Geometria Algebrica Reale

Agnese Gini

29 Ottobre 2016

Indice

Introduzione

La geometria algebrica è quella branca della matematica che unisce lo studio di luoghi geometrici a quello di strutture algebriche. Classicamente tra le ipotesi che si fanno c'è anche quella che il campo base sia algebricamente chiuso, ma questa è in effetti una richiesta abbastanza restrittiva dal momento in cui, ad esempio, in molte applicazioni si richiede i punti che si vanno a considerare sono punti a coordinate intere o reali.

Passando da uno spazio della forma $\mathbb{C}^n$ a $\mathbb{R}^n$ è già semplice osservare che molte buone proprietà, quali la chiusura della classe degli insiemi algebrici rispetto alla proiezione su un sottospazio oppure la corrispondenza tra ideali radicali e le varietà algebriche, si vanno a perdere. Tuttavia qualcosa è recuperabile e la Geometria Algebrica Reale si occupa di studiare che cosa accade quando il campo base si comporta circa come $\mathbb{R}$.
Facciamo un passo indietro, quando si passa da $\mathbb{C}$ a $\mathbb{R}$ è vero che si acquista la garanzia di trovare sempre una radice per un polinomio univariato, però si perde un'importante proprietà: l'ordinabilità. L'idea chiave allora è quella di sfruttare quest'ultima per costruire una nuova teoria che leghi oggetti geometrici su campi ordinabili e oggetti algebrici.

Questo testo nasce dalla curiusità e dalla voglia di comprendere meglio le dinamiche appena introdotte e come quaderno di appunti del corso di Geometria Reale del Prof. Fabrizio Broglia dell'a.a. 2015/2016. Qui sono perciò raccolte definizioni e nozioni base per lo studio della Geometria Algebrica Reale.
Nel primo capito si trova un sunto sulla teoria dei campi reali e un'introduzione al teorema di Tarski–Seidenberg; nel secondo capitolo l'inizio della teoria degli insiemi dei semialgebrici compresa la decomposizione algebrica cilindrica e lo studio della dimensione; nel terzo capitolo sono definite le varietà algebriche reali con particolare attenzione allo studio dei punti regolari; infine nell'ultimo capitolo si trovano raccolte le strutture algebriche che più sono adatte per questa teoria: si definiscono gli ideali reali, si dimostrano il Teorema di Artin-Lang, il Nullstellensatz e il Positivstellensatz reali, a conclusione si mostra inoltre una soluzione del 17esimo problema di Hilbert che discende naturalmente dai risultati appena citati.

Con la speranza di aver raccolto quanto serve e che questi appunti siano ben strutturati e chiari a chi come me è rimasto incuriosito da questo mondo (e so-

prattutto che non ci siano troppi errori), auguro una buona lettura.

Agnese Gini

Capitolo 1

Campi Reali

Iniziamo dando alcune definizioni e risultati a proposito dei campi reali, che ci saranno utili per la trattazione. Non intendiamo tuttavia essere troppo esaustivi ma fissare solamente alcuni concetti della teoria di Artin-Schreier. Per ampliare questo argomento può essere utile il testo [Pre84].

1.1 Ordini e preordini

Definizione 1.1. Sia F campo. Un **ordinamento** $\leq$ di F è una relazione binaria tale che

(i) $a \leq a$

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

(iii) $a \leq b$ o $b \leq a$

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

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

Definizione 1.2. 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. $\tau \cap (-\tau) = \{0\}$
4. $\tau \cup (-\tau) = F$

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

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

Risulta così naturale identificare questi due concetti, nel seguito ci riferiremo quindi a τ come ad un ordine e chiameremo (F, τ) **campo ordinato**.

Osservazione 1.1. Assumendo le altre proprietà si ha che 3. equivale a $-1 \notin \tau$: infatti se $-1 \in \tau$ per ogni $a \in \tau \setminus \{0\}$ si ha che $-a = -1 \cdot a \in \tau$ e quindi $\tau \cap (-\tau) \neq \{0\}$; viceversa se $\tau \cap (-\tau) \supsetneq \{0\}$ allora esiste $a \in \tau \cap (-\tau) \setminus \{0\}$, per 2. si ha che $1 \in F^2 \subseteq \tau$ e dunque l'inverso di un elemento deve avere il suo stesso segno, allora $\frac{1}{a} \in \tau$ cosicché $-1 = -a \cdot \frac{1}{a} \in \tau$.

Consideriamo adesso una nozione più generica, che ci servirà per dimostrare proprietà utili alla trattazione.

Definizione 1.3. Sia A un anello commutativo con identità, diremo che $\sigma \subset A$ è un preordine o **precono** 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 1.2.

- Assumendo le altre proprietà si ha che *3.* equivale a $\sigma \cap (-\sigma) = \{0\}$.
- Ogni ordine 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

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

Vogliamo adesso esplicitare il rapporto tra ordini e preordini su un campo. Preso un preordine $\sigma \subset F$ definiamo dunque

$$\Gamma_\sigma \coloneqq \{\sigma_0 | \sigma_0 \text{ preordine di } F \colon \sigma \subseteq \sigma_0\}$$

$$\chi_\sigma \coloneqq \{\tau | \tau \text{ ordine di } F \colon \sigma \subseteq \tau\}$$

Per completezza enunciamo il seguente lemma generale, di cui in realtà a noi interessa il corollario. È istruttivo tuttavia dimostrare indipendente la proprietà per i campi poiché la dimostrazione è, in certo senso, costruttiva e ci fornisce un primo esempio di estensione.

Lemma 1.4. Sia σ un preordine sull'anello A. Allora esiste un estensione σ_0 di σ tale che

$$\sigma_0 \cup (-\sigma_0) = A \tag{1.1}$$

Corollario 1.5. Ogni preordine τ_0 di un campo F si estende ad un ordine τ di F.

Proposizione 1.6. Preso un qualsiasi preordine σ di un campo F , abbiamo che

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

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

Dimostrazione. (i) Le proprietà $1 - 3$ discendono direttamente dalle ipotesi. L'unica cosa da mostrare è che $-1 \notin \sigma[a]$. Supponiamo per assurdo che vi appartenga, allora esistono $x, y \in \sigma$ tali che $-1 = x + ay$. Se $y = 0$ allora $-1 \in \sigma$, altrimenti $-a = (1/y)^2 y(1 + x) \in \sigma$. In entrambi i casi otteniamo un assurdo.

(ii) Usando il Lemma di Zorn possiamo trovare un elemento massimale τ in Γ_σ. Dobbiamo dimostrare che $\tau \cup \tau = F$. Se $a \in F$ tale che $a \notin \tau$ è possibile costruire $\tau[-a]$, per massimalità $\tau[-a] = \tau$ e dunque $-a \in \tau$.

□

Corollario 1.7. Dato un preordine σ

$$\sigma = \bigcap \{\tau \mid \tau \in \chi_\sigma\}$$

Di particolare importanza è l'insieme delle somme di quadrati di elementi di un campo F

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

infatti gode delle seguenti proprietà:

Proposizione 1.8.

i. $\sum F^2$ è contenuto in ogni preordine di F ,

ii. $\sum F^2$ è chiuso per somma,

iii. $\sum F^2$ 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. $\sum F^2$ è il più piccolo preordine di $F \iff -1 \notin \sum F^2$

Per le sue particolari proprietà useremo la notazione $re \coloneqq \sum F^2$, che sarà più chiara in seguito.

Definiamo ora la struttura centrale di questa teoria:

Definizione 1.10. Un campo F è detto **reale** o ordinabile se ammette un qualche ordinamento.

Teorema 1.11 (E.Artin)**.** Sia F un campo qualsiasi, i seguenti fatti sono equivalenti:

i. F reale

ii. $-1 \notin re$

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

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 ordine. □

Corollario 1.12. Se F è un campo reale

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

Osservazione 1.3. Un campo reale ha caratteristica zero e dunque possiede un sottocampo isomorfo a $\mathbb{Q}$.

Definiamo $\chi(F)$ l'insieme degli ordini di F e concludiamo con due proprietà dei campi reali.

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 $\chi(F) = \{re\}$

1.2 Campi reali chiusi

Analogamente a quanto si fa nella teoria dei campi classica ha senso definire gli elementi massimali di questa classe di campi:

Definizione 1.15. Un campo F è detto reale chiuso se è reale e non ha estensioni reali algebriche proprie.

Esempio 1.

- $\mathbb{R}$ 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. Daremo per buoni questi fatti, abbiamo quindi una caratterizzazione più esplicita di questi campi:

Lemma 1.16. Un campo F è reale chiuso se e solo se è massimamente ordinato e ha un unico ordine .

Dimostrazione. ($\Rightarrow$) Sia $\tau \in \chi(F)$, prendendo $\tau = re$ si ha la tesi.
($\Leftarrow$) Se $\{\tau\} = \chi(F)$ ogni ordine τ_1 di un'estensione reale F_1 estende τ e dunque $F_1 = F$ se F_1 è algebrica. □

I campi reali chiusi godono di molte buone proprietà che li rendono molto simili al campo reale che fa da modello, ossia $\mathbb{R}$, ma che sopratutto permettono di lavorare agilmente su di essi. La prima e più importante è enunciata nel **Teorema di Artin-Schreier (AS)** che esprime tre caratterizzazioni equivalenti che tuttavia si focalizzano su aspetti differenti.

Teorema 1.17. Sia F un campo, i seguenti fatti sono equivalenti:

a. F reale chiuso.

b. $\sum F^2$ è un ordine di F e ogni polinomio in $F[X]$ di grado dispari ha una radice in F.

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

Osservazione 1.4. Sottolineiamo che se F è un campo reale chiuso ha un unico ordinamento che quindi è proprio re.

Valgono poi anche i seguenti fatti (la cui dimostrazione non viene riportata) che richiamano alcuni teoremi dell'analisi classica:

Teorema 1.18. Sia F un campo reale chiuso.

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

Definizione 1.19. Sia F un campo reale chiuso e $p, g \in F[X]$. Definiamo **sequenza di Sturm** di p e g la successione di polinomi $(p_0, \ldots, p_k)$ tali che $p_0 = p$, $p_1 = p'g$ e p_i è l'opposto del resto della divisione euclidea tra p_{i-2} e p_{i-1} ($p_i = p_{i-1}g_i - p_{i-2}$ con $g_i \in F[X]$ e $deg(p_i) < deg(p_{i-1})$) per $i = 1 \ldots k$.
Presa inoltre $a \in F$ 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.

Osservazione 1.5. La sequenza di Sturm è finita e $p_k = \gcd(p, p'g)$.

Teorema 1.20 (Teorema di Sturm). $p \in F[X]$, $a, b \in F$ con $a < b$ che non siano radici di p, allora il numero di radici di p in $]a, b[$ è uguale a

$$v(p, 1; b) - v(p, 1; a).$$

Dimostrazione. Basta osservare che cosa accade alla funzione $x \mapsto v(p, 1; x)$ quando x passa da una radice c di uno dei polinomi della sequenza:

- Se c è una radice di p i segni di p_0 e p_1 cambiano rispettando le seguenti regole

x		c	
p_0	$-$	0	$+$
p_1	$+$	$+$	$+$

oppure

x		c	
p_0	$+$	0	$-$
p_1	$-$	$-$	$-$

  e in entrambi i casi $v(p, 1; x)$ decrescresce di una unità.

- Se c è una radice di p_i per $i = 1 \dots k$ allora $p_{i-1}(c) = p_{i+1}(c) \neq 0$ il contributo della terna p_{i-1}, p_i, p_{i+1} a $v(p, 1; x)$ non cambia e rimane uguale a 1.

□

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

Definizione 1.21. Un estensione algebrica R di (F, τ) è detta **chiusura reale** se R è un campo reale chiuso e il suo unico ordine estende τ.

Riguardo la chiusura reale vale che:

Teorema 1.22. (F, τ) campo reale ammette una chiusura reale R che è unica a meno di F-isomorfismo.

L'unicità della chiusura reale è più forte dell'unicità della chiusura algebrica in quanto si può dimostrare che l'unico F-automorfismo che possiede è l'identità.

1.3 Il principio di Tarski-Seidenberg

Come ultima cosa in questo capitolo presentiamo il Principio di Tarski-Seidenberg che è un principio, si può dire logico, valido anche nel contesto dei campi ordinati e che vedremo sarà di fondamentale importanza nello studio degli insiemi semialgebrici, quindi lo studio delle varietà reali, e nella discussione a proposito del diciassettesimo problema di Hilbert e il Nullstellensatz Reale, in poche parole tutto il contenuto di questa trattazione.

Teorema 1.23 (**Principio di Tarski-Seidenberg [prima forma]**). Se R campo reale chiuso. Sia dato un sistema di equazioni polinomiali nelle variabili $T = (T_1, \dots, T_p)$ e X a coefficienti in R, che indichiamo con $\mathcal{S}(T, X)$:

$$\begin{cases} S_1(T, X) \circledast_1 0 \\ S_2(T, X) \circledast_2 0 \\ \dots \\ S_l(T, X) \circledast_l 0 \end{cases}$$

con $\circledast_i \in \{=, \neq, >, \geq\}$ e $S_i(T, X) \in R[T, X]$ per $i = 1, \ldots, l$. Allora esiste un metodo algoritmico per produrre una lista $\mathcal{C}_1(T), \ldots, \mathcal{C}_k(T)$ di sistemi di equazioni e disequazioni in $R[T]$, con k finito, tali che per ogni $t \in R^p$ i seguenti fatti siano equivalenti:

i. $\mathcal{S}(t, X)$ ha soluzione

ii. almeno uno dei $\mathcal{C}_j(t)$ è soddisfatto.

In altri termini il teorema afferma che l'asserto $''\exists X \ \mathcal{S}(T, X)''$ equivale a $''\mathcal{C}_1(T) \vee \cdots \vee \mathcal{C}_k(T)''$, dunque ci permette di eliminare la variabile X e il quantificatore d'esistenza.
Non entriamo nei dettagli della dimostrazione ma ne riassumiamo i passi principali, che sono quanto ci serve per comprendere quali sono le idee che stanno dietro a questo importante teorema. Iniziamo facendo una osservazione preliminare che ci permette di restringerci ad un caso più semplice da gestire e introduciamo la mappa segno.

Osservazione 1.6. Dato un sistema $\mathcal{S}(T, X)$ è possibile ottenere degli ulteriori sistemi, che chiameremo **sistemi con gradi fissati**, $(\mathcal{S}(T, X), \mathcal{D}(T))$, aggiungendo in $\mathcal{D}(T)$ le condizioni[1] $lc_X S_i \neq 0$. Questi sistemi sono convenienti e più facili da studiare perché permettono di tenere sotto controllo il grado dei polinomi. Visto che ogni sistema può essere scritto come unione disgiunta di sistemi con gradi fissati (induttivamente sul grado si separa il caso in cui il leading coefficient sia uguale o diverso da zero) supporremo sempre di essere in tale ipotesi.

Definizione 1.24. Sia F un campo reale chiuso, la funzione $sign : F \to \{-1, 0, 1\}$ è così definita:

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

Dimostrazione. (TSI) Grazie all'osservazione senza perdita di generalità intenderemo sempre, parlando di sistema, un sistema con gradi fissati.

Passo 1 Sistemi con una solo equazione.
Sia $(P, Q_1, \ldots, Q_l)$ una l-upla di polinomi in $R[T, X]$, algoritmicamente si trovano $R_1(T), \ldots, R_k(T) \in R[T]$ e una funzione $c\colon \{-1, 0, 1\}^k \to \mathbb{N}$ tali che per ogni $t \in R^p$ e per ogni $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_k) \in \{-1, 0, 1\}^k$, se vale

$$''\mathcal{D}(t) \wedge sign(R_1(t)) = \varepsilon_1 \wedge \cdots \wedge sign(R_k(t)) = \varepsilon_k''$$

allora il sistema

$$P = 0 \wedge Q_1 > 0 \wedge \cdots \wedge Q_l > 0$$

[1] Con $lc_X f$ intendiamo il coefficiente direttivo, o leading coefficient, del polinomio f considerato come univariato in X.

ha $c(\varepsilon_1, \ldots, \varepsilon_k)$ soluzioni.
Questo fatto, che si dimostra usando la sequenza di Sturm (niente dettagli), ci basta per concludere: detto $\mathcal{C}_\varepsilon(T)$ il sistema polinomiale

$$\begin{cases} sign(R_1(t)) = \varepsilon_1 \\ \ldots \\ sign(R_k(t)) = \varepsilon_k \\ c(\varepsilon) > 0 \end{cases}$$

allora se esiste $\tilde{\varepsilon}$ tale che in $(t, \tilde{\varepsilon})$ $\mathcal{C}_\varepsilon(T)$ ha soluzione la ha anche $\mathcal{S}(T, X)$; viceversa se esiste una soluzione per $\mathcal{S}(t, X)$ supponendo che nessuno dei $\mathcal{C}_{\tilde{\varepsilon}}(t)$ abbia soluzione avremmo sempre che $c(\varepsilon) = 0$, quindi che $\mathcal{S}(t, X)$ avrebbe zero soluzioni, assurdo.

Passo 2 Caso generale.
Se ci sono più equazioni di grado positivo rispetto ad X $P_1 = \cdots = P_b = 0$ si possono sostituire con $P_1^2 + \cdots + P_b^2 = 0$ e ricondurci al passo 1. Altrimenti siamo nel caso in cui il sistema è

$$Q_1 > 0 \wedge \cdots \wedge Q_l > 0$$

con almeno un polinomio di grado positivo in X. In tal caso il sistema ha soluzione in un intervallo aperto e illimitato se e solo se i coefficienti direttori dei polinomi hanno tutti lo stesso segno. Altrimenti il sistema ha soluzione in un in intervallo le cui soluzioni i cui estremi sono radici di $Q = \prod Q_j$ se e solo se il sistema[2]

$$Q' = 0 \wedge Q_1 > 0 \wedge \cdots \wedge Q_l > 0$$

ha soluzioni reali (il che ci riconduce ancora una volta al passo 1).

Per concludere riflettiamo ancora un attimo su quanto detto sin ora. Il fulcro della dimostrazione è che sui campi reali siamo in grado di dire in un intervallo quante radici reali ci sono e quindi caratterizzare il segno ha un polinomio (contando i cambiamenti di segno della valutazione di altri polinomi nei soli estremi). Questo procedimento è fattibile algoritmicamente in un numero finito di passi, cosicché andando a ritroso si trovano un numero finito di polinomi univariati, quindi un sistema, il cui studio delle soluzioni è realizzabile in molteplici modalità, anch'esse algoritmiche. □

[2]Con l'apice intendiamo l'operazione $\frac{\partial}{\partial X}$.

Capitolo 2

Insiemi semialgebrici

Nell'ambito della geometria algebrica reale gli insiemi semialgebrici vedremo saranno la base naturale su cui lavorare; in geometria algebrica classica questo ruolo è assunto dagli insiemi algebrici, ma lavorando su campi non algebricamente chiusi come i campi reali questi insiemi perdono una proprietà fondamentale: la proiezione di un sottoinsieme algebrico di $\mathbb{R}^n$ su un sottospazio non è algebrica. Vedremo in questo capitolo che invece i semialgebrici godono di questa e molte altre proprietà e poi studieremo un primo modo di decomporre questi spazi che ci permetterà anche di definire la dimensione di un semialgebrico.
Qui svilupperemo la teoria usando come campo $\mathbb{R}$ anche se, con pochissime accortezze, quello che diremo vale per qualsiasi campo reale chiuso.

2.1 Insiemi algebrici

Prima di definire che cosa è un semialgebrico, è bene richiamare precisamente la nozione di insieme algebrico e cercare di capire la differenza tra gli insiemi algebrici reali e quelli complessi:

Definizione 2.1. Sia $\mathbb{K}$ un campo e $B \subseteq \mathbb{K}[X_1, \ldots, X_n]$. L'insieme degli zeri di B è

$$\mathcal{V}(B) \coloneqq \{x \in \mathbb{K}^n \mid \forall f \in B \ f(x) = 0\}$$

Un **insieme algebrico** V è un sottoinsieme di $\mathbb{K}^n$ tale per cui esiste B e $V = \mathcal{V}(B)$.

Inoltre fissiamo la seguente notazione.

Definizione 2.2. Sia $\mathbb{K}$ un campo e $S \subseteq \mathbb{K}^n$. Indichiamo con

$$\mathcal{I}(S) \coloneqq \{f \in \mathbb{K}[X_1, \ldots, X_n] \mid \forall x \in S \ f(x) = 0\}$$

l'ideale dei polinomi che si annullano su S.

Richiamiamo, senza troppi dettagli, alcuni risultati base di geometria algebrica (per una trattazione più completa e le dimostrazioni rimandiamo a [Shape])

sia perché ci serviranno più avanti per trattare alcune nozioni, sia per capire le peculiarità del caso reale.

