Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

TEOREMA DI BÉZOUT:
un approccio algebrico

Tesi di Laurea

Relatore:
ANDREA PETRACCI

Presentata da:
MARCO SIMONE CENCINI

Anno Accademico 2023-2024

Introduzione

Attribuito ad Étienne Bézout, il teorema è un primo approccio alla teoria dell'intersezione di varietà algebriche risolvendo il caso di due curve proiettive piane. Il lavoro iniziale di Bézout – pubblicato nel 1779 – per il quale il teorema gli è stato attribuito, riguarda tuttavia la risoluzione di sistemi di equazioni algebriche. Inoltre, il concetto di molteplicità di intersezione che modifica ed arricchisce la prima formulazione di Bézout era ai suoi tempi sconosciuto.

È solo nel secolo scorso che è stata data una definizione accurata di molteplicità di intersezione, prima solo sul campo dei numeri complessi e successivamente su ogni campo algebricamente chiuso portando così alla versione definitiva del teorema. La definizione classica di molteplicità di intersezione di due curve algebriche piane proiettive utilizza il risultante di due polinomi e la proiezione su una retta da un punto scegliendo un opportuno sistema di coordinate omogenee. L'obiettivo di questa tesi è quello di dare una definizione della molteplicità di intersezione di due curve nel piano proiettivo tramite l'algebra commutativa. Ciò renderà evidente come questa sia invariante per cambi lineari di coordinate.

Il Capitolo 1 si apre rinfrescando proprietà elementari dei polinomi omogenei. Successivamente introduciamo le ipersuperfici affini e proiettive studiandone le loro proprietà. Il capitolo si chiude con lo studio locale delle curve algebriche piane affini e proiettive.

Nel Capitolo 2 passiamo all'esposizione dei preliminari dal punto di vista algebrico. Dopo una breve esposizione della teoria basilare degli anelli, introduciamo la struttura algebrica dei moduli e studiamo le loro prime basilari proprietà, nello specifico dei moduli finitamente generati. Introduciamo anche brevemente la struttura di algebra e la nozione di successione esatta corta, fondamentale in algebra commutativa.

Il Capitolo 3 è forse il più ricco di contenuti. Iniziamo il capitolo con la costruzione degli anelli di frazioni dando particolare enfasi alle localizzazioni, più interessanti dal punto di vista geometrico. Segue poi la costruzioni dei moduli di frazioni che posseggono proprietà più interessanti. Studiando i moduli di frazioni introduciamo il supporto ed indaghiamo il suo comportamento. Successivamente introduciamo il concetto di proprietà locale e mostriamo come alcune di queste siano ben note così da poterle sfruttare nelle dimostrazioni del prosieguo della tesi.

Dopo gli anelli e moduli di frazioni vogliamo definire la lunghezza di un modulo. A tale scopo introduciamo delle condizioni sulla finitezza delle catene di sottomoduli. Tramite il Teorema di Jordan-Hölder leghiamo queste condizioni alla lunghezza di un modulo e ne mostriamo la buona positura come quantità ed il suo legame con la dimensione come $\mathbb{K}$-spazio vettoriale se l'anello è una $\mathbb{K}$-algebra.

Il capitolo si chiude con una breve introduzione al prodotto tensoriale al fine di costruire l'algebra esterna e le potenze esterne di un modulo.

Nel Capitolo 4 introduciamo alcune nozioni elementari della geometria algebrica. In particolare ci soffermiamo sullo studio dell'anello delle funzioni regolari e quello dei germi delle funzioni regolari di una varietà affine.

Nel Capitolo 5 torniamo ad un approccio più classico esponendo brevemente la teoria del risultante di due polinomi e studiando il suo legame con la fattorizzazione dei polinomi ne caso in cui i coefficienti siano in un UFD. Fatto ciò questo è lo strumento tramite il quale

diamo la prima definizione di molteplicità di intersezione tra curve algebriche piane proiettive. Tale definizione avviene una volta scelto un sistema di coordinate omogenee opportuno. Utilizzando dunque l'algebra commutativa sviluppata nel Capitolo 3 ed introducendo gli anelli a valutazione discreta (DVR) studiamo nuove proprietà della lunghezza dei moduli su DVR. Mostriamo come la molteplicità di intersezione definita tramite il risultante si leghi ad una quantità invariante per cambi lineari di coordinate.

A questo punto la dimostrazione del Teorema di Bézout con la definizione classica di risultante e la scelta di un opportuno sistema di coordinate omogenee può essere presentata.

Indice

Introduzione i

Capitolo 1. Curve algebriche piane 1
1.1. Polinomi 1
1.2. Spazio proiettivo 2
1.3. Ipersuperfici affini e proiettive 5
1.4. Curve algebriche piane 11

Capitolo 2. Anelli 13
2.1. Anelli ed ideali 13
2.2. Moduli 15

Capitolo 3. Localizzazioni e condizioni di catena 21
3.1. Localizzazioni 21
3.2. Proprietà locali 25
3.3. Condizioni sulle catene 26
3.4. Prodotto tensoriale e potenza esterna 32

Capitolo 4. Rudimenti di geometria algebrica 39

Capitolo 5. Teorema di Bézout 45
5.1. Risultante e molteplicità di intersezione 45
5.2. Teorema di Bézout 48

Bibliografia 55

CAPITOLO 1

Curve algebriche piane

Iniziamo questo capitolo con il richiamare alcune definizioni e proprietà basilari dei polinomi a coefficienti in un campo $\mathbb{K}$ in n indeterminate, e fissare le notazioni che useremo da qui in avanti per questi ultimi. Una volta introdotto l'ambiente di lavoro, lo *spazio proiettivo standard n-dimensionale*, tali richiami algebrici ci permetteranno di poter iniziare lo studio delle *ipersuperfici proiettive*, di cui le *curve algebriche piane* sono un caso particolare per $n = 2$, in una trattazione più classica.

1.1. Polinomi

Indichiamo con $\mathbb{K}[x_0, \dots, x_n]$ l'anello dei polinomi nelle indeterminate $x_0, \dots, x_n$ a coefficienti in $\mathbb{K}$ e con $\deg F$ il grado di un polinomio $F(x_0, \dots, x_n)$. Denoteremo poi con F_{x_i} la derivata parziale rispetto alla variabile x_i, ed in modo analogo le derivate parziali di ordine maggiore.

Definizione 1.1. Sia $\mathbb{K}$ un campo, un polinomio $F \in \mathbb{K}[x_0, \dots, x_n]$ si dice *omogeneo* se tutti i suoi monomi hanno lo stesso grado. In particolare il polinomio nullo è omogeneo di ogni grado.

Per i polinomi omogenei valgono inoltre delle importanti proprietà utili da rammentare:

- un polinomio $F(x_0, \dots, x_n)$ è omogeneo di grado d se e solo se vale l'identità $F(tx_0, \dots, tx_n) = t^d F(x_0, \dots, x_n)$ in $\mathbb{K}[t, x_0, \dots, x_n]$;
- *(identità di Eulero)* se $F[x_0, \dots, x_n]$ è omogeneo, allora vale l'uguaglianza
$$\sum_{i=0}^{n} x_i F_{x_i} = (\deg F)F;$$
- ogni polinomio che divide un polinomio omogeneo non nullo è omogeneo.

Definizione 1.2. Sia $F(x_0, \dots, x_n) \in \mathbb{K}[x_0, \dots, x_n]$ un polinomio omogeneo di grado d, il polinomio $f(x_1, \dots, x_n) = F(1, x_1, \dots, x_n)$ è detto il *deomogenizzato* di F rispetto x_0, che indichiamo con F^{dh,x_0}. Se $f(x_1, \dots, x_n) \in \mathbb{K}[x_1, \dots, x_n]$ è un polinomio di grado d, il polinomio
$$F(x_0, \dots, x_n) = x_0^d f\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right)$$
è detto il polinomio *omogeneizzato* di f rispetto x_0, che indichiamo con f^{h,x_0}.

Osservazione 1.3. Se F è omogeneo di grado d e x_0 non divide F, allora $\deg F^{dh,x_0} = d$. Se f è un polinomio di grado d, allora f^{h,x_0} è omogeneo di grado d ed x_0 non divide f^{h,x_0}.

Le due operazioni appena definite a primo acchito possono sembrare l'una l'inversa dell'altra, tuttavia servono delle piccole accortezze per trarre tale conclusione.

Proposizione 1.4. Siano $f \in \mathbb{K}[x_1, \dots, x_n]$ polinomio di grado d ed $F \in \mathbb{K}[x_0, \dots, x_n]$ polinomio omogeneo di grado d. Allora:

(1) $(f^{h,x_0})^{dh,x_0} = f$, mentre $(F^{dh,x_0})^{h,x_0} = F$ se e solo se $x_0 \nmid F$.
(2) Siano $F(x_0, \dots, x_n)$ ed $f(x_1, \dots, x_n)$ polinomi ottenuti l'uno dall'altro per omogeneizzazione e deomogeneizzazione rispetto x_0 (dunque in particolare $x_0 \nmid F$),

allora f è irriducibile se e solo se F è irriducibile. Più precisamente, se F si fattorizza come $F = cF_1^{m_1} \dots F_s^{m_s}$ con $c \in \mathbb{K}^*$, $F_1, \dots, F_s$ polinomi irriducibili distinti ed $m_1, \dots, m_s \in \mathbb{Z}_{>0}$ tali che $\sum_{i=1}^{s} m_i \deg F_i = \deg F$, allora f si fattorizza come $f = cf_1^{m_1} \dots f_s^{m_s}$, dove gli f_i si ottengono a partire dagli F_i per deomogeneizzazione rispetto x_0 e viceversa.

DIMOSTRAZIONE. (1) Per l'osservazione precedente sappiamo che f^{h,x_0} è omogeneo di grado d e non divisibile per x_0, dunque sempre per la stessa abbiamo che la deomogeneizzazione di quest'ultimo è ancora di grado d. Allora $(f^{h,x_0})^{dh,x_0}(x_1, \dots, x_n) = 1^d f\left(\frac{x_1}{1}, \dots, \frac{x_n}{1}\right) = f(x_1, \dots, x_n)$. ($\Rightarrow$) Se per assurdo $x_0 \mid F$ allora F^{dh,x_0} avrebbe grado strettamente minore di d perciò la sua omogeneizzazione avrebbe tale grado e dunque non varrebbe l'uguaglianza. ($\Leftarrow$) Se $x_0 \nmid F$ allora F^{dh,x_0} ha ancora grado d dunque se $x_0 \neq 0$

$$\begin{aligned}(F^{dh,x_0})^{h,x_0}(x_0, \dots, x_n) &= x_0^d F\left(1, \frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) = \\ &= F\left(x_0, \frac{x_0 x_1}{x_0}, \dots, \frac{x_0 x_n}{x_0}\right) = \\ &= F(x_0, \dots, x_n).\end{aligned}$$

Per $x_0 = 0$ l'identità è ovvia per omogeneità di F.

(2) Si osserva facilmente che entrambe le operazioni commutano i prodotti ed in particolare dunque con l'elevamento a potenza dunque vale l'identità sulle fattorizzazioni. ($\Leftarrow$) Se per assurdo f fosse riducibile come $f = f_1 f_2$ si avrebbe che $F = f_1^{h,x_0} f_2^{h,x_0}$ e sarebbe riducibile. ($\Rightarrow$) Analogo.

□

Le operazioni di omogeneizzazione e deomogeneizzazione possono essere definite in modo del tutto equivalente rispetto ad ogni altra indeterminata x_i e continuano a valere per ciascuna le proprietà sopra enunciate e mostrate.

Introduciamo adesso nell'anello dei polinomi $\mathbb{K}[x_1, \dots, x_n]$ una relazione di equivalenza così definita: siano $f, g \in \mathbb{K}[x_1, \dots, x_n]$ diciamo che

$$f \sim g \text{ se e solo se esiste } \lambda \in \mathbb{K}^* \text{ tale che } f = \lambda g.$$

Diremo in questo caso che f e g sono *proporzionali*.

1.2. Spazio proiettivo

DEFINIZIONE 1.5. Sia $\mathbb{K}$ un campo. Lo *spazio proiettivo standard* n-dimensionale sul campo $\mathbb{K}$ è definito come l'insieme delle rette passanti per l'origine di $\mathbb{K}^{n+1}$ e si indica con $\mathbb{P}^n(\mathbb{K})$, cioè

$$\mathbb{P}^n(\mathbb{K}) = \frac{\mathbb{K}^{n+1} \setminus \{0\}}{\sim}$$

dove $\sim$ è la relazione di equivalenza così definita: siano $x, y \in \mathbb{K}^{n+1} \setminus \{0\}$ allora

$$x \sim y \text{ se e solo se esiste } \lambda \in \mathbb{K}^* \text{ tale che } x = \lambda y.$$

Denotiamo con $\pi : \mathbb{K}^{n+1} \setminus \{0\} \to \mathbb{P}^n(\mathbb{K})$ la mappa di proiezione al quoziente e con $[x_0 \colon \cdots \colon x_n]$ la classe di equivalenza di $(x_0, \dots, x_n) \in \mathbb{K}^{n+1} \setminus \{0\}$.

DEFINIZIONE 1.6. Per ogni $i = 0, \dots, n$ consideriamo i seguenti sottoinsiemi di $\mathbb{P}^n(\mathbb{K})$:

$$\begin{aligned}U_i &\coloneqq \{[x_0 \colon \cdots \colon x_n] \in \mathbb{P}^n(\mathbb{K}) \mid x_i \neq 0\}, \\ H_i &\coloneqq \{[x_0 \colon \cdots \colon x_n] \in \mathbb{P}^n(\mathbb{K}) \mid x_i = 0\}.\end{aligned}$$

U_i e H_i prendono rispettivamente i nomi di *i-esima carta affine standard* e *i-esimo iperpiano standard*.

Si osserva facilmente che $U_i = \mathbb{P}^n(\mathbb{K}) \setminus H_i$. Possiamo poi definire, per ogni $i = 0, \dots, n$, due naturali bigezioni:

- $j_i \colon \mathbb{K}^n \to U_i$ definita da $j_i(x_1, \dots, x_n) = [x_1 \colon \cdots \colon x_{i-1} \colon 1 \colon x_i \colon \cdots \colon x_n]$ la cui inversa è definita da $j_i^{-1}([x_0 \colon \cdots \colon x_{i-1} \colon x_i \colon x_{i+1} \colon \cdots \colon x_n]) = \left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i}\right)$. (Notiamo che è ben posta la divisione per x_i poiché non nulla in U_i);
- $h_i \colon \mathbb{P}^{n-1}(\mathbb{K}) \to H_i$ definita da $h_i([x_0 \colon \cdots \colon x_{n-1}]) = [x_0 \colon \cdots \colon x_{i-1} \colon 0 \colon \cdots \colon x_{n-1}]$ con inversa $h_i^{-1}([x_0 \colon \cdots \colon x_{i-1} \colon 0 \colon x_{i+1} \colon \cdots \colon x_n]) = [x_0 \colon \cdots \colon x_{i-1} \colon x_{i+1} \colon \cdots \colon x_n]$.

Si noti dunque che componendo una qualunque delle j_i con l'inclusione naturale di U_i in $\mathbb{P}^n(\mathbb{K})$ si ottiene un'immersione di $\mathbb{K}^n$ in $\mathbb{P}^n(\mathbb{K})$; per cui possiamo intendere $\mathbb{P}^n(\mathbb{K})$ come un ampliamento di $\mathbb{K}^n$ attraverso l'aggiunta dell'iperpiano "improprio" H_i.

Nota 1.7. Sarà sempre utilizzata come scelta privilegiata l'immersione di $\mathbb{K}^n$ mediante la mappa j_0 nella carta U_0.

Osservazione 1.8. La costruzione delle mappe fatta per U_i ed H_i può essere generalizzata ad un qualsiasi iperpiano $H \subseteq \mathbb{P}^n(\mathbb{K})$. Vedi [**FFP16**, 1.3.8 Carte affini, pag. 10].

Possiamo in generale definire lo spazio proiettivo su di un qualunque $\mathbb{K}$-spazio vettoriale V.

Definizione 1.9. Sia V un $\mathbb{K}$-spazio vettoriale, si chiama *spazio proiettivo* associato a V l'insieme quozione $\mathbb{P}(V) = (V \setminus \{0\}) / \sim$, dove $\sim$ è la relazione di equivalenza su V definita da

$$v \sim w \text{ se e solo se esiste } \lambda \in \mathbb{K}^* \text{ tale che } v = \lambda w.$$

Definizione 1.10. Sia $W \subseteq \mathbb{K}^{n+1}$ sottospazio vettoriale. L'insieme $\mathbb{P}(W) = \pi(W \setminus \{0\})$ è detto *sottospazio proiettivo*, con π la proiezione al quoziente. Si pone $\dim \mathbb{P}(W) = \dim(W) - 1$. Se $W = \{0\}$ allora $\mathbb{P}(W) = \varnothing$ e $\dim(\varnothing) = -1$.

Un sottospazio proiettivo viene detto *retta proiettiva* se ha dimensione 1, *piano proiettivo* se ha dimensione 2, *iperpiano proiettivo* se ha dimensione $n-1$. Chiamiamo *codimensione* di un sottospazio proiettivo $\mathbb{P}(W) \subseteq \mathbb{P}^n(\mathbb{K})$ l'intero $\operatorname{codim}(\mathbb{P}(W)) = \dim(\mathbb{P}^n(\mathbb{K})) - \dim(\mathbb{P}(W))$ (si noti che $\operatorname{codim}(\mathbb{P}(W)) = \operatorname{codim}(W)$).

