cap \widetilde{I^{(1)}} = (xy - 2y, x^3 - 2x^2 + x - 2, 5y^5 - 7x^2 - 7)$$

  ideale di dimensione zero. J non è in posizione generale, ma usando un cambio di coordinate si trova che $\cap_j M_j = \sqrt[re]{J} = (y^5 - 7, x - 2)$.
- In conclusione $\sqrt[re]{I} = (x^3 + xy - 2) \cap (y^5 - 7, x - 2) = (x^4 - 2x^3 + x^2y - 2xy - 2x + 4, x^3y^5 + xy^6 - 2y^5 - 7x^3 - 7xy + 14)$.

Esempio 3.25. Consideriamo adesso l'ideale

$$\begin{aligned} K = (&x^2y + xz + yz,\\ &y^2z^3 + y^2z,\\ &xz^5 + xz^3 + yz^5 + yz^3,\\ &x^2yz^2 + x^2y + xz^3 + xz + yz^3 + yz) \end{aligned}$$

di dimensione 1 in $\mathbb{Q}[x,y,z]$ allora

$$\begin{aligned} \sqrt{K} =&(yz^3 + yz, xz^3 + xz, xyz^2 + xy, x^2y + xz + yz)\\ =&(y,z) \cap (z^2 + 1, x^2y + xz + yz) \cap (x,z) \cap (x,y) \end{aligned}$$

mentre

$$\sqrt[re]{K} = (yz, xz, xy) = (y,z) \cap (x,z) \cap (x,y)$$

Possiamo osservare infatti che preso $J = (z^2 + 1, x^2y + xz + yz)$ si ha che $\sqrt[re]{J} = \mathbb{Q}[x,y,z]$, infatti seguendo i passaggi dell'algoritmo si ha che

- $\sqrt{J} = J$;

- Calcolando ${S_h}^{-1}J$ otteniamo

  i. ${S_1}^{-1}J = ((-x^4-1)\cdot y + (-x^3)\cdot z + (-x), z^2+1) \subseteq \mathbb{Q}(x)[y,z]$ è un ideale di dimensione zero e dunque per avere il radicale reale ci basterà calcolare la parte reale di z^2+1 che è chiaramente, a meno di invertibili, 1 (è una somma di quadrati); perciò $\sqrt[re]{{S_1}^{-1}J} = \mathbb{Q}(x)[y,z]$.

  ii. ${S_2}^{-1}J = (z^2+1, (y)\cdot x^2 + xz + (y)\cdot z) \subseteq \mathbb{Q}(y)[x,z]$ è un ideale di dimensione zero e dunque per avere il radicale reale ci basterà calcolare la parte reale di z^2+1 che è anche qui un invertibile; perciò $\sqrt[re]{{S_2}^{-1}J} = \mathbb{Q}(y)[x,z]$.

  iii. ${S_3}^{-1}J = \mathbb{Q}(z)[x,y]$.

  Perciò $\cap_i P_i = \mathbb{Q}[x,y,z]$.

- Calcolando la decomposizione equidimensionale otteniamo $J = J^{(1)}$, il cui luogo singolare è $\mathbb{Q}[x,y,z]$, e banalmente $\cap_j M_j = \mathbb{Q}[x,y,z]$.

E quindi come volevasi dimostrare $\sqrt[re]{J} = \bigcap_i P_i \cap \bigcap_j M_j = \mathbb{Q}[x,y,z]$.

Conclusioni e osservazioni

Partendo dal problema di ripristinare tutte le corrispondenze tra le varietà reali e gli ideali che si hanno quando si lavora in campi algebricamente chiusi, abbiamo introdotto il radicale reale per ideali di polinomi. Il resto della trattazione è stato rivolto a descrivere un possibile metodo per calcolare questo particolare ideale, cercando di spiegare come tutto si riducesse a isolare le radici reali di singoli polinomi univariati.
L'algoritmo ***Realrad*** per il calcolo del radicale reale che abbiamo illustrato è facilmente implementabile, tuttavia potrebbe essere proposto anche un algoritmo diverso per esempio invertendo all'inizio del calcolo quelle variabili che non compaiono nella base ridotta dell'ideale o cercando di accorpare le procedure ***NonZeroIntersection*** e ***ZeroIntersection***.
Nella seconda edizione dell'articolo in effetti Neuhaus propone una versione alternativa unendo i due approcci al calcolo delle componenti zero-dimensionali in modo da poter lavorare direttamente nelle localizzazioni. Per i dettagli vedere *Roger Neuhaus. Computation of real radicals of polynomial ideals - ii. Journal of Pure and Applied Algebra, 124:261–280, 1998.*

Bibliografia

[AM69] Atiyah and Macdonald. *Introduction to Commutative Algebra.* Addison-Wesley, 1969.

[BCR98] Bochnak, Coste, and Roy. *Real Algebraic Geometry.* Springer, 1998.

[Bec81] Becker. Valuation and real places in the theory of formally real fields. *Géométrie Algébrique Réelle et Formes Quadratiques, Lecture Notes in Mathematics*, 959:1–40, 1981.

[BGL+12] Bachmann, Greuel, Lossen, Pfister, and Schönemann. *A Singular Introduction to Commutative Algebra.* Springer Berlin Heidelberg, 2012.

[BN93] Becker and Neuhaus. On the computation of the real radical. *Progress in Mathematics*, 109:1–20, 1993.

[BPR06] Basu, Pollack, and Roy. *Algorithms in Real Algebraic Geometry.* Springer, 2006.

[CLO07] Cox, Little, and O'Shea. *Ideal, Varieties and Algorithms.* Springer, 2007.

[DGPS15] Decker, Greuel, Pfister, and Schönemann. SINGULAR 4-0-2 — A computer algebra system for polynomial computations. `http://www.singular.uni-kl.de`, 2015.

[Dub69] Dubois. A nullstellensatz for ordered fields. *Arkiv for Math*, 8:111–114, 1969.

[Kri64] Krivine. Anneaux préordonnés. *Journal d'Analyse Mathématique*, 12:307–326, 1964.

[Lan05] Lang. *Undergraduate Algebra.* Springer, 2005.

[Liu02] Liu. *Algebraic Geometry and Arithmetic Curves.* Oxford University Press Inc., New York, 2002.

[Neu98] Neuhaus. Computation of real radicals of polynomial ideals - ii. *Journal of Pure and Applied Algebra*, 124:261–280, 1998.

[Pre84] Prestel. *Lectures on Formally Real Fields.* Springer, Berlin, 1984.

[Ris70] Risler. Une caractérisation des idréaux des variètérs algébriques réelles. *Arkiv for Math*, 1970.

[Sei74] Seidenberg. Costructions in algebra. *Transaction of AMS*, 197:273–313, 1974.

[XZZ14] Xiao, Zeng, and Zeng. An improved algorithm for deciding semidefinite polynomials. *Journal of Algebra*, 417:72–94, 2014.

[ZZ04] Zeng and Zeng. An effective decision method for semidefinite polynomials. *Journal of Symbolic Computation*, 37(1):83 – 99, 2004.