Osserviamo come prima cosa che un insieme $A \subseteq \mathbb{K}^n$ è algebrico se e solo se $A = \mathcal{V}(\mathcal{I}(A))$. Definiamo per $S \subset \mathbb{K}^n$ **anello delle funzioni polinomiali su** S:

$$\mathcal{P}(S) = {}^{\mathbb{K}[X_1,\dots,X_n]}\!/_{\mathcal{I}(S)}$$

Ovvero possiamo identificare $\mathcal{P}(S)$ con l'anello delle funzioni da S su $\mathbb{K}$ che sono restrizioni di polinomi; il lemma di normalizzazione di Noether ci dice anche che questo anello è intero su un anello di polinomi su $\mathbb{K}$.
Si dice che un insieme algebrico non vuoto $A \subseteq \mathbb{K}^n$ è **irriducibile** se non può essere scritto come unione di due suoi sottoinsiemi algebrici propri. Vale che se A è irriducibile allora $\mathcal{I}(A)$ è un ideale primo e quindi $\mathcal{P}(A)$ è un dominio, in particolare è ben definito il campo delle frazioni $k(A)$, il **campo delle funzioni razionali** su A.
La **dimensione** di un insieme algebrico A è definita come la dimensione di Krull di $\mathcal{P}(A)$, ossia la massima lunghezza di una catena di ideali primi di tale anello. Questa definizione prettamente algebrica permette di caratterizzare, nel caso l'insieme sia irriducibile, la dimensione come grado di trascendenza di $k(A)$ su $\mathbb{K}$. Dato un insieme algebrico A esiste unica **decomposizione in componenti irriducibili** non ridondante, ossia $A_1, \dots, A_s$ algebrici irriducibili tali che $A_j \nsubseteq \cup_{k\neq j} A_k$ e $A = A_1 \cup \dots \cup A_s$. Vale che:

Teorema 2.3.

i. Sia A un insieme algebrico e A_i con $i = 1 \dots s$ le sue componenti irriducibili, allora $\dim(A) = \max_i\{\dim(A_i)\}$.

ii. $V \subseteq \mathbb{K}^n$ e $W \subseteq \mathbb{K}^m$ algebrici allora $V \times W$ è algebrico in $\mathbb{K}^n \times \mathbb{K}^m$ e vale che $\mathcal{P}(V \times W) = \mathcal{P}(V) \otimes_{\mathbb{K}} \mathcal{P}(W)$. Inoltre prodotto di irriducibili è irriducibile e $\dim(V \times W) = \dim V + \dim W$.

Se $S \subseteq \mathbb{K}^n$ è un sottoinsieme qualsiasi,

$$\mathrm{Clos}_Z(S) \coloneqq \mathcal{V}(\mathcal{I}((S)))$$

è il più piccolo insieme algebrico che lo contiene ed è chiamato **chiusura di Zariski** di S. Sostanzialmente stiamo prendendo la chiusura rispetto alla topologia di Zariski su $S \subseteq \mathbb{K}^n$, i cui chiusi sono tutti e soli gli algebrici.

Concentriamoci adesso sul campo reale e quello complesso. Ogni insieme algebrico complesso $A \subseteq \mathbb{C}^n$ può essere visto come sottoinsieme di $\mathbb{R}^{2n}$ e gli insiemi algebrici reali che possono essere visti come realizzazione di un algebrico complesso godono di particolari proprietà, infatti nel capitolo 7 di [Shape] viene mostrato che:

Proposizione 2.4. Sia $A \subset \mathbb{C}^n$ un algebrico irriducibile, con dimensione complessa d, considerato come sottoinsieme algebrico di $\mathbb{R}^{2n}$. Allora:

1. A è connesso,

2. A è illimitato (eccetto se è un punto),

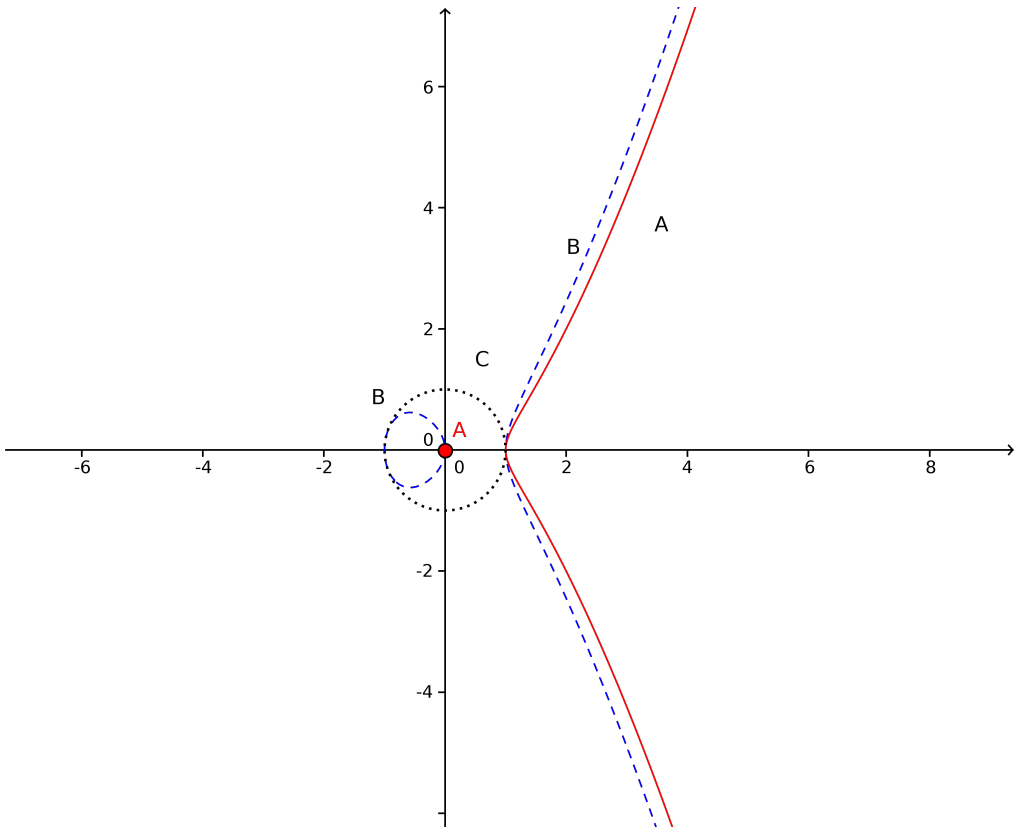
3. $\dim V_x$, ossia la dimensione locale in $x \in A$, è $2d$.

Questo significa che gli insiemi algebrici che possono essere scritti come algebrici complessi si comportano molto bene, ma le condizioni che li caratterizzano sono abbastanza restrittive. Già a partire da un solo polinomio si ottengono insiemi che non le soddisfano. Riportiamo qualche esempio che illustri diverse patologie:

Esempio 2.

1. I luoghi di zeri in $\mathbb{R}^2$ delle cubiche $y^2 - x^3 + x^2$ e $y^2 - x^3 + x$ hanno entrambi due componenti connesse, la prima ha un punto isolato, ma sono irriducibili.

2. $S^1 \subset \mathbb{R}^2$ è un insieme algebrico limitato.



3. L'ombrello di Cartan è la superficie $z(x^2 + y^2) = x^3$ di $\mathbb{R}^3$, questa è irriducibile e connessa ma ha un manico in corrispondenza dell'asse z i cui punti hanno tutti dimensione 1.

2.2 Insiemi semialgebrici e stabilità per proiezione

Definizione 2.5. Un **insieme semialgebrico** di $\mathbb{R}^n$ è un insieme di punti

$$x = (x_1, \ldots, x_n) \in \mathbb{R}^n$$

che soddisfano una combinazione booleana di equazioni e disequazioni polinomiali a coefficienti reali. In particolare, chiameremo semialgebrici la più piccola classe di sottoinsiemi di $\mathbb{R}^n$, che indicheremo con $\mathcal{SA}_n$, tale che

(i) Se $p \in \mathbb{R}[X_1, \ldots, X_n]$, allora

$$\{x \in \mathbb{R}^n |\ p(x) = 0\} \in \mathcal{SA}_n$$

$$\{x \in \mathbb{R}^n |\ p(x) > 0\} \in \mathcal{SA}_n$$

(ii) È chiusa per unione, intersezione, passaggio al complementare.

Proposizione 2.6. Ogni $A \in \mathcal{SA}_n$ è unione finita di insiemi della forma

$$\{x \in \mathbb{R}^n |\ P(x) = 0 \wedge Q_1(x) > 0 \wedge \cdots \wedge Q_s(x) > 0\}$$

con $P, Q_1, \ldots, Q_s \in \mathbb{R}[X_1, \ldots, X_n]$

Esempio 3.

1) In $\mathbb{R}$ i semialgebrici sono unioni finite di punti e intervalli aperti.

2) Gli algebrici sono semialgebrici.

3) Siano $F\colon \mathbb{R}^n \to \mathbb{R}^m$ mappa polinomiale e $A \in \mathcal{SA}_m$, allora $F^{-1}(A) \in \mathcal{SA}_n$.

4) $A \in \mathcal{SA}_m$ e $B \in \mathcal{SA}_n$ allora $A \times B \in \mathcal{SA}_{m+n}$.

Nel capitolo 1 abbiamo enunciato il Teorema di Tarski-Seidenberg (1.23), facciamo vedere adesso che la chiusura rispetto alla proiezione della classe dei semialgebrici ne è un corollario:

Teorema 2.7 (**Tarski-Seidenberg [seconda forma]**). Sia $A \in \mathcal{SA}_{n+1}$ e

$$\pi\colon \mathbb{R}^{n+1} \to \mathbb{R}^n$$

la proiezione sulle prime coordinate. Allora $\pi(A) \in \mathcal{SA}_n$.

Dimostrazione. A è unione finita di insiemi della forma $\{x \in \mathbb{R}^{n+1} |\ P(x) = 0 \wedge Q_1(x) > 0 \wedge \cdots \wedge Q_s(x) > 0\}$ per il teorema 1.23 esiste una combinazione booleana $\mathcal{C}(X_1, \ldots, X_n)$ di equazioni e disequazioni polinomiali tali che

$$\pi(A) = \{y \in \mathbb{R}^n \mid \exists x_{n+1} \in \mathbb{R}\ (y, x_{n+1}) \in A\}$$

sia l'insieme degli $y = (x_1, \ldots, x_n)$ tale che $\mathcal{C}(x_1, \ldots, x_n)$ sia vero, ossia $\pi(A)$ è semialgebrico. □

Corollario 2.8.

1. Se $A \in \mathcal{SA}_{n+k}$ e $\pi\colon \mathbb{R}^{n+k} \to \mathbb{R}^n$ allora $\pi(A) \in \mathcal{SA}_n$.
2. Se $A \in \mathcal{SA}_m$ e $F\colon \mathbb{R}^n \to \mathbb{R}^m$ mappa polinomiale allora $F(A) \in \mathcal{SA}_n$.

Dimostrazione. Il primo punto si fa per induzione. Per il secondo basta notare $B = \{(x,y) \in \mathbb{R}^{m+n} \mid x \in A \text{ e } y = F(x)\} \in \mathcal{SA}_{m+n}$ e $F(A) = \pi_m(B)$. □

Corollario 2.9. Se $A \in \mathcal{SA}_n$ la chiusura in $\mathbb{R}^n$

$$\mathrm{Clos}(A) = \{x \in \mathbb{R}^n \mid \forall \varepsilon \in \mathbb{R}\colon \varepsilon > 0 \Rightarrow \exists y \in \mathbb{R}^n,\ y \in A \wedge \|x-y\|^2 < \varepsilon\}$$

è semialgebrica.

Dimostrazione. Per sfruttare le chiusura per proiezione dei semialgebrici cerchiamo una scrittura alternativa di questo insieme. Le variabili in questione formano una tripla

$$(x, \varepsilon, y) \in \mathbb{R}^n \times \mathbb{R} \times \mathbb{R}^n$$

e la condizione sulla norma può essere espressa con la disuguaglianza polinomiale

$$\sum_{i=1}^{n} (x_i - y_i)^2 < \varepsilon^2.$$

Consideriamo ora il semialgebrico

$$B = (\mathbb{R}^n \times \mathbb{R} \times A) \cap \{(x, \varepsilon, y) \in \mathbb{R}^n \times \mathbb{R} \times \mathbb{R}^n \mid \|x-y\|^2 < \varepsilon\} \subseteq \mathbb{R}^{2n+1}$$

e le proiezioni

$$\begin{array}{rccc} \pi_1\colon & \mathbb{R}^{n+1} & \longrightarrow & \mathbb{R}^n \\ & (x, \varepsilon) & \longmapsto & x \end{array}$$

$$\begin{array}{rccc} \pi_2\colon & \mathbb{R}^{2n+1} & \longrightarrow & \mathbb{R}^{n+1} \\ & (x, \varepsilon, y) & \longmapsto & (x, \varepsilon) \end{array}$$

allora

$$\mathrm{Clos}(A) = \mathbb{R}^n \setminus (\pi_1(\{(x,\varepsilon) \in \mathbb{R}^n \times \mathbb{R} \mid \varepsilon > 0\} \setminus \pi_2(B)))$$

e quindi è algebrico. □

È utile anche un terza forma del teorema in termini logici, più facile da usare. Dobbiamo però richiamare qualche definizione per enunciarla.
Per noi una **formula al primo ordine** è una proposizione ottenuta con le seguenti regole:

1. $\Lambda \leftarrow (p \in \mathbb{R}[X_1, \ldots, X_n] \Rightarrow p = 0 \vee p > 0)$
2. $\Lambda \leftarrow (\Phi \vee \Psi), (\Phi \wedge \Psi), (\neg \Psi)$
3. $\Lambda \leftarrow (\exists x \Psi), (\forall x \Psi)$

dove con le lettere greche abbiamo indicato formule al prim'ordine e con x un elemento di $\mathbb{R}$; in pratica stiamo dicendo che ad esempio $\Lambda = (\forall x \neg(\Phi \vee \Psi))$ è una formula al prim'ordine. Di solito se la formula dipende da uno o più parametri lo indichiamo tra parentesi, nell'esempio allo avremmo potuto scrivere $\Lambda(x)$. Inoltre, se una formula è ottenuta usando solo i primi due punti è detta *libera da quantificatori*.

Osservazione 2.1. Un sottoinsieme $A \subseteq \mathbb{R}^n$ è semialgebrico se e solo se esiste una formula libera da quantificatori Φ tale che

$$(x_1, \ldots, x_n) \in A \iff \Phi(x_1, \ldots, x_n)$$

Teorema 2.10 (**Tarski-Seidenberg [terza forma]**)**.** Se $\Phi(X_1, \ldots, X_n)$ è una formula al prim'ordine, l'insieme dei $(x_1, \ldots, x_n) \in \mathbb{R}^n$ che soddisfano tale formula formano un semialgebrico.

Dimostrazione. Per induzione sulla costruzione della formula. La prima regola produce solo sottoinsiemi semialgebrici; l'applicazione della seconda, visto che è un operazione finita, produce un semialgebrico. Se l'insieme

$$\{(x_1, \ldots, x_{n+1}) \in \mathbb{R}^{n+1} \mid \Psi(x_1, \ldots, x_{n+1})\}$$

è semialgebrico allora

$$\{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid \exists y \in \mathbb{R} \colon \Psi(x_1, \ldots, x_n, y)\}$$

è la sua proiezione sulle prime n coordinate e dunque è semialgebrico. Per concludere riguardo le formule ottenute con la terza regola, osserviamo che

$$\forall x \Psi \iff \neg \exists x \neg \Psi.$$

□

Osservazione 2.2. Stiamo dicendo in poche parole che ogni formula al prim'ordine è equivalente ad una formula libera da quantificatori.

2.3 Mappe semialgebriche

Introduciamo adesso i morfismi che meglio si adattano a alla classe dei semialgebrici:

Definizione 2.11. Siano $A \in \mathcal{SA}_m$ e $B \in \mathcal{SA}_n$, una $f \colon A \to B$ è detta **mappa semialgebrica** se il suo grafico

$$\Gamma_f = \{(x, y) \in \mathbb{R}^{m+n} \mid y = f(x)\}$$

è semialgebrico.

Esempio 4.

- Le mappe polinomiali e le le funzioni regolari sono semialgebriche.
- Se $f\colon A \to B$ è semialgebrica allora $|f|$ è semialgebrica.
- Se $f\colon A \to B$ è semialgebrica e positiva su tutto il dominio allora $\sqrt{f}$ è semialgebrica.

Usando le proprietà sopra enunciate, in particolare la chiusura rispetto alla proiezione, otteniamo che:

Proposizione 2.12.

1. Se $f\colon A \to B$ è semialgebrica allora $f^{-1}(B)$ e $f(A)$ sono semialgebrici.
2. $f\colon A \to B$ e $g\colon B \to C$ mappe semialgebriche, allora $g \circ f$ è semialgebrica.
3. L'insieme $\mathcal{S}_A F \coloneqq \{f\colon A \to \mathbb{R} \mid \text{mappa semialgebrica}\}$ è un anello.

A partire dalla proposizione sopra enunciata e notando che l'identità è una mappa semialgebrica e le mappe semialgebriche sono associative, si può dire che i semialgebrici con queste frecce sono una categoria.

Nei contesti dove dir ciò ha senso, le mappe semialgebriche si comportano bene definitivamente. Specifichiamo il significato di quanto appena detto riportando due risultati, il primo dei quali mostra che in dimensione uno la crescita di una mappa semialgebrica è limitata da un polinomio. Ci sarà utile il seguente lemma:

Lemma 2.13. Sia $p(x) = \sum_{j=0}^{d} a_j x^{d-j}$ dove $a_0 \neq 0$. Se $c \in \mathbb{C}$ è una radice di p, allora

$$|c| \leq \max_{i=1,\dots,d} \left(d \left| \frac{a_i}{a_0} \right| \right)^{\frac{1}{i}}.$$

Dimostrazione. Sia

$$M = \max_{i=1,\dots,d} \left(d \left| \frac{a_i}{a_0} \right| \right)^{\frac{1}{i}}$$

e $z \in \mathbb{C}$ un numero tale che $|z| > M$. Allora

$$|a_i| < |a_0| \frac{|z|^i}{d}$$

e dunque

$$\left| \sum_{j=1}^{d} a_j z^{d-j} \right| \leq \sum_{j=1}^{d} |a_j| |z|^{d-j} < |a_0 z^d|$$

e $p(z) \neq 0$. □

Proposizione 2.14. Sia $f\colon (a, +\infty) \to \mathbb{R}$ una mappa semialgebrica non necessariamente continua. Allora esistono $b \geq a$ e un intero positivo n tale che $|f| \leq x^n$ per ogni $x \in (b, +\infty)$.

Dimostrazione. Per definizione il grafico di f è un semialgebrico e dunque si scrive come una unione finita $\Gamma = G_1 \cup \cdots \cup G_l$ con

$$G_i = \{(x,y) \in \mathbb{R}^2 |\ P^i(x,y) = 0 \wedge Q^i_1(x,y) > 0 \wedge \cdots \wedge Q^i_{s_i}(x,y) > 0\}.$$

Osserviamo se se esistesse un j tale che $\deg_y P^j = 0$, allora se un punto $(x_0, y_0) \in G_j$ avremmo che tutto un intervallo di $\{x_0\} \times \mathbb{R}$ sta G_j, ma questo è assurdo per la definizione di funzione (avrei più immagini per un punto). Possiamo quindi assumere $\deg_y P^i > 0$ per ogni i e ha senso la scrittura

$$\Lambda(x,y) = \prod_{i=1}^{l} P^j(x,y) = a_0(x)y^d + \cdots + a_d(x)$$

con $d > 0$ e $a_0 \neq 0$. Possiamo quindi scegliere $c \geq a$ tale che $a_0(x) \neq 0$ per $x \in (c, +\infty)$.
Gli elementi che si scrivono come $f(x)$, ossia che stanno nell'immagine della mappa, sono radici di Λ e quindi

$$|f(x)| \leq \max_i \left(d \left| \frac{a_i(x)}{a_0(x)} \right| \right)^{\frac{1}{i}}$$

facendo il limite per x che va a più infinito si vede che questo massimo si comporta come x^α con $\alpha \in \mathbb{Q}$. Basta scegliere n come la parte intera superiore di $\mathbb{Q}$ e scegliere $b > c$. □

Dimostriamo adesso un risultato in ogni dimensione, a meno di restringerci ai compatti, che in realtà è particolarmente utile per lo studio delle varietà reali analitiche.

Teorema 2.15 (Disuguaglianza di Łojasiewicz)**.** Sia $K \in \mathbb{R}^n$ un semialgebrico compatto e siamo $f, g \colon K \to \mathbb{R}$ due mappe semialgebriche continue tali che

$$\forall x \in K\ f(x) = 0 \Rightarrow g(x) = 0$$

Allora esistono $n \in \mathbb{N}$ e una costante $C \geq 0$ tale che

$$\forall x \in K\ |g(x)|^n \leq C|f(x)|.$$

Dimostrazione. Sia $t > 0$, definiamo $F_t = \{x \in K \mid t|g(x)| = 1\}$. Questo insieme è un chiuso e dunque è compatto; allora possiamo definire una funzione

$$\begin{array}{rccc} \theta \colon & (0,+\infty) & \to & \mathbb{R} \\ & t & \mapsto & \theta(t) \end{array}$$

come segue:

- se $F_t \neq \varnothing$, visto che per ipotesi per $y \in F_t$ $f(y) \neq 0$, $\theta(t) = \max\{x \mapsto |1/f(x)|\}$,

- se $F_t = \varnothing$ allora $\theta(t) = 0$.

Questa è una mappa semialgebrica dal momento che

$$\Gamma_\theta = \{(t,s) \in \mathbb{R}^+ \times \mathbb{R} \mid (F_t = \varnothing \wedge s = 0) \vee ((\exists x \in F_t \colon s = f(x)) \wedge (\forall y \in F_t \; 1 \leq |f(x)|s))\}.$$

e F_t è definito semialgebricamente[1]. Per la proposizione precedente allora esistono $b \geq 0$ e un intero positivo n tale che $|\theta(t)| \leq t^n$ per ogni $t \in (b, +\infty)$, che equivale a dire che

$$\forall x \in K \;\; 0 < |g(x)| < \frac{1}{b} \Rightarrow \left|\frac{1}{f(x)}\right| \leq \left|\frac{1}{g(x)}\right|^n$$

Sia ora $d = \max \frac{|g(x)|^n}{|f(x)|}$ su $\{x \in K \mid |g(x)| \geq \frac{1}{b}\}$ (che esiste perché questo insieme è compatto), allora se $C = \max\{1, d\}$

$$\forall x \in K \; |g(x)|^n \leq C|f(x)|.$$

□

2.4 Decomposizione di insiemi semialgebrici

Ogni $A \in \mathcal{SA}_1$ si scrive come unione finita di punti e intervalli aperti. Il nostro scopo per il resto di questo sottocapitolo sarà mostrare che è possibile decomporre, per un n qualsiasi, ogni semialgebrico in $\mathcal{SA}_n$ come unione disgiunta di pezzi che sono semialgebricamente omeomorfi a ipercubi aperti di dimensione d, ossia $(0,1)^d$. Notiamo che assumendo che per $d = 0$ l'ipercubo sia un punto, nel caso di $\mathbb{R}$ ritroviamo quanto sapevamo.
È bene precisare la seguente nozione:

Definizione 2.16. Un omeomorfismo semialgebrico $h \colon S \to T$ è una mappa continua biunivoca e semialgebrica con inversa continua.