Come viene fatto negli spazi vettoriali possiamo definire delle operazioni tra sottospazi proiettivi di $\mathbb{P}^n(\mathbb{K})$:

- siano $\mathbb{P}(W_1), \mathbb{P}(W_2) \subseteq \mathbb{P}^n(\mathbb{K})$ sottospazi proiettivi. Poiché $\mathbb{P}(W_1) \cap \mathbb{P}(W_2) = \mathbb{P}(W_1 \cap W_2)$, l'intersezione di due o più sottospazi proiettivi è ancora un sottospazio proiettivo. I sottospazi $\mathbb{P}(W_1)$ e $\mathbb{P}(W_2)$ sono detti *incidenti* se $\mathbb{P}(W_1) \cap \mathbb{P}(W_2) \neq \varnothing$, sono detti *sghembi* se invece hanno intersezione vuota;
- sia $A \subseteq \mathbb{P}^n(\mathbb{K})$ un sottoinsieme non vuoto, chiamiamo *sottospazio generato* da A il sottospazio proiettivo $L(A)$ ottenuto come intersezione di tutti i sottospazi proiettivi di $\mathbb{P}^n(\mathbb{K})$ contenenti A. Indichiamo con $L(p_1, \dots, p_m)$ il sottospazio generato dai punti $p_1, \dots, p_m \in \mathbb{P}^n(\mathbb{K})$;
- siano $\mathbb{P}(W_1), \mathbb{P}(W_2) \subseteq \mathbb{P}^n(\mathbb{K})$ sottospazi proiettivi. L'insieme $U = \mathbb{P}(W_1) \cup \mathbb{P}(W_2)$ in generale non è un sottospazio proiettivo, il sottospazio generato da U sarà denotato con $L(\mathbb{P}(W_1), \mathbb{P}(W_2))$ e si ha che $L(\mathbb{P}(W_1), \mathbb{P}(W_2)) = \mathbb{P}(W_1 + W_2)$.

Vale inoltre l'equivalente della Formula di Grassmann per sottospazi proiettivi (vedi [**FFP16**, Proposizione 1.2.1, pag. 4]) che ci fornisce dunque l'utile criterio per il quale, dati $\mathbb{P}(W_1), \mathbb{P}(W_2) \subseteq \mathbb{P}^n(\mathbb{K})$ sottospazi proiettivi, se $\dim(\mathbb{P}(W_1)) + \dim(\mathbb{P}(W_2)) \geq n$ allora i due sottospazi sono incidenti.

Definizione 1.11. Siano V e W due $\mathbb{K}$-spazi vettoriali di dimensione finita, diciamo che l'applicazione $f \colon \mathbb{P}(V) \to \mathbb{P}(W)$ è un *trasformazione proiettiva* se esiste un'applicazione lineare iniettiva $\varphi \colon V \to W$ tale che $f([v]) = [\varphi(v)]$ per ogni $v \in V \setminus \{0\}$. In tal caso scriviamo $f = \overline{\varphi}$.

Se f è indotta da un isomorfismo lineare φ diciamo che f è un *isomorfismo proiettivo*. Due spazi proiettivi su un campo $\mathbb{K}$ si dicono *isomorfi* se esiste un isomorfismo proiettivo tra di essi. Un isomorfismo proiettivo $f\colon \mathbb{P}(V) \to \mathbb{P}(V)$ è chiamato una *proiettività* di $\mathbb{P}(V)$. Due sottoinsiemi $A, B \subseteq \mathbb{P}^n(\mathbb{K})$ si dicono *proiettivamente equivalenti* se esiste una proiettività f di $\mathbb{P}^n(\mathbb{K})$ tale che $f(A) = B$.

Osservazione 1.12. Nella definizione di una trasformazione proiettiva f la richiesta di φ iniettiva non è rimovibile: difatti se φ non fosse iniettiva allora la proiettività $f = \overline{\varphi}$ non sarebbe ben definita sul sottospazio proiettivo $\mathbb{P}(\ker \varphi)$. Possiamo tuttavia estendere la definizione di trasformazione proiettiva per ammettere quelle indotte da applicazioni lineari non iniettive, dette *trasformazioni proiettive degeneri* (vedi [**FFP16**, 1.2.6, pag. 5]).

Sia φ un'applicazione lineare che induce la trasformazione proiettiva f, allora l'insieme di tutte le applicazioni lineari che inducono f è $\{k\varphi \mid k \in \mathbb{K}^*\}$, cioè tale applicazione lineare è determinata a meno di un multiplo scalare non nullo. Le proiettività di $\mathbb{P}^n(\mathbb{K})$ formano un gruppo rispetto alla composizione, detto *gruppo lineare proiettivo* e denotato con $\mathrm{PGL}(n+1, \mathbb{K})$. Per quanto osservato sulle applicazioni lineari che inducono una proiettività questo è isomorfo a

$$\mathrm{PGL}(n+1, \mathbb{K}) \cong \frac{GL_{n+1}(\mathbb{K})}{\sim},$$

ove $\sim$ è la relazione di equivalenza così definita: date $A, B \in GL_{n+1}(\mathbb{K})$ allora

$$A \sim B \text{ se e solo se esiste } \lambda \in \mathbb{K}^* \text{ tale che } A = \lambda B.$$

Più avanti ci servirà un particolare tipo di trasformazione proiettiva di $\mathbb{P}^n(\mathbb{K})$: la proiezione di centro un sottospazio, nel caso particolare di un punto.

Definizione 1.13. Siano $H = \mathbb{P}(W)$ ed $S = \mathbb{P}(U)$ sottospazi proiettivi di $\mathbb{P}^n(\mathbb{K})$ tali che $H \cap S = \varnothing$ e $L(S, H) = \mathbb{P}^n(\mathbb{K})$. L'applicazione $\pi_{H,S}\colon \mathbb{P}^n(\mathbb{K}) \setminus H \to S$ definita da $\pi_{H,S}(p) = L(H, p) \cap S$ è detta la *proiezione di* $\mathbb{P}^n(\mathbb{K})$ *su* S *di centro* H.

L'applicazione di proiezione $\pi_{H,S}$ è ben posta per la formula di Grassmann: se poniamo $k = \dim(S)$ e $h = \dim(H)$ allora per la formula di Grassmann $k + h = n - 1$. Allora per ogni $p \in \mathbb{P}^n(\mathbb{K}) \setminus H$ si ha che $\dim L(H, p) = h + 1$, per cui di nuovo dalla formula di Grassmann otteniamo che $\dim(L(H, p) \cap S) = 0$, cioè $L(H, p)$ interseca S in esattamente un punto.

Nota 1.14. In particolare a noi interesserà nel proseguo la proiezione di $\mathbb{P}^n(\mathbb{K})$ di centro un punto su un iperpiano $\pi_{p,H}$, con $H \subseteq \mathbb{P}^n(\mathbb{K})$ iperpiano e $p \in \mathbb{P}^n(\mathbb{K}) \setminus H$.

Abbiamo indicato i punti di $\mathbb{P}^n(\mathbb{K})$ con $[x_0\colon \cdots \colon x_n]$ quando parlavamo della classe di equivalenza del punto $(x_0, \ldots, x_n) \in \mathbb{K}^{n+1} \setminus \{0\}$ utilizzando dunque implicitamente un sistema di coordinate indotto da quello dato dalla base canonica $\{e_0, \ldots, e_n\}$ di $\mathbb{K}^{n+1}$. Possiamo tuttavia, come succede per i cambi di base di un $\mathbb{K}$-spazio vettoriale, cambiare il nostro riferimento proiettivo.

Definizione 1.15. I punti $p_0 = [v_0], \ldots, p_m = [v_m]$ di $\mathbb{P}^n(\mathbb{K})$ si dicono *linearmente indipendenti* se lo sono i vettori $v_0, \ldots, v_m$ in $\mathbb{K}^{n+1}$. In particolare $\mathbb{P}^n(\mathbb{K})$ ci sono al più $n+1$ punti linearmente indipendenti. Più in generale, diciamo che i punti $p_0, \ldots, p_k \in \mathbb{P}^n(\mathbb{K})$ sono in *posizione generale* se sono linearmente indipendenti (per $k \leq n$) oppure se $k > n$, presi qualunque $n + 1$ di questi sono linearmente indipendenti.

Definizione 1.16. Un *riferimento proiettivo* di $\mathbb{P}^n(\mathbb{K})$ è un insieme ordinato $\mathcal{R} = \{p_0, \ldots, p_n, p_{n+1}\}$ di $n + 2$ punti in posizione generale; i punti $p_0, \ldots, p_n$ sono detti i *punti fondamentali* del riferimento, mentre p_{n+1} viene detto *punto unità*.

I sistemi di riferimento proiettivi svolgono il ruolo che hanno le basi in uno spazio vettoriale e difatti sono ad esse legati. Difatti data una base $\mathcal{B} = \{v_0, \ldots, v_n\}$ di $\mathbb{K}^{n+1}$ consideriamo il vettore $u = v_0 + \ldots + v_n$. Si osserva facilmente che $\mathcal{R} = \{[v_0], \ldots, [v_n], [u]\}$ è un

riferimento proiettivo di $\mathbb{P}^n(\mathbb{K})$. Chiamiamo $\mathcal{B}$ una *base normalizzata* di $\mathcal{R}$. Sia allora $[v] \in \mathbb{P}^n(\mathbb{K})$, se $v = \sum_{i=0}^n x_i v_i$ diciamo che $(x_0, \dots, x_n)$ è una $(n+1)$-upla di *coordinate omogenee* per $[v]$ rispetto al riferimento $\mathcal{R}$ e scriveremo $[v]_{\mathcal{R}} = [x_0 \colon \cdots \colon x_n]$. In $\mathbb{P}^n(\mathbb{K})$ si chiama *riferimento proiettivo standard* quello formato dai punti $[1 \colon \cdots \colon 0], \dots, [0 \colon \cdots \colon 1], [1 \colon \cdots \colon 1]$, di cui una base normalizzata è la base canonica di $\mathbb{K}^{n+1}$. Quanto è stato fissato un riferimento proiettivo e quindi è stato dato un sistema di coordinate su $\mathbb{P}^n(\mathbb{K})$, invece di $[p]_{\mathcal{R}} = [x_0 \colon \cdots \colon x_n]$ scriveremo più brevemente $p = [x_0 \colon \cdots \colon x_n]$.

Osservazione 1.17. Fissare un riferimento proiettivo $\mathcal{R}$ di $\mathbb{P}^n(\mathbb{K})$ equivale a fissare una proiettività $\Phi_{\mathcal{R}} \colon \mathbb{P}^n(\mathbb{K}) \to \mathbb{P}^n(\mathbb{K})$ dove diamo al dominio il riferimento proiettivo standard ed al codominio il riferimento proiettivo $\mathcal{R}$, dunque la mappa è definita da $\Phi_{\mathcal{R}}(p) = [p]_{\mathcal{R}}$. Tale proiettività risulta dunque essere indotta dall'isomorfismo lineare di cambio di base dalla base canonica di $\mathbb{K}^{n+1}$ ad una qualsiasi base normalizzata $\mathcal{B}_u$ associata ad $\mathcal{R}$.

Proposizione 1.18. Siano $\mathcal{R}$ ed $\mathcal{R}'$ due riferimenti proiettivi di $\mathbb{P}^n(\mathbb{K})$. Esiste una matrice $A \in GL_{n+1}(\mathbb{K})$, individuata solo a meno di un multiplo scalare non nullo, tale che se $p \in \mathbb{P}^n(\mathbb{K})$ ha coordinate omogenee $x = (x_0, \dots, x_n)$ nel riferimento $\mathcal{R}$, allora coordinate omogenee $y = (y_0, \dots, y_n)$ del punto p nel riferimento $\mathcal{R}'$ sono date dalla formula $y = Ax$.

Dimostrazione. Vedi [**Ser00**, pag. 319, 320; Proposizione 27.1] □

1.3. Ipersuperfici affini e proiettive

Raccogliamo in questa sezione nozioni e risultati generali per le ipersuperfici per poi applicarli ai nostri casi particolari. Ricordiamo innanzitutto la relazione di proporzionalità che abbiamo dato all'anello dei polinomi $\mathbb{K}[x_1, \dots, x_n]$ in 1.1. Indicheremo poi da qui in avanti con $\mathbb{A}^n_{\mathbb{K}}$ l'insieme $\mathbb{K}^n$ che chiameremo *spazio affine n-dimensionale* sul campo $\mathbb{K}$ (o più brevemente $\mathbb{A}^n$ quando è ovvio il campo base).

Definizione 1.19. Si chiama *ipersuperficie affine* $\mathcal{I}$ di $\mathbb{A}^n_{\mathbb{K}}$ ogni classe di proporzionalità di polinomi di grado positivo in $\mathbb{K}[x_1, \dots, x_n]$. Un'ipersuperficie affine viene detta *curva piana affine* nel caso $n = 2$.

Se $f \in \mathbb{K}[x_1, \dots, x_n]$ è un rappresentante per l'ipersuperficie $\mathcal{I}$, diciamo che $f(x_1, \dots, x_n) = 0$ è un'*equazione dell'ipersuperficie* e chiamiamo *grado* di $\mathcal{I}$ il grado di f. Se $\mathcal{I} = [f]$ e $\mathcal{J} = [g]$, denotiamo con $\mathcal{I}+\mathcal{J}$ l'ipersuperficie $[fg]$ e, per ogni intero positivo m, denotiamo $m\mathcal{I} = [f^m]$. L'ipersuperficie $\mathcal{I}$ è detta *irriducibile* se lo è uno – e quindi ciascuno – dei suoi rappresentanti. Se $f = cf_1^{m_1} \dots f_s^{m_s}$, con $c \in \mathbb{K}^*$, $m_1, \dots, m_s \in \mathbb{Z}_{>0}$ tali che $\sum_{i=1}^s m_i = \deg F$ ed $f_1, \dots, f_s$ coprimi a due a due, le ipersuperfici $\mathcal{I}_i = [f_i]$ sono dette le *componenti irriducibili* di $\mathcal{I}$ e l'intero m_i è detto la *molteplicità* della componente $\mathcal{I}_i$; in tal caso scriveremo $\mathcal{I} = m_1\mathcal{I}_1 + \dots + m_s\mathcal{I}_s$. Ogni componente irriducibile di molteplicità $m_i > 1$ è detta *componente multipla*; le ipersuperfici senza componenti multiple sono dette *ridotte*.

Definizione 1.20. Per ogni $f \in \mathbb{K}[x_1, \dots, x_n]$ denotiamo

$$\mathbf{V}(f) = \{(x_1, \dots, x_n) \in \mathbb{A}^n \mid f(x_1, \dots, x_n) = 0\}.$$

Poiché $\mathbf{V}(\lambda f) = \mathbf{V}(f)$ per ogni $\lambda \in \mathbb{K}^*$, chiamiamo *supporto* dell'ipersuperficie $\mathcal{I} = [f]$ l'insieme – ben definito – $\mathbf{V}(\mathcal{I}) = \mathbf{V}(f)$.

Osservazione 1.21. Un'ipersuperficie determina univocamente il suo supporto, il viceversa in generale non è vero. Ad esempio le ipersuperfici di equazione $f = 0$ ed $f^m = 0$ hanno lo stesso supporto pur essendo ipersuperfici diverse.

Aggiungendo tuttavia l'ipotesi che il campo $\mathbb{K}$ sia algebricamente chiuso la corrispondenza fra ipersuperficie e supporto diventa biunivoca nel caso delle ipersuperfici ridotte (corrispondenza che verrà esplicitata dal Nullstellensatz 4.7 nel Capitolo 4). Possiamo invece facilmente osservare che senza questa ipotesi sul campo $\mathbb{K}$ ciò è non vero: ad esempio

se $\mathbb{K} = \mathbb{R}$ le due ipersuperfici di equazione rispettivamente $x_1^2 + x_2^2 = 0$ ed $x_1^4 + x_2^4 = 0$ sono diverse ma hanno lo stesso supporto.

Un altro fenomeno da osservare legato al campo base è che, se $n \geq 2$, nel caso di un campo $\mathbb{K}$ algebricamente chiuso il supporto di ogni ipersuperficie contiene infiniti punti.

PROPOSIZIONE 1.22. Sia $\mathcal{I} = [f]$ ipersuperficie affine su $\mathbb{K}$ ed $n \geq 2$.

1) Se $\mathbb{K} = \overline{\mathbb{K}}$ allora $\#\mathbf{V}(\mathcal{I}) = +\infty$.
2) Se $\mathbb{K}$ è infinito allora $\#\,\mathbb{A}^n \setminus \mathbf{V}(\mathcal{I}) = +\infty$.

DIMOSTRAZIONE. Proviamo prima 2). Se per assurdo fosse finito, allora $\mathbb{A}^n \setminus \mathbf{V}(f) = \{p_1, \ldots, p_N\}$ e dunque $\mathbb{A}^n = \mathbf{V}(f) \cup \{p_1, \ldots, p_N\}$. Tuttavia $\mathbb{A}^n$ con la topologia di Zariski definita in 4.3 è irriducibile secondo la Definizione 4.4. Siccome $\mathbf{V}(f)$ e $\{p_1, \ldots, p_N\}$ sono chiusi in tale topologia $\mathbb{A}^n = \mathbf{V}(f)$, ma allora $f = 0$ il che è assurdo.

1) Possiamo scrivere $f = \sum_{i=0}^{d} g_i x_n^i$ con $g_i \in \mathbb{K}[x_1, \ldots, x_{n-1}]$ e $g_d \neq 0$. Si consideri π la composizione delle mappe $\mathbf{V}(f) \hookrightarrow \mathbb{A}^n$ di inclusione e $\mathbb{A}^n \twoheadrightarrow \mathbb{A}^{n-1}$ di proiezione sulle prime $n-1$ componenti. Sia $\overline{x} \in \mathbb{A}^{n-1} \setminus \mathbf{V}(g_d)$ si ha che il polinomio $\sum_{i=0}^{d} g_i(\overline{x}) x_n^i \in \mathbb{K}[x_n]$ è non costante e poiché il campo è algebricamente chiuso ha almeno una radice $\overline{x}_n$. Allora $(\overline{x}, \overline{x}_n) \in \mathbf{V}(f)$ e quindi $\overline{x} \in \pi(\mathbf{V}(f))$; dunque $\pi(\mathbf{V}(f)) \supseteq \mathbb{A}^{n-1} \setminus \mathbf{V}(g_d)$. Se per assurdo $\mathbf{V}(f)$ fosse finito allora $\pi(\mathbf{V}(f))$ sarebbe finito ma dunque per il punto 2) $g_d = 0$; il che è assurdo. □

Ciò non è tuttavia vero per campi non algebricamente chiusi: possiamo prendere di nuovo come esempio $\mathbb{K} = \mathbb{R}$ in cui l'ipersuperficie già presa in esame di $\mathbb{A}^2_{\mathbb{R}}$ data dall'equazione $x_1^2 + x_2^2 = 0$ ha come supporto un solo punto. Esistono in quest'ultimo caso anche ipersuperfici con supporto vuoto come quella data dall'equazione $x_1^2 + x_2^2 + 1 = 0$ in $\mathbb{A}^2_{\mathbb{R}}$.

DEFINIZIONE 1.23. Un'ipersuperficie affine $\mathcal{I}$ viene detta *cono* se esiste un punto $p \in \mathcal{I}$ (detto *vertice* del cono) tale che, per ogni punto $q \in \mathcal{I} \setminus \{p\}$, la retta congiungente p e q è interamente contenuta in nel supporto di $\mathcal{I}$.

OSSERVAZIONE 1.24. Si osserva facilmente che le ipersuperfici $\mathcal{I} = [f]$ in $\mathbb{A}^n$, con $f \in \mathbb{K}[x_1, \ldots, x_n]$ omogeneo di grado positivo d, sono tutti coni con vertice nell'origine. Infatti, stante che $0 \in \mathcal{I}$ poiché f omogeneo di grado positivo, preso $p \in \mathcal{I} \setminus \{0\}$ di coordinate $(p_1, \ldots, p_n)$, parametrizziamo la retta r congiungente 0 e p come $(x_1, \ldots, x_n) = t(p_1, \ldots, p_n)$ con $t \in \mathbb{K}$. A questo punto, sia $(x_1, \ldots, x_n) \in r$, vale $f(x_1, \ldots, x_n) = f(tp_1, \ldots . tp_n) = t^d f(p_1, \ldots, p_n) = t^d\, 0 = 0$.

DEFINIZIONE 1.25. Si chiama *ipersuperficie proiettiva* $\mathcal{I}$ di $\mathbb{P}^n(\mathbb{K})$ ogni classe di proporzionalità di polinomi omogenei non nulli di grado positivo in $\mathbb{K}[x_0, \ldots, x_n]$. Un'ipersuperficie proiettiva viene detta *curva piana proiettiva* nel caso $n = 2$.

Vengono poi date in modo analogo al caso affine le definizioni di *equazione* e *grado* di un'ipersuperficie proiettiva, di *ipersuperficie proiettiva irriducibile*, di *componente irriducibile*, di *molteplicità* di una componente e di *cono*. Anche il *supporto* di un'ipersuperficie proiettiva $\mathcal{I} = [F]$ può essere definito in modo analogo come $\mathbb{V}(F) = \{[x_0 \colon \cdots \colon x_n] \in \mathbb{P}^n(\mathbb{K}) \mid F(x_0, \ldots, x_n) = 0\}$. Questa è una buona definizione poiché non dipende né dalla scelta del rappresentante per $\mathcal{I}$ (come per il caso affine), né dalle coordinate omogenee del punto $p = [x_0 \colon \cdots \colon x_n]$: infatti, poiché F è omogeneo, vale l'identità $F(tx_0, \ldots, tx_n) = t^{\deg F} F(x_0, \ldots, x_n)$ in $\mathbb{K}[t, x_0, \ldots, x_n]$.

OSSERVAZIONE 1.26. Ogni iperpiano di $\mathbb{P}^n(\mathbb{K})$ è supporto di un'ipersuperficie di grado 1 (che chiamiamo ancora iperpiano).

La corrispondenza tra supporti ed ipersuperfici ridotte nel caso delle ipersuperfici affini vale anche per ipersuperfici proiettive se il campo base $\mathbb{K}$ è algebricamente chiuso.

Abbiamo già osservato come $\mathbb{A}^n_{\mathbb{K}}$ possa essere identificato con $U_0 \subseteq \mathbb{P}^n(\mathbb{K})$ attraverso la mappa $j_0 \colon \mathbb{A}^n \to U_0$. Questo fatto permette di dare una relazione fra le ipersuperfici affini e le ipersuperfici proiettive.

DEFINIZIONE 1.27. Sia F un polinomio omogeneo che definisce l'ipersuperficie proiettiva $\mathcal{I}$ di $\mathbb{P}^n(\mathbb{K})$. Supponiamo che F non abbia x_0 come unico fattore irriducibile. Si chiama *parte affine* di $\mathcal{I}$ nella carta U_0 l'ipersuperficie affine di $\mathbb{A}^n_{\mathbb{K}}$ definita dal polinomio f ottenuto per deomogeneizzazione del polinomio F rispetto la variabile x_0. Tale ipersuperficie ha come supporto $j_0^{-1}(\mathcal{I} \cap U_0)$; conveniamo di denotarla con $\mathcal{I} \cap U_0$.

OSSERVAZIONE 1.28. La parte affine $\mathcal{I} \cap U_0$ ha lo stesso grado di $\mathcal{I}$ se e solo se $x_0 \nmid F$ per la Proposizione 1.4.

Sia $\mathcal{I}$ ipersuperficie di $\mathbb{P}^n(\mathbb{K})$ e $\pi\colon \mathbb{K}^{n+1} \setminus \{0\} \to \mathbb{P}^n(\mathbb{K})$ la proiezione al quoziente. Abbiamo che l'insieme $\pi^{-1}(\mathcal{I}) \cup \{0\}$ è un cono di $\mathbb{K}^{n+1}$ di vertice l'origine. La parte affine di $\mathcal{I}$ della carta U_0 può dunque essere interpretata come l'intersezione del cono $\pi^{-1}(\mathcal{I}) \cup \{0\}$ con l'iperpiano affine di $\mathbb{K}^{n+1}$ di equazione $x_0 = 1$.

OSSERVAZIONE 1.29. In modo analogo, per ogni iperpiano $H \subset \mathbb{P}^n(\mathbb{K})$ può essere definita la parte affine di una ipersuperficie $\mathcal{I}$ ipersuperficie di $\mathbb{P}^n(\mathbb{K})$ nella carta affine $U_H = \mathbb{P}^n(\mathbb{K}) \setminus H$.

DEFINIZIONE 1.30. Sia $\mathcal{I} = [f]$ un'ipersuperficie affine di $\mathbb{A}^n$. Se F è il polinomio ottenuto da f per omogeneizzazione rispetto alla variabile x_0, diciamo che l'ipersuperficie proiettiva $\overline{\mathcal{I}} = [F]$ di $\mathbb{P}^n(\mathbb{K})$ è la *chiusura proiettiva* di $\mathcal{I}$ mediante la carta U_0.

OSSERVAZIONE 1.31. La Definizione 1.30 è data stante la Nota 1.7. Possiamo replicare la definizione per ogni carta affine standard U_i, con $i \in \{0, 1, \ldots, n\}$, tramite la mappa j_i.

Come si osserva facilmente le due operazioni sono fortemente legate all'omgeneizzazione e la deomogeneizzazione dei polinomi rappresentanti le ipersuperfici. Dalla Proposizione 1.4 segue dunque facilmente che:

(1) partendo da una ipersuperficie affine $\mathcal{I} = [f]$ allora $\overline{\mathcal{I}} \cap U_0 = \mathcal{I}$. Inoltre, poiché $x_0 \nmid F$, l'intersezione di $\overline{\mathcal{I}}$ con l'iperpiano standard H_0 è un'ipersuperficie di H_0 con lo stesso grado di $\overline{\mathcal{I}}$. Ad esempio se $n = 2$ la chiususra proiettiva di $\mathcal{I}$ contiene un numero finito di punti sulla retta di equazione $x_0 = 0$, che sono detti *punti impropri* o *punti all'infinito* di $\mathcal{I}$;
(2) se $\mathcal{I} = [F]$ è un'ipersuperficie proiettiva e $x_0 \nmid F$, allora $\overline{\mathcal{I} \cap U_0} = \mathcal{I}$.

Vogliamo adesso introdurre anche tra le ipersuperfici, affini o proiettive che siano, una relazione di equivalenza. Ricordiamo che due sottoinsiemi di $\mathbb{A}^n$ si dicono *affinemente equivalenti* se esiste un'affinità φ che trasporta l'uno nell'altro. Poiché come abbiamo già osservato un'ipersuperficie non è univocamente determinata dal suo supporto, introduciamo una nozione di equivalenza partendo dalle loro equazioni.

Sia $\mathcal{I} = [f]$ un'ipersuperficie affine di $\mathbb{A}^n$ (risp. $\mathcal{I} = [F]$ ipersuperficie proiettiva di $\mathbb{P}^n(\mathbb{K})$) di equazione $f(X) = 0$, con $X = (x_0, \ldots, x_n)$, (risp. $F(X) = 0$, con $X = (x_0, \ldots, x_n)$), e sia $\varphi(X) = AX + b$ un'affinità di $\mathbb{A}^n$, con $A \in GL_n(\mathbb{K})$ e $b \in \mathbb{K}^n$ (risp. g una proiettività di $\mathbb{P}^n(\mathbb{K})$ indotta dall'applicazione lineare associata alla matrice $N \in GL_{n+1}(\mathbb{K})$). Denotiamo con $\varphi(\mathcal{I})$ (risp. $g(\mathcal{I})$) l'ipersuperficie affine (risp. proiettiva) di equazione $f(\varphi^{-1}(X)) = 0$ (risp. $F(N^{-1}X)) = 0$). Questa nozione è coerente con il fatto che φ (risp. g) trasporta il supporto di $\mathcal{I}$ nel supporto di $\varphi(\mathcal{I})$ (risp. $g(\mathcal{I})$).

DEFINIZIONE 1.32. Due ipersuperfici affini (risp. proiettive) $\mathcal{I}$ e $\mathcal{J}$ di $\mathbb{K}^n$ (risp. di $\mathbb{P}^n(\mathbb{K})$) si dicono *affinemente equivalenti* (risp. *proiettivamente equivalenti*) se esiste un'affinità φ di $\mathbb{A}^n$ (risp. una proiettività g di $\mathbb{P}^n(\mathbb{K})$) tale che $\mathcal{I} = \varphi(\mathcal{J})$ (risp. $\mathcal{I} = g(\mathcal{J})$). Segue dunque che supporti di ipersuperfici affinemente (risp. proiettivamente) equivalenti sono insiemi affinemente (risp. proiettivamente) equivalenti.

È importante osservare che il grado, il numero e la molteplicità delle componenti irriducibili di un'ipersuperficie si conservano mediante un'affinità (risp. proiettività). In particolare per ipersuperfici proiettive mediante cambi di coordinate omogenee di $\mathbb{P}^n(\mathbb{K})$.

Osservazione 1.33. Siano $\mathcal{I}$ e $\mathcal{J}$ due ipersuperfici proiettive che non hanno $[x_0]$ come componente irriducibile e sia g una proiettività tale che $\mathcal{I} = g(\mathcal{J})$. Se g fissa la carta U_0, allora la restrizione di g alla carta affine U_0 corrisponde ad una affinità di $\mathbb{K}^n$ data da $\psi = j_0 \circ g_{|_{U_0}} \circ j_0^{-1}$ tale per cui $\mathcal{I} \cap U_0 = \psi(\mathcal{J} \cap U_0)$. Allo stesso modo g ristretta all'iperpiano standard H_0 corrisponde ad una proiettività di H_0 che manda $\mathcal{I} \cap H_0$ in $\mathcal{J} \cap H_0$. Analogamente, se $\mathcal{I}$ e $\mathcal{J}$ sono ipersuperfici di $\mathbb{A}^n$ e φ è un'affinità tale per cui $\mathcal{I} = \varphi(\mathcal{J})$, possiamo pensarlo come la restizione di una proiettività g di $\mathbb{P}^n(\mathbb{K})$ che fissa la carta U_0 e tale che $\overline{\mathcal{I}} = g(\overline{\mathcal{J}})$ e $\mathcal{I} \cap H_0 = g|_{H_0}(\mathcal{J} \cap H_0)$. Dunque chiusure proiettive e parti all'infinito di ipersuperfici affinemente equivalenti sono ipersuperfici proiettivamente equivalenti.

Già a questo livello possiamo avvicinarci al teorema di Bézout analizzando e mostrando un suo caso particolare, facilmente generalizzabile in una qualsiasi dimensione n, con le sole nozioni introdotte. Studieremo quindi adesso l'intersezione di un'ipersuperficie proiettiva con una retta proiettiva. Tale risultato verrà utilizzato per altri scopi. Richiamiamo prima cosa voglia dire essere una radice omogenea di un polinomio omogeneo in due variabili ed un importante risultato sulla fattorizzazione di questi ultimi se i coefficienti sono in un campo algebricamente chiuso.

Definizione 1.34. Sia $F \in \mathbb{K}[x_0, x_1]$ un polinomio omogeneo di grado d. Allora la coppia omogenea $[a : b] \in \mathbb{P}^1(\mathbb{K})$ si dice una *radice* di F se $F(a, b) = 0$. La *molteplicità* di una radice $[a : b]$ di F è $\min\{k \in \mathbb{Z}_{\geq 0} : (ax_1 - bx_0)^k \mid F\}$.

Teorema 1.35 (Teorema fondamentale dell'algebra omogeneo). Siano $\mathbb{K}$ un campo algebricamente chiuso ed $F(x_0, x_1) \in \mathbb{K}[x_0, x_1]$ un polinomio omogeneo di grado positivo d. Allora esistono $(a_1, b_1), \ldots, (a_s, b_s) \in \mathbb{K}^2 \setminus \{(0, 0)\}$ a due a due non proporzionali ed $m_1, \ldots, m_s \in \mathbb{Z}_{>0}$, tali che $\sum_{i=1}^{s} m_i = d$, e

$$F(x_0, x_1) = \prod_{i=1}^{s} (a_i x_1 - b_i x_0)^{m_i}.$$

Le coppie (a_i, b_i) sono univocamente determinate a meno dell'ordine e di costanti moltiplicative non nulle.

Dimostrazione. Vedi [**Kir92**, Lemma 2.8 pag. 31] □

Data una retta proiettiva $r \subseteq \mathbb{P}^n(\mathbb{K})$ esiste un isomorfismo proiettivo con $\mathbb{P}^1(\mathbb{K})$. Presi qualunque due punti distinti $x, y \in r$, una volta fissati due rappresentanti $(x_0, \ldots, x_n)$ ed $(y_0, \ldots, y_n)$ rispettivamente di x ed y, possiamo parametrizzare dunque tutti i punti della retta r come $[\lambda x_0 + \mu y_0 \colon \cdots \colon \lambda x_n + \mu y_n]$ al variare di $[\lambda \colon \mu] \in \mathbb{P}^1(\mathbb{K})$ che, con un piccolo abuso notazionale, indichiamo per snellire la notazione come $\lambda x + \mu y$. Dunque troviamo i punti di intersezione tra $\mathcal{I}$ ed r risolvendo l'equazione

$$G(\lambda, \mu) = F(\lambda x + \mu y) = 0.$$

Osserviamo facilmente che se $r \subseteq \mathcal{I}$ allora il polinomio G è identicamente nullo, altrimenti nel caso di un campo base algebricamente chiuso $\mathbb{K}$ ha esattamente $d = \deg F$ radici omogenee contate con molteplicità in $\mathbb{P}^1(\mathbb{K})$.

Definizione 1.36. Data $\mathcal{I} = [F]$ ipersuperficie di $\mathbb{P}^n(\mathbb{K})$ ed $r \subseteq \mathbb{P}^n(\mathbb{K})$ una retta proiettiva. Dati $x, y \in r$ punti distinti, se $[\lambda_0 \colon \mu_0]$ è una radice omogenea del polinomio $G(\lambda, \mu) = F(\lambda x + \mu y)$ di molteplicità m, diciamo che $\mathcal{I}$ ed r hanno *molteplicità di intersezione* m nel punto corrispondente $p = [\lambda_0 x_0 + \mu_0 y_0 \colon \ldots \colon \lambda_0 x_n + \mu_0 y_n]$. In tal caso scriviamo $I(\mathcal{I}, r, p) = m$.

Per convenzione poniamo $I(\mathcal{I}, r, p) = \infty$ se $r \subseteq \mathcal{I}$.

Osservazione 1.37. La definizione appena data di molteplicità di intersezione tra una ipersuperficie $\mathcal{I}$ ed una retta r in un punto è ben posta poiché non dipende dai punti x ed y scelti sulla retta.