Osservazione 2.3. La condizione che l'inversa sia semialgebrica è necessaria visto che $\Gamma_h = \Gamma_{h^{-1}}$.

Introduciamo ora la *Decomposizione algebrica cilindrica* (CAD) di $\mathbb{R}^n$ che, vedremo, sarà risolutiva rispetto lo scopo che ci siamo prefissi, la quale è anche particolarmente interessante per due motivi: il primo è che ne esiste un raffinamento tale per cui è possibile che una famiglia di polinomi abbia segno costante su ciascun pezzo della decomposizione, il secondo è che questa procedura è intrinsecamente algoritmica.

Definizione 2.17. Una **decomposizione algebrica cilindrica** di $\mathbb{R}^n$ è un lista $\mathcal{C}_1, \ldots, \mathcal{C}_n$, dove per $1 \leq k \leq n$ l'insieme $\mathcal{C}_k$ è una partizione di $\mathbb{R}^k$ in sottoinsiemi semialgebrici, detti **celle**, che soddisfano le seguenti proprietà:

[1] Stiamo utilizzando la terza forma del teorema di Tarski-Seidenberg.

(a) Ogni $C \in \mathcal{C}_1$ è un punto o un intervallo aperto.

(b) Per ogni $k = 1, \ldots, n-1$ e per ogni cella $C \in \mathcal{C}_k$ esistono delle funzioni semialgebriche continue

$$\xi_{C,1} < \cdots < \xi_{C,s_C} : C \to \mathbb{R}$$

tali per cui il cilindro $C \times \mathbb{R} \subseteq \mathbb{R}^{k+1}$ sia unione disgiunta di celle di $\mathcal{C}_{k+1}$ che sono di esattamente uno dei seguenti tipi:

(i) il **grafico** di una $\xi_{C,j}$ per $j = 1, \ldots, s_C$

$$A_{C,j} = \{(x', x_{k+1}) \in C \times \mathbb{R} \mid x_{k+1} = \xi_{C,j}(x')\}$$

(ii) una **banda** del cilindro limitata superiormente e inferiormente rispettivamente dai due grafici delle $\xi_{C,j}$ e $\xi_{C,j+1}$ con $j = 0, \ldots, s_C + 1$ (dove poniamo $\xi_{C,0} = -\infty$ e $\xi_{C,s_C+1} = +\infty$)

$$B_{C,j} = \{(x', x_{k+1}) \in C \times \mathbb{R} \mid \xi_{C,k+1}(x') < x_k < \xi_{C,k+1}(x')\}$$

Lemma 2.18. Ogni cella di una CAD $\mathcal{C}_1, \ldots, \mathcal{C}_n$ è semialgebricamente omeomorfa a $(0,1)^d$ per d opportuno.

Dimostrazione. Per induzione su k; $k = 1$ è vero per definizione. Se $k > 1$, data $C \in \mathcal{C}_k$ per costruzione abbiamo che ogni $A_{C,j}$ è omeomorfo semialgebricamente a C tramite

$$\begin{array}{rccc} \varphi\colon & C & \to & A_{C,j} \\ & x' & \mapsto & (x', \xi_{C,j}(x')) \end{array}$$

mentre ogni $B_{C,j}$ è omeomorfa a $C \times (0,1)$ tramite la mappa

$$\lambda(x', t) = \begin{cases} (x', (1-t)\xi_{C,j}(x') + t\xi_{C,j+1}(x')) & 0 < j < l_C \\ (x', -\frac{1}{t} + \frac{1}{1-t}) & j = l_C = 0 \\ (x', -\frac{1-t}{t} + \xi_{C,1}(x')) & j = 0, l_C \neq 0 \\ (x', \frac{t}{t+1} + \xi_{C,l_C}(x')) & j = l_C \neq 0 \end{cases}$$

Applicando l'ipotesi induttiva abbiamo la tesi. □

Abbiamo anticipato che è possibile costruire la decomposizione in modo che sui pezzi della CAD, che ora sappiamo chiamarsi celle, una famiglia di polinomi abbia segno costante:

Definizione 2.19. Sia $(P_1, \ldots, P_r)$ una $r-$upla di polinomi in $\mathbb{R}[X_1, \ldots, X_n]$. Diremo che un sottoinsieme $C \subseteq \mathbb{R}^n$ è $(P_1, \ldots, P_r)$-**invariante** se ogni P_j ha segno segno costante su C per $j = 1, \ldots, r$.

Definizione 2.20. Siano $(P_1, \ldots, P_r)$ una $r-$upla di polinomi in $\mathbb{R}[X_1, \ldots, X_n]$ e $\mathcal{C}_1, \ldots, \mathcal{C}_n$ una CAD di $\mathbb{R}^n$; diremo che è **adatta** a $(P_1, \ldots, P_r)$ se vale anche

(c) Ogni cella $C \in \mathcal{C}_n$ è $(P_1, \ldots, P_r)-$invariante.

Soffermiamoci un attimo sul perché è sensato aggiungere questa ipotesi. La nostra attenzione, ricordiamo, è rivolta allo studio degli insiemi semialgebrici, i quali possono essere espressi tramite combinazioni booleane di equazioni e disequazioni polinomiali; questo vuol dire che se prendiamo una decomposizione algebrica cilindrica adatta alla famiglia dei polinomi che descrivono un fissato $S \in \mathcal{SA}_n$ questo si scriverà come unione finita di alcune delle celle di grado n. Dunque dimostrando che a partire dalle equazioni che descrivono un semialgebrico siamo in grado di costruire una CAD, avremo anche provato che esso è semialgebricamente omeomorfo ad un'unione finita di ipercubi aperti di dimensione al più n.

Rimane da dimostrare che una decomposizione algebrica cilindrica esiste; riportiamo qui una dimostrazione costruttiva, la quale ci fornisce anche un algoritmo esplicito.
Enunciamo un paio di fatti che ci serviranno per far ciò (cerchiamo di mantenere una notazione coerente con la costruzione anche se i fatti valgono più in generale).

Lemma 2.21. Sia $P(X_1, \ldots, X_n) \in \mathbb{R}[X_1, \ldots, X_n]$ e $C \subseteq \mathbb{R}^{n-1}$ un sottoinsieme algebrico connesso e $0 < k \leq d$ interi tale che per ogni $\tilde{x} \in C$ il polinomio $P(\tilde{x}, X_n)$ ha grado d ed esattamente k radici distinte in $\mathbb{C}$. Allora esistono $l \leq k$ funzioni semialgebriche continue

$$\xi_1 < \cdots < \xi_l \colon C \to \mathbb{R}$$

tali che per ogni $\tilde{x} \in C$ l'insieme delle radici reali di $P(\tilde{x}, X_n)$ è $\{\xi_1(\tilde{x}), \ldots, \xi_l(\tilde{x})\}$. Inoltre per ogni $i = 1, \ldots, l$, la molteplicità di $\xi_i(\tilde{x})$ è costante al variare del punto in C.

Prima di dimostrare il lemma enunciamo (la dimostrazione si fa come nel caso generale) il principio di continuità delle radici in queste particolari ipotesi:

Proposizione 2.22. Sia $P(X_1, \ldots, X_n) \in \mathbb{R}[X_1, \ldots, X_n]$ e $\tilde{a} \in C \subseteq \mathbb{R}^{n-1}$ e siano $z_1, \ldots, z_k$ radici distinte di $P(\tilde{a}, X_n)$ con $z_1, \ldots, z_k$ le rispettivamente molteplicità. Dato $\varepsilon > 0$ tale che i dischi D_j di centro z_j e raggio ε, contenuti in $\mathbb{C}$ per ogni j, siano tutti disgiunti ; se $\tilde{b}$ è sufficientemente vicino ad $\tilde{a}$ allora $P(\tilde{b}, X_n)$ ha esattamente m_j radici in D_j per ogni j.

Dimostriamo il Lemma 2.21:

Dimostrazione. Consideriamo $P(X_1, \ldots, X_n) \in \mathbb{R}[X_1, \ldots, X_n]$. Per la proposizione 2.22, con la stessa notazione, preso $\tilde{b} \in C$ il polinomio $P(\tilde{b}, X_n)$ in ogni disco D_j di centro z_j e raggio ε ha esattamente una radice di molteplicità m_j per le ipotesi fatte su C (il numero di radici distinte è fissato): chiamiamo questa radice ζ_j. Osserviamo che se z_j è reale lo è anche ζ_j, analogamente se vale se è puramente immaginaria.

Se $\tilde{a} \in C$ e $\tilde{b} \in C$ sono abbastanza vicini allora i polinomi $P(\tilde{a}, X_n)$ e $P(\tilde{b}, X_n)$ hanno lo stesso numero di radici reali; ma visto che C è connesso in realtà questo vale per tutti i punti e dunque il numero di radici reali è costante su tutto C e verrà indicato con l. Definiamo allora per ogni $1 \leq i \leq l$

$$\begin{array}{rccc} \xi_i \colon & C & \to & \mathbb{R} \\ & \tilde{x} & \mapsto & \zeta_{\tilde{x},i} \end{array}$$

dove $\zeta_{\tilde{x},1} < \cdots < \zeta_{\tilde{x},l}$ sono le radici reali di $P(\tilde{x}, X_n)$. Ovviamente le ξ_i sono continue e $\xi_i(\tilde{x})$ ha molteplicità costante come radice. Inoltre visto che C è semialgebrico esiste una formula $\Theta(\tilde{x})$ che lo descrive e i grafici delle ξ si possono scrivere nel seguente modo:

$$\begin{aligned} \Gamma_{\xi_i} = \{(\tilde{x}, x_n) \in \mathbb{R}^n \mid \Theta(\tilde{x}) \wedge (\exists y_1 < y_2 \cdots < y_l \wedge \\ P(\tilde{x}, y_1) = 0 \wedge \cdots \wedge P(\tilde{x}, y_l) = 0 \wedge x_n = y_i)\} \end{aligned}$$

E dunque le ξ_i sono anche semialgebriche. □

Se la famiglia di polinomi constasse solo di un elemento, questo lemma sarebbe sufficiente, tuttavia questo è un caso molto speciale. In generale è opportuno capire come interagiscono tra di loro queste funzioni se i polinomi in gioco sono almeno due, anzi senza perdita di generalità possiamo ridurci a studiare proprio questo caso. Faremo vedere infatti che se due funzioni α e β trovate come nel lemma precedente (rispettivamente a due diversi polinomi) coincidono in un punto allora coincidono su tutto il dominio C; nell'ottica di costruire una CAD questo ci dice che quelle che avevamo indicato con $\xi_{C,1} < \cdots < \xi_{C,s_C}$ possono essere scelte come l'unione delle mappe semialgebriche che troviamo grazie al Lemma 2.21 per ognuno dei due polinomi.

Lemma 2.23. Siano $P, Q \in \mathbb{R}[X_1, \ldots, X_n]$ e $C \in \mathbb{R}^{n-1}$ un semialgebrico connesso tale che per ogni $\tilde{x} \in C$ siano costanti

- il grado e il numero di radici distinte di $P(\tilde{x}, X_n)$ (risp. $Q(\tilde{x}, X_n)$)
- il grado in X_n del $\gcd(P(\tilde{x}, X_n), Q(\tilde{x}, X_n))$.

e siano $\alpha, \beta \colon C \to \mathbb{R}$ due mappe semialgebriche continue tali che per ogni $\tilde{x} \in C$ $P(\tilde{x}, \alpha(\tilde{x})) = 0$ e $Q(\tilde{x}, \beta(\tilde{x})) = 0$. Allora se esiste $\tilde{a} \in C$ per cui $\alpha(\tilde{a}) = \beta(\tilde{a})$ necessariamente $\alpha \equiv \beta$.

Dimostrazione. Indichiamo con $z_1 = \alpha(\tilde{a}) = \beta(\tilde{a}), z_2, \ldots, z_k$ le radici distinte in $\mathbb{C}$ del polinomio prodotto $P(\tilde{a}, X_n)Q(\tilde{a}, X_n)$ e con m_i e p_j per $i, j = 1, \ldots, k$ le rispettive molteplicità[2] come radici di $P(\tilde{a}, X_n)$ e $Q(\tilde{a}, X_n)$. Allora il grado di $\gcd(P(\tilde{a}, X_n), Q(\tilde{a}, X_n))$ è esattamente $\sum_i^k \min\{m_i, p_i\}$.
Scegliamo $\varepsilon > 0$ in modo che $D_j = D(\varepsilon, z_j)$ siano aperti disgiunti in $\mathbb{C}$, allora per la Proposizione 2.22 per ogni $\tilde{x} \in C$ vicino ad $\tilde{a}$ si ha che ogni disco contiene

[2]Ricordiamo che per convenzione dicendo che $z \in \mathbb{C}$ ha molteplicità zero come radice di un certo polinomio p si intende che $p(z) \neq 0$.

una radice di molteplicità m_j di $P(\tilde{x}, X_n)$ e una di molteplicità p_j di $Q(\tilde{x}, X_n)$. Il grado del gcd è costante su C per ipotesi si ha anche che questo ha una radice in ogni disco di molteplicità $\min\{m_j, p_j\}$ (dove questa quantità è non nulla). Per connessione allora deve valere che per ogni $\tilde{x} \in C$ $\alpha(\tilde{x}) = \beta(\tilde{x})$. □

Abbiamo fin qui gettato le basi per quello che sarà il passo induttivo dell'algoritmo. Prima di poterlo illustrare dobbiamo introdurre uno strumento algebrico che generalizza il noto risultante di due polinomi: i *coefficienti sottorisultanti principali.*

Definizione 2.24. Consideriamo $A(y) = a_0 y^d + \cdots + a_d$ e $B(y) = b_0 y^e + \cdots + b_e$ due polinomi tali che $a_0.b_0 \neq 0$ e la matrice

$$S = \begin{bmatrix} a_0 & \dots & a_d & & \\ & \ddots & & \ddots & \\ & a_0 & & \dots & a_d \\ & & b_0 & \dots & b_e \\ b_0 & \dots & b_e & & \end{bmatrix}$$

che è una permutazione della matrice di Sylvester di A e B. Definiamo $j-$esimo **coefficiente sottorisultante principale PSRC**$_j(A, B)$ per $j = 0, \dots, \min(e, d)$ come il determinate della sottomatrice quadrata di taglia $d + e - 2j$ ottenuta da S eliminando le prime e le ultime j righe e j colonne.

Abbiamo introdotto questi coefficienti perché vale una proprietà molto utile:

Lemma. Sono fatti equivalenti:

- A ha r radici complesse distinte.
- $\mathrm{PSRC}_{d-r}(A, A') \neq 0$ e $\mathrm{PSRC}_l(A, A') = 0$ per ogni $0 \leq l < d - r$.

Vediamo come sfruttare questo strumento. Sia $(P_1, \dots, P_r)$ una $r-$upla di polinomi in $\mathbb{R}[X_1, \dots, X_n]$. Possiamo vedere ogni P_j come polinomio in X_n e definiamo **PROJ**$(P_1, \dots, P_r)$ la più piccola famiglia di polinomi in $\mathbb{R}[X_1, \dots, X_n]$ tali che per $i, j, k = 1, \dots, r$

1. se $\deg_{X_n} P_j = d > 2$ allora $\mathrm{PROJ}(P_1, \dots, P_r)$ contiene tutti i polinomi non costanti tra i $\mathrm{PSRC}_s(P_j, \frac{\partial P_j}{\partial_{X_n}})$ per $s = 0 \dots d-1$;
2. se $1 \leq d = \min\{\deg_{X_n} P_i, \deg_{X_n} P_k\}$ allora $\mathrm{PROJ}(P_1, \dots, P_r)$ contiene tutti i polinomi non costanti tra i $\mathrm{PSRC}_s(P_k, P_i)$ per $s = 0 \dots d$;
3. se $\deg_{X_n} P_j \geq 2$ e $\mathrm{lc}_{x_n}(P_j) \notin \mathbb{R}$ allora $\mathrm{PROJ}(P_1, \dots, P_r)$ contiene $\mathrm{lc}_{X_n}(P_j)$ e $\mathrm{PROJ}(P_1, \dots, Q, \dots, P_r)$ dove Q è la *coda* di P_j, ossia[3] $Q = P_j - \mathrm{lt}_{X_n}(P_j)$;
4. se $\deg_{X_n} P_j = 0$ e P_j non costante allora $P_j \in \mathrm{PROJ}(P_1, \dots, P_r)$.

[3]Con $\mathrm{lt}(F)$ si intende il termine di testa del polinomio F.

Abbiamo dato tutti gli ingredienti che ci permettono di enunciare il teorema giustifica quello che sarà il passo induttivo:

Teorema 2.25. Sia $(P_1, \dots, P_r)$ una $r-$upla di polinomi in $\mathbb{R}[X_1, \dots, X_n]$ e $C \subseteq \mathbb{R}^{n-1}$ un sottoinsieme connesso semialgebrico e PROJ$(P_1, \dots, P_r)$-invariante. Allora esistono

$$\xi_1 < \cdots < \xi_l \colon C \to \mathbb{R}$$

funzioni semialgebriche continue tali che $\{\xi_1(\tilde{x}), \dots, \xi_l(\tilde{x})\}$ sia l'insieme delle radici reali di $P_1(\tilde{x}, X_n), \dots, P_r(\tilde{x}, X_n)$, non nulli, per ogni $\tilde{x} \in C$. Inoltre i grafici di ogni ξ_i e le bande del cilindro $C \times \mathbb{R}$ delimitate da tali grafici sono

- insiemi semialgebrici connessi,
- semialgebricamente omeomorfi rispettivamente a C e $C \times (0, 1)$,
- $(P_1, \dots, P_r)$-invarianti.

Dimostrazione. Per dimostrare la tesi ci basta far vedere che le ipotesi dei Lemmi 2.21 e 2.23 sono soddisfatti. In particolare capiamo cosa vuol dire che C è PROJ$(P_1, \dots, P_r)$-invariante: le condizioni 3. e 4. ci danno che il grado rispetto X_n è costante su C e quindi lo è anche il numero di radici come polinomi nell'ultima variabile; la condizione 1. invece dà che il gcd tra ogni polinomio e la sua derivata abbia grado costante e unito a quelle precedenti dunque che il numero di zeri distinti sia costante; infine la condizione 2. ci dà che il numero di zeri comuni di ogni coppia di polinomi sia costante. □

Possiamo costruire quindi una CAD adatta iterativamente. Ripetendo PROJ $n-1$ volte arriviamo a una famiglia finita di polinomi nella variabile X_1, per i quali è facile costruire una CAD adattata di $\mathbb{R}$ (i loro zeri reali tagliano la retta reale in un numero finito di punti e intervalli aperti); a questo punto grazie al Teorema 2.25 siamo in grado di rimontare i pezzi.
Otteniamo dunque che:

Corollario 2.26. Per ogni $(P_1, \dots, P_r)$ una r-upla di polinomi in $\mathbb{R}[X_1, \dots, X_n]$ esiste una CAD di $\mathbb{R}^n$ $(P_1, \dots, P_r)$-adatta.

Omettiamo i dettagli algoritmici e lo studio delle complessità (doppiamente esponenziale in n). Ci pare invece opportuno fornire un esempio di questa costruzione:

Esempio 5. Costruiamo un CAD di $\mathbb{R}^3$ adatta a $p(x, y, z) = x^2 + y^2 + z^2 - 1$.

Step 1 Calcoliamo iterativamente PROJ.

- $\partial_z p = 2z$, $\text{PSRC}_0 = -4(x^2 + y^2 + 1)$ e $\text{PSRC}_1 = 2$ allora PROJ $= \{-(x^2 + y^2 - 1)\}$;
- Sia $q = -(x^2 + y^2 - 1)$ allora $\partial_y(q) = -2y$, $\text{PSRC}_0 = x^2 - 1$ e $\text{PSRC}_1 = -1$ allora $\text{PROJ}^2(p) = \{x^2 - 1\}$;

Indichiamo con $r(x) = x^2 - 1 = (x-1)(x+1)$, questo polinomio ha due radici in $\mathbb{R}$ 1 e -1, dunque

$$\mathcal{C}_1 = \{(-\infty, -1), \{-1\}, (-1, 1), \{1\}, (1, \infty)\}.$$

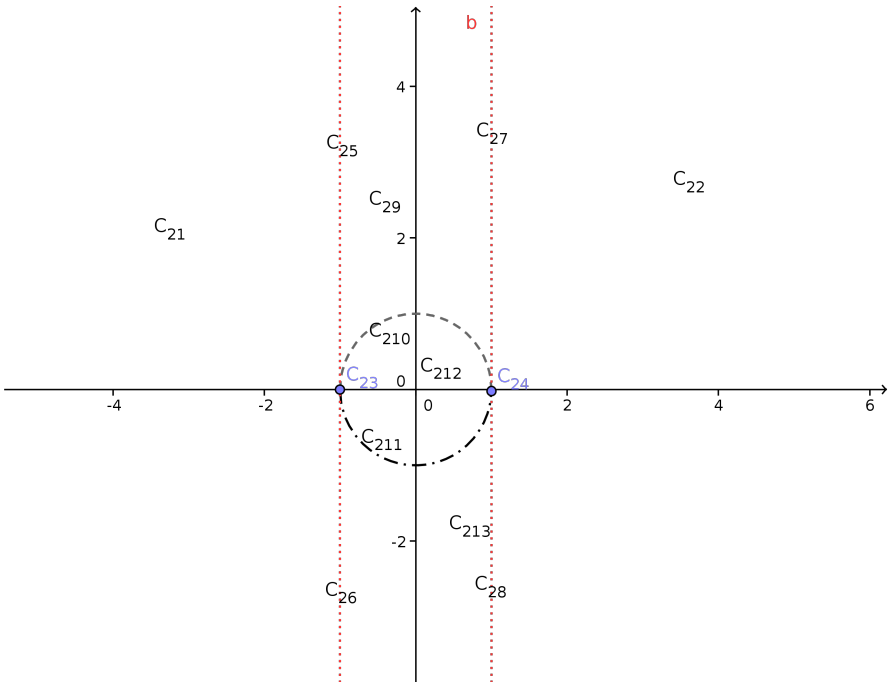
Step 2 Calcoliamo $\mathcal{C}_2$

- Fissiamo $a \in (-\infty, -1) = C_{1,1}$, allora $q(a, y) = -(y^2 + a^2 - 1)$ non ha radici reali. Allora otteniamo una banda $C_{2,1} = (-\infty, -1) \times \mathbb{R}$.
- Analogamente al caso precedente da $(1, \infty)$ otteniamo $C_{2,2} = (1, \infty) \times \mathbb{R}$.
- Fissiamo il punto $\{-1\}$, $q(-1, y) = -y^2$ che si annulla solo per $y = 0$ e quindi otteniamo che $C_{2,3}$ è il grafico di $\xi_{-1} \equiv 0$ più due bande.
- Analogamente al caso precedente da $\{1\}$ otteniamo di nuovo $C_{2,4}$ più due bande.
- Fissiamo $a \in (-1, 1)$ ci sono due casi casi

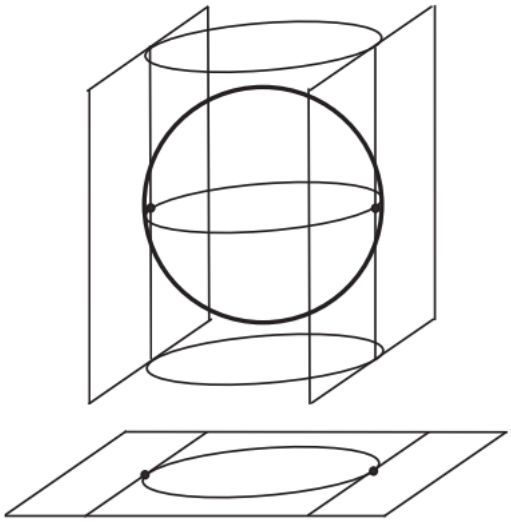
$$\begin{cases} \text{se } y > 0 \; y = \sqrt{1 - a^2} \\ \text{se } y > 0 \; y = -\sqrt{1 - a^2} \end{cases}$$

Otteniamo quindi due grafici e tre bande.

Graficamente $\mathcal{C}_2$ risulta:



Step 3 In breve per quanto riguarda $\mathcal{C}_3$: su $C_{2,1}$,$C_{2,2}$,$C_{2,5}$,$C_{2,6}$,$C_{2,7}$, $C_{2,8}$ il polinomio p non ha radici, su $C_{2,3}$, $C_{2,4}$, $C_{2,11}$ e $C_{2,10}$ una sola radice e su $C_{2,12}$ abbiamo otto possibili grafici. La decomposizione è schematizzabile come segue:



2.4.1 Componenti connesse di un insieme semialgebrico

L'esistenza di una CAD ha molte conseguenze e corollari, ad esempio come vedremo nel prossimo capitolo permette di definire la nozione di dimensione. Qui la useremo per dimostrare che un semialgebrico si scrive come unione di una quantità finita di componenti connesse.

Teorema 2.27. Ogni insieme semialgebrico ha una quantità finita di componenti connesse semialgebriche. Inoltre ogni insieme semialgebrico è localmente connesso.

Dimostrazione. Sia $S \in \mathcal{SA}_n$, il Corollario 2.26 e la teoria sviluppata riguardo la CAD implicano che S può essere scritto come unione disgiunta di $C_1, \ldots, C_p$ semialgebrici che sono semialgebricamente omeomorfi a $(0,1)^{d_i}$ per $i = 1, \ldots, p$ (vedi Lemma 2.18); ovviamente questi insiemi sono connessi.
Vogliamo quindi trovare le componenti connesse di S a partire dalle celle. Diremo che C_i e C_j sono adiacenti se $C_i \cap \mathrm{Clos}(C_j) \neq 0$ e indicheremo con $\sim$ la relazione d'equivalenza sulle celle indotta dall'adiacenza. Dunque $C_i \sim C_j$ se esiste una sequenza ordinata $C_i, \ldots, C_k, \ldots, C_j$ di celle adiacenti. Allora abbiamo che $S_1, \ldots, S_r$, dove ogni S_i è unione massimale di celle adiacenti, è una partizione di S in semialgebrici disgiunti. Osserviamo che ogni S_i è chiuso in S, infatti se $C_j \cap \mathrm{Clos}(S_i) \neq 0$ allora C_j è adiacenti ad almeno una cella di S_i e dunque è $C_j \subseteq S_i$. Tuttavia visto che il complementare è unione finita di chiusi, ogni S_i è anche aperto.
Rimane da far vedere che sono connessi. Supponiamo di avere $S_i = F_1 \sqcup F_2$ unione disgiunta di due chiusi, allora si deve avere sia che ogni cella appartiene è contenuta (per connessione) in uno solo dei due chiusi sia che due celle adiacenti devono stare nello stesso F_s; perciò $S_i = F_1$ oppure $S_i = F_2$.
Dire che $S \in \mathcal{SA}_n$ è localmente connesso significa che per ogni $x \in S$ ogni palla di centro x contiene un intorno connesso di x in S. Una palla B è un semialgebrico e dunque lo è anche $S \cap B$, è per quanto dimostrato sopra è unione

finita di componenti connesse, in particolare quella che contiene x è l'intorno che cercavamo. □

2.5 Dimensione di un semialgebrico

La CAD permette di decomporre un semialgebrico S in un'unione finita di celle semialgebricamente omeomorfe a ipercubi di varie dimensioni d_i, un buon candidato come dimensione di S potrebbe essere il massimo di tali dimensioni. Il nostro scopo in questa sezione è dimostrare che in effetti questa è una buona definizione e che nel caso degli insiemi algebrici coincide con la classica definizione, ovvero la dimensione di Krull dell'anello delle funzioni polinomiali sull'insieme.

Ci sono due strade percorribili dato un $S \in \mathcal{SA}_n$:

- Definire, a partire da una decomposizione di S come unione disgiunta di semialgebrici C_i, ognuno dei quali semialgebricamente omeomorfo a $(0,1)^{d_i}$, la dimensione
$$d = \max\{d_i \mid i = 1, \ldots, p\};$$
dimostrare che poi il massimo dei d_i non dipende dalla decomposizione e quindi mostrare l'equivalenza. ([Cos00] § 3.3)

- Definire la dimensione di S come la dimensione (algebrica) della sua chiusura di Zariski e far vedere che, fissata una decomposizione, il numero d coincide con essa, ottenendo anche che non dipende dalla decomposizione scelta. ([BR98] §2.8)

Sebbene il primo dei due iter sia di carattere più geometrico richiederebbe di introdurre altra teoria sui semialgebrici, come l'esistenza di una *stratificazione* ([Cos00] § 3). Scegliamo di intraprendere il secondo perché invece sfrutta solo la teoria nota nel caso algebrico e la chiusura per proiezione dei semialgebrici.

Definizione 2.28. Sia $A \subseteq R^n$ un insieme semialgebrico, ricordiamo che
$$\mathcal{P}(A) = {}^{\mathbb{R}[X_1, \ldots, X_n]}\!/_{\mathcal{I}(A)}$$
è l'anello dei polinomi su A. La **dimensione** di A, indicata con $\dim A$, è la dimensione di Krull di $\mathcal{P}(A)$.

Proposizione 2.29. $A \subseteq \mathbb{R}^n$ insieme semialgebrico, allora $\dim A$ è uguale alla dimensione della sua chiusura di Zariski.

Dimostrazione. Basta ricordare il corollario 2.9 e osservare che $\mathcal{I}(A) = \mathcal{I}(\operatorname{Clos} A) = \mathcal{I}(\operatorname{Clos}_Z A)$. □

Osservazione 2.4. Con questa definizione otteniamo direttamente che per un insieme algebrico la dimensione algebrica e semialgebrica coincidono.

Calcoliamo la dimensione in un caso particolare e poi dimostriamo alcune conseguenze di questa definizione "più algebrica".

Teorema 2.30. Sia U un insieme semialgebrico aperto non vuoto di $\mathbb{R}^n$. Allora $\dim U = n$.

Dimostrazione. Per induzione su n.
$n = 1$. U è infinito infatti contiene un intervallo aperto e quindi $\mathcal{I}(U) = \{0\}$ (un polinomio non nullo ha un numero di radici pari al suo grado, dunque d finite).
$n > 1$. Esisterà $\tilde{U} \in \mathbb{R}^{n-1}$ aperto e semialgebrico tale che $\tilde{U} \times (a, b) \subseteq U$. Indicando con $\tilde{X} = (X_1, \ldots, X_{n-1})$, consideriamo un $P(\tilde{X}, X_n) = Q_d(\tilde{X})X_n^d + \cdots + Q_0(\tilde{X}) \in \mathcal{I}(U)$, allora $P(\tilde{x}, X_n) \in \mathcal{I}((a, b))$ per ogni $\tilde{x} \in \tilde{U}$. Per ipotesi induttiva allora $P(\tilde{x}, X_n) = 0$, ossia $Q_d(\tilde{x}) = \cdots = Q_0(\tilde{x}) = 0$ e quindi $\mathcal{I}(U) = 0$.
In particolare $\mathcal{P}(U) = \mathbb{R}[X_1, \ldots, X_n]$ e dunque $\dim U = n$. □

Corollario 2.31. $\dim(0, 1)^d = d$.

Proposizione 2.32.

(a) Sia $A = \cup_{i=1}^s A_i$ un unione finita di insiemi semialgebrici allora

$$\dim(A) = \max_i \{\dim(A_i)\}.$$

(b) Siano A, B due insiemi semialgebrici, allora

$$\dim(A \times B) = \dim A + \dim B$$

Dimostrazione. Per (a) basta osservare che $\mathcal{I}(A) = \cap_{i=1}^s \mathcal{I}(A_i)$. (b) è una conseguenza del Teorema 2.3 una volta osservato che

$$\mathrm{Clos}_Z((A \times B) = \mathrm{Clos}_Z(A) + \mathrm{Clos}_Z(B).$$

□

Per poter dimostrare che la dimensione è il massimo delle dimensioni delle celle vorremmo poter procedere, in un certo senso, a ritroso e ricondurci a lavorare su sottospazi sempre più piccoli: è a questo punto che diventa cruciale la chiusura della classe dei semialgebrici rispetto alla proiezione. Enunciamo e dimostriamo due fatti che ci permetteranno di provare quanto suddetto:

Proposizione 2.33. Sia $A \subseteq \mathbb{R}^{n+1}$ un sottoinsieme semialgebrico e sia

$$\pi \colon \mathbb{R}^{n+1} \to \mathbb{R}^n$$

la proiezione sulle prime n coordinate, allora

$$\dim(\pi(A)) \leq \dim(A).$$

Dimostrazione. Possiamo ridurci a considerare A un insieme algebrico irriducibile per la Proposizione 2.29 e Teorema 2.3. Allora l'algebrico $B = \mathrm{Clos}_Z(\pi(A))$ è anch'esso irriducibile, se infatti $B = F_1 \cup F_2$ avremmo

$$A = (A \cap \pi^{-1}F_1) \cup (A \cap \pi^{-1}F_2)$$

e quindi $A \subseteq \pi^{-1}F_1$ o $A \subseteq \pi^{-1}F_2$, cosicché $B \subset F_1$ o $B \subset F_2$.
La proiezione induce un mappa iniettiva $\pi^*\colon \mathcal{P}(B) \to \mathcal{P}(A)$ e, visto che gli insiemi sono irriducibili, anche un omomorfismo $\pi^*\colon k(B) \to k(A)$. Il grado di trascendenza del primo campo allora è minore o uguale di quello del secondo, da cui la tesi. □

Lemma 2.34. Sia $A \subseteq \mathbb{R}^n$ semialgebrico e $f\colon A \to \mathbb{R}$ una mappa semialgebrica. Allora esiste una partizione di A in un numero finito di semialgebrici A_i con $i = 1, \ldots, s$ e per ogni i un polinomio $Q_i(T, X) \in \mathbb{R}[T_1, \ldots, T_n, X]$, tale che $Q_i(t, X)$ non sia identicamente zero per $t \in A_i$ e $Q_i(t, f(t)) = 0$,

Dimostrazione. Γ_f è un semialgebrico di $\mathbb{R}^{n+1}$ e quindi si scrive come combinazione booleana di condizioni sul segno di una famiglia di polinomi $Q_i(T, X) \in \mathbb{R}[T_1, \ldots, T_n, X]$. Abbiamo mostrato che esiste una CAD $(Q_1, \ldots, Q_s)-$invariante di $\mathbb{R}^{n+1}$ che ci fornisce una decomposizione di A in semialgebrici (celle $\mathcal{C}_n$) e delle mappe semialgebriche continue

$$\xi_{C,1} < \cdots < \xi_{C,s_C}\colon C \to \mathbb{R}$$

al variare di $C \in \mathcal{C}_n$. Il grafico di f ristretto ad A_i inoltre coincide con il grafico di un $\xi_{C,j}$, che ci dà quanto voluto. □

Proposizione 2.35. Sia $A \subseteq \mathbb{R}^n$ semialgebrico e $f\colon A \to \mathbb{R}^p$ una mappa semialgebrica. Allora

$$\dim \Gamma_f = \dim A.$$

Dimostrazione. Se $p = 1$, per il Lemma 2.34 (con la medesima notazione) esistono $Q_1, \ldots, Q_s$ e dei semialgebrici A_i. Fissiamo k e scegliamo una componente irriducibile V di $\mathrm{Clos}_Z(A_k)$, allora $V \cap A_k \neq \varnothing$ e quindi esiste $v \in V$ tale che $Q_i(v, X) \neq 0$. Allora $\mathcal{V}(Q_i) \cap (V \times \mathbb{R}) \subsetneq V \times \mathbb{R}$ e usando l'irriducibilità si ha che $V \times \mathbb{R}$ è irriducibile e ha dimensione $\dim V + 1$. Inoltre abbiamo che

$$\dim \Gamma_{f|_{A_i \cap V}} \leq \dim(\mathcal{V}(Q_i) \cap (V \times \mathbb{R})) < \dim V + 1 \leq \dim A_i + 1$$

Facendo variare k e usando ancora la Proposizione 2.32 abbiamo che $\dim \Gamma_f \leq \dim A$. L'altra disuguaglianza segue dalla Proposizione 2.33.
Se $p > 1$ scriviamo $f = (\tilde{f}, f_p)$ con $\tilde{f}\colon A \to \mathbb{R}^{p-1}$ e $f_p\colon A \to \mathbb{R}$. Indichiamo con B il grafico si $\tilde{f}$, ora possiamo allora scrivere Γ_f come il grafico della mappa

$$\begin{array}{rccc} g\colon & B & \to & \mathbb{R} \\ & (x, \tilde{y}) & \mapsto & f_p(x) \end{array}$$

ossia $\Gamma_f = \Gamma_g$: per il caso $p = 1$ $\dim \Gamma_g = \dim B$ e per ipotesi induttiva $\dim B = \dim A$. □

Il seguente teorema diviene, alla luce di queste proposizioni, una banale osservazione:

Teorema 2.36. Sia $A \subseteq \mathbb{R}^n$ semialgebrico e $f\colon A \to \mathbb{R}^p$ una mappa semialgebrica. Allora

$$\dim f(A) \leq \dim A.$$

Se f è anche una bigezione tra A e la sua immagine allora $\dim f(A) = \dim A$.

Dimostrazione. La proiezione del grafico su $\mathbb{R}^p$ è $f(A)$, per quanto visto sin qui

$$\dim A = \dim \Gamma_f \geq \dim f(A).$$

Se f è una bigezione possiamo fare lo stesso ragionamento con l'inversa. □

Corollario 2.37. Se $A = \cup_{i=1}^{s} A_i$ è un'unione finita di insiemi semialgebrici tale che per ogni $i = 1, \ldots, s$ A_i è semialgebricamente omeomorfo a $(0,1)^{d_i}$, allora

$$\dim A = \max\{d_i \mid i = 1, \ldots, s\}.$$

Dimostrazione. La proposizione 2.32 ci dà che $\dim A = \max_i \dim A_i$; per il Teorema 2.36 e il Corollario 2.31 allora $\dim A_i = d_i$, da cui la tesi.

□

Per trattare le varietà nel prossimo capitolo ci sarà utile aver studiato che cosa accade "vicino"ai punti. A conclusione di questa sezione perciò introduciamo la dimensione locale e mostriamo che cosa accade quando sull'insieme algebrico è definita la struttura di varietà differenziabile.

Lemma. $A \subseteq \mathbb{R}^n$ insieme semialgebrico e x un suo punto. Allora esiste un intorno semialgebrico U tale che per ogni altro U' in esso contenuto allora $\dim U = \dim U'$.

Dimostrazione. Basta osservare che $\mathbb{R}[X]$ è un anello noetheriano e quindi qualsiasi catena di ideali della forma $\mathcal{I}(U)$ è stazionaria. In particolare se si staziona su un certo $I = \mathcal{I}(U)$ allora per ogni $U' \subseteq U$ abbiamo che $I = \mathcal{I}(U')$, da cui $\dim U = \dim U'$. □

Definizione 2.38. $A \subseteq \mathbb{R}^n$ un insieme semialgebrico e x un suo punto. La **dimensione locale di** A **in** x, indicata con $\dim(A_x)$, è la dimensione dell'insieme U del Lemma precedente.

Proposizione 2.39. Sia $A \in \mathcal{SA}_n$ semialgebrico di dimensione d. Allora $A^{(d)} = \{x \in A \mid \dim(A_x) = d\} \subseteq A$ è un insieme semialgebrico chiuso non vuoto.

Dimostrazione. Consideriamo una CAD, allora $A = \cup_{i=1}^{s} A_i$ e per ogni $i = 1, \ldots, s$ A_i è semialgebricamente omeomorfo a $(0,1)^{d_i}$. Supponiamo, a meno di permutare gli indici, che $\dim A_j = d$ per $j = 1, \ldots, k \leq s$ e poniamo

$$B = \mathrm{Clos}_Z\left(\bigcup_{j=1}^{k} A_i\right) \subseteq A.$$

Ovviamente $B \subseteq A^{(d)}$, facciamo vedere che sono uguali. Se $x \notin B$ allora esiste un intorno U tale che $\dim(A_x) \neq d$, in particolare esiste un certo indice per cui $A_l \cap U \neq \varnothing$ e quindi $d_l < d$, cosicché $x \notin A^{(d)}$.

□

Proposizione 2.40. Sia $A \subseteq \mathbb{R}^n$ un insieme semialgebrico che è anche una varietà differenziabile C^∞ embedded in $\mathbb{R}^n$ allora di dimensione t. Allora la dimensione semialgebrica di A è $\dim A = t$.

Dimostrazione. Prendiamo $x \in A$ e sia T_xA lo spazio tangente di A in x. La mappa $A \to T_xA$ è semialgebrica e mappa bigettivamente un intorno aperto semialgebrico di x contenuto in A in un sottoinsieme semialgebrico aperto di T_xA. Dato che il tangente è uno spazio vettoriale di dimensione t e per il Teorema 2.36 e la Proposizione 2.30, si ha

$$\dim A_x = \dim T_xA = t.$$

Per concludere ci basta osservare che grazie alla Proposizione 2.39

$$\dim A = \max\{\dim A_x \mid x \in A\}.$$

□

Capitolo 3

Varietà Reali

Tradizionalmente una varietà algebrica è l'insieme degli zeri di una famiglia di polinomi. La geometria algebrica classica sviluppa tale concetto lavorando su campi algebricamente chiusi, su questi campi il Teorema degli zeri di Hilbert rende particolarmente facile passare dal geometrico all'algebrico e viceversa. Abbiamo studiato nel primo capitolo la caratteristiche del campo $\mathbb{R}$ e sappiamo che non è algebricamente chiuso, quindi non possiamo utilizzare la definizione suddetta. Vedremo nel prossimo capitolo come il fatto che $\mathbb{R}$ sia reale chiuso permette di sviluppare un analogo del Nullstellensatz.
Siamo però in grado di aggirare questo fatto utilizzando una definizione più astratta, la quale caratterizza gli insiemi che sono varietà a partire dalle mappe che sono definite localmente. In questi termini non è ancora chiaro quale sia la struttura che di cui stiamo parlando e come si raccordi con l'idea classica di varietà algebrica, già dalle prime definizioni però sarà chiara la direzione che prenderemo.
A conclusione di questo capitolo discuteremo anche la nozione di punto regolare in una varietà reale.

3.1 Varietà Algebriche Reali

Consideriamo un insieme algebrico $V \subset \mathbb{R}^n$. Nel capitolo 2.1 abbiamo definito $\mathcal{P}(V)$ l'anello delle funzioni polinomiali da V in $\mathbb{R}$; dato $W \subseteq \mathbb{R}^p$ indichiamo ora con

$$\mathcal{P}(V, W) = \{(f_1, \dots, f_p) \colon V \to W \mid f_1, \dots, f_p \in \mathcal{P}(V)\}$$

Definizione 3.1. Sia U un sottoinsieme aperto di Zariski di $V \subseteq \mathbb{R}^n$ insieme algebrico. Diremo che f è una **funzione regolare** su U se esistono $g, h \in \mathcal{P}(V)$ e $h^{-1}(0) \cap U = \varnothing$ tali che $f = g/h$ in U.