DIMOSTRAZIONE. È evidente che nei casi in cui $p \notin \mathcal{I} \cap r$ ed $r \subseteq \mathcal{I}$ non dipendano dalla scelta dei punti x ed y. Sia $z \in r \setminus \{x, y\}$, allora esiste $[\overline{\lambda}\colon \overline{\mu}] \in \mathbb{P}^1(\mathbb{K})$ tale che $z = \overline{\lambda}x + \overline{\mu}y$. Allora siano $[\lambda_0\colon \mu_0]$ e $[\lambda_1\colon \mu_1]$ radici omogenee dei polinomi $G_0(\lambda, \mu) = F(\lambda x + \mu y)$ e $G_1(\lambda, \mu) = F(\lambda x + \mu z)$ relative allo stesso punto di intersezione $p_0 \in \mathcal{I} \cap r$, dobbiamo mostrare che hanno la stessa molteplicità. I polinomi G_0 e G_1 descrivono due ipersuperfici in r, identificata come $\mathbb{P}^1(\mathbb{K})$, ed abbiamo che tramite i coefficienti $[\overline{\lambda}\colon \overline{\mu}]$ possiamo definire una proiettività di r che scambia i punti y e z indotta dall'applicazione lineare con matrice associata $\begin{pmatrix} \frac{1}{\lambda} & 0 \\ \overline{\mu} & \end{pmatrix}$. Osserviamo che la matrice è invertibile poiché $\overline{\mu}$ deve essere necessariamente non nullo affinché x, y e z siano punti distinti di r. Dunque le ipersuperfici definite in r da G_0 e G_1 sono proiettivamente equivalenti ed abbiamo già osservato come la molteplicità delle componenti irriducibili si conservi. Allora le molteplicità delle componenti irriducibili $\lambda_0\mu - \mu_0\lambda$ e $\lambda_1\mu - \mu_1\lambda$ delle due ipersuperfici coincidono ed entrambe coincidono con $I(\mathcal{I}, r, p_0)$. □

Valgono inoltre le seguenti proprietà:

PROPOSIZIONE 1.38. Data $r \subseteq \mathbb{P}^n(\mathbb{K})$ retta proiettiva:

(1) sia $\mathcal{I}$ ipersuperficie di $\mathbb{P}^n(\mathbb{K})$ e g una proiettività di $\mathbb{P}^n(\mathbb{K})$, allora $I(\mathcal{I}, r, p) = I(g(\mathcal{I}), g(r), g(p))$ per ogni $p \in \mathbb{P}^n(\mathbb{K})$;
(2) siano $\mathcal{I}$ e $\mathcal{J}$ ipersuperfici di $\mathbb{P}^n(\mathbb{K})$ vale che $I(\mathcal{I}+\mathcal{J}, r, p) = I(\mathcal{I}, r, p) + I(\mathcal{J}, r, p)$ per ogni $p \in \mathbb{P}^n(\mathbb{K})$ (con la convenzione che $\infty + \infty = \infty$ e $\infty + k = \infty$ per ogni $k \in \mathbb{Z}_{\geq 0}$);
(3) se $\mathbb{K} = \overline{\mathbb{K}}$ e la retta r non è contenuta nell'ipersuperficie proiettiva $\mathcal{I}$ di $\mathbb{P}^n(\mathbb{K})$ allora, sia d il grado di $\mathcal{I}$, si ha che $\sum_{p \in r} I(\mathcal{I}, r, p) = d$.

DIMOSTRAZIONE.
(1) Se r è contenuta in $\mathcal{I}$ allora anche $g(r)$ è contenuta in $g(\mathcal{I})$ e dunque vale l'identità banalmente. Presi $x, y \in r$ distinti, si noti che se $p \in r$ ha coordinate omogenee $[\lambda\colon \mu]$, allora il punto $g(p) \in g(r)$ viene descritto mediante le stesse coordinate omogenee rispetto a $g(x)$ e $g(y)$ che sono ancora distinti in $g(r)$. Allora è facile osservare che il polinomio $F(g^{-1}(\lambda g(x) + \mu g(y))) = F(\lambda x + \mu y)$ per cui $I(\mathcal{I}, r, p) = I(g(\mathcal{I}), g(r), g(p))$.
(2) Se $r \subseteq \mathcal{I}$ o $r \subseteq \mathcal{J}$ l'identità è banale. Siano F_1 ed F_2 rappresentanti rispettivamente delle ipersuperfici $\mathcal{I}$ e $\mathcal{J}$, l'ipersuperficie $\mathcal{I}+\mathcal{J}$ è descritta dal polinomio $F = F_1F_2$. Dalla definizione di molteplicità di intersezione è dunque ancora ovvia l'identità.
(3) Poiché r non è contenuta in $\mathcal{I}$ allora non esiste $p \in r$ tale che $I(\mathcal{I}, r, p) = \infty$. Allora dato che, siano $[\lambda\colon \mu]$ le coordinate omogenee di $\mathbb{P}^1(\mathbb{K})$ che identificano il punto $p \in r$, $I(\mathcal{I}, r, p)$ coincide con la molteplicità di $[\lambda\colon \mu]$ come radice del polinomio $G(\lambda, \mu)$ che ha ancora grado d. Concludiamo per il Teorema 1.35.

□

In modo del tutto analogo si definisce la molteplicità di intersezione tra una retta ed una ipersuperficie nel caso affine. Infatti, se $\mathcal{I} = [f]$ è una ipersuperficie di $\mathbb{A}^n$ ed r è la retta congiungente due punti distinti $x, y \in \mathbb{A}^n$ questa può essere parametrizzata mediante $t \in \mathbb{K}$ come $(1-t)x + ty$. Definiamo dunque $I(\mathcal{I}, r, p) = m$ se $p = (1-t_0)x + t_0y$ e t_0 è radice di molteplicità m per il polinomio in una variabile $f((1-t)x + ty)$. Procedendo in modo analogo si mostra che la definizione è ben posta e non dipende dalla scelta dei due punti $x, y \in r$.

PROPOSIZIONE 1.39. Sia $\mathcal{I}$ ipersuperficie affine, $r \subseteq \mathbb{A}^n$ retta e $p \in \mathbb{A}^n$. Dato $H \subseteq \mathbb{P}^n(\mathbb{K})$ iperpiano e $j_H\colon \mathbb{A}^n \to U_H$ l'immersione di $\mathbb{A}^n$ nella carta U_H. Allora $I(\mathcal{I}, r, p) = I(\overline{\mathcal{I}}, \overline{r}, p)$, con $\overline{\mathcal{I}}$ e $\overline{r}$ le chiusure proiettive di $\mathcal{I}$ ed r mediante U_H.

Quest'ultimo risultato ha come importante conseguenza il fatto che la molteplicità di intersezione di una ipersuperficie proiettiva $\mathcal{I}$ con una retta r può essere calcolata in una carta affine contenente il punto p.

DEFINIZIONE 1.40. Sia $\mathcal{I}$ un'ipersuperficie proiettiva di $\mathbb{P}^n(\mathbb{K})$ di grado d e sia $p \in \mathcal{I}$. Definiamo la *molteplicità di $\mathcal{I}$ in p* il numero intero

$$m_p(\mathcal{I}) = \min_{r \ni p} I(\mathcal{I}, r, p).$$

OSSERVAZIONE 1.41. Poiché la molteplicità di $\mathcal{I} = [F]$ in p è definita come un minimo escludiamo le rette contenute in $\mathcal{I}$, si ha dunque che $0 \leq m_p \leq \deg \mathcal{I}$; inoltre $m_p = 0$ se e solo se $p \notin \mathcal{I}$. Immediatamente dalla definizione segue poi che $m_p(\mathcal{I}) \leq I(\mathcal{I}, r, p)$ per ogni retta r passante per p.

Valgono inoltre proprietà speculari alle Proposizioni 1.38 e 1.39:

(1) sia $\mathcal{I}$ ipersuperficie di $\mathbb{P}^n(\mathbb{K})$ e g una proiettività, allora $m_p(\mathcal{I}) = m_{g(p)}(g(\mathcal{I}))$;
(2) siano $\mathcal{I}$ e $\mathcal{J}$ ipersuperfici di $\mathbb{P}^n(\mathbb{K})$ allora $m_p(\mathcal{I}+\mathcal{J}) = m_p(\mathcal{I}) + m_p(\mathcal{J})$;
(3) la molteplicità $m_p(\mathcal{I})$ può essere calcolata in qualunque carta affine U contente p.

Lavorando in una carta affine dove p ha coordinate affini $(0, \ldots, 0)$, la parte affine di $\mathcal{I}$ ha equazione $f = f_m + f_{m+1} + \ldots + f_d$, dove ogni f_i è un polinomio omogeneo di $\mathbb{K}[x_1, \ldots, x_n]$ di grado i ed $f_m \neq 0$. In tal caso ogni retta r passante per p ha molteplicità di intersezione con $\mathcal{I}$ in p maggiore o uguale ad m e le rette r per cui $I(\mathcal{I}, r, p) > m$ sono esattamente quelle la cui parte affine è contenuta nell'ipersuperficie $C_p(\mathcal{I})$ di $\mathbb{A}^n$ di equazione $f_m = 0$, detta *cono tangente affine* a $\mathcal{I}$ in p. La chiusura proiettiva $\overline{C_p(\mathcal{I})}$ di $C_p(\mathcal{I})$ è detta *cono proiettivo tangente* a $\mathcal{I}$ in p ed il suo supporto coincide con l'unione di p e delle rette proiettive per p tali che $I(\mathcal{I}, r, p) > m$.

ESEMPIO 1.42. Consideriamo la curva affine in $\mathbb{A}^2_{\mathbb{C}}$ di equazione $x_1^2 + x_2^2 - x_1^3 = 0$, abbiamo che il cono affine tangente in $(0, 0)$ è dato dall'equazione $x_1^2 + x_2^2 = 0$, cioè dalle rette di equazione $x_1 - ix_2$ e $x_1 + ix_2$. La chiusura proiettiva mediante U_0 di $\mathcal{I}$ è data $x_0x_1^2 + x_0x_2^2 - x_1^3$ ed il suo cono proiettivo tangente nel punto $p = [1\colon 0\colon 0]$ è dato dunque dall'ipersuperficie proiettiva di equazione $x_1^2 + x_2^2$.

Se interpretiamo $f = f_m + f_{m+1} + \ldots + f_d$ come lo sviluppo di Taylor di f centrato in $p = (0, \ldots, 0)$, si osserva subito che $p \in \mathcal{I}$ è un punto di molteplicità 1 se e solo se almeno una derivata prima di f che non si annulla p. In tal caso si dice che p è un *punto semplice*. Invece p è un punto di molteplicità $m > 1$ se e solo se f e tutte le derivate di f di ordine inferiore ad m si annullano in p ed esiste almeno una derivata di f di ordine m che non si annulla in p. Se non lavoriamo in una carta affine ma utilizziamo un'equazione omogenea $F = 0$ che definisce $\mathcal{I}$, allora per l'identità di Eulero p è un punto di molteplicità $m > 1$ se e solo se tutte le derivate parziali di F di ordine $m - 1$ si annullano in p ed esiste almeno una derivata parziale di ordine m che non si annulla in p.

DEFINIZIONE 1.43. Sia $\mathcal{I}$ un'ipersuperficie proiettiva di $\mathbb{P}^n(\mathbb{K})$ di grado d e sia r una retta proiettiva. Diciamo che la retta r è *tangente* ad $\mathcal{I}$ in p se $I(\mathcal{I}, r, p) \geq 2$. L'insieme delle rette tangenti ad $\mathcal{I}$ in un punto $p \in \mathcal{I}$ si dice *spazio tangente* ad $\mathcal{I}$ in p e si denota con $T_p\mathcal{I}$.

OSSERVAZIONE 1.44. Se una retta r è contenuta in una ipersuperficie $\mathcal{I}$, allora essa è tangente in ogni suo punto.

DEFINIZIONE 1.45. Sia $\mathcal{I} = [F]$ una ipersuperficie proiettiva su $\mathbb{K}$. Un punto $p \in \mathbb{P}^n(\overline{\mathbb{K}})$ si dice *singolare* per $\mathcal{I}$ se

$$\begin{cases} F(p) = 0 \\ \nabla F(p) = 0 \end{cases}.$$

Un'ipersuperficie proiettiva $\mathcal{I}$ su $\mathbb{K}$ si dice *liscia* se l'ipersuperficie $\mathcal{I}_{\overline{\mathbb{K}}}$, cioè l'ipersuperficie $\mathcal{I}$ vista sulla chiusura algebrica di $\mathbb{K}$, non ha punti singolari.

LEMMA 1.46. Sia $\mathcal{I}$ una ipersuperficie proiettiva su $\mathbb{K}$, $\mathcal{I} = [F]$, e $p \in \mathcal{I}$. Allora lo spazio tangente ad $\mathcal{I}$ in p coincide con l'iperpiano proiettivo di equazione

$$F_{x_0}(p)x_0 + \ldots + F_{x_n}(p)x_n = 0.$$

DIMOSTRAZIONE. Vedi [**SKKT00**, Teorema pag. 85]. □

OSSERVAZIONE 1.47. Analogamente, sia $\mathcal{I} = [f]$ ipersuperficie affine su $\mathbb{K}$ e $p \in \mathbb{A}^n$ una retta r è *tangente* ad $\mathcal{I}$ in p se $I(\mathcal{I}, r, p) \geq 2$. Si dice *liscia* se $\mathcal{I}_{\overline{\mathbb{K}}}$ non ha punti singolari. Inoltre lo *spazio tangente* ad $\mathcal{I}$ in p coincide con l'iperpiano affine di equazione

$$f_{x_1}(p)(x_1 - p_1) + \ldots + f_{x_n}(p)(x_n - p_n) = 0.$$

È valida la stessa referenza data per il Lemma 1.46.

1.4. Curve algebriche piane

Nella precedente sezione abbiamo presentato in generale le ipersuperfici nel caso affine e proiettivo per ogni dimensione n. La nostra trattazione si focalizzerà nello studio del caso $n = 2$, per questo in questa sezione parleremo più nello specifico delle *curve algebriche piane* e dello studio delle loro proprietà presentate in questo capitolo.

DEFINIZIONE 1.48. Si chiamano *curve algebriche piane* sul campo $\mathbb{K}$ le ipersuperfici nel caso $n = 2$. In particolare si dicono *curve algebriche piane affini* le ipersuperfici affini di $\mathbb{A}^2_{\mathbb{K}}$ e *curve algebriche piane proiettive* le ipersuperfici proiettive di $\mathbb{P}^2(\mathbb{K})$.

Sia $\mathcal{C}$ una curva proiettiva di grado d di $\mathbb{P}^2(\mathbb{K})$ e sia $p \in \mathbb{P}^2(\mathbb{K})$. Se $F(x_0, x_1, x_2) = 0$ è un'equazione omogenea di $\mathcal{C}$, allora come già detto p è un punto semplice per $\mathcal{C}$ se e solo se $F(p) = 0$ ed almeno una delle derivate parziali di F non si annulla in p. In tal caso la retta tangente a $\mathcal{C}$ in p (vedi Lemma 1.46) ha equazione

$$F_{x_0}(p)x_0 + F_{x_1}(p)x_1 + F_{x_2}(p)x_2 = 0.$$

Un punto $p \in Sing(\mathcal{C})$ si dice *punto doppio* se $m_p(\mathcal{C}) = 2$, *triplo* se $m_p(\mathcal{C}) = 3$, *m-uplo* se $m_p(\mathcal{C}) = m$. Il punto $p \in \mathcal{C}$ risulta m-uplo se e solo se tutte le derivate $(m-1)$-esime di F si annullano in p ed esiste almeno una derivata m-esima di F che non si annulla in p.

PROPOSIZIONE 1.49. Se $\mathcal{C}$ e $\mathcal{D}$ sono due curve piane proiettive su $\mathbb{K} = \overline{\mathbb{K}}$ irriducibili e ridotte. Allora $\mathcal{C} \cap \mathcal{D}$ è finito.

DIMOSTRAZIONE. Immediata conseguenza del teorema di Bézout 5.30. □

TEOREMA 1.50. Sia $\mathcal{C}$ una curva algebrica in $\mathbb{P}^2(\mathbb{K})$. Se $\mathcal{C} = m_1\mathcal{C}_1 + \ldots + m_s\mathcal{C}_s$ è la scomposizione in componenti irriducibili di $\mathcal{C}$ allora

$$Sing(\mathcal{C}) = \bigcup_{\substack{1 \leq i \leq s \\ \text{t.c. } m_i = 1}} Sing(\mathcal{C}_i) \cup \bigcup_{\substack{1 \leq i < j \leq s \\ \text{t.c. } m_i = m_j = 1}} (\mathcal{C}_i \cap \mathcal{C}_j) \cup \bigcup_{\substack{1 \leq i \leq s \\ \text{t.c. } m_i > 1}} \mathcal{C}_i.$$

DIMOSTRAZIONE. Siano $F_1, \ldots, F_s$ polinomi omogenei rappresentanti le componenti irriducibili $\mathcal{C}_1, \ldots, \mathcal{C}_s$ abbiamo per la regola di Leibniz

$$\nabla F = \sum_{i=1}^{s} m_i F_1^{m_1} \cdots F_i^{m_i - 1} \cdots F_s^{m_s} \cdot \nabla F_i.$$

Se p appartiene a più di una componente irriducibile di $\mathcal{C}$ oppure ad una componente irriducibile di molteplicità $m_i > 1$ allora il membro a destra dell'uguaglianza è nullo e dunque $p \in Sing(\mathcal{C})$. Se invece p appartiene soltanto ad una componente irriducibile $\mathcal{C}_j$ che è di molteplicità 1 allora abbiamo che $\nabla F = c' \nabla F_j$ con $c' = \prod_{\substack{i=1 \\ i \neq j}}^{s} F_i^{m_i}(p) \neq 0$. Dunque $\nabla F(p) = 0$ se e solo se $\nabla F_j(p) = 0$. □

COROLLARIO 1.51. Sia $\mathcal{C}$ una curva algebrica piana proiettiva ridotta su $\mathbb{K} = \overline{\mathbb{K}}$. Allora $Sing(\mathcal{C})$ è finito.