Le funzioni regolari formano un anello, che indicheremo con $\mathcal{O}(U)$. Inoltre una mappa da U in $W \subseteq R^p$ è detta regolare se ha coordinate regolari. L'insieme di queste mappe è denotato con $\mathcal{O}(U, W)$.
Da un punto di vista algebrico l'**anello delle funzioni regolari** $\mathcal{O}(U)$ non è

altro che la localizzazione di $\mathcal{P}(U)$ rispetto al sottoinsieme moltiplicativo

$$S_U = \{h \in \mathcal{P}(U) \mid h^{-1}(0) \cap U = \varnothing\}.$$

$\mathcal{O}(U) = {S_U}^{-1}\mathcal{P}(U)$.

In generale la nozione di funzione regolare ha una natura locale, usando la topologia di Zariski però possiamo dimostrare in questo contesto assume un valore globale:

Proposizione 3.2. Sia $V \subset \mathbb{R}^n$ un insieme algebrico e $\{U_i\}_{i=1,\dots,p}$ una famiglia finita di sottoinsiemi di Zariski di V. Consideriamo f una funzione da $U = \cup_{i=1}^{p} U_i$ a $\mathbb{R}$, se per ogni i esistono $P_i, Q_i \in \mathcal{P}(U_i)$ tali che $Q_i^{-1}(0) \cap U_i = \varnothing$ e $f|_{U_i} = P_i/Q_i$, allora esistono $P, Q \in \mathcal{P}(V)$ con Q che non si annulla mai su U e $f = P/Q$.

Dimostrazione. Basta prendere $S_i \in \mathcal{P}(V)$ che si annulli ovunque eccetto su U_i allora $Q = \sum_i S_i^2 Q_i$. □

Questo fatto, la cui dimostrazione è banale, permette di definire però la struttura di fascio ([Shape] 5§2):

Definizione 3.3. Un **prefascio** $\mathcal{F}$ su uno spazio topologico X è un'applicazione che associa a ogni aperto $U \subseteq X$ l'elemento $\mathcal{F}(U)$di una fissata categoria localmente piccola, detto insieme delle **sezioni** di U, e tale che se $U \subseteq V$ è un inclusione tra due aperti allora esiste un omomorfismi della categoria $\rho_U^V \colon \mathcal{F}(V) \to \mathcal{F}(U)$, detta di **restrizione**, tale che

(a) $\mathcal{F}(\varnothing)$ ha un solo elemento[1]

(b) per ogni U aperto $\rho_U^U = id_U$

(c) dati degli aperti $U \subseteq V \subseteq W$ allora $\rho_U^W = \rho_U^V \rho_V^W$

Inoltre se per ogni aperto U e ogni ricoprimento aperto $U = \cup_{\alpha \in A} U_\alpha$ sono soddisfatte le seguenti condizioni:

(d) $\rho_{U_\alpha}^U s_1 = \rho_U^U s_2$ per $s_1, s_2 \in \mathcal{F}(U)$ e tutti gli U_α allora $s_1 = s_2$

(e) se $s_\alpha \in \mathcal{F}(U_\alpha)$ sono tali che $\rho_{U_\alpha \cap U_\beta}^U s_\alpha = \rho_{U_\alpha \cap U_\beta}^U s_\beta$ allora esiste $s \in \mathcal{F}(U)$ tale che $s_\alpha = \rho_{U_\alpha}^U s$ per ogni U_α

diremo che $\mathcal{F}$ è un **fascio**.

Osservazione 3.1. Le ultime due proprietà ci dicono rispettivamente che le sezioni sono univocamente definite dalle loro restrizioni locali e che sezioni locali compatibili si incollano. Inoltre solitamente se le sezioni sopra U sono funzioni con tale aperto come dominio si usa la seguente notazione: $f \in \mathcal{F}(U)$ e $V \subseteq U$ $f|_V = \rho_V^U f$.

[1] Il vuoto è contenuto in ogni aperto perciò se siamo nel caso di gruppi o anelli o moduli si ha che $\mathcal{F}(\varnothing) = \{0\}$.

Corollario 3.4. Sia $V \subseteq \mathbb{R}^n$ un insieme algebrico, allora $\mathcal{O}\colon U \to \mathcal{O}(U)$ è un fascio di anelli su V per la topologia di Zariski.

Studiamo ora le mappe tra insiemi algebrici che rispettano la nuova struttura che abbiamo definito (questo risultato vale più in generale):

Proposizione 3.5. Siano $V \subseteq \mathbb{R}^n$ e $V' \subseteq \mathbb{R}^p$ due insiemi algebrici e $U \subset V$ e $U' \subset V'$ due aperti di Zariski. Ogni mappa regolare $\varphi\colon U \to U'$ induce un morfismo di $\mathbb{R}$-algebre

$$\begin{array}{rccc} \varphi^*\colon & \mathcal{O}(U') & \to & \mathcal{O}(U) \\ & f & \mapsto & f \circ \varphi \end{array}$$

Inoltre la mappa $\varphi \mapsto \varphi^*$ è una bigezione tra $\mathcal{O}(U, U')$ e l'insieme degli omomorfismi di $\mathbb{R}$-algebre da $\mathcal{O}(U')$ a $\mathcal{O}(U)$.

La proposizione suggerisce allora una relazione d'equivalenza:

Definizione 3.6. Siano $V \subseteq \mathbb{R}^n$ e $V' \subseteq \mathbb{R}^p$ due insiemi algebrici e $U \subset V$ e $U' \subset V'$ due aperti di Zariski. Diremo che $U \to U'$ regolare biettiva con inversa regolare è un **isomorfismo biregolare**. In tal caso scriveremo $U \sim_b U'$.

Corollario 3.7. $U \sim_b U'$ se e solo se $\mathcal{O}(U')$ e $\mathcal{O}(U)$ sono isomorfe come algebre.

Osservazione 3.2. In un linguaggio algebrico stiamo dicendo che si potrebbe parlare di equivalenza di categorie.

Possiamo ora definire il concetto di varietà. Lo facciamo prima in un caso particolare, che sarà quello con cui lavoreremo, e poi nel caso generale:

Definizione 3.8. Una **varietà algebrica reale affine** è uno spazio topologico X dotato di un fascio $\mathcal{O}_X$ di funzioni a valori in $\mathbb{R}$ (**fascio delle funzioni regolari**), isomorfo a un insieme algebrico $V \subseteq \mathbb{R}^n$ con la topologia di Zariski e dotato di $\mathcal{O}(V)$.

Proposizione 3.9. Se $(X, \mathcal{O}_X)$ varietà algebrica reale affine e U un suo aperto di Zariski allora $(U, \mathcal{O}_{X_{|U}})$ è una varietà algebrica reale affine a sua volta.

Dimostrazione. Sia $P \in \mathcal{P}$ tale che $P^{-1}(0) = V \setminus U$. Allora U biregolare isomorfa a $W = \{(x, y) \in \mathbb{R}^{n+1} \mid x \in V \wedge yP(x) = 1\}$ e quindi $(U, \mathcal{O}_{U|_U}) \simeq (W, \mathcal{O}_W)$. □

Definizione 3.10. Una **varietà algebrica reale** è uno spazio topologico X dotato di un fascio $\mathcal{O}_X$ di funzioni a valori in $\mathbb{R}$ (**fascio delle funzioni regolari**), tale che esiste un ricoprimento finito di aperti su cui la restrizione del fascio dà una struttura di varietà affine. La topologia di X inoltre sarà detta topologia di Zariski.

Proposizione 3.11. Se $(X, \mathcal{O}_X)$ varietà algebrica reale e U un suo aperto di Zariski allora $(U, \mathcal{O}_{X_{|U}})$ è una varietà algebrica reale a sua volta.

Proposizione 3.12. Sia X un insieme unione di una famiglia di sottoinsiemi $\{X_i\}_{i \in I}$, tali che ognuno di essi sia dotato di una struttura di varietà algebrica reale e

(i) $X_i \cap X_j$ aperto in X_i per ogni $i \in I$

(ii) la struttura indotta su $X_i \cap X_j$ da X_i e X_j coincide per ogni $i, j \in I$.

Allora esiste un'unica struttura di varietà algebrica reale su X per cui ogni X_i è un aperto di Zariski e la topologia e la topologia indotta è coerente.

Quella che abbiamo dato sin qui è una descrizione che, sebbene estremamente formale, risulta poco intuitiva nell'immediato. Iniziamo chiarendo cos'è un aperto di Zariski U in V (un insieme algebrico di $\mathbb{R}^n$): un insieme algebrico è un chiuso per la topologia di Zariski su $\mathbb{R}^n$, allora $U = V \cap \bar{U}$ con ($\bar{U}$ aperto di di $\mathbb{R}^n$) sarà unioni e intersezioni finite di insiemi della forma

$$\{x \in \mathbb{R}^n \mid f_1(x) > 0 \wedge \cdots \wedge f_s(x) > 0\} \cap V$$

con $f_1, \ldots, f_s \in \mathbb{R}[X_1, \ldots, X_n]$; questo ci dice che utilizzando la topologia di Zariski non ci muoviamo dalla classe dei semialgebrici.
Una varietà algebrica reale affine è perciò uno spazio topologico con un fascio di anelli su cui si può lavorare, a meno di isomorfismi, come in un insieme algebrico di un certo $\mathbb{R}^k$ col fascio delle funzioni regolari a valori in $\mathbb{R}$. Grazie a questa struttura siamo allora in grado di ridurci a lavorare su spazi che conosciamo e possiamo maneggiare più agevolmente. Inoltre è bene sottolineare che le mappe che andiamo a considerare tra le varietà si comportano bene rispetto alla relazione che c'è tra le varietà reali algebriche e insiemi semialgebrici

Lemma 3.13. Siano $V \subseteq \mathbb{R}^n$ e $V' \subseteq \mathbb{R}^p$ due insiemi algebrici e $U \subset V$ e $U' \subset V'$ due aperti di Zariski. Se la mappa $\varphi\colon U \to U'$ è un isomorfismo biregolare, allora U e U' sono semialgebricamente omeomorfi rispetto alla topologia euclidea.

Dimostrazione. U e U' sono due semialgebrici e le entrate della mappa φ sono quozienti di polinomi. In particolare la mappa è continua e aperta, ma per ipotesi è anche bigettiva. □

Abbiamo due conseguenze importanti:

Corollario 3.14.

(i) Data una varietà reale algebrica X possiamo definire su X la topologia euclidea usando come base di aperti è gli insiemi

$$\{x \in U \mid f_1(x) > 0 \wedge \cdots \wedge f_s(x) > 0\}$$

con U aperto di Zariski per X e $f_1, \ldots, f_s$ elementi dell'anello delle funzioni regolari.

(ii) Data una varietà reale algebrica X possiamo definire su X un insieme semialgebrico come la combinazione booleana della base sopra. Se X è anche affine e $\varphi\colon X \to U$ un isomorfismo biregolare su un aperto di Zariski in un insieme algebrico. Allora un sottoinsieme S di X è semialgebrico se e solo se $\varphi(S)$ è semialgebrico nel senso usuale.

Per concludere enunciamo che cosa accade puntualmente:

Definizione 3.15. Data una varietà algebrica X, l'**anello locale dei germi di funzioni regolari nel punto** $x \in X$, che indichiamo con $\mathcal{O}_{X,x}$, è il limite degli $\mathcal{O}_X(U)$ con U intorno di x nella topologia di Zariski:

$$\mathcal{O}_{X,x} = \varinjlim \mathcal{O}_X(U)$$

Osservazione 3.3. Se $V \subseteq \mathbb{R}^n$ insieme algebrico e $x \in V$ allora $\mathcal{O}_{V,x}$ è la localizzazione $\mathcal{O}(V)_{\mathfrak{m}_x}$ per l'ideale massimale $\mathfrak{m}_{V,x}$ dei polinomi che si annullano su x.

3.2 Punti regolari

Le nozioni che vogliamo introdurre in questo paragrafo sono di tipo locale, non è quindi restrittivo dapprima supporre che la varietà che andremo a considerare sia una varietà algebrica reale affine $(X, \mathcal{O}_X)$ e quindi a meno di isomorfismi ridurci a lavorare su un insieme $V \subseteq \mathbb{R}^n$ algebrico, il cui fascio delle funzioni regolari ricordiamo è $\mathcal{O}(V) = {S_V}^{-1}\mathcal{P}(V)$. Inoltre possiamo assumere che V sia irriducibile.
Abbiamo anche definito l'anello dei germi di funzione regolari in ogni punto x e osservato che, nel caso in cui ci siamo ridotti, è $\mathcal{O}_{V,x} = \mathcal{P}(V)_{\mathfrak{m}_x}$ con $\mathfrak{m}_x < \mathcal{P}(V)$ l'ideale massimale che si annulla in x.

Introduciamo gli anelli che ci permettono di caratterizzare i punti:

Definizione 3.16. Se A è un anello noetheriano locale, con $\mathfrak{m}$ ideale massimale e $k = A/\mathfrak{m}$ 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.

Definizione 3.17. Sia $V \subseteq \mathbb{R}^n$ un insieme algebrico irriducibile. Diremo che un punto $x \in V$ è **nonsingolare** o **regolare** se l'anello locale $\mathcal{O}_{V,x}$ dei germi di funzioni regolari in x è regolare.

Gli anelli regolari hanno molte buone proprietà:

Proposizione 3.18. Sia A è un anello regolare locale, con $\mathfrak{m}$ ideale massimale e $k = A/\mathfrak{m}$ 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 $\mathfrak{m}/\mathfrak{m}^2$ su k. E in tal caso si dicono **sistema regolare** di parametri.

Dimostrazione. Vedi [ZS76] §VIII.11 □

Prima di dare la definizione generale, cerchiamo di trovare una caratterizzazione più geometrica. Diamo ora la nozione di spazio tangente rispetto alla topologia di Zariski e poi facciamo vedere che è una buona definizione:

Definizione 3.19. Sia $V \subseteq \mathbb{R}^n$ un insieme algebrico e $\mathcal{I}(V) = (p_1, \dots, p_k)$. Preso un qualsiasi $x \in V$, lo **spazio di Zariski tangente** a V in x è il sottospazio lineare di $\mathbb{R}^n$

$$T_x^Z(V) \coloneqq \ker(\mathrm{Jac}(p_1, \dots, p_k)) = \ker \left(\frac{\partial p_i}{\partial x_j} \right)_{j=1,\dots,n}^{i=1,\dots,k}.$$

Osservazione 3.4. Consideriamo ora una famiglia di generatori di tale ideale $\mathcal{I}(V) = (f_1, \dots, f_l)$ e $x \in V$

$$\mathrm{Jac}(f_1, \dots, f_k) = \left(\frac{\partial f_i}{\partial x_j} \right)_{j=1,\dots,n}^{i=1,\dots,k}$$

matrice a coefficienti nel campo residuo $\mathcal{I}(V)$ (V è irriducibile e dunque l'ideale è primo). Questo spazio è ben definito: infatti se prendiamo un altro set di generatori $(g_1, \dots, g_s)$, abbiamo che

$$g_h(t) = \sum_j a_{jh}(t) f_j(t)$$

$$\frac{\partial g_h}{\partial x_k}(t) = \sum_j \frac{\partial a_{jh}}{\partial x_k}(t) f_j(t) + a_{jh}(t) \frac{\partial f_j}{\partial x_k}(t)$$

e valutando in $x \in V$, o equivalentemente passando al campo residuo, si ha

$$\frac{\partial g_h}{\partial x_k}(x) = \sum_j a_{jh}(x) \frac{\partial f_j}{\partial x_k}(x).$$

Questo mostra che

$$\mathrm{Span}\left(\frac{\partial f_i}{\partial x_k} \right) \supseteq \mathrm{Span}\left(\frac{\partial g_i}{\partial x_k} \right)$$

e usando che anche i g_i sono generatori si ha l'uguaglianza.

Osservazione 3.5.

- Lo spazio tangente è un semialgebrico:

$$T_x^Z(V) = \bigcap_{i=1}^k \left\{ x \in \mathbb{R}^n \mid \sum_{j=1}^n \frac{\partial p_i}{\partial X_j}(z) x_j = 0 \right\}.$$

- È ben definita la funzione **rango** di x

$$\begin{aligned} r \colon V &\longrightarrow \mathbb{N} \\ x &\longmapsto r_x = \mathrm{rk}(\mathrm{Jac}(p_1, \dots, p_k)) \end{aligned}$$

Il nostro scopo ora è dimostrare che vale il seguente fatto:

Teorema 3.20. Sia $V \subseteq \mathbb{R}^n$ un insieme algebrico irriducibile. Un punto $x \in V$ è nonsingolare se e solo se

$$\dim V = \dim T_x^Z(V)$$

La dimostrazione di questo teorema non è per niente immediata, anzi dobbiamo prima provare alcuni risultati.

Lemma 3.21. Sia $x \in V$ allora $\mathfrak{m}_{V,x}/\mathfrak{m}_{V,x}^2$ e T_xV sono isomorfi come $O_{V,x}/\mathfrak{m}_{V,x}$ spazi vettoriali

Dimostrazione. Consideriamo $\mathcal{I}(x) = \mathfrak{m}_x < \mathbb{R}[X_1, \ldots, X_n]$ e definiamo la mappa:

$$\begin{array}{rccc} \theta\colon & \mathfrak{m}_x & \to & (\mathbb{R}^n)^* \\ & f & \mapsto & \sum_j \frac{\partial f}{\partial X_j}(x) X_j \end{array}$$

$\theta(X_i - x_i)$ sono una base di $(\mathbb{R}^n)^*$ e $\mathfrak{m}_x^2 = \ker\theta$, perciò è ben definito l'isomorfismo

$$\theta'\colon \mathfrak{m}_x/\mathfrak{m}_x^2 \to (\mathbb{R}^n)^*.$$

Se $(p_1, \ldots, p_k) = \mathcal{I}(V)$ allora

$$T_x(V) = \ker(\theta(p_1), \ldots, \theta(p_k))$$

e identificando il duale del tangente con il quoziente $(\mathbb{R}^n)^*$ per il generato da

$$\theta(p_1), \ldots, \theta(p_k)$$

abbiamo che la controimmagine di tale generato tramite θ' è uguale a $\mathcal{I}(V)$. Dunque $T_x(V)$ è isomorfo a $\mathfrak{m}_x/(\mathfrak{m}_x^2 + \mathcal{I}(V)) = \mathfrak{m}_{V,x}/\mathfrak{m}_{V,x}^2$. □

Osserviamo che dal lemma discende che se x è un punto regolare allora

$$\dim \mathcal{O}_{V,x} = \dim \mathfrak{m}_{V,x}/\mathfrak{m}_{V,x}^2 = \dim T_x^Z V$$

Questo ci fornisce quanto basta per dimostrare una freccia del teorema dato che vale il segue fatto:

Lemma 3.22. Sia $V \subseteq \mathbb{R}^n$ un insieme algebrico irriducibile e $x \in V$. Allora

$$\dim V = \dim \mathcal{O}_{V,x}$$

Dimostrazione. Sia d la dimensione di V. Per definizione $d = \dim \mathcal{P}(V)$, visto che V è irriducibile $\mathcal{I}(V)$ è primo e $\mathcal{O}_{V,x}$ è la localizzazione di $\mathcal{P}(V)$ per un massimale[2], vale che $\dim \mathcal{O}_{V,x} = d$.

□

[2]I massimali hanno tutti la stessa altezza perché l'anello è catenario.

In generale dai lemmi precedenti abbiamo la seguente catena di disuguaglianze:

$$\dim V = \dim \mathcal{O}_{V,x} \leq \dim \mathfrak{m}_{V,x}/\mathfrak{m}_{V,x}^2 = \dim T_x^Z V$$

Se dunque $\dim V = \dim T_x^Z V$ vale anche l'uguaglianza al centro e quindi il punto è regolare.

Vorremmo adesso dare la definizione per una varietà algebrica reale $(X, \mathcal{O}_X)$ qualsiasi. Quanto detto sin qui in realtà si estende in maniera immediata grazie al fatto che la dimensione di un semialgebrico è il massimo delle dimensioni delle componenti irriducibili e è invariante per omeomorfismo e che la nozione di fascio è una nozione che ci permette di poter operare localmente:

Definizione 3.23. Sia $(X, \mathcal{O}_X)$ una varietà algebrica reale. Un punto $x \in X$ è detto nonsingolare o **regolare in dimensione** d se l'anello locale dei germi di funzioni regolari $\mathcal{O}_{X,x}$ è una anello regolare di dimensione d. Una varietà algebrica reale è detta regolare o liscia se tutti i suoi punti sono nonsingolari.

Cerchiamo ora di capire meglio che cosa accade quando l'insieme non è irriducibile. Prima però dimostriamo una proprietà molto utile riguardo gli anelli regolari:

Lemma 3.24. Sia A un anello regolare locale di dimensione n, con $\mathfrak{m}$ ideale massimale e $k = A/\mathfrak{m}$ campo residuo. Sia q è un ideale di A, se A/q è regolare allora q è generato da elementi di $\mathfrak{m}$ le cui classi modulo $\mathfrak{m}^2$ sono indipendenti su k o equivalentemente esiste un sistema regolare di parametri che genera q.

Dimostrazione. Sia $\overline{\mathfrak{m}} = \mathfrak{m}/q$, allora l'omomorfismo di proiezione induce

$$\varphi \colon \mathfrak{m}\big/_{\mathfrak{m}^2} \longrightarrow \overline{\mathfrak{m}}\big/_{\overline{\mathfrak{m}}^2}$$

Se la dimensione di A/q è δ allora $\overline{\mathfrak{m}}\big/_{\overline{\mathfrak{m}}^2}$ è un k-spazio vettoriale di dimensione δ e φ risulta anche k-lineare. In particolare $\dim \ker(\varphi) = n - \delta$ e in q, che contiene tale nucleo, possiamo trovare $n - \delta$ elementi $x_1, \ldots, x_{n-\delta}$ le cui classi modulo $\mathfrak{m}^2$ linearmente indipendenti su k: vogliamo far vedere che sono dei generatori di q. $x_1, \ldots, x_{n-\delta}$ sono un sottoinsieme di un sistema regolare di parametri e se indichiamo con p l'ideale da loro generato A/p è un anello regolare (per questioni di dimensioni) e ha dimensione δ. Visto che $p \subseteq q$ si ha anche

$$A/p \supseteq A/p\big/_{q/p} = A/q,$$

ma A/p è un dominio quindi[3] se p fosse strettamente contenuto avremmo che $\delta = \dim A/q < \dim A/p = \delta$, assurdo. □

[3] Vedi Teorema dell'ideale principale di Krull.

Osservazione 3.6. Nel nostro caso il lemma ci dice che se un punto è regolare siamo in grado di trovare un numero ben determinato di coordinate locali: prendiamo ad esempio $V \subseteq \mathbb{R}^n$ un insieme algebrico irriducibile di dimensione δ e $x \in V$ nonsingolare, allora per definizione[4] gli anelli $\mathcal{O}_{\mathbb{R}^n,x}$ e

$$\mathcal{O}_{V,x} = \left(\mathbb{R}[X_1,\dots,X_n]/\mathcal{I}(V)\right)_{\mathfrak{m}_x} = \mathcal{O}_{\mathbb{R}^n,x}/\mathcal{I}(V)\mathcal{O}_{\mathbb{R}^n,x}$$

sono anelli regolari locali di dimensione rispettivamente n e δ. Allora per il Lemma 3.24 esistono $n-\delta$ elementi $g_1,\dots,g_{n-\delta} \in \mathcal{I}(V)_{\mathfrak{m}_x}$ che formano un sottoinsieme di un sistema regolare di parametri; nella proposizione che segue mostriamo che allora gli stessi elementi localmente possono essere usati come un sistema di coordinate.

Proposizione 3.25. Sia $V \subseteq \mathbb{R}^n$ un insieme algebrico e $x \in V$. I seguenti fatti sono equivalenti:

a) x è nonsingolare in dimensione d.

b) Esiste una componente irriducibile di V di dimensione d, che indichiamo con V', la quale è l'unica componente irriducibile di V che contiene x e x è non singolare in V'.

c) Esistono $n-d$ polinomi $p_1,\dots,p_{n-d} \in \mathcal{I}(V)$ e un intorno aperto U di x in $\mathbb{R}^n$ tale che $V \cap U = \mathcal{V}(p_1,\dots,p_{n-d}) \cap U$ e il rango della matrice jacobiana

$$\left(\frac{\partial p_i}{\partial X_j}(x)\right)$$

è uguale a $n-d$.

Dimostrazione. Dimostriamo l'equivalenza facendo vedere $a) \Rightarrow b) \Rightarrow c) \Rightarrow a)$.
$a) \Rightarrow b)$ Se x appartenesse a due componenti irriducibili l'anello $\mathcal{O}_{V,x}$ non sarebbe un dominio di integrità e quindi neanche un anello regolare.
$b) \Rightarrow c)$ Consideriamo in prima istanza solo V', l'anello locale

$$\mathcal{O}_{V',x} = \mathcal{O}_{\mathbb{R}^n,x}/\mathcal{I}(V')\mathcal{O}_{\mathbb{R}^n,x}$$

per ipotesi è regolare. Per il Lemma 3.24, riprendendo quanto detto nell'Osservazione 3.6, esiste un sistema regolare di parametri di $\mathcal{O}_{\mathbb{R}^n,x}$ tali che i polinomi $p_1,\dots,p_{n-d}$ generino $\mathcal{I}(V')\mathcal{O}_{\mathbb{R}^n,x}$ e a meno di moltiplicazione per elementi invertibili possiamo supporre che queste funzioni siano effettivamente dei polinomi. Vogliamo ora trovare un intorno di Zariski U tale per cui $(p_1,\dots,p_{n-d})\mathcal{O}(U) = \mathcal{I}(V')\mathcal{O}(U)$, o equivalentemente

$$\left(\mathcal{I}(V')/(p_1,\dots,p_{n-d})\right)\mathcal{O}(U) = 0.$$

[4]Ogni punto di $\mathbb{R}^n$, visto come insieme algebrico, è regolare.

Consideriamo $M = \mathcal{I}(V')/(p_1, \ldots, p_{n-d})$ che è un $\mathbb{R}[X_1, \ldots, X_n]$-modulo finitamente generato, il suo annullatore $\mathrm{Ann}(M)$ è un ideale non vuoto che non è contenuto in $\mathcal{I}(V)$: infatti si ha per ipotesi $M_{\mathfrak{m}_x} = 0$ e quindi $\mathfrak{m}_x \not\supseteq \mathrm{Ann}(M)$, ma dato che $x \in V$ vale anche $\mathfrak{m}_x \supseteq \mathcal{I}(V)$. Allora esiste $f \in \mathrm{Ann}(M) \setminus \mathcal{I}(V)$ e $U = V \setminus \mathcal{V}(f)$ è l'aperto che cercavamo.
Moltiplicando ognuno dei p_k con un'equazione dell'unione di tutte le altre componenti irriducibili di V si ha la tesi.
$c) \Rightarrow a)$ Supponiamo cheil minore

$$M = \left(\frac{\partial p_i}{\partial X_j}(x)\right)_{j=1,\ldots,n-d}^{i=d+1,\ldots,n}$$

della matrice jacobiana sia invertibile. La funzione data da $X \mapsto (X_1 - x_1, \ldots, X_d - x_d, p_1, \ldots, p_{n-d})$ manda x in zero e ha come differenziale una matrice triangolare a blocchi che ha sulla diagonale proprio l'identità e tale minore

$$\begin{bmatrix} I_d & 0 \\ * & M \end{bmatrix}$$

e dunque è invertibile in x. Applicando il teorema della funzione inversa[5] otteniamo un diffeomorfismo semialgebrico f da un intorno semialgebrico Ω dell'origine in $\mathbb{R}^n$ in un intorno semialgebrico W di x in $\mathbb{R}^n$ tali che

$$f((\mathbb{R}^d \times \{0\}) \cap \Omega) = V \cap W.$$

In particolare allora visto che dimensione è invariante per omeomorfismi semialgebrici si ha che $\dim V_x = d$ e quindi, visto che la dimensione può solo crescere, che $\dim \mathcal{O}_{V,x} \geq d$.
Per ipotesi localmente la varietà coincide $\mathcal{V}(p_1, \ldots, p_{n-d})$ e quindi $\mathcal{O}_{V,x}$ è un quoziente di

$$\mathcal{O}_{\mathbb{R}^n,x} \big/ (p_1, \ldots, p_{n-d})$$

che è un anello regolare di dimensione d, per questione di dimensione allora $\dim \mathcal{O}_{V,x} = d$ e i due anelli coincidono.

□

Corollario 3.26. Sia $V \subseteq \mathbb{R}^n$ un insieme algebrico irriducibile di dimensione d e $x \in V$ regolare. Allora esistono $n - d$ polinomi $p_1, \ldots, p_{n-d} \in \mathcal{I}(V)$ e un intorno aperto U di x in $\mathbb{R}^n$ tale che $V \cap U = \mathcal{V}(p_1, \ldots, p_{n-d}) \cap U$ e il rango della matrice jacobiana

$$\left(\frac{\partial p_i}{\partial X_j}(y)\right)$$

è uguale a $n - d$ per ogni $y \in U$.

[5] La funzione che stiamo considerando è semialgebrica quindi possiamo utilizzare la formulazione del Corollario 2.9.8 in [BR98].

Dimostrazione. Il corollario è un caso particolare dell'implicazione $a) \Rightarrow c)$ della proposizione precedente eccetto per il fatto che aggiunge che la condizione sul rango vale per tutti i punti di U. □

Dalla dimostrazione di $a) \Leftrightarrow b)$ si deduce anche che:

Corollario 3.27. Sia $V \subseteq \mathbb{R}^n$ un insieme algebrico e $x \in V$ un punto regolare in dimensione d. Allora esiste un intorno aperto semialgebrico U di x in V tale che $U \cap V$ è una varietà differenziabile C^∞ di dimensione d in $\mathbb{R}^n$.

Osservazione 3.7. Dato $V \subseteq \mathbb{R}^n$ un insieme algebrico e un punto regolare $x \in V$ in un intorno abbastanza piccolo è definita la struttura di varietà differenziabile C^∞ e la relativa nozione di spazio tangente; si ha che in effetti le due nozioni coincidono.

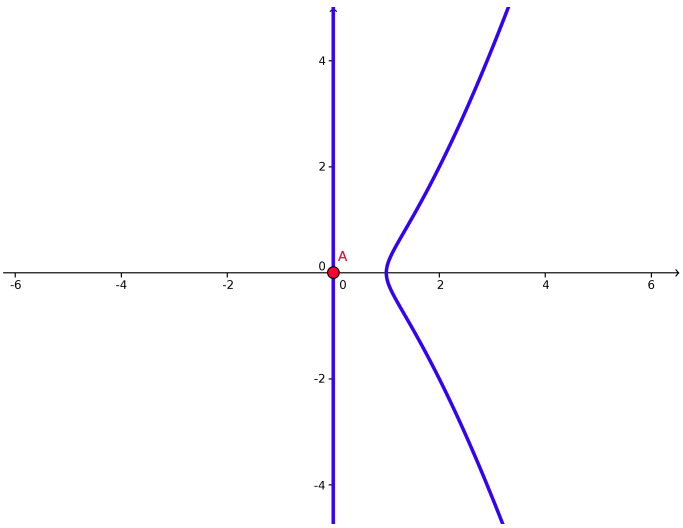
Il Corollario 3.27 e la Proposizione 3.25 giustificano l'introduzione della seguente nozione:

Definizione 3.28. Sia X un insieme reale. Un punto $x \in X$ è detto **liscio** se esiste un sistema di funzioni regolari su X tali che in un intorno del punto x siano un sistema locale di coordinate, ossia che X_x sia diffeomorfo ad un $\mathbb{R}^k$.

Riportiamo adesso due esempi con lo scopo chiarire quanto detto sin qui. Il primo mostra che è essenziale, nello studio della regolarità di un punto, tenere ben presente quali siano le funzioni ammesse e che le coordinate locali vadano scelte nell'ideale associato all'insieme considerato; il secondo invece mostra che sebbene ogni punto regolare sia liscio non vale il viceversa.

Esempio 6.

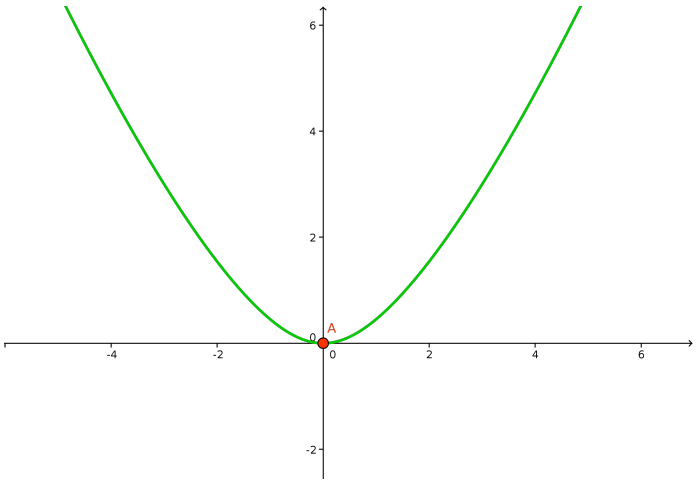
1. Consideriamo l'insieme $V = \mathcal{V}(X(Y^2 + X^2 - X^3))$ il cui luogo reale è



In un intorno dell'origine $A = (0, 0)$ coincide con $\mathcal{V}(X)$, lo jacobiano è $\left(\frac{\partial X}{\partial X}, \frac{\partial X}{\partial Y}\right)$ in A ha rango 1. Ma $A = \mathcal{V}(X) \cap \mathcal{V}(Y^2 + X^2 - X^3)$ e perciò

è intersezione di due componenti irriducibili di V e dunque non vale la condizione b) della Proposizione 3.25. Allora A non è un punto regolare di V.

2. Consideriamo l'insieme irriducibile $V = \mathcal{V}(F(X,Y))$ con $F(X,Y) = Y^3 + 2X^2Y - X^4$ il cui luogo reale è



Concentriamoci sull'origine $A = (0,0) \in \mathbb{R}^2$. Lo jacobiano

$$\frac{\partial F(X,Y)}{\partial X \partial Y} = \left(4XY - 4X^3, 3Y^2 + 2X^2\right)$$

in A è il vettore nullo e quindi questo punto non è regolare. Però lo stesso insieme coincide con $G(X,Y) = X^2 - Y(1+\sqrt{1+Y}) = 0$ il cui jacobiano è

$$\frac{\partial G(X,Y)}{\partial X \partial Y} = \left(2X, -\left(1 + \frac{Y}{2\sqrt{1+Y}} + \sqrt{1+Y}\right)\right)$$

e in A ha rango 1. Allora V è un sottovarietà differenziabile di $\mathbb{R}^2$ e A è un punto liscio (in senso differenziale).

Osservazione 3.8. Sin qui abbiamo sfruttato molte proprietà di tipo differenziale di $\mathbb{R}^n$, come il teorema della funzione implicita, che però continuano a valere anche nel caso di un campo reale qualsiasi R. La nozione di varietà differenziabile C^∞ però deve essere sostituita con quella equivalente di varietà di Nash. Rimandiamo per i dettagli a [BR98] §2.9.

Definizione 3.29. Sia V un insieme algebrico di dimensione d. Indichiamo con $\mathrm{Reg}(V)$ l'insieme dei punti regolari in dimensione d di V e con $\mathrm{Sing}(V)$ il suo complementare.

Proposizione 3.30. Sia V un insieme algebrico di dimensione d. Allora $\mathrm{Sing}(V)$ è un insieme algebrico di dimensione minore di d. In particolare $\mathrm{Reg}(V)$ è un aperto di Zariski non vuoto di V della stessa dimensione.

Dimostrazione. Sia V_1 una componente irriducibile di V. Se $\dim V_1 < \dim V$ allora $V_1 \subseteq \mathrm{Sing}(V)$ è l'unione di $\mathrm{Sing}(V_1)$ e dell'intersezione di V_1 con l'unione delle altre componenti irriducibili di V. Questa intersezione è algebrica e strettamente contenuta in V_1. Quindi possiamo assumere che V sia irriducibile.
Il teorema 3.20 dà che $\mathrm{Sing}(V)$ è un insieme algebrico mentre $\mathcal{I}(\mathrm{Sing}(V)) \subsetneq \mathcal{I}(V)$ e dunque $\dim \mathrm{Sing}(V) < \dim V$. □

3.2.1 Ideali associati alla varietà

Precisiamo con esempio una questione che potrebbe indurre in errore e che in un certo senso giustifica il prossimo capitolo:

Esempio 7. Prendiamo in $\mathbb{R}[x, y]$ gli ideali $I = (x, y)$ e $J = (x^2 + y^2)$. Siano $V = \mathcal{V}(I)$ e $W = \mathcal{V}(J)$, facilmente si vede che $V = W = \{(0, 0)\} \subseteq \mathbb{R}^2$. Gli Jacobiani in $(0, 0)$ relativi a I e J sono

$$M_I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

e $M_J = (0, 0)$; il primo ha rango massimo e il secondo no.
Qual'è la differenza? (0,0) è regolare?

L'ideale su cui andiamo a lavorare essenziale: la chiave dell'esempio è che $\mathcal{I}(W) \neq J$ e nelle nostre ipotesi consideriamo solo con ideali del tipo $\mathcal{I}(W)$. Il nostro studio infatti parte dagli insiemi reali e poi determina gli anelli di funzioni: così ci sono ideali, come J, i quali danno luogo ad anelli, come $\mathbb{R}[x, y]/(x^2 + y^2)$, che non possono essere presi in considerazione. Nel prossimo capitolo discuteremo quali sono gli ideali non buoni e quelli che non sono buoni e sopratutto come trovare questi ultimi.

Possiamo comunque introdurre una nozione di nonsingolarità che faremo vedere caratterizza gli ideali che abbiamo detto essere buoni:

Definizione 3.31. Sia $I = (p_1, \ldots, p_k)$ un ideale primo di dimensione d in $R[T_1, \ldots, T_n, X]$. Un punto di $\mathcal{V}(I)$ è detto **zero non singolare** di I se

$$\mathrm{rk} \left(\frac{\partial p_i}{\partial x_j}(x) \right)_{j=1,\ldots,n}^{i=1,\ldots,k}$$

è $n - d$.

Proposizione 3.32. Sia $I = (p_1, \ldots, p_k)$ un ideale primo di dimensione d in $R[T_1, \ldots, T_n, X]$. Se I ha uno zero non singolare allora $I = \mathcal{I}(\mathcal{V}(I))$.

Capitolo 4

Algebra Reale

La non chiusura algebrica dei campi reali, abbiamo appurato sin qui, complica abbastanza la doppia identità, geometrica e algebrica, delle varietà algebriche. Da quanto visto, ad esempio nello studio delle singolarità, il fatto che dal supporto non sia immediato risalire ad un ideale e dunque poter maneggiare algebricamente una varietà richiede del lavoro in più. In questo capitolo faremo vedere che introducendo una serie di strumenti algebrici, che per l'appunto saranno spesso detti "reali", è possibile ristabilire alcune delle corrispondenze della geometria algebrica classica. In prima istanza dimostreremo il Teorema di Artin Lang che sarà il fulcro da cui si snoderà il resto; poi dimostreremo il Nullstellensatz Reale, che non è altro che la versione equivalente dell' Hilbert Nullstellensatz, e il Positivstellensatz, che caratterizza i polinomi che sono positivi su certi semialgebrici reali; a conclusione del capitolo invece faremo vedere come dal teorema di Artin Lang si possa ottenere una soluzione al 17esimo problema di Hilbert sull'anello dei polinomi a coefficienti reali.

4.1 Il teorema di Artin Lang

Enunciamo la proprietà di Artin Lang ricordando che $\chi(k)$ è l'insieme degli ordini totali sul campo k.

Definizione 4.1. Sia k il campo dei quozienti di un anello di funzioni a valori in $\mathbb{R}^n$. Diremo che gode della proprietà di **Artin Lang (AL)** se per ogni m-upla $f_1, \dots, f_m \in k$ i seguenti fatti sono equivalenti:

i. $\{\beta \in \chi(k) \mid f_i >_\beta 0 \; i = 0, \dots, m\} \neq \varnothing$

ii. $\{x \in \mathbb{R}^n \mid f_i(x) > 0 \; i = 0, \dots, m\} \neq \varnothing$

Teorema 4.2 (Artin Lang)**.** Il campo $\mathbb{R}(X_1, \dots, X_n)$ gode della proprietà AL.

La dimostrazione del teorema è lunga e articolata, abbiamo scelto perciò di suddividerla.

Un ordine $\beta \in \chi(k)$ è detto **centrato** in $x_0 \in \mathbb{R}^n$ se il suo cono positivo contiene tutte le funzioni di k positive su x_0.

Osservazione 4.1. Data una $f \in k$, se esiste $x \in \mathbb{R}^n$ tale che $f(x) \geq 0$ allora f appartiene al cono posivo di ogni ordine centrato in x e quindi ii.⇒i. .

Consideriamo adesso i seguenti fatti dove con d indichiamo un naturale:

A_d Sia A una $\mathbb{R}$-algebra finitamente generata di dimensione d ordinabile e f un elemento che non sia un divisore di zero di A. Allora esiste un omomorfismo di algebre $\varphi\colon A \longrightarrow \mathbb{R}$ tale che $\varphi(f) \neq 0$.

B_d Sia A una $\mathbb{R}$-algebra finitamente generata di dimensione d, che sia totalmente ordinata da β e sia anche un dominio. Presi $f_1, \ldots, f_m \in A \setminus \{0\}$ qualsiasi, allora esiste $\varphi\colon A \longrightarrow \mathbb{R}$ omomorfismo di algebre tale che $\varphi(f_i)$ abbia lo stesso segno di f_i per ogni $i = 0, \ldots, m$.

C_d Sia β un ordine totale di $\mathbb{R}(X_1, \ldots, X_n)$ e $f_1, \ldots, f_m \in \mathbb{R}[X_1, \ldots, X_n] \setminus \{0\}$ allora esiste $\varphi\colon \mathbb{R}[X_1, \ldots, X_n] \longrightarrow \mathbb{R}$ omomorfismo di algebre tale che $\varphi(f_i)$ abbia lo stesso segno di f_i per ogni $i = 0, \ldots, m$.