DIMOSTRAZIONE. Se $\deg \mathcal{C} = 1$ allora è una retta e dunque è liscia. Assumiamo dunque $\deg \mathcal{C} \geq 2$. Per il teorema precedente abbiamo che

$$Sing(\mathcal{C}) = \bigcup_{1 \leq i \leq s} C_i \cup \bigcup_{\substack{1 \leq i < j \leq s \\ \text{t.c. } m_i = m_j = 1}} (\mathcal{C}_i \cap \mathcal{C}_j)$$

con $\mathcal{C}_i$ le componenti irriducibili di $\mathcal{C}$. Sappiamo per il Teorema di Bézout 5.30 che $\mathcal{C}_i \cap \mathcal{C}_j$, $i \neq j$, è composto al più da $\deg \mathcal{C}_i \deg \mathcal{C}_j$ punti. Per concludere è sufficiente mostrare che se $\mathcal{C}$ è irriducibile allora $Sing(\mathcal{C})$ è finito. Sia $\mathcal{C} = [F]$. Dato che $F \neq 0$ allora esiste almeno una derivata parziale $F_{x_i} \neq 0$, senza perdere di generalità supponiamo F_{x_0}, e dunque, posta $\mathcal{D} = [F_{x_i}]$ ha grado $\deg \mathcal{C} - 1$, si ha che $Sing(\mathcal{C}) \subseteq \mathcal{C} \cap \mathcal{D}$ che ha cardinalità finita ancora per il teorema di Bézout 5.30 dato che $\mathcal{C}$ e $\mathcal{D}$ non hanno componenti in comune poiché $\deg \mathcal{C} > \deg \mathcal{D}$ e $\mathcal{C}$ è irriducibile. Dunque $Sing(\mathcal{C})$ è finito come unione finita di insiemi finiti. □

COROLLARIO 1.52. Sia $\mathcal{C}$ una curva algebrica piana proiettiva su un campo algebricamente chiuso. Se $\mathcal{C}$ è non singolare allora è irriducibile e ridotta.

DIMOSTRAZIONE. Se per assurdo $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2$ fosse riducibile si avrebbe che i punti di $\mathcal{C}_1 \cap \mathcal{C}_2$ sarebbero singolari per $\mathcal{C}$. Analogamente se non fosse ridotta i punti della componente multipla sarebbero singolari. □

DEFINIZIONE 1.53. Una retta r viene detta *tangente principale* ad una curva $\mathcal{C}$ nel punto p se $I(\mathcal{C}, r, p) > m_p(\mathcal{C})$.

Osserviamo che nei punti semplici la nozione di tangente e di tangente principale coincidono. Se p è un punto multiplo di molteplicità m allora tutte le rette passanti per p sono tangenti mentre le tangenti principali sono quelle contenute nel cono tangente a $\mathcal{C}$ in p.

Per studiare localmente la curva in un punto p è utile scegliere una carta dove $p = (0, 0)$ in coordinate affini. In tale carta si osserva facilmente che, se f è il polinomio che descrive la parte affine di $\mathcal{C}$ in tale carta e lo scriviamo come somma di parti omogenee, la molteplicità nell'origine coincide con il grado della parte omogenea non nulla di grado minimo di f. Le parti affini delle tangenti principali in p sono allora definite dai fattori lineari di tale parte omogenea. Segue dunque dal Teorema 1.35 che se $\mathbb{K}$ è algebricamente chiuso che la curva $\mathcal{C}$ in p ha esattamente m tangenti principali, contate con molteplicità.

DEFINIZIONE 1.54. Sia $\mathbb{K}$ algebricamente chiuso e sia p un punto singolare di una curva $\mathcal{C}$. Il punto si dice *ordinario* se la curva ha esattamente $m_p(\mathcal{C})$ tangenti principali distinte in p. Un punto doppio viene chiamato *nodo* se è ordinario, *cuspide* se è non ordinario; più precisamente si parla di *cuspide ordinaria* se l'unica tangente principale in p ha molteplicità di intersezione esattamente 3 con la curva nel punto.

Se in una carta affine la curva $\mathcal{C}$ ha equazione $f(x, y) = 0$ e $p = (a, b)$ è non singolare, allora la retta di equazione

$$f_x(a, b)(x - a) + f_y(a, b)(y - b) = 0$$

è la parte affine della tangente (principale) a $\mathcal{C}$ in p e si chiama *tangente affine* a $\mathcal{C}$ in p.

DEFINIZIONE 1.55. Una retta affine r viene detta *asintoto* per una curva affine $\mathcal{D}$ se la sua chiusura proiettiva $\overline{r}$ è tangente principale a $\overline{\mathcal{D}}$ in uno dei suoi punti impropri.

CAPITOLO 2

Anelli

2.1. Anelli ed ideali

DEFINIZIONE 2.1. Un *anello* è una terna $(A, +, \cdot)$ dove A è un insieme e $+$ e $\cdot$ sono due operazioni binarie su A chiamate rispettivamente addizione e moltiplicazione tali che:

(i) A è un gruppo abeliano rispetto all'operazione di addizione;
(ii) la moltiplicazione è associativa e distributiva rispetto all'addizione, cioè per ogni $x, y, z \in A$

$$(xy)z = x(yz) = xyz,$$
$$(x + y)z = xz + yz,$$
$$x(y + z) = xy + xz.$$

Un anello A si dice *commutativo* se per ogni $x, y \in A$ $xy = yx$. Un anello si dice *unitario*, o *con identità*, se esiste un elemento $e \in A$ tale che $xe = ex = x$ per ogni $x \in A$; poiché tale elemento è ovviamente unico lo denotiamo con 1.

NOTA 2.2. Tutti gli anelli che prenderemo in considerazione sono commutativi con unità.

DEFINIZIONE 2.3. Dati due anelli A e B, un *omomorfismo di anelli* tra A e B è un'applicazione $\varphi\colon A \to B$ tale che:

i) φ è un omomorfismo di gruppi abeliani,
ii) $\varphi(xy) = \varphi(x)\varphi(y)$ per ogni $x, y \in A$,
iii) $\varphi(1_A) = 1_B$.

In altre parole φ conserva l'addizione, la moltiplicazione ed il suo elemento neutro. Un omomorfismo di anelli φ si dice un *isomorfismo* se è bigettivo (l'inversa è automaticamente un omomorfismo di anelli).

Un sottoinsieme $A' \subseteq A$ si dice un *sottoanello* di A se è un sottogruppo additivo chiuso rispetto alla moltiplicazione e contiene l'elemento unità di A. Se $\varphi\colon A \to B$ e $\psi\colon B \to C$ sono omomorfismi di anelli, anche la loro composizione $\psi \circ \varphi\colon A \to C$ lo è.

DEFINIZIONE 2.4. Un *ideale* di A è un sottoinsieme $I \subseteq A$ che è un sottogruppo additivo e gode della proprietà di assorbimento, cioè $xy \in I$ per ogni $x \in A$ e per ogni $y \in I$.

OSSERVAZIONE 2.5. Dato un omomorfismo di anelli $\varphi\colon A \to B$, il *nucleo* di φ $\ker(\varphi)$ è un ideale di A e l'*immagine* di φ $\mathrm{im}(\varphi)$ è un sottoanello di B.

OSSERVAZIONE 2.6. Sia $x \in A$, i multipli di x formano un ideale, detto *principale*, di A denotato con (x). Un dominio dove ogni ideale è principale si dice *dominio ad ideali principali* (PID).

Dato un ideale I in A, il gruppo quoziente A/I eredita una moltiplicazione definita in modo unico da A che lo rende un anello, chiamato l'*anello quoziente*. Gli elementi di A/I sono le classi laterali di a in A e la moltiplicazione è definita come $[x][y] = [xy]$ per ogni $[x], [y] \in A/I$, ben definita sui rappresentati della classe, e con elemento unità $[1]$. La mappa di proiezione al quoziente $\Phi\colon A \to A/I$ è un morfismo di anelli. È bene tenere a mente il seguente risultato:

PROPOSIZIONE 2.7. Sia A un anello ed $I \subseteq A$ un ideale. Allora esiste una corrispondenza biunivoca, che conserva l'ordinamento, tra gli ideali $J \subseteq A$ che contengono I e gli ideali $\overline{J}$ di A/I data da $J = \Phi^{-1}(\overline{J})$ e $\overline{J} = J/I$.

DEFINIZIONE 2.8. Un elemento $x \in A$ si dice:

a) un *divisore dello zero* se esiste $y \in A \setminus \{0\}$ tale che $xy = 0$. Un anello non nullo senza divisori dello zero non nulli si dice *dominio di integrità*, o più brevemente *dominio*;
b) *invertibile* se esiste $y \in A$ tale che $xy = yx = 1$. Un anello non nullo dove ogni elemento non nullo è invertibile si dice un *campo*;
c) *nilpotente* se esiste $n \in \mathbb{Z}_{>0}$ tale che $x^n = 0$. Un anello in cui l'unico elemento nilpotente è nullo si dice *ridotto*.

OSSERVAZIONE 2.9. Sia $x \in A$ un elemento invertibile, allora $(x) = A$.

Ci sono due importanti proprietà degli ideali da ricordare e da analizzare più nel dettaglio al fine della localizzazione:

DEFINIZIONE 2.10. Un ideale $\mathfrak{p} \subseteq A$ si dice *primo* se $\mathfrak{p} \neq (1)$ e se per ogni $x, y \in A$ tali che $xy \in \mathfrak{p}$ allora $x \in \mathfrak{p}$ o $y \in \mathfrak{p}$.

Un ideale $\mathfrak{m} \subsetneq A$ si dice *massimale* se $\mathfrak{m} \neq (1)$ e se non esiste alcun ideale $I \subsetneq A$ tale che $\mathfrak{m} \subsetneq a$. Indichiamo con $\mathrm{Spec}(A)$ l'insieme degli ideali primi di A e con $\mathrm{Specm}(A)$ l'insieme degli ideali massimali di A.

OSSERVAZIONE 2.11. Le definizioni di ideale primo e massimale possono essere date in modo equivalente come:

$\mathfrak{p}$ è primo se e solo se $A/\mathfrak{p}$ è un dominio di integrità;

$\mathfrak{m}$ è massimale se e solo se $A/\mathfrak{m}$ è un campo.

Da questa nuova definizione possiamo facilmente dedurre che un ideale massimale $\mathfrak{m}$ è anche primo, mentre non è tuttavia vero in generale il viceversa. L'ideale nullo è primo se e solo se A è un dominio di integrità.

Inoltre, se $\varphi\colon A \to B$ è un omomorfismo di anelli e $\mathfrak{q}$ è un ideale primo di B, allora $\varphi^{-1}(\mathfrak{q})$ è un ideale primo di A, poiché $A/\varphi^{-1}(\mathfrak{q})$ è isomorfo ad un sottoanello di $B/\mathfrak{q}$ che è un dominio. Se invece $\mathfrak{n}$ è un ideale massimale di B, non è necessariamente vero che $\varphi^{-1}(\mathfrak{n})$ massimale in A, possiamo solo dire che è primo.

ESEMPIO 2.12. Considerando banalmente $A = \mathbb{Z}$, $B = \mathbb{Q}$ ed $\mathfrak{n} = 0$ l'ideale nullo. Si ha che $\mathfrak{n}$ è massimale in $\mathbb{Q}$ perché questo è un campo, mentre $\varphi^{-1}(\mathfrak{n}) = 0$, con φ data da $k \mapsto k/1$, non è un ideale massimale in $\mathbb{Z}$.

Poiché gli ideali primi sono particolarmente importanti per i nostri fini, abbiamo il seguente teorema ed i suoi corollari che ci assicurano che ce ne sia sempre una quantità sufficiente.

TEOREMA 2.13. Ogni anello A non nullo possiede almeno un ideale massimale.

DIMOSTRAZIONE. Sia Σ l'insieme di tutti gli ideali propri di A ed ordiniamo Σ rispetto l'inclusione. Osserviamo che $\Sigma \neq \varnothing$ poiché abbiamo perlomeno l'ideale nullo. Sia (I_α) una catena di ideali in Σ, cioè una famiglia tale che per ogni coppia di indici α, β si ha che $I_\alpha \subseteq I_\beta$ oppure $I_\beta \subseteq I_\alpha$. Poniamo $I = \bigcup_\alpha I_\alpha$ si verifica facilmente che questo è ancora un ideale e $1 \notin I$ poiché $1 \notin I_\alpha$ per ogni α. Allora $I \in \Sigma$ ed è un maggiorante della catena. Per il lemma di Zorn Σ possiede un elemento massimale, cioè A possiede un ideale massimale. □

COROLLARIO 2.14. Se I è un ideale proprio di un anello A allora esiste un ideale massimale di A che lo contiene.

DIMOSTRAZIONE. Applicando il Teorema 2.13 all'anello A/I, che è non nullo, otteniamo un ideale massimale $\overline{\mathfrak{m}}$ in A/I. Per la corrispondenza vista questo corrisponde ad un ideale $\mathfrak{m} = \Phi^{-1}(\overline{\mathfrak{m}})$ in A contenente I. Φ è suriettiva e dunque $\mathfrak{m}$ è un ideale massimale in A. □

COROLLARIO 2.15. Ogni elemento non invertibile di un ideale A è contenuto in un ideale massimale.

DEFINIZIONE 2.16. Sia A un anello. Definiamo il *radicale di Jacobson* $J(A)$ di A come $J(A) = \bigcap_{\mathfrak{m}\in \mathrm{Specm}(A)} \mathfrak{m}$.

Se la definizione del radicale di Jacobson non dà particolari informazioni sugli elementi che ne fanno parte, questi possono essere caratterizzati nel seguente modo:

PROPOSIZIONE 2.17. Sia A un anello, sia $x \in A$. Allora $x \in J(A)$ se e solo se $1 - xy$ è invertibile in A per ogni $y \in A$.

DIMOSTRAZIONE. ($\Rightarrow$) Supponiamo per assurdo che $1 - xy$ non sia invertibile per qualche $y \in A$. Allora per quanto visto esiste un ideale massimale $\mathfrak{m}$ tale che $1 - xy \in \mathfrak{m}$; ma $x \in J(A) \subseteq \mathfrak{m}$, dunque $xy \in \mathfrak{m}$ e pertanto allora $1 \in \mathfrak{m}$, il che è assurdo.

($\Leftarrow$) Supponiamo che $x \notin \mathfrak{m}$ per qualche ideale massimale $\mathfrak{m}$. Allora $(x) + \mathfrak{m} = A$ e pertanto esistono $y \in A$ ed $u \in \mathfrak{m}$ tali che $1 = u + xy$. Ne segue allora che $1 - xy \in \mathfrak{m}$ e non può essere dunque invertibile. □

DEFINIZIONE 2.18. Un anello A si dice *locale* se ha un solo ideale massimale $\mathfrak{m}$. Il suo quoziente $A/\mathfrak{m}$ è chiamato il *campo residuo di* A. Si dice *semilocale* se ha un numero finito di ideali massimali.

DEFINIZIONE 2.19. Sia $f\colon A \to B$ un omomorfismo di anelli. Sia I un ideale di A si definisce l'*estensione* di I come l'ideale $Bf(I)$ generato da $f(I)$ in B: esplicitamente $Bf(I)$ è l'insieme di tutte le somme del tipo $\sum y_i f(x_i)$ dove $x_i \in I$, $y_i \in B$. Se J è un ideale di B, allora $f^{-1}(J)$ è sempre un ideale in A ed è chiamato la *contrazione* di J in A.

OSSERVAZIONE 2.20. Se $\mathfrak{q}$ è un ideale primo in B, $f^{-1}(\mathfrak{q})$ è primo in A. Se $\mathfrak{p}$ è primo in A non è detto che $Bf(\mathfrak{p})$ sia primo in B.

DIMOSTRAZIONE. Supponiamo $\mathfrak{q}$ primo in B. Siano $x, y \in A$ tali che $xy \in f^{-1}(\mathfrak{q})$ allora esiste $z \in \mathfrak{q}$ tale che $f(xy) = f(x)f(y) = z$, allora poiché $\mathfrak{q}$ è primo $f(x) \in \mathfrak{q}$ oppure $f(y) \in \mathfrak{q}$, dunque $x \in f^{-1}(\mathfrak{q})$ oppure $y \in f^{-1}(\mathfrak{q})$. Presa ad esempio $f\colon \mathbb{Z} \to \mathbb{Q}$ definita come $x \mapsto x/1$, allora sia I un ideale proprio non nullo di $\mathbb{Z}$, si ha che $f(I)\mathbb{Q} = \mathbb{Q}$ che non mai è un ideale primo. □

DEFINIZIONE 2.21. Sia A un anello e $\mathfrak{p}$ un suo ideale primo. Definiamo l'*altezza* di $\mathfrak{p}$ come $\operatorname{height}\mathfrak{p} := \sup\{n \in \mathbb{Z}_{\geq 0} \mid \exists\ \mathfrak{p}_0, \ldots, \mathfrak{p}_{n-1} \in \operatorname{Spec} A \text{ tali che } \mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_{n-1} \subsetneq \mathfrak{p}\}$. Definiamo poi la *dimensione di Krull* di A come $\dim A := \sup\{\operatorname{height}\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Spec}(A)\}$.

OSSERVAZIONE 2.22. Sia A un anello. Se $\dim A = 0$ allora ogni coppia di ideali primi è incomparabile. Ciò equivale dunque a dire che ogni ideale primo è massimale in un anello con dimensione di Krull nulla.