Lemma 4.3. Per ogni $d \in \mathbb{N}$ valgono A_d, B_d e C_d.
In particolare

1. $A_d \Rightarrow C_{d+1} \Rightarrow A_{d+1}$
2. $A_d \Rightarrow B_d$

Dimostrazione. Dimostriamo il lemma con una sorta di induzione concatenata: $A_0 \simeq C_0 \simeq \mathbb{R}$ e quindi godono delle proprietà banalmente. Mostrando 1. e 2. si ha allora la tesi.
$A_d \Rightarrow C_{d+1}$. Siano $f_1, \ldots, f_m \in \mathbb{R}[X_1, \ldots, X_{d+1}] \setminus \{0\}$ con segno rispetto a β e possiamo assumere che siano anche irriducibili. Indichiamo per ogni n con L_n la chiusura reale di $(\mathbb{R}(X_1, \ldots, X_n), \beta)$, se prendiamo ordini compatibili allora $L_d \subseteq L_{d+1}$ e ogni elemento $g \in \mathbb{R}[X_1, \ldots, X_{d+1}]$ può essere visto come $g(X_{d+1}) \in L_d[X_{d+1}]$. Allora possiamo scrivere ogni polinomio della famiglia come segue

$$f_i(X_{d+1}) = \prod_j (X_{d+1} - \alpha_j)^{m_j} \prod_l ((X_{d+1} - a_l^i)^2 + b_l^{i2})^{h_l}$$

dove $\alpha_1 < \cdots < \alpha_s$ sono tutte le radici reali degli f_i in L_d (poniamo $\alpha_0 = -\infty$ e $\alpha_{s+1} = +\infty$) e $a_l^i, b_l^i \in L_d$. In questa rappresentazione il segno del polinomio è dato dalla posizione di X_{d+1} rispetto alle radici visto che solo i fattori di grado uno influiscono sul segno.
Supponiamo allora che per un certo $r \geq 0$ si abbia $\alpha_r < X_{d+1} < \alpha_{r+1}$, allora esiste $\theta \in L_d \cap (\alpha_r, \alpha_{r+1})$ che sia algebrico su $\mathbb{R}(X_1, \ldots, X_d)$ e in particolare possiamo supporre che sia intero su $\mathbb{R}[X_1, \ldots, X_d]$. Per ogni j allora $\theta - \alpha_j$ è nonnullo e dunque esistono $c_j \in L_d$ e $\varepsilon_j \in \{-1, +1\}$ tali che

$$\theta - \alpha_j = c_j^2 \varepsilon_j$$

dove stiamo usando che il campo L_d è la chiusura reale e dunque contiene tutte le radici dei numeri positivi. Sia ora A la $\mathbb{R}$-algebra generata da $X_1, \ldots, X_d, \theta$,

a_j^i, b_j^i, c_j, dato che è intera su $\mathbb{R}[X_1, \ldots, X_d]$ ha dimensione d per il lemma di normalizzazione di Noether e rientra allora nelle ipotesi di A_d. Allora esiste un omomorfismo di algebre $\varphi\colon A \longrightarrow \mathbb{R}$ tale che $\varphi(c_1 \cdots c_s \cdot \theta) \neq 0$.
Possiamo definire allora il morfismo

$$\begin{array}{rccccc} \psi\colon & \mathbb{R}[X_1, \ldots, X_d] & \longrightarrow & \mathbb{R} & & \\ & X_i & \longmapsto & \varphi(X_i) & i = 1, \ldots, d \\ & X_{d+1} & \longmapsto & \varphi(\theta) & & \end{array}$$

Allora $\psi(f_i) = f_i(\theta)$ e il segno è quello giusto per la scelta di theta.

$C_l \Rightarrow A_l$ Ovviamente data A finitamente generata di dimensione l possiamo, a meno di quozientare per un ideale primo P tale che $f \neq 0 \mod P$, supporre che A sia un dominio. Per il teorema di normalizzazione di Noether A è intera su $R = \mathbb{R}[X_1, \ldots, X_l]$ (UFD⇒normale) e detto $F_l = \mathbb{R}(X_1, \ldots, X_l)$ e K il campo dei quozienti di A si ha che K/F_l è algebrica

$$\begin{array}{ccc} A & \subset & K \\ \cup & & \cup \\ R & \subset & F_l \end{array}$$

e $s \coloneqq [K : F_l]$. I campi a caratteristica zero sono separabili e dunque vale il teorema dell'elemento primitivo e $K = F_l(\theta)$. È lecito supporre che θ sia intero e per la normalità di R si ha che il polinomio minino di teta ha coefficienti in R, ossia $\mu(t) \in R[t]$. Per quanto appena detto allora il discriminate del campo $\delta = disc(K) \in \mathbb{R}[X_1, \ldots, X_l]$. Facciamo vedere come tutto questo ci permette di trovare il morfismo voluto.
Sia $f \in A \setminus \{0\}$ mostriamo che $\delta \cdot f \in \mathbb{R}[X_1, \ldots, X_l]$. Dato che $f \in A \subseteq K = F_l(\theta)$ allora esistono $b_0, \ldots, b_{s-1} \in F_l$ tali che

$$f = b_0 + \cdots + b_{s-1}\theta^{s-1}.$$

Se $Gal(K/F_l) = \{\sigma_1 = id, \ldots, \sigma_d\}$ e $t_i \in A$ per $i = 2, \ldots, d$ sono i coniugati di θ, vale che

$$\sigma_j(f) = b_0 + \cdots + b_{s-1}t_j^{s-1}.$$

Cosicché otteniamo il sistema

$$\begin{bmatrix} 1 & \theta & \cdots & \theta^{s-1} \\ 1 & t_2 & \cdots & t_2^{s-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & t_s & \cdots & t_s^{s-1} \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ \vdots \\ \vdots \\ b_{s-1} \end{bmatrix} = \begin{bmatrix} \sigma_1(f) \\ \vdots \\ \vdots \\ \sigma_s(f) \end{bmatrix}$$

e detta M la matrice del sistema e $t_0 = \theta$ notiamo che $(\det M)^2 = \prod_{i<j}(t_i - t_j)^2 = disc(K) = \delta$.
Allora posta M_k la matrice M in cui la colonna $k$esima è stata sostituita con il vettore dei termini noti, la regola di Cramer dà che

$$b_k = \frac{\det M_k}{\det M}$$

e visto che $\theta, t_2, \dots, t_s \in A$ e $\sigma_j(f) \in A$ per ogni i, si ha che $\det M_k \in A$ e quindi $b_k \cdot \delta \in A$. Ma allora

$$b_k \cdot \delta \in A \cap F_l = \mathbb{R}[X_1, \dots, X_l].$$

Perciò $\delta \cdot f = c_0 + \cdots + c_{s-1}\theta^{s-1}$ con $c_j \in \mathbb{R}[X_1, \dots, X_l]$ e detto $\rho(t) = \sum_{i=0}^{s-1} c_i t^i \in R[t]$, poniamo $h = \gcd(\rho, \mu)$. Allora esistono $a, b \in R[t]$ tali che

$$h(t) = a(t)\rho(t) + b(t)\mu(t)$$

valutando in θ otteniamo $a(\theta)\delta f = h(\theta) \in R$. Questo ragionamento in effetti vale per un qualsiasi $y \in A$ e dunque vale che

$$A \subseteq B \coloneqq \mathbb{R}[X_1, \dots, X_l, \theta, \frac{1}{\delta}] \subseteq K$$

Perciò se riusciamo a definire un morfismo di $\mathbb{R}$-algebre $\psi\colon B \to \mathbb{R}$ in modo che $\psi(f) \neq 0$ la restrizione sarà il morfismo cercato.
Per trovare un tale morfismo in effetti ci basta $\varphi\colon \mathbb{R}[X_1, \dots, X_l] \to \mathbb{R}$ tale che $\varphi(h \cdot \delta) \neq 0$ e $\varphi(\mu(t)) = \mu_\varphi(t)$ abbia una radice $\alpha \in \mathbb{R}$. Infatti, ponendo

$$\begin{array}{rccc} \psi\colon & B & \longrightarrow & \mathbb{R} \\ & R & \longmapsto & \varphi(R) \\ & \frac{1}{\delta} & \longmapsto & \varphi(\delta)^{-1} \\ & \theta & \longmapsto & \varphi(\alpha) \end{array}$$

avremmo concluso.
Trovare il morfismo φ è equivalente ad individuare un punto $a = (a_1, \dots, a_{l+1}) \in \mathbb{R}^{l+1}$ tale che

$$\begin{cases} \delta(a_1, \dots, a_{l+1}) \cdot h(a_1, \dots, a_{l+1}) \neq 0 \\ \mu(a_1, \dots, a_{l+1}) = 0 \end{cases}$$

Consideriamo allora $q_0, \dots, q_k \in R[t]$ una sequenza di Sturm (1.19) per $\mu(t)$ e $M \in R$ tale che $-M < \theta < M$ per un ordine che estenda quello di F_l a K. Allora visto che μ ha una radice reale θ nella chiusura reale di F_l

$$v(\mu, 1; M) - v(\mu, 1; -M) > 0$$

. Se prendiamo ora la lista

$$L = \{\delta, h, q_0(-M), \dots, q_k(-M), q_0(M), \dots, q_k(M)\}$$

C_l ci dà che esiste

$$\varphi\colon \mathbb{R}[X_1, \dots, X_l] \to \mathbb{R}$$

tale che per ogni $p \in L$ $sign(p) = sign(\varphi(p))$ e dunque $\varphi(h \cdot \delta) \neq 0$ e visto che i $\varphi(q_j)$ sono una sequenza di Sturm per $\mu_\varphi(t)$ esiste una radice $\alpha \in [\varphi(-M), \varphi(M)]$. Allora φ è proprio il morfismo cercato.

$A_d \Rightarrow B_d$ Presi $f_1, \dots, f_m \in A \setminus \{0\}$ come abbiamo fatto per la prima implicazione possiamo prendere L_d la chiusura reale e degli interi su A tali che $f_i = \varepsilon_i c_i^2$. Presa poi l'algebra B generata dai c_j e A di dimensione d abbiamo che esiste $\varphi\colon B \to \mathbb{R}$ tale che $\varphi(c_1 \cdots c_m) \neq 0$. Allora $\varphi|_A$ è l'omomorfismo in tesi. $\square$

Abbiamo mostrato che i fatti A_d, B_d e C_d sono veri per ogni $d \in \mathbb{N}$, sebbene siano interessanti di per se ricordiamo che il nostro scopo è dimostrare il Teorema di Artin Lang:

Dimostrazione. i.⇒ii. (AL) Siano $f_1, \ldots, f_m \in \mathbb{R}(X_1, \ldots, X_n) = k$ tali che esiste $\chi(k)$ tale che $f_i >_\beta 0$ $i = 0, \ldots, m$; il nostro scopo trovare un $x \in \mathbb{R}^n$ tale che $f_i(x) > 0$ per ogni $i = 0, \ldots, m$. Possiamo considerare la restrizione $\bar{\beta} = \beta|_R$, con $R = \mathbb{R}[X_1, \ldots, X_n]$, allora per ogni $g \in \{f_1, \ldots, f_m\}$ esistono $p, q \in R$ tali che

$$g = \frac{p}{q}$$

e visto che $\bar{\beta}$ è di anelli abbiamo che

$$sign(g) = sign(p) \cdot sign(q).$$

Dunque usando che vale B_n con $A = \mathbb{R}[X_1, \ldots, X_n]$ e $\{p_i, q_i\}_{i=0,\ldots,m}$ otteniamo

$$\begin{array}{rccccc} \varphi\colon & \mathbb{R}[X_1, \ldots, X_n] & \longrightarrow & \mathbb{R} & \\ & X_i & \longmapsto & a_i & i = 1, \ldots, m \end{array}$$

Allora dato che $f_i >_\beta 0$

$$\varphi(f_i) = \frac{p_i(a_1, \ldots, a_n)}{q_i(a_1, \ldots, a_n)} > 0$$

e dunque il punto che cercavamo è proprio $(a_1, \ldots, a_n) \in \mathbb{R}^n$. □

Osservazione 4.2. Il teorema di Artin Lang afferma che in $\mathbb{R}(X_1, \ldots, X_n)$ essere positivo vuol dire essere positivo. Spieghiamoci, la frase precedente non è una tautologia ma sottolinea la coerenza della teoria dei campi reali rispetto alla nozione comune di positività; infatti AL ci dice che una funzione è ovunque positiva, nel senso positiva sul supporto, è positiva a prescindere dall'ordine si sceglie per il campo. Già da qui si comincia dunque a intravedere come la struttura algebrica arricchita di quella data dall'ordine permetta di ampliare la quantità di informazione gestibile, dandoci speranza di ristabilire la dualità tanto cara allo studio delle varietà.

Durante tutte le dimostrazioni non abbiamo mai usato proprietà di $\mathbb{R}$ che non fossero quelle che ha un qualsiasi campo reale. La dimostrazione del Teorema 4.2 perciò è perfettamente ricalcabile per un campo reale R qualsiasi e dà luogo ad un principio più generale che rientra sempre sotto il nome di Artin Lang:

Teorema 4.4 (Artin Lang)**.** Sia R un campo reale chiuso. Allora il campo $R(X_1, \ldots, X_n)$ gode della proprietà **AL**.

In letteratura si trovano molti varianti equivalenti del teorema di Artin Lang, più o meno adatte alle sue applicazioni in diverse aree della matematica come la formulazione di Becker:

Teorema 4.5 (Artin-Lang [Bec81])**.** Sia F un campo reale e A un dominio finitamente generato su F con campo delle frazioni k. Dati $a_1, \dots, a_n \in A \setminus \{0\}$, elementi qualsiasi, i seguenti fatti sono equivalenti:

- Esiste una chiusura reale R di F e un F-omomorfismo $\varphi : A \longrightarrow R$ tale che:
  - $\varphi(a_i) > 0, i = 1, \dots, n$;
  - $\mathfrak{M} = \ker \varphi$ è un ideale massimale regolare, ossia $A_{\mathfrak{M}}$ è regolare[1].
- esiste un ordine σ di k tale per cui $a_1, \dots, a_n \in \sigma$.

Ci sono poi delle varianti che hanno enunciati più adatti all'uso diretto:

Teorema 4.6 (Teorema d'omomorfismo di Artin Lang [BR98])**.** Sia R un campo reale chiuso e A un R-algebra di tipo finito. Se esiste un omomorfismo di R-algebre

$$\varphi\colon A \longrightarrow R_1$$

con R_1 un'estensione reale chiusa di R, allora esiste un omomorfismo di R-algebre

$$\psi\colon A \longrightarrow R.$$

Di questo teorema vogliamo riportare una dimostrazione che passa attraverso il Principio di Tarski-Seidenberg, per sottolineare che quello che fa funzionare in realtà tutto questo "macchinario"sia il teorema di Sturm.
Enunciamo prima il seguente corollario di TS:

Proposizione 4.7. Sia R_1 un'estensione reale chiusa di un campo reale chiuso R e $\mathcal{B}(X)$ una combinazione di equazioni e disequazioni polinomiali nelle variabili $X = (X_1, \dots, X_n)$ a coefficienti in R. Se $\mathcal{B}(y)$ vale per qualche $y \in R_1^n$ allora esiste $x \in R^n$ tale che $\mathcal{B}(x)$.

Dimostrazione. Indichiamo con $T = (X_1, \dots, X_{n-1})$ e mostriamo il risultato per induzione su n. Il caso $n = 0$ è banale.
Se $n \geq 1$, per ipotesi esiste $y = (t, x_n) \in R_1^n$ con $t = (t_1, \dots, t_{n-1})$ tale che $\mathcal{B}(y)$, allora per il Teorema 1.23 esiste un sistema $\mathcal{C}(T)$ che ha $t \in R_1^{n-1}$ come soluzione. Per ipotesi induttiva esiste $u \in R^{n-1}$ tale che valga $\mathcal{C}(u)$ e quindi sempre per TSI esiste $x_n \in R$ tale che $x = (u, x_n) \in R^n$ sia una soluzione per $\mathcal{B}(X)$. □

Dimostriamo ora il teorema di omomorfismo di Artin Lang:

Dimostrazione (Teorema 4.6). Possiamo supporre che A sia della forma $R[X_1, \dots, X_n]/I$ con I un ideale generato da $f_1, \dots, f_s$. Indichiamo con b_i le immagini tramite φ della classe modulo I di X_i per $i = 1, \dots, n$; allora $(b_1, \dots, b_n) = b \in R_1^n$ è una soluzione per il sistema

$$f_1 = \cdots = f_s = 0$$

[1] Vedi Definizione 3.16

e dunque per la proposizione precedente ne esiste anche una del tipo $a = (a_1, \ldots, a_n) \in R^n$. L'omomorfismo

$$\begin{array}{rccl} \Psi\colon & \mathbb{R}[X_1, \ldots, X_n] & \longrightarrow & R \\ & X_i & \longmapsto & a_i \quad i = 1, \ldots, s \end{array}$$

allora passa a quoziente e ci dà lo ψ voluto. □

Osservazione 4.3. L'idea morale del teorema d'omomorfismo è che tramite φ, visto che è un omomorfismo di R-algebre, si può portare indietro il cono positivo di R_1 e prendere un ordinamento generato a partire da questo insieme in A. A è un'algebra di tipo finito dunque possiamo prenderne dei generatori, che quindi saranno nonnulli, e tramite B_d ottenere ψ.

4.1.1 Artin-Lang su insiemi algebrici

Vorremmo poter dimostrare il teorema di Artin Lang per gli insiemi algebrici, ma consideriamo il seguente esempio:

Esempio 8. Prendiamo l'ombrello di Cartan, $V = \{z(x^2+y^2) = x^3\}$ in $\mathbb{R}^3$, questa abbiamo detto che è una superficie irriducibile e connessa che ha un manico in corrispondenza dell'asse z. Allora $f = x^2 + y^2 - z^2 \in \mathcal{P}(V)$ è negativa su l'asse z ma è somma di quadrati in $\mathrm{Quot}(\mathcal{P}(V))$:

$$f = x^2 + y^2 - \frac{x^6}{(x^2+y^2)^2} = \frac{3x^4y^2 + 3x^2y^2 + y^6}{(x^2+y^2)^2}$$

Passando dunque agli insiemi algebrici non è più vero che una somma di quadrati è ovunque positiva. Come chiaro dall'esempio il problema sorge al momento in cui presa una funzione regolare su tutta la varietà che si scrive come somma di quadrati può succedere che uno degli addendi abbia denominatore che si annulla valutando in un certo punto; in tal caso cambiando rappresentante non si ha la certezza, anzi succede solo per insiemi particolari, di ottenere un altro quadrato. Si può dire qualcosa di più sui punti danno luogo a questo fenomeno:

Proposizione 4.8. Sia R un campo reale chiuso, $V \subseteq R^n$ un insieme algebrico di dimensione d e $f \in \mathcal{P}(V)$. Indicando con $k = \mathrm{Quot}(\mathcal{P}(V))$ seguenti fatti sono equivalenti:

i. $f \in \sum k^2$

ii. f è non negativo su un aperto di Zariski non vuoto di V.

Dimostrazione. Supponiamo che

$$f = \frac{g_1^2}{h_1^2} + \cdots + \frac{g_s^2}{h_s^2}$$

con $g_i, h_i \in \mathcal{P}(V)$ e $h_i \neq 0$ per ogni $i = 1, \ldots, s$. Consideriamo $Z = \mathcal{V}_V(h_1, \ldots, h_s) \subsetneq V$. Se $x \in V \setminus Z$ allora $f(x) \geq 0$.

Se $f(x) \geq 0$ per ogni $x \in U$, un aperto di Zariski non vuoto di V, e sia $Z = V \setminus U$. Prendiamo $h \in \mathcal{P}(V)$ tale che $Z = h^{-1}(0)$, si ha che $h \neq 0$ in $\mathcal{P}(V)$. Supponiamo che f non sia una somma di quadrati in k. Allora esiste un ordine di k tale per cui f è negativo, dunque detta L la chiusura reale di k rispetto tale ordine, esiste una radice quadrata di $-f$ in L e un omomorfismo di R-algebre

$$(\mathcal{P}(V)_h)[T]/(fT^2 + 1) \longrightarrow L$$

e quindi per il Teorema d'omomorfismo di Artin-Lang esiste un punto di V tale che $h(x) \neq 0$ e $f(x) < 0$, assurdo. □

Osservazione 4.4. Se $f = g/h$ dove g e h sono polinomi, allora $f = gh/h^2$ e $gh(x) < 0$ se e solo se f è definito in x e $f(x) < 0$.

4.2 Nullstellensatz Reale e Radicale Reale

Definizione 4.9. Sia A un anello commutativo e $I \subseteq A$ un ideale, diremo che è **reale** se per ogni successione di elementi $a_1, \ldots, a_p \in A$ vale

$$a_1^2 + \cdots + a_p^2 \in I \Longrightarrow a_i \in I, \ \forall i = 1, \ldots, p.$$

Ricordando che re è l'insieme delle somme finite di quadrati:

Definizione 4.10. Sia A un anello commutativo e $I \subseteq A$ un ideale, il **radicale reale** di I è l'insieme

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

Enunciamo alcune buone proprietà degli ideali reali:

Proposizione 4.11. Sia A un anello commutativo e $I \subseteq A$ un suo ideale. Allora

1. Se I è reale è anche radicale.
2. $\sqrt[re]{I} = I$ se e solo se I è reale.
3. $\sqrt[re]{I}$ è un ideale reale, in particolare se A è noetheriano ogni suo primo minimale P è reale.
4. $\sqrt[re]{I} = \bigcap P$ con P che varia tra tutti i primi reali su I.

Dimostrazione.

1. Facciamo vedere che se $x^n \in I$ allora $x \in I$ per induzione forte su n. Se n è pari allora $n = 2m$, allora $x^m \in I$ con $m < n$ e per ipotesi induttiva si ha la tesi; la tesi si ottiene analogamente nel caso in cui $n = 2m - 1$ osservando che $x \cdot x^n = x^{2m} \in I$.
2. È ovvio.

3. Dalla definizione non è chiaro che $\sqrt[re]{I}$ sia un ideale, in particolare è da dimostrare la chiusura additiva di questo insieme. Prendiamo $f, g \in \sqrt[re]{I}$, allora per definizione esistono $r, r' \in \mathbb{N}$ e $s, t \in re$ tali per cui $f^{2r} + s \in I$ e $g^{2r'} + t \in I$. A meno di maggiorazione, possiamo supporre $r = r'$, consideriamo adesso l'elemento $(f+g)^{4r} + (f-g)^{4r}$, vogliamo mostrare che esiste un elemento $u \in re$ 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

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

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 $t \in re$. 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 $y \in P$. Per ipotesi $y \notin P$ e dunque $a \in P$, che implica evidentemente che $P = \sqrt[re]{P}$.