DEFINIZIONE 2.23. Sia A un anello ed I un suo ideale. Definiamo il *radicale* di I, denotato con $\sqrt{I}$, come $\sqrt{I} := \{a \in A \mid a^k \in I \text{ per qualche } k \in \mathbb{Z}_{>0}\}$. Diciamo che un ideale I di A è *radicale* se $I = \sqrt{I}$.

2.2. Moduli

DEFINIZIONE 2.24. Sia A un anello. Un *A-modulo* è una coppia (M, μ), dove M è un gruppo abeliano e $\mu\colon A \times M \to M$ è un'applicazione da $A \times M$ ad M, denotata con

$\mu(a,x) = ax$, tale che per ogni $a, b \in A$ e per ogni $x, y \in M$ vale che:

$$\begin{aligned} a(x+y) &= ax + ay, \\ (a+b)x &= ax + bx, \\ (ab)x &= a(bx), \\ 1x &= x. \end{aligned}$$

Seppur la nozione di A-modulo sia appena stata introdotta, si osserva facilmente come sia una generalizzazione che accoglie molti oggetti familiari, di cui possiamo dare alcuni esempi:

ESEMPIO 2.25. 1) Un ideale I di un anello A è un A-modulo, così come A stesso.
2) Un gruppo abeliano è uno $\mathbb{Z}$-modulo.
3) Se invece A è un campo $\mathbb{K}$ è chiaro che la nozione di A-modulo coincide con quella di $\mathbb{K}$-spazio vettoriale.
4) Se $A = \mathbb{K}[x]$, dove $\mathbb{K}$ è un campo, un A-modulo è un $\mathbb{K}$-spazio vettoriale V insieme ad una trasformazione $\mathbb{K}$-lineare $f \in \mathrm{End}_{\mathbb{K}}(V)$.
5) Sia G un gruppo abeliano finito ed $A = \mathbb{K}[G]$ l'algebra-gruppo di G sul campo $\mathbb{K}$. Allora gli A-moduli sono le $\mathbb{K}$-rappresentazioni di G.

Come per ogni struttura algebrica è naturale dare la definizione di morfismo.

DEFINIZIONE 2.26. Siano A un anello ed M, N due A-moduli, Un'applicazione $f\colon M \to N$ è un *omomorfismo di A-moduli* (ossia è *A-lineare*) se per ogni $x, y \in M$ e per ogni $a \in A$

$$\begin{aligned} f(x+y) &= f(x) + f(y), \\ f(ax) &= af(x). \end{aligned}$$

Se l'applicazione f è bigettiva si dice che f è un *isomorfismo* di A-moduli.

In altri termini un omomorfismo di A-moduli è un omomorfismo di gruppi abeliani che commuta rispetto all'azione di ogni elemento $x \in A$. Se A è un campo, un omomorfismo di A-moduli è la stessa cosa di una trasformazione lineare. La composizione di omomorfismi di A-moduli è ancora un omomorfismo di A-moduli. L'insieme di tutti gli omomorfismi di A-moduli da M ad N può essere anch'esso dotato di una struttura di A-modulo nel seguente modo: dati due omomorfismi di A-moduli $f, g\colon M \to N$ ed $a \in A$ definiamo $f+g$ ed af come $(f+g)(x) = f(x)+g(x)$ ed $(af)(x) = af(x)$ per ogni $x \in M$. Tale A-modulo si denota con $\mathrm{Hom}_A(M,N)$ (o anche $\mathrm{Hom}(M,N)$ se non vi è ambiguità rispetto all'anello A). Dati due omomorfismi di A-moduli $u\colon M' \to M$ e $v\colon N \to N''$ inducono delle applicazioni

$$u^*\colon \mathrm{Hom}(M,N) \to \mathrm{Hom}(M',N) \quad \text{e} \quad v_*\colon \mathrm{Hom}(M,N) \to \mathrm{Hom}(M,N'')$$

definite come

$$u^*(f) = f \circ u \quad \text{e} \quad v_*(f) = v \circ f.$$

Tali applicazioni sono omomorfismi di A-moduli. Per un qualsiasi A-modulo M c'è un isomorfismo naturale $\mathrm{Hom}(A,M) \cong M$: dato un omomorfismo di A-moduli $f\colon A \to M$ questo è univocamente determinato da $f(1)$ che può essere un arbitrario elemento di M. Allora costruiamo la corrispondenza come $f \mapsto f(1)$.

Un *A-sottomodulo* M' di un A-modulo M è un sottogruppo di M chiuso rispetto alla moltiplicazione per elementi di A. Il gruppo abeliano quoziente M/M' allora eredita una struttura di A-modulo da M, definita ponendo $a[x] = [ax]$. L'A-modulo M/M' è il *quoziente* di M rispetto ad M'. L'applicazione naturale di proiezione al quoziente di M su M/M' è un omomorfismo di A-moduli. Analogamente a quanto enunciato nella Proposizione 2.7 esiste una corrispondenza biunivoca tra gli A-sottomoduli del modulo quoziente M/M' e gli A-sottomoduli di M contenenti M' (di cui dunque il caso per gli ideali di un anello è un caso particolare).

Se $f\colon M \to N$ è un omomorfismo di A-moduli, allora il *nucleo* di f è l'insieme $\ker(f) = \{x \in M \mid f(x) = 0\}$ ed è un sottomodulo di M. L'*immagine* di f è l'insieme $\operatorname{im}(f) = f(M)$ ed è un sottomodulo di N. Il *conucleo* di f è $\operatorname{coker}(f) = N/\operatorname{im}(f)$ ed è un modulo quoziente di N. Se M' è un A-sottomodulo di M tale che $M' \subseteq \ker(f)$, allora f dà origine ad un omomorfismo $\overline{f}\colon M/M' \to N$ definito come $\overline{f}([x]) = f(x)$. Il nucleo di $\overline{f}$ è $\ker(f)/M'$. L'omomorfismo di A-moduli $\overline{f}$ è detto l'omomorfismo *indotto* da f. In particolare, come accade nella maggior parte delle strutture algebriche, prendendo $M' = \ker(f)$ si ha un isomorfismo di A-moduli $M/\ker(f) \cong \operatorname{im}(f)$.

Sia adesso M un A-modulo e sia $\{M_i\}_{i\in I}$ un famiglia di A-sottomoduli. La loro *somma* $\sum_{i\in I} M_i$ è l'insieme di tutte le somme $\sum_{i\in I} x_i$ dove $x_i \in M_i$ per ogni $i \in I$ e gli x_i sono tutti nulli tranne che un numero finito. È naturale la struttura di A-modulo su $\sum_{i\in I} M_i$ ed esso è il più piccolo A-sottomodulo di M contenente tutti gli M_i. Anche la loro intersezione $\bigcap_{i\in I} M_i$ è un A-sottomodulo di M.

Proposizione 2.27. Sia A un anello.

i) Se $N \subseteq M \subseteq L$ sono A-moduli, allora $(L/N)/(M/N) \cong L/M$.
ii) Se M_1, M_2 sono A-sottomoduli di M, allora $(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2)$.

Dimostrazione. i) Definiamo l'applicazione $\psi\colon L/N \to L/M$ definita come $[x]_N \mapsto [x]_M$. Poiché abbiamo per ipotesi $N \subseteq M$ tale è ben posta. È inoltre ovviamente un omomorfismo di A-moduli. Tale omomorfismo è ovviamente suriettivo dato che $[x]_M$ è immagine di $[x]_N$ per definizione, mentre $\ker\psi = \{[x]_N \in L/N \mid x \in M\} = M/N$. Allora per quanto detto $L/M \cong (L/N)/\ker\psi = (L/N)/(M/N)$.

ii) Consideriamo l'omomorfismo composto $M_2 \to M_1 + M_2 \to (M_1 + M_2)/M_1$ data da $x_2 \mapsto x_2 \mapsto [x_2]_{M_1}$. Questo è suriettivo: sia $[x_1 + x_2]_{M_1}$ abbiamo che questo coincide con $[x_2]_{M_1}$ che è l'immagine di x_2 tramite l'omomorfismo dato sopra. Il suo nucleo è $\{x \in M_2 \mid x \in M_1\} = M_1 \cap M_2$. Dunque la tesi.

□

Non avendo un prodotto tra gli elementi di M non si può definire il *prodotto* di due – e quindi più – sottomoduli, ma si può definire il prodotto IM, dove I è un ideale di A ed M è un A-modulo; esso è l'insieme delle somme finite $\sum_i a_i x_i$ con $a_i \in I$, $x_i \in M$, ed è un A-sottomodulo di M.

Osservazione 2.28. Abbiamo detto che dato un anello A esso stesso un A-modulo e che i suoi ideali sono i suoi A-sottomoduli. In questo caso allora ritroviamo dalle operazioni appena definite sui sottomoduli le note operazione sugli ideali con in aggiunta il prodotto tra ideali, che discende dal prodotto IM tra ideale e modulo.

Definizione 2.29. Siano N, P A-sottomoduli un A-modulo M, si definisce l'*ideale quoziente* tra N e P come $(N : P) = \{a \in A \mid aP \subseteq N\}$ ed esso è un ideale di A. In particolare, $\operatorname{Ann}_A(M) := (0 : M) = \{a \in A \mid aM = 0\}$ è chiamato l'*annulatore* di M.

Osservazione 2.30. Sia $I \subseteq \operatorname{Ann}(M)$ un ideale. Possiamo considerare M come un A/I-modulo nel modo seguente: se $[x] \in A/I$ è rappresentata da $x \in A$ definiamo $[x]m = xm$ con $m \in M$. Ciò è indipendente dalla scelta del rappresentante di $[x]$ poiché $IM = 0$ stando nell'annullatore di M. Si dice che un A-modulo è *fedele* se $\operatorname{Ann}(M) = 0$. Dunque in generale M è fedele come $A/\operatorname{Ann}(M)$-modulo.

Proposizione 2.31. Siano M_1, M_2 A-sottomoduli di un A-modulo M. Allora:

i) $\operatorname{Ann}(M_1 + M_2) = \operatorname{Ann}(M_2) \cap \operatorname{Ann}(M_2)$;
ii) $(M_1 \colon M_2) = \operatorname{Ann}((M_1 + M_2)/M_1)$.

Se $x \in M$, l'insieme $\{ax \mid a \in A\}$ è un A-sottomodulo di M, denotato con Ax. Se $M = \sum_{i\in I} Ax_i$, si dice che gli elementi x_i formano un *sistema di generatori* di M; ciò significa che ogni suo elemento può essere espresso (non necessariamente in modo unico)

come combinazione A-lineare finita degli x_i. Un A-modulo M si dice *finitamente generato* se possiede un sistema finito di generatori.

DEFINIZIONE 2.32. Se M, N sono A-moduli, la loro *somma diretta* $M \oplus N$ è l'insieme di tutte le coppie ordinate (x, y) con $x \in M$, $y \in N$. Esso è un A-modulo se definiamo l'addizione e la moltiplicazione per uno scalare nel modo ovvio:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$
$$a(x, y) = (ax, ay).$$

Più in generale, se $(M_i)_{i \in I}$ è una qualsiasi famiglia di A-moduli, si può definire la loro *somma diretta* $\bigoplus_{i \in I} M_i$: i suoi elementi sono le famiglie $(x_i)_{i \in I}$ tali che $x_i \in M_i$ per ogni $i \in I$ e quasi tutti gli x_i tranne un numero finito sono nulli. Se si elimina la restrizione sul numero di elementi x_i non nulli, si ottiene il *prodotto diretto* $\prod_{i \in I} M_i$.

DEFINIZIONE 2.33. Un A-modulo *libero* è un A-modulo isomorfo ad uno della forma $\bigoplus_{i \in I} M_i$ dove ciascun $M_i \cong A$ (come A-modulo). Si usa talvolta la notazione $A^{(I)}$. Un A-modulo libero finitamente generato è pertanto isomorfo ad $A \oplus \ldots \oplus A$ con n addendi, che si denota $A^{\oplus n}$ (Per convenzione, A^0 è il modulo nullo). La cardinalità di una – e quindi di ciascuna – base è detta il *rango* del modulo libero M.

PROPOSIZIONE 2.34. M è un A-modulo finitamente generato se e solo se M è isomorfo ad un quoziente di A^n per qualche $n \geq 0$.

DIMOSTRAZIONE. ($\Rightarrow$) Siano $x_1, \ldots, x_n$ un sistema di generatori di M e $\Phi \colon A^{\oplus n} \to M$ definita come $\Phi(a_1, \ldots, a_n) = a_1 x_1 + \ldots + a_n x_n$. Allora Φ è suriettivo poiché $x_i = \Phi(0, \ldots, 1, \ldots, 0)$ (con 1 in i-esima posizione), e pertanto $M \cong A^{\oplus n} / \ker \Phi$.

($\Leftarrow$) Si ha un omomorfismo di A-moduli suriettivo Φ di $A^{\oplus n}$ su M. Se indichiamo con $e_i = (0, \ldots, 1, \ldots, 0)$ l'elemento avente 1 all'i-esimo posto e tutti 0 altrove, abbiamo che gli $e_1, \ldots, e_n$ generano $A^{\oplus n}$ e quindi gli elementi $\Phi(e_1), \ldots, \Phi(e_n)$ generano M. □

LEMMA 2.35 (Lemma di Nakayama). Sia M un A-modulo finitamente generato e I un ideale di A contenuto nel radicale di Jacobson $J(A)$ di A. Allora $IM = M$ implica $M = 0$.

DIMOSTRAZIONE. Supponiamo $M \neq 0$, e siano $u_1, \ldots, u_n$ un sistema minimale di generatori per M. Allora $u_n \in IM$, sicché si ha un'equazione della forma $u_n = a_1 u_1 + \ldots + a_n u_n$, con $a_i \in I$. Dunque

$$(1 - a_n) u_n = a_1 u_1 + \ldots + a_{n-1} u_{n-1};$$

poiché $a_n \in J(A)$ abbiamo per la Proposizione 2.17 $1 - a_n$ è invertibile in A. Ne segue che u_n appartiene al sottomodulo di M generato da $u_1, \ldots, u_{n-1}$: ciò è una contraddizione alla minimalità. □

COROLLARIO 2.36. Sia M un A-modulo finitamente generato, N un A-sottomodulo di M, $I \subseteq J(A)$ un ideale di A. Allora $M = IM + N$ implica $M = N$.

DIMOSTRAZIONE. Applichiamo il Lemma di Nakayama al modulo M/N osservando che $I(M/N) = (IM + N)/N = M/N$. □

Sia A un anello locale, $\mathfrak{m}$ il suo ideale massimale e $\mathbb{K} = A/\mathfrak{m}$ il suo campo residuo. Sia M un A-modulo finitamente generato. Il modulo quoziente $M/\mathfrak{m}M$ è annullato da $\mathfrak{m}$, dunque è in modo naturale un $A/\mathfrak{m}$-modulo, cioè un $\mathbb{K}$-spazio vettoriale, e come tale ha dimensione finita (poiché M è finitamente generato).

PROPOSIZIONE 2.37. Sia $(A, \mathfrak{m})$ un anello locale ed M un A-modulo finitamente generato. Siano $u_1, \ldots, u_n \in M$ e $\overline{u}_i = \pi(u_i)$ per ogni $1 \leq i \leq n$ con $\pi \colon M \twoheadrightarrow M/\mathfrak{m}M$. Allora $\{u_1, \ldots, u_n\}$ è un sistema minimale di generatori per M come A-modulo se e solo se $\{\overline{u}_1, \ldots, \overline{u}_n\}$ è una base di $M/\mathfrak{m}M$ come $A/\mathfrak{m}$-spazio vettoriale

DIMOSTRAZIONE. Siano $\{u_i\}$ elementi di M tali che $\{\overline{u}_i\}$ generano $M/\mathfrak{m}M$ come $A/\mathfrak{m}$-spazio vettoriale. Sia $N = \sum_{i=1}^{n} Au_i$. L'applicazione composta $N \hookrightarrow M \twoheadrightarrow M/\mathfrak{m}M$ è suriettiva; dunque $N + \mathfrak{m}M = M$, da cui $N = M$ per il Lemma 2.35 e dunque gli u_i generano M come A-modulo.

($\Rightarrow$) Se per assurdo $\{\overline{u}_i\}$ non fosse una base allora un suo sottinsieme sarebbe una base. Allora un sottoinsieme degli $\{u_i\}$ sarebbe un sistema di generatori contraddicendo la minimalità.

($\Leftarrow$) Se per assurdo adesso $\{u_i\}_{1\leq i\leq n}$ non fosse un sistema minimale di generatori avremo che un suo sottoinsieme genererebbe M come A-modulo. Allora un sottoinsieme degli $\{\overline{u}_i\}_{1\leq i\leq n}$ genererebbe $M/\mathfrak{m}M$ come $A/\mathfrak{m}$-spazio vettoriale; il che è assurdo. □

COROLLARIO 2.38. Sia $(A, \mathfrak{m})$ anello locale e sia M un A-modulo finitamente generato. Allora ogni insieme minimale di generatori per M come A-modulo ha cardinalità $\dim_{A/\mathfrak{m}} M/\mathfrak{m}M$.

Uno strumento dell'algebra molto forte che utilizzeremo per alcune delle nostre future dimostrazioni è la nozione di *successione esatta*.

DEFINIZIONE 2.39. Una successione di A-moduli e di omomorfismi di A-moduli

$$\to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to$$

si dice *esatta in* M_i se $\mathrm{im}(f_i) = \ker(f_{i+1})$. La successione è *esatta* se è esatta in ciascun M_i. Un particolare tipo di successione esatta è la *successione esatta corta*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

che equivale al fatto che f sia iniettiva, g suriettiva e $\ker(g) = \mathrm{im}(f)$.

Nella definizione di modulo, e di tutto ciò che lo riguarda, è sempre stata particolarmente evidenziata l'importanza dell'anello A su cui la struttura di modulo si basa. Un naturale quesito è quello di indagare quando sullo stesso gruppo additivo M possa essere data una struttura di modulo su anelli distinti, in particolare quali anelli "accetta" e come le sue proprietà di modulo si modifichino.

DEFINIZIONE 2.40. Sia $f\colon A \to B$ un omomorfismo di anelli e sia N un B-modulo. Allora N è anche un A-modulo ottenuto per *restrizione degli scalari*, con una struttura di A-modulo definita nel seguente modo: $ax = f(a)x$ per ogni $a \in A$ e per ogni $x \in N$. In particolare, f definisce una struttura di A-modulo su B.

PROPOSIZIONE 2.41. Sia $f\colon A \to B$ un omomorfismo di anelli ed N un B-modulo. Supponiamo che N sia finitamente generato come B-modulo e che B-sia finitamente generato come A-modulo. Allora N è finitamente generato come A-modulo.

DIMOSTRAZIONE. Siano $y_1, \ldots, y_n$ un sistema di generatori per N sopra B e $x_1, \ldots, x_m$ un sistema di generatori di B come A-modulo. Allora gli mn prodotti $x_i y_j$ generano N come A-modulo. □

La comprensione dell'operazione di restrizione degli scalari è utile al fine di definire una nuova struttura algebrica.

DEFINIZIONE 2.42. Sia A un anello, una *A-algebra* è una coppia (B, f) dove B è un anello ed $f\colon A \to B$ è un omomorfismo di anelli

Se la definizione di algebra data può sembrare poco chiara questa può essere sviscerata per capirne la struttura. Abbiamo già potuto osservare come un anello B è in automatico un B-modulo con il suo prodotto. Adesso grazie all'operazione di restrizione degli scalari sappiamo come avere un omomorfismo di anelli $f\colon A \to B$ ci dia anche una struttura di A-modulo su B. Adesso si verifica che le due strutture sono compatibili, nel senso che le due addizioni su B dall'essere un anello ed un modulo sono le stesse e dati $a \in A,\ b \in B$ *e* $x \in B$ allora $a(bx) = (ab)x = b(ax)$.

Osservazione 2.43. 1) Se A è un campo $\mathbb{K}$ e $B \neq 0$ allora f è automaticamente iniettivo e pertanto $\mathbb{K}$ può venire identificato in modo canonico con la sua immagine in B. Dunque una $\mathbb{K}$-algebra non nulla è sostanzialmente un anello che contiene $\mathbb{K}$ come sottoanello.

2) Sia A un anello. Poiché A contiene l'elemento unità allora esiste un unico omomorfismo dell'anello degli interi $\mathbb{Z}$ in A. Dunque ogni anello unitario è automaticamente uno $\mathbb{Z}$-modulo, e dunque una $\mathbb{Z}$-algebra.

Definizione 2.44. Siano B, C due A-algebre. Un omomorfismo di A-algebre $f\colon B \to C$ è un omomorfismo di anelli che è anche un omomorfismo di A-moduli o equivalentemente è commutativo il seguente diagramma $\begin{array}{ccc} B & \xrightarrow{f} & C \\ \uparrow & \nearrow & \\ A & & \end{array}$.

Definizione 2.45. Un omomorfismo di anelli $f\colon A \to B$ è *finito*, e B è una A-algebra *finita*, se B è un A-modulo finitamente generato. L'omomorfismo $f\colon A \to B$ è *di tipo finito*, e B è una *A-algebra finitamente generata* o *di tipo finito*, se esiste un insieme finito di elementi $x_1, \dots, x_n$ in B tale che ogni elemento di B può essere espresso come un polinomio in $x_1, \dots, x_n$ a coefficienti in $f(A)$; oppure, in modo equivalente, se esiste un omomorfismo suriettivo di A-algebre da un anello di polinomi $A[t_1, \dots, t_n]$ a B.

Proposizione 2.46. Le due definizione date di A-algebra di tipo finito sono equivalenti.

Dimostrazione. Supponiamo che B ammetta un sistema finito di generatori $x_1, \dots, x_n$ come A-algerba. Allora definiamo $\Phi\colon A[t_1, \dots, t_n] \to B$ come la composizione dell'omomorfismo indotto da f tra gli anelli dei polinomi $A[t_1, \dots, t_n]$ e $B[t_1, \dots, t_n]$ seguito dall'omomorfismo di valutazione in $x_1, \dots, x_n$.

Viceversa, se esiste un omomorfismo di A-algebre $\Phi\colon A[t_1, \dots, t_n] \twoheadrightarrow B$ suriettivo, allora abbiamo che $A[t_1, \dots, t_n]/\ker\Phi \cong B$. Poiché $A[t_1, \dots, t_n]/\ker\Phi$ è generata come algebra da $[t_1], \dots, [t_n]$ allora B sarà generata da $\overline{\Phi}([t_1]), \dots, \overline{\Phi}([t_n])$, con $\overline{\Phi}$ l'isomorfismo indotto al quoziente da Φ. □

CAPITOLO 3

Localizzazioni e condizioni di catena

Avendo richiamato la struttura algebrica di anello ed introdotto quella di modulo, possiamo introdurre alcuni degli strumenti dell'algebra commutativa. Primo tra tutti quello della formazione dell'anello delle frazioni, in particolar modo della localizzazione. Successivamente, al fine di definire la lunghezza di un modulo, studieremo più in generale le condizioni sulle catene. Per collegamenti che faremo più avanti sarà necessario introdurre il prodotto tensoriale, così da poter costruire e comprendere la potenza esterna.

3.1. Localizzazioni

Ora che sono state richiamate e rinfrescate le definizioni e le proprietà basilari degli anelli e dei moduli possiamo introdurre un importante strumento dell'algebra commutativa: le *localizzazioni*. Per dare un'idea intuitiva dell'importanza di questo strumento per mostrare il teorema di Bézout, la localizzazione geometricamente corrisponde al concentrare l'attenzione su di un aperto o nell'intorno di un punto. Il processo di localizzazione cerca di generalizzare quello della costruzione del campo delle frazioni $\mathrm{Frac}(A)$ di un dominio A. Ricordiamola.

Definizione 3.1. Sia A un dominio. Consideriamo l'insieme $A \times (A \setminus \{0\})$ ed introduciamo su di esso la relazione di equivalenza data da:

$$(a, s) \sim (b, t) \text{ se e solo se } at - bs = 0.$$

L'insieme $\dfrac{A \times (A \setminus \{0\})}{\sim}$ prende il nome di *campo delle frazioni*, o *campo dei quozienti*, di A; denotato con $\mathrm{Frac}(A)$. Indichiamo con a/s la classe di equivalenza di (a, s).

Ciò vale soltanto se A è un dominio, in particolare perché la prova della transitività della relazione di equivalenza $\sim$ nella definizione sfrutta la legge di cancellazione del prodotto. Dobbiamo dunque generalizzare il più possibile questa costruzione.

Definizione 3.2. Sia A un anello. Un *sottoinsieme moltiplicativamente chiuso* di A, o più brevemente, una *parte moltiplicativa* di A, è un sottoinsieme S di A tale che $1 \in S$ ed S è chiuso rispetto alla moltiplicazione. Cioè S è un sotto-semigruppo del semigruppo moltiplicativo di A.

Adesso sia S una parte moltiplicativa di un anello A, definiamo una relazione su di $A \times S$ nel modo seguente:

$$(a, s) \sim (b, t) \text{ se e solo se esiste } u \in S \text{ tale che } (at - bs)u = 0.$$

Appare ovvio che la relazione appena definita sia riflessiva e simmetrica. Non è invece chiaro dalla definizione che sia transitiva. Verifichiamolo: supponiamo di avere tre coppie $(a, s) \sim (b, t)$ e $(b, t) \sim (c, u)$. Allora per definizione esistono $v, w \in S$ tali che $(at-bs)v = 0$ e $(bu-ct)w = 0$. Allora moltiplicando la prima identità per uw e la seconda per sv otteniamo dunque che $autvw - bsuvw = 0 = bsuvw - cstuvw$, dunque $(au - cs)tvw = 0$ con $tvw \in S$ poiché parte moltiplicativa. Cioè $(a, s) \sim (c, u)$.

Definizione 3.3. Sia A un anello ed S una parte moltiplicativa di A. Definiamo l'*anello delle frazioni* di A rispetto ad S come $S^{-1}A \coloneqq (A \times S)/\sim$, con le operazioni definite come:

$$(a/s) + (b/t) = (at + bs)/st,$$
$$(a/s)(b/t) = ab/st.$$

Si ha inoltre un naturale omomorfismo di anelli $f\colon A \to S^{-1}A$ dato da $f(x) = x/1$. Esso non è iniettivo in generale, infatti il suo nucleo è $\{a \in A \mid \text{esiste } s \in S \text{ tale che } sa = 0\}$.

Osservazione 3.4. Se A è un dominio ed $S = A \setminus \{0\}$ allora $S^{-1}A = \mathrm{Frac}(A)$, il campo delle frazioni di A.

L'anello delle frazioni $S^{-1}A$ possiede una proprietà universale.

Proposizione 3.5. Sia $g\colon A \to B$ un omomorfismo di anelli tale che $g(s)$ è invertibile in B per ogni $s \in S$, parte moltiplicativa di A. Allora esiste un unico omomorfismo di anelli $h\colon S^{-1}A \to B$ tale che $g = h \circ f$.

Dimostrazione. Poniamo $h(a/s) = g(a)g(s)^{-1}$. A patto che sia ben definito h sarà chiaramente un omomorfismo di anelli. Supponiamo dunque che $a/s = a'/s'$; allora esiste un elemento $t \in S$ tale che $(as' - a's)t = 0$, da cui applicando g si ottiene

$$(g(a)g(s') - g(a')g(s))g(t) = 0;$$

ora per ipotesi $g(t)$, $g(s)$ e $g(s')$ sono invertibili in B, sicché $g(a)g(s)^{-1} = g(a')g(s')^{-1}$. Dobbiamo adesso verificare che l'omomorfismo h appena definito sia unico. Difatti sia $h'\colon S^{-1}A \to B$ soddisfacente le ipotesi, allora per ogni $a \in A$ $h'(a/1) = h'(f(a)) = g(a)$. Se invece $s \in S$ abbiamo che $h'(1/s) = h'((s/1)^{-1}) = h'(s/1)^{-1} = g(s)^{-1}$ e pertanto $h'(a/s) = h'((a/1)(1/s)) = h'(a/1)h'(1/s) = g(a)g(s)^{-1}$. h è pertanto unica. □

È facile osservare come l'anello $S^{-1}A$ e l'omomorfismo $f\colon A \to S^{-1}A$ possiedano le seguenti proprietà:

1) per ogni $s \in S$ $f(s)$ è invertibile in $S^{-1}A$;
2) se $f(a) = 0$ allora esiste $s \in S$ tale che $as = 0$;
3) ogni elemento di $S^{-1}A$ è della forma $f(a)f(s)^{-1}$ per qualche $a \in A$ e qualche $s \in S$.

Viceversa queste tre proprietà definiscono l'anello $S^{-1}A$ a meno di isomorfismo.

Corollario 3.6. Siano S una parte moltiplicativa di A ed $f\colon A \to S^{-1}A$ dato da $a \mapsto a/1$. Sia $g\colon A \to B$ un omomorfismo di anelli tali che:

i) per ogni $s \in S$ $g(s)$ è invertibile in B;
ii) se $g(a) = 0$ allora esiste $s \in S$ tale che $as = 0$;
iii) ogni elemento di B è della forma $g(a)g(s)^{-1}$ per qualche $a \in A$ ed $s \in S$.

Allora esiste ed è unico un isomorfismo $h\colon S^{-1}A \to B$ tale che $g = h \circ f$.

Dimostrazione. La proprietà i) garantisce per il teorema precedente l'esistenza ed unicità di $h\colon S^{-1}A \to B$ definita come $h(a/s) = g(a)g(s)^{-1}$. Non resta dunque che provare che tale mappa così definita è una bigezione. Stante iii) abbiamo che h è suriettiva. Sia $a/s \in \ker h$, allora abbiamo che $g(a) = 0$ (poiché $g(s)$ è invertibile per ipotesi); dunque stante ii) abbiamo che esiste $t \in S$ tale che $at = 0$, cioè $a/s = 0$ in $S^{-1}A$. Dunque h è un isomorfismo. □

Proposizione 3.7. Siano A un anello, S una sua parte moltiplicativa ed $f\colon A \to S^{-1}A$ la mappa canonica $x \mapsto x/1$.

I) Se $I \subseteq A$ è un ideale, allora $S^{-1}I \coloneqq \{a/s \in S^{-1}A \mid a \in I, s \in S\}$ è l'esteso di I tramite f.
II) Ogni ideale $J \subseteq S^{-1}A$ è della forma $S^{-1}f^{-1}(J)$, cioè è un ideale esteso. Dunque la mappa $J \mapsto f^{-1}(J)$ è un'iniezione dall'insieme degli ideali di $S^{-1}A$ e all'insieme degli ideali di A.
III) Per un ideale $I \subseteq A$ sono equivalenti:
   i) I è il contratto tramite f di un ideale di $S^{-1}A$;
   ii) per ogni $s \in S$, $s + I$ non è un divisore dello zero in A/I.
IV) La mappa $I \mapsto f^{-1}(I)$ è una bigezione tra gli ideali primi di $S^{-1}A$ e gli ideali primi di A disgiunti da S.

DIMOSTRAZIONE. I) Sia $J = f(I)S^{-1}A$ l'esteso di I tramite f. Allora l'inclusione $S^{-1}I \subseteq J$ è ovvia. Sia adesso $x/s \in J$. Per definizione di ideale esteso questo si scrive come somma finita $\sum_i (a_i x_i)/s_i$ con $a_i \in A$, $s_i \in S$ e $x_i \in I$. Allora portando a denominatore comune e sfruttando la proprietà di assorbimento di I questo è della forma y/s con $y \in I$ ed $s \in S$.

II) Sia $I = f^{-1}(J)$. L'inclusione $J \supseteq S^{-1}I$ è immediata. Sia dunque $a/s \in J$, allora $a \in I$ e dunque $a/s \in S^{-1}I$. Segue dunque che $J \mapsto f^{-1}(J)$ è un'iniezione.

III) $i) \Rightarrow ii)$ Se $I \subseteq A$ è un ideale contratto segue dal punto II) che $I = f^{-1}(S^{-1}I)$. Sia $s \in S$ ed $x \in A$. Se $sx \in I$ esistono allora $y \in I,\ t \in S$ tali che $f(sx) = y/t = f(s)f(x)$, dunque $f(x) = y/ts \in S^{-1}I$, dunque $x \in I$. Allora nessun elemento di S è un divisore dello zero in A/I. $ii) \Rightarrow i)$ Supponiamo che nessun elemento di S sia un divisore dello zero in A/I. Sia $x \in f^{-1}(S^{-1}I)$, allora $x/1 \in S^{-1}I$, dunque $x/1 = y/s$ per qualche $y \in I,\ s \in S$. Per definizione $tsx = ty$ per qualche $t \in S$. Dato che per ipotesi ts non è un divisore dello zero in A/I abbiamo che $x \in I$; dunque $I = f^{-1}(S^{-1}I)$, perciò è un ideale contratto.

IV) La mappa è una restrizione nel dominio e nel codominio della mappa nel punto II) ed è dunque ancora iniettiva. Sia adesso $\mathfrak{p}$ un ideale di A tale che $\mathfrak{p} \cap S = \varnothing$. Abbiamo che $A/\mathfrak{p}$ è un dominio di integrità e poiché $s + \mathfrak{p} \neq \mathfrak{p}$ per ogni $s \in S$, si ha che $\mathfrak{p}$ è un ideale contratto per il punto III). Non resta che mostrare che $S^{-1}\mathfrak{p}$ è un ideale primo di $S^{-1}A$. Siano allora $x/s,\ y/t \in S^{-1}A$ tali che $x/s \cdot y/t \in S^{-1}\mathfrak{p}$. Allora esiste $t \in S$ tale che $txy \in \mathfrak{p}$, ma dato che $\mathfrak{p}$ è primo e $t \notin \mathfrak{p}$ si ha che $xy \in \mathfrak{p}$; dunque $x \in \mathfrak{p}$ o $y \in \mathfrak{p}$ e da qui la tesi.

□

OSSERVAZIONE 3.8. La corrispondenza del punto $a)$ della proposizione precedente preserva le inclusioni e le intersezioni grazie alla proprietà della retroimmagine. In più per quanto detto sugli ideali contratti questa porta ideali primi in ideali primi.

OSSERVAZIONE 3.9. Segue facilmente dalla proposizione che se $f \in A$ è un elemento non nilpotente allora esiste un ideale primo in A che non contiene f. Consideriamo la parte moltiplicativa $S = \{f^n\}_{n \in \mathbb{Z}_{\geq 0}}$, dato che S non contiene lo zero l'anello $S^{-1}A$ non è l'anello nullo e pertanto possiede un ideale massimale, che è anche primo, la cui contrazione è un ideale primo $\mathfrak{p}$ in A che non incontra S, in particolare $f \notin \mathfrak{p}$.

Abbiamo un importante esempio, che è ciò che a noi interessa, di costruzione dell'anello delle frazioni rispetto ad una particolare parte moltiplicativa. Sia $\mathfrak{p}$ un ideale primo di A abbiamo che $S = A \setminus \mathfrak{p}$ è una parte moltiplicativa. In tal caso particolare scriveremo $A_\mathfrak{p}$ al posto di $S^{-1}A$. Il procedimento appena descritto di passaggio da A ad $A_\mathfrak{p}$ prende il nome di *localizzazione* in $\mathfrak{p}$.

COROLLARIO 3.10. Siano A un anello e $\mathfrak{p}$ un suo ideale primo. Gli ideali primi in $A_\mathfrak{p}$ sono in corrispondenza biunivoca con gli ideali primi di A contenuti in $\mathfrak{p}$.

DIMOSTRAZIONE. Abbiamo per la Proposizione 3.7 che gli ideali primi di $A_\mathfrak{p}$ sono in corrispondenza biunivoca con gli ideali primi in A che non incontrano $S = A \setminus \mathfrak{p}$, cioè con gli ideali primi di A contenuti in $\mathfrak{p}$. □

PROPOSIZIONE 3.11. Sia A un anello e $\mathfrak{p}$ un suo ideale primo. L'insieme $\mathfrak{p}A_\mathfrak{p} \coloneqq \{a/s \in A_\mathfrak{p} \mid a \in \mathfrak{p}\}$ è l'unico ideale massimale di $A_\mathfrak{p}$. In altre parole $A_\mathfrak{p}$ è un anello locale.

DIMOSTRAZIONE. Mostriamo innanzitutto che $\mathfrak{p}A_\mathfrak{p}$ è un ideale. Siano $a/s, b/t \in \mathfrak{p}A_\mathfrak{p}$ allora $a/s + b/t = (at + bs)/st \in \mathfrak{p}A_\mathfrak{p}$ poiché per assorbimento di $\mathfrak{p}$ $at, bs \in \mathfrak{p}$ e dunque $at + bs \in \mathfrak{p}$. Se $a/s \in \mathfrak{p}A_\mathfrak{p}$ allora $a \in \mathfrak{p}$, dunque $-a \in \mathfrak{p}$ e perciò $-a/s \in \mathfrak{p}A_\mathfrak{p}$. $0 \in \mathfrak{p}$ e dunque $0 \in \mathfrak{p}A_\mathfrak{p}$. Osserviamo che se $b/t \notin \mathfrak{p}A_\mathfrak{p}$, allora $b \notin \mathfrak{p}$ e dunque $b \in S$: pertanto b/t è invertibile in $A_\mathfrak{p}$. Sia allora I un ideale tale che $\mathfrak{p}A_\mathfrak{p} \subsetneq I$, per quanto detto sopra I contiene un invertibile e dunque $I = A_\mathfrak{p}$. Dunque $\mathfrak{p}A_\mathfrak{p}$ è un ideale massimale. Allo stesso

modo quanto detto lo rende l'unico ideale massimale di $A_\mathfrak{p}$ poiché che se per assurdo $\mathfrak{n}$ fosse un altro ideale massimale di $A_\mathfrak{p}$, allora $\mathfrak{n} \not\subseteq \mathfrak{p}A_\mathfrak{p}$ e dunque come sopra $\mathfrak{n}$ conterrebbe un invertibile, cioè $\mathfrak{n} = A_\mathfrak{p}$. □

La costruzione di $S^{-1}A$ può essere replicata con un A-modulo M al posto dell'anello A. Prendiamo una parte moltiplicativa S di A e definiamo una relazione d'equivalenza su $M \times S$ definita come segue:

$$(m, s) \sim (m', s') \text{ se e solo se esiste } t \in S \text{ tale che } t(sm' - s'm) = 0.$$

Denotiamo anche in questo caso con m/s la classe di equivalenza della coppia (m, s) e con $S^{-1}M$ l'insieme di tali frazioni. Su $S^{-1}M$ può essere introdotta una naturale struttura di $S^{-1}A$-modulo definendo in modo ovvio l'addizione e la moltiplicazione per uno scalare. Anche in questo caso se $\mathfrak{p}$ è un ideale primo di A scriviamo $M_\mathfrak{p}$ in luogo di $(A \setminus \mathfrak{p})^{-1}M$.

Definizione 3.12. Sia A un anello ed M un A-modulo. Definiamo il *supporto di* M come l'insieme $\operatorname{Supp}(M) \coloneqq \{\mathfrak{p} \in \operatorname{Spec}(A) \mid M_\mathfrak{p} \neq 0\}$.

Come nel caso degli anelli abbiamo una naturale mappa $f\colon M \to S^{-1}M$ definita come $f(m) = m/1$ e continua a valere l'analogo della Proposizione 3.5 e del suo corollario. Valgono inoltre risultati del tutto analoghi a quelli dati per la creazione degli anelli di frazioni.

Sia poi $u\colon M \to N$ un omomorfismo di A-moduli. Esso dà origine ad un omomorfismo di $S^{-1}A$-moduli $S^{-1}u\colon S^{-1}M \to S^{-1}N$, definito come $S^{-1}u(m/s) = u(m)/s$. Vale inoltre che dati tre A-moduli M, N e P e due omomorfismi di A-moduli $u\colon M \to N$ e $v\colon N \to P$ allora $S^{-1}(v \circ u) = S^{-1}(v) \circ S^{-1}u$. In altri termini si potrebbe dire, utilizzando il linguaggio categorico, che S^{-1} è un funtore covariante dalla categoria degli A-moduli a quella degli $S^{-1}A$-moduli.

Lemma 3.13. Sia A un anello ed S una sua parte moltiplicativa, allora il funtore S^{-1} è esatto, ossia, se la successione $M' \xrightarrow{f} M \xrightarrow{g} M''$ è esatta in M, allora la successione $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} M''$ è esatta in $S^{-1}M$.

Dimostrazione. Abbiamo che $g \circ f = 0$, da cui $S^{-1}g \circ S^{-1}f = S^{-1}(0) = 0$, dunque $\operatorname{im}(S^{-1}f) \subseteq \ker(S^{-1}g)$. Sia adesso $m/s \in \ker(S^{-1}g)$, allora $g(m)/s = 0$ in $S^{-1}M''$; dunque per definizione esiste $t \in S$ tale che $tg(m) = 0$ in M''. Poiché g è un omomorfismo di A-moduli allora $tg(m) = g(tm) = 0$, sicché $tm \in \ker(g) = \operatorname{im}(f)$ e pertanto $tm = f(m')$ per qualche $m' \in M'$. Allora in $S^{-1}M$ si ha che $m/s = f(m')/st = (S^{-1}f)(m'/st) \in \operatorname{im}(S^{-1}f)$, per tanto $\ker(S^{-1}g) \subseteq \operatorname{im}(S^{-1}f)$. □

Corollario 3.14. Sia A un anello ed S una sua parte moltiplicativa. Siano N, P A-sottomoduli di un A-modulo M allora:

i) $S^{-1}(N + P) = S^{-1}N + S^{-1}P$;
ii) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$;
iii) $S^{-1}(M/N) \cong (S^{-1}M)/S^{-1}N$ come $S^{-1}A$-moduli.

Dimostrazione. *i)* Segue dalla definizione. *ii)* L'inclusione $\subseteq$ è ovvia: se $m/s \in S^{-1}(N \cap P)$ con $m \in N \cap P$ per definizione dunque $m/s \in S^{-1}N \cap S^{-1}P$. Sia invece un elemento in $S^{-1}N \cap S^{-1}P$ questo può essere scritto come $y/s = z/t$ con $y \in N,\ z \in P,\ s, t \in S$. Allora per definizione esiste $u \in S$ tale che $u(ty - sz) = 0$, sicché $w = uty = usz \in N \cap P$. Allora $y/s = w/sut \in S^{-1}(N \cap P)$. *iii)* Grazie al lemma precedente è sufficiente applicare S^{-1} alla successione esatta corta $0 \to N \hookrightarrow M \twoheadrightarrow M/N \to 0$. □

Proposizione 3.15. Sia A un anello ed S una sua parte moltiplicativa. Sia M un A-modulo finitamente generato. Allora $S^{-1}M = 0$ se e solo se esiste $s \in S$ tale che $sM = 0$.

Dimostrazione. ($\Rightarrow$) Supponiamo $S^{-1}M = 0$. Siano allora $x_1, \ldots, x_n$ generatori di M su A si ha che per ogni $1 \leq i \leq n$ esiste $s_i \in S$ tale che $s_i x_i = 0$. Posto allora

$s = s_1 \dots s_n$ questo è ancora un elemento di S poiché parte moltiplicativa e si ha che $sM = 0$. ($\Leftarrow$) Se esiste $s \in S$ tale che $sM = 0$ allora per ogni $m \in M$ e $t \in S$ si ha che $x/t = (sm)/(st) = 0/(st) = 0$; dunque $S^{-1}M = 0$. □

COROLLARIO 3.16. Sia A un anello ed M un A-modulo finitamente generato. Allora $\operatorname{Supp} M$ è l'insieme degli ideali primi di A contenenti l'annullatore di M.

DIMOSTRAZIONE. Stante la proposizione si ha che $M_\mathfrak{p} \neq 0$ se e solo se non esiste $s \in A \setminus \mathfrak{p}$ tale che $sM = 0$; dunque $\operatorname{Ann}(M) \cap (A \setminus \mathfrak{p}) = \varnothing$. In altre parole $\operatorname{Ann}(M) \subseteq \mathfrak{p}$. Pertanto $\mathfrak{p} \in \operatorname{Supp}(M)$ se e solo se $\operatorname{Ann}(M) \subseteq \mathfrak{p}$. □

OSSERVAZIONE 3.17. Consideriamo A ed un suo ideale primo $\mathfrak{p}$. Dal corollario alla Proposizione 3.7, segue che il passaggio da A alla suo localizzazione $A_\mathfrak{p}$ fa sparire tutti gli ideali primi tranne quelli contenuti in $\mathfrak{p}$. Se consideriamo invece il passaggio da A al suo quoziente $A/\mathfrak{p}$, scompaiono invece tutti gli ideali primi tranne quelli contenenti $\mathfrak{p}$. Ne segue dunque che se $\mathfrak{p}$, $\mathfrak{q}$ sono ideali primi di A tali che $\mathfrak{q} \subseteq \mathfrak{p}$, localizzando rispetto a $\mathfrak{p}$ e prendendo poi il quoziente modulo $\mathfrak{q}A_\mathfrak{p}$ (tale processo può essere in realtà eseguito in qualsiasi ordine stante il punto *iii*) del Corollario 3.14), si restringe l'attenzione agli ideali primi che si trovano tra $\mathfrak{p}$ e $\mathfrak{q}$. In particolare, se $\mathfrak{p} = \mathfrak{q}$, ciò che otteniamo è un campo, detto il *campo residuo di* $\mathfrak{p}$. Questo può essere ottenuto o come il campo delle frazioni del dominio $A/\mathfrak{p}$ oppure come il campo residuo dell'anello locale $A_\mathfrak{p}$. Si denota con $\kappa(\mathfrak{p})$.

3.2. Proprietà locali

Oltre all'importanza geometrica la localizzazione ha inoltre utili applicazioni in dimostrazioni in cui bisogna verificare certe proprietà, che chiameremo locali.

DEFINIZIONE 3.18. Una proprietà P degli anelli (o dei moduli) si dice una *proprietà locale* se vale la seguente condizione: A (risp. M) possiede la proprietà P se e solo se $A_\mathfrak{p}$ (risp. $M_\mathfrak{p}$) possiede la proprietà P per ogni ideale primo $\mathfrak{p}$ in A.

PROPOSIZIONE 3.19. Sia M un A-modulo. Allora le seguenti condizioni sono equivalenti:

i) $M = 0$;
ii) $M_\mathfrak{p} = 0$ per ogni ideale primo $\mathfrak{p}$ di A;
iii) $M_\mathfrak{m} = 0$ per ogni ideale massimale $\mathfrak{m}$ di A.

DIMOSTRAZIONE. Chiaramente *i*) $\Rightarrow$ *ii*) $\Rightarrow$ *iii*). Supponiamo che valga la condizione *iii*) e $M \neq 0$. Sia x un elemento non nullo in M e poniamo $I = \operatorname{Ann}(x)$: I è un ideale proprio di A ed è dunque per questo contenuto in un ideale massimale $\mathfrak{m}$. Consideriamo allora l'elemento $x/1 \in M_\mathfrak{m}$. Poiché per ipotesi $M_\mathfrak{m} = 0$ si ha che $x/1 = 0$, dunque x è annullato in qualche elemento in $A \setminus \mathfrak{m}$; ma ciò è assurdo poiché $\operatorname{Ann}(x) \subseteq \mathfrak{m}$. □

PROPOSIZIONE 3.20. Sia $f\colon M \to N$ un omomorfismo di A-moduli. Allora le seguenti condizioni sono equivalenti:

i) f è iniettivo;
ii) $f_\mathfrak{p}$ è iniettivo per ogni $\mathfrak{p} \in \operatorname{Spec}(A)$;
iii) $f_\mathfrak{m}$ è iniettivo per ogni $\mathfrak{m} \in \operatorname{Specm}(A)$.

DIMOSTRAZIONE. *i*) $\Rightarrow$ *ii*) Se f è iniettivo allora la successione $0 \to M \to N$ è esatta, dunque è esatta la successione $0 \to M_\mathfrak{p} \to N_\mathfrak{p}$ per ogni $\mathfrak{p} \in \operatorname{Spec}(A)$ e pertanto $f_\mathfrak{p}$ è iniettivo per ogni $\mathfrak{p} \in \operatorname{Spec}(A)$.

ii) $\Rightarrow$ *iii*) Ovvio poiché ogni ideale massimale è anche primo .

iii) $\Rightarrow$ *i*) Posto $M' = \ker f$ la successione $0 \to M' \hookrightarrow M \to N$ è esatta, quindi è esatta $0 \to M'_\mathfrak{m} \hookrightarrow M_\mathfrak{m} \to N$ e dunque $M'_\mathfrak{m} \cong \ker f_\mathfrak{m} = 0$ poiché $f_\mathfrak{m}$ è iniettivo. Allora per la Proposizione 3.19 poiché $M'_\mathfrak{m} = 0$ per ogni $\mathfrak{m} \in \operatorname{Specm}(A)$ vale che $M' = \ker f = 0$. □

Vale una proposizione analoga legata alla suriettività:

PROPOSIZIONE 3.21. Sia $f\colon M \to N$ un omomorfismo di A-moduli. Allora le seguenti condizioni sono equivalenti:

i) f è suriettivo;
ii) $f_{\mathfrak{p}}$ è suriettivo per ogni $\mathfrak{p} \in \operatorname{Spec}(A)$;
iii) $f_{\mathfrak{m}}$ è suriettivo per ogni $\mathfrak{m} \in \operatorname{Specm}(A)$.

DIMOSTRAZIONE. *i)* $\Rightarrow$ *ii)* Se f è suriettivo allora è esatta la successione $M \twoheadrightarrow N \to 0$, dunque è esatta la successione $M_{\mathfrak{p}} \to N_{\mathfrak{p}} \to 0$ per ogni $\mathfrak{p} \in \operatorname{Spec}(A)$ e pertanto $f_{\mathfrak{p}}$ è suriettivo per ogni $\mathfrak{p} \in \operatorname{Spec}(A)$.

ii) $\Rightarrow$ *iii)* Anche in questo caso l'implicazione è ovvia poiché un ideale massimale è in particolare primo.

iii) $\Rightarrow$ *i)* Consideriamo la successione esatta $M \to N \twoheadrightarrow \operatorname{coker} f \to 0$. Dunque è esatta la successione $M_{\mathfrak{m}} \to N_{\mathfrak{m}} \twoheadrightarrow \operatorname{coker} f_{\mathfrak{m}} \to 0$ per ogni $\mathfrak{m} \in \operatorname{Specm}(A)$. Per ipotesi $f_{\mathfrak{m}}$ è suriettiva per ogni $\mathfrak{m} \in \operatorname{Specm}(A)$ e pertanto $\operatorname{coker} f_{\mathfrak{m}} = 0$ per ogni $\mathfrak{m} \in \operatorname{Specm}(A)$. Allora per la Proposizione 3.19 $\operatorname{coker} f = 0$. □

Dalle due precedenti proposizione segue dunque che anche la biettività è una proprietà locale.

COROLLARIO 3.22. Sia $f\colon M \to N$ un omomorfismo di A-moduli. Allora le seguenti condizioni sono equivalenti:

i) f è bigettiva;
ii) $f_{\mathfrak{p}}$ è bigettiva per ogni $\mathfrak{p} \in \operatorname{Spec}(A)$;
iii) $f_{\mathfrak{m}}$ è bigettiva per ogni $\mathfrak{m} \in \operatorname{Specm}(A)$.

3.3. Condizioni sulle catene

Una volta definita la lunghezza di un modulo, al fine di imporre alcune condizioni di finitezza, la strada più conveniente è quella delle "condizioni sulle catene". Seguendo questo approccio otteniamo delle simmetrie tra catene ascendenti e discendenti.

PROPOSIZIONE 3.23. Sia $(\Sigma, \leq)$ un insieme parzialmente ordinato mediante una relazione $\leq$. Allora le seguenti condizioni su Σ sono equivalenti:

i) Ogni successione crescente $x_1 \leq x_2 \leq \dots$ in Σ è stazionaria.
ii) Ogni sottoinsieme non vuoto di Σ possiede un elemento massimale.

DIMOSTRAZIONE. *i)* $\Rightarrow$ *ii)* Supponiamo che *ii)* non sia vera; allora esiste un sottoinsieme non vuoto T di Σ privo di elementi massimali. Grazie a questo possiamo costruire una successione crescente non stazionaria in T.

ii) $\