4. Basta osservare che $\sqrt[re]{I}$ è un ideale radicale e che per ogni $K, J \in A$ ideali

$$\sqrt[re]{K \cap J} = \sqrt[re]{K} \cap \sqrt[re]{J} = \sqrt[re]{K \cdot J}.$$

□

Teorema 4.12 (Nullstellensatz Reale)**.** Sia R un campo reale chiuso e $I \subseteq R[X_1, \ldots, X_n]$ un ideale. Allora

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

se e solo se I è reale.

Dimostrazione. Indichiamo con A $R[X_1, \dots, X_n]$. Supponiamo che $\mathcal{I}(\mathcal{V}(I)) = I$, allora prendiamo una famiglia di polinomi $a_1, \dots, a_p \in A$ tali che $a_1^2 + \cdots + a_p^2 \in I$. Per ogni $x \in \mathcal{V}(I)$ allora $a_1^2(x) + \cdots + a_p^2(x) = 0$ e dunque $a_i(x) = 0$. Allora $a_i \in \mathcal{I}(\mathcal{V}(I)) = I \ \forall i = 1, \dots, p$, ossia I è reale.
Viceversa supponiamo che I sia reale. Per la Proposizione 4.11, visto che A è noetheriano possiamo supporre che sia primo. Detto $S = {}^{A}\!/_{I}$, S è un dominio e se prendiamo $f \notin I$ allora esiste per Artin Lang (proprietà A_n) un omomorfismo di algebre

$$\varphi \colon S \to R$$

tale che $\varphi(f) \neq 0$. Consideriamo $y = (\varphi(\bar{X}_1), \dots, \varphi(\bar{X}_n))$, dove con $\bar{p}$ abbiamo indicato la classe modulo I di un polinomio $p \in A$, allora deve valere che $f(y) \neq 0$. Ma $y \in \mathcal{V}(I)$ e quindi $f \notin \mathcal{I}(\mathcal{V}(I))$. Abbiamo quindi fatto vedere che non esiste $f \in \mathcal{I}(\mathcal{V}(I)) \setminus I$, ossia che i due ideali concidono. □

Grazie a questo teorema otteniamo l'oggetto algebrico che svolge il ruolo analogo al radicale è proprio il radicale reale:

Corollario 4.13. Sia R un campo reale chiuso e $I \subseteq R[X_1, \dots, X_n]$ un ideale. Allora

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

Dimostrazione. Dal Teorema 4.12 deriva $\mathcal{I}(\mathcal{V}(I))$ è il più piccolo ideale reale che contiene I che dalla Proposizione 4.11 sappiamo essere proprio $\sqrt[re]{I}$. □

Corollario 4.14. Sia $V \subseteq R^n$ un insieme algebrico e $I \subseteq \mathcal{P}(V)$ un ideale. Allora $p \in \mathcal{P}(V)$ si annulla su $\mathcal{V}_V(I)$ se e solo se esistono un numero finito di funzioni polinomiali $q_1, \dots, q_s \in \mathcal{P}(V)$ e un intero m tali che $p^{2m} + q_1^2 + \cdots + q_s^2 \in I$, ossia

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

4.3 Positivstellensatz

I semialgebrici sono gli insiemi su cui si snoda naturalmente la geometria algebrica reale, dunque più che a controllare algebricamente i luoghi di zeri siamo interessati a studiare i luoghi di positività.
Come fatto già nel terzo capitolo concentriamoci, prima di parlare di varietà e dunque di funzioni regolari, su un caso più semplice ossia su gli insiemi algebrici. Dobbiamo però ampliare la teoria sui coni sviluppata nel primo capitolo e la nozione di radicale del paragrafo precedente.

Consideriamo un anello commutativo con identità con un preordine (A, σ)[2] e introduciamo la nozione di σ-radicale:

Definizione 4.15. Sia $I \subseteq A$ un ideale, il **σ-radicale** è l'insieme

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

[2] Vedi1.3

Definizione 4.16. I è detto **σ-reale** se e solo se $\sqrt[\sigma]{I} = I$.

Definizione 4.17. Sia $P \subset A$ un ideale primo, consideriamo adesso $k(P) = \mathrm{Quot}(A/P)$ il *campo residuo* e le sue classi $\overline{a} := a + P \in k(P)$.

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

Ci sarà comodo avere un'altra scrittura di questo insieme:

Lemma 4.18.

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

Dimostrazione. Se $x \in k(P)$ allora esistono $\alpha, \beta \in A/P$ tali che $x = \frac{\alpha}{\beta}$, dove $\alpha = \overline{a}$ e $\beta = \overline{b}$.
Dunque

$$\sum x_i^2 \overline{s} = \sum \left(\frac{\alpha_i}{\beta_i} \right)^2 \overline{s} = \sum \frac{\alpha_i^2}{\beta_i^2} \overline{s} = \sum \frac{\widetilde{\alpha}_i^2}{\beta^2} \overline{s}$$

Dove $\beta = \gcd(\beta_i)$. Sfuttando la chiusura di σ rispetto a prodotto e somma e che per ogni $a \in A$ allora $a^2 \in \sigma$ otteniamo:

$$\sum x_i^2 \overline{s} = \frac{\overline{t}}{\beta^2}$$

con $t \in \sigma$. □

Osservazione 4.5. Se $\sigma = \sum A^2$ e A è un anello di polinomi a coefficienti reali ritroviamo quanto già detto.

Lemma 4.19. Sono equivalenti:

1. $\overline{\sigma}$ è un preordine[3]
2. $-1 \notin \overline{\sigma}$
3. $\sqrt[\sigma]{P} = P$
4. dati $r \in \sigma$ e $a \in A$, se $a^2 + r \in P$ allora $a \in P$

Dimostrazione. Chiaramente i primi due e gli ultimi 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 $P \subsetneq \sqrt[\sigma]{P}$. Suppondo di avere un elemento nel radicale non in P si dimostra facilmente che possiamo ottenere una scrittura di -1 in $\overline{\sigma}$. □

[3]Definizione 4.17

Grazie a questi due Lemmi si può dimostrare, ricalcando quella della Proposizione 4.11, la seguente:

Proposizione 4.20.

- $\sqrt[\sigma]{I}$ è un ideale e ogni suo primo minimale P è σ-reale.
- $\sqrt[\sigma]{I} = \bigcap P$ con P che varia tra tutti i primi σ-reali su I.
- Un ideale P primo in A è σ-reale se e solo se $\overline{\sigma}$ è un preordine su $k(P)$.

Definizione 4.21. Sia α un precono per un anello A e $(b_i)_{i\in I}$ una famiglia di elementi di A. Indicando con M il monoinde[4] moltiplicativo generato da tale famiglia, chiameremo **precono generato** da $(b_i)_{i\in I}$

$$\alpha[(b_i)_{i\in I}] \coloneqq \{p + \sum_{j=1}^{r} q_j a_j \mid \forall j\, p, q_j \in \alpha,\ a_j \in M\}.$$

Proviamo ora un caso speciale della Proposizione 4.8:

Corollario 4.22. Sia R un campo reale chiuso, $V \subseteq R^n$ un insieme algebrico e $f \in \mathcal{P}(V)$. Indicando con $k = \mathrm{Quot}(\mathcal{P}(V))$ e $V \subseteq R^n$ un insieme algebrico irriducibile, $k = \mathrm{Quot}(\mathcal{P}(V))$ il campo residuo di $\mathcal{I}(V)$ e

$$W = \{x \in V \mid g_1(x) \geq 0, \dots g_s(x) \geq 0\},$$

con σ è il precono di $\mathcal{P}(V)$ generato da $g_1, \dots, g_s$, preso $f \in \mathcal{P}(V)$. I seguenti fatti sono equivalenti:

i. $f \in \bar{\sigma}$

ii. f è non negativo su un aperto di Zariski non vuoto di W per la topologia di sottospazio indotta da V.

Dimostrazione. Supponiamo che

$$f = \frac{a_1^2}{s_1^2} + \dots + \frac{a_p^2}{s_p^2} + \sum_{j=1}^{r} \frac{b_j^2}{t_j^2} e_j$$

con $a_i, s_i, b_j, t_j \in \mathcal{P}(V)$ e $s_i, t_j \neq 0$ per ogni $i = 1, \dots, p$ e $j = 1, \dots, r$ e e_j nel monoinde generato da $g_1, \dots, g_s$. Consideriamo $Z = \mathcal{V}_V(s_1, \dots, s_p, t_1, \dots, t_r) \subsetneq V$. Se $x \in (V \setminus Z) \cap W$, che è aperto per la topologia di sottospazio, allora $f(x) \geq 0$.
Se $f(x) \geq 0$ per ogni $x \in U$, un aperto di Zariski non vuoto di W allora esiste U' aperto di V tale che $U = U' \cap W$, e sia $Z = V \setminus U'$. Prendiamo $h \in \mathcal{P}(V)$ tale che $Z = h^{-1}(0)$, si ha che $h \neq 0$ in $\mathcal{P}(V)$. Supponiamo che f non stia $\bar{\sigma}$. Allora esiste un ordine in $\chi_{\bar{\sigma}}(k)$ tale per cui f è negativo, dunque detta L la

[4]Un **monoide** è un insieme munito di una singola operazione binaria, chiuso rispetto a quest'ultima e tale per cui esista un elemento neutro e valga la proprietà associativa.

chiusura reale di L rispetto tale ordine, esiste una radice quadrata di $-f$ in k e un omomorfismo di R-algebre

$$(\mathcal{P}(V)_h)[T]/(fT^2+1) \longrightarrow L$$

e quindi per il Teorema d'omomorfismo di Artin-Lang esiste un punto di V tale che $h(x) \neq 0$ e $f(x) < 0$, se facciamo vedere che $x \in W$ abbiamo trovato l'assurdo. Ma per costruzione $g_1, \ldots, g_s$ sono positivi e quindi deve valere che $g_j(x) \geq 0$. □

Teorema 4.23 (Positivstellensatz)**.** Sia $V \subset R^n$ un insieme algebrico e $g_1, \ldots, g_s \in \mathcal{P}(V)$. Sia

$$W = \{x \in V \mid g_1(x) \geq 0, \ldots g_s(x) \geq 0\},$$

e σ è il precono di $\mathcal{P}(V)$ generato da $g_1, \ldots, g_s$, sia $f \in \mathcal{P}(V)$. Allora:

i. Per ogni $x \in W$ $f(x) \geq 0$ se e solo se $\exists m \in \mathbb{N}\ \exists g, h \in \sigma$ tali che $fg = f^{2m}+h$.

ii. Per ogni $x \in W$ $f(x) = 0$ se e solo se $\exists m \in \mathbb{N}\ \exists h \in \sigma$ tali che $f^{2m} + h = 0$.

Osservazione 4.6. Questo teorema ci dà delle condizioni algebriche necessarie e sufficienti per dire se un polinomio è positivo o meno su un semialgebrico.

Dimostrazione. Assumiamo senza perdere di generalità V irriducibile. Osserviamo che posto $\alpha = \sigma \cap R[X_1, \ldots, X_n]$ abbiamo che $\bar{\alpha}$ coincide con l'estensione a precono di $\mathrm{Quot}(\mathcal{P}(V))$ di σ, allora potremo parlare di $\bar{\sigma}$ per indicare entrambi questi ultimi.
Inoltre se per ogni $x \in W$ $f(x) \geq 0$ allora per il Corollario 4.22 $f \in \bar{\sigma}$ ossia

$$f = \frac{s}{c^2} \text{ con } c \in R[X_1, \ldots, X_n] \setminus \mathcal{I}(V), s \in \alpha$$

$$fc^2 - s = d \in \mathcal{I}(V) \subset \sigma$$

allora detto $g = c^2 > 0$

$$fg \equiv s \mod \mathcal{I}(V).$$

Alla luce di queste osservazioni dimostriamo gli asserti:

i. Supponiamo che esistano $m \in \mathbb{N}$ e $g, h \in \sigma$ tali che $fg = f^{2m}+h$ e prendiamo $x \in W$. Valutando abbiamo

$$f(x)g(x) = f^{2m}(x) + h(x) \geq 0$$

e visto che $g(x) \geq 0$ deve valere anche $f(x) \geq 0$.
Viceversa se per ogni $x \in W$ $f(x) \geq 0$ allora abbiamo mostrato che esistono $g = c^2 \in \sigma \setminus \{0\}$, $s \in \alpha$ e $d \in \mathcal{I}(V) \subset \sigma$ tali che $fg = s + d$. Per concludere dobbiamo far vedere che s può essere scritto come $f^{2m} + h$ con $h \in \sigma$ e $m \in \mathbb{N}$. Dato che $f \in \sigma$ allora usando le proprietà di precono abbiamo che modulo l'ideale associato alla varietà valgono le seguenti uguaglianze

$$s + f^{2m} = fg + f^{2m}$$

$$s + f^{2m} = f(g + f^{2m-1})$$

posto $q = g + f^{2m-1} \in \sigma$ allora abbiamo la scrittura voluta.

ii. Supponiamo che esistano $m \in \mathbb{N}$ e $h \in \sigma$ tali che $f^{2m} + h = 0$ e prendiamo $x \in W$. Valutando abbiamo

$$-h(x) = f^{2m}(x) \geq 0$$

e visto che $h(x) \geq 0$ deve valere anche $h(x) = 0$ e quindi $f(x) = 0$.
Viceversa se per ogni $x \in W$ $f(x) = 0$ allora abbiamo sia che $f(x) \geq 0$ sia che $-f(x) \geq 0$ e quindi per i. $\exists m \in \mathbb{N}\ \exists g, s \in \sigma$ tali che

$$-fg = (-f)^{2m} + s = f^{2m} + s$$

$$f^{2m} + s + fg = 0$$

ma per quanto visto $f \in \sigma$ e quindi $h = fg + s \in \sigma$, da cui $f^{2m} + h = 0$.

□

Corollario 4.24. Sia $V \subset R^n$ un insieme algebrico e $g_1, \ldots, g_s \in \mathcal{P}(V)$. Sia

$$W = \{x \in V \mid g_1(x) \geq 0, \ldots g_s(x) \geq 0\},$$

e σ è il precono di $\mathcal{P}(V)$ generato da $g_1, \ldots, g_s$.
Un ideale I di $\mathcal{P}(V)$ è σ-radicale se e solo se $I = \mathcal{I}_{\mathcal{P}(V)}(W \cap \mathcal{V}_V(I))$ e in particolare per ogni ideale I di $\mathcal{P}(V)$ vale

$$\sqrt[\sigma]{I} = \mathcal{I}_{\mathcal{P}(V)}(W \cap \mathcal{V}_V(I))$$

Dimostrazione. $f \in \sqrt[\sigma]{I}$ se e solo se esistono $m \in \mathbb{N}$ e $h \in \sigma$ $f^{2m} + h \equiv 0 \mod I$ se e solo se $f \in \mathcal{I}_{\mathcal{P}(V)}(W \cap \mathcal{V}_V(I))$. □

Dimostriamo a conclusione dimostriamo Nullstellensatz e Positivstellensatz per le funzioni regolari:

Teorema 4.25. Sia $V \subset R^n$ un insieme algebrico e I un ideale di $\mathcal{O}(V)$. Allora un elemento $g \in \mathcal{O}(V)$ si annulla su $\mathcal{V}_V(I)$ se e solo se esistono $g_1, \ldots, g_k \in \mathcal{O}(V)$ e $m \in \mathbb{N}$ tali che

$$f^{2m} + g_1^2 + \cdots + g_k^2 \in I.$$

Ossia $\mathcal{I}_{\mathcal{O}(V)}(\mathcal{V}_V(I)) = \sqrt[re]{I}$

Dimostrazione. Per la corrispondenza di ideali nella localizzazione possiamo scrivere $I = (h_1, \ldots, h_r)\mathcal{O}(V)$ con $h_1, \ldots, h_r \in \mathcal{P}(V)$. Allora $f = a/s$ con $a, b \in \mathcal{P}(V)$ e $b \notin \mathcal{I}(V)$. Allora per il Corollario 4.14

$$a^{2m} + q_1 + \cdots + q_k \in (h_1, \ldots, h_r)$$

per $q_i \in \mathcal{P}(V)$. Allora dividendo questa relazio per b^{2m} si ha la tesi. □

Teorema 4.26. Sia $V \subset R^n$ un insieme algebrico e $g_1, \ldots, g_s \in \mathcal{O}(V)$. Sia

$$W = \{x \in V \mid g_1(x) \geq 0, \ldots g_s(x) \geq 0\},$$

e σ è il precono di $\mathcal{O}(V)$ generato da $g_1, \ldots, g_s$, sia $f \in \mathcal{O}(V)$. Allora:

i. Per ogni $x \in W$ $f(x) \geq 0$ se e solo se $\exists m \in \mathbb{N}\ \exists g, h \in \sigma$ tali che $fg = f^{2m} + h$.

ii. Per ogni $x \in W$ $f(x) = 0$ se e solo se $\exists m \in \mathbb{N}\ \exists h \in \sigma$ tali che $f^{2m} + h = 0$.

Dimostrazione. Possiamo supporre che $g_1, \ldots, g_s \in \mathcal{P}(V)$ sostituendo a $g_i = a_i/s_i$ $a_i s_i = g_i s_i^2 \in \mathcal{P}(V)$. Se $f = a/s$ per il Teorema 4.23 abbiamo $fs \in \mathcal{P}(V)$ e dividendo per un opportuna potenza di s si ha la tesi. □

4.4 Il 17esimo problema di Hilbert

> **H17** Sia f un elemento di un anello A di funzioni a coefficienti in $\mathbb{R}$ tale che $f(x) \geq 0$ per ogni $x \in X$, allora f è somma di quadrati di A?

Questa è la formulazione algebrica del diciassettesimo della lista problemi compilata da Hilbert nel 1900. Che cosa c'entra con quanto detto sin qui? Abbiamo visto che nel contesto dei campi reali chiusi le somme finite di quadrati hanno un ruolo centrale.
Concentriamoci allora sulla seguente questione:

> *Sia* $f \in \mathbb{R}[X_1, \ldots, X_n]$ *tale che* $f(x) \geq 0$ *per ogni* $x \in X$ *esistono* $g_1, \ldots, g_k \in \mathbb{R}[X_1, \ldots, X_n]$ *tali che* $f = \sum g_j^2$*?*

La risposta è positiva se $n = 1$ ma già per $n = 2$ abbiamo il controesempio di Motzkin:

$$m(x, y, z) = 1 + x^2y^2(x^2 + y^2 - 3)$$

m è positivo ma non è somma di quadrati (vedi [BR98]).

Artin nel 1927 tutto provò che rendendo più debole l'asserto la soluzione diventa positiva:

Teorema 4.27. Sia $f \in \mathbb{R}[X_1, \ldots, X_n]$ tale che $f(x) \geq 0$ per ogni $x \in \mathbb{R}^n$. Allora f è somma di quadrati nell'anello delle frazioni di $\mathbb{R}[X_1, \ldots, X_n]$, ossia esistono $g_1, \ldots, g_k \in \mathbb{R}(X_1, \ldots, X_n)$ tali che $f = \sum g_j^2$.

La dimostrazione di questo fatto non è altro che una banale applicazione del Teorema di Artin Lang. Ci basterà infatti provare il seguente fatto:

Lemma 4.28. Posto $k = \mathbb{R}(X_1, \ldots, X_n)$ sono equivalenti:

a) Il Teorema 4.27.

b) $\{\beta \in \chi(k) \mid f >_\beta 0\} \neq \varnothing \iff \{x \in \mathbb{R}^n \mid f(x) > 0\} \neq \varnothing$

Dimostrazione. *a)* $\Rightarrow$ *b)* Supponiamo che f sia positivo rispetto ad un certo ordine β e che non ci siano $x \in \mathbb{R}^n$ tali che $f(x) > 0$, allora $-f(x) \geq 0$. Per il Teorema 4.27 allora $-f \in \sum k^2 \subset \beta$, assurdo. Viceversa se $f(x) > 0$ possiamo considerare il precono $\sigma[f] = \{p \in k \mid p = a + bf, a, b \in \sum k^2\}$. Allora f è

positivo in una qualsiasi estensione di $\sigma[f]$.
$b) \Rightarrow a)$ Sia $f \in \mathbb{R}[X_1, \ldots, X_n]$ tale che $f(x) \geq 0$ per ogni $x \in \mathbb{R}^n$. Supponiamo allora che preso $\beta \in \chi(k)$ si abbia $f <_\beta 0$ allora $-f \in \beta$. b) ci dà allora che deve esistere $z \in \mathbb{R}^n$ tale che $f(z) < 0$, assurdo. Allora f positivo in ogni ordine di k e dunque è una somma di quadrati per il Corollario 1.12. □

Bibliografia

[AT11] M. Abate and F. Tovena. *Geometria Differenziale*. UNITEXT. Springer Milan, 2011.

[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.

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

[BR98] Coste Bochnak and Roy. *Real Algebraic Geometry*. Springer, 1998.

[Cos00] Coste. *An introduction to semialgebraic geometry*. Dip. Mat. Univ.Pisa, Dottorato di Ricerca in Matematica, 2000.

[HP53] W. V. D. Hodge and D. Pedoe. *Methods of algebraic geometry*. Cambridge, 1953.

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

[Shape] Shafarevich. *Basic algebraic geometry*. Springer, 1977pe.

[ZCS75] O. Zariski, I.S. Cohen, and P. Samuel. *Commutative Algebra I*. Graduate Texts in Mathematics. Springer New York, 1975.

[ZS76] O. Zariski and P. Samuel. *Commutative Algebra II*. Graduate Texts in Mathematics. Springer New York, 1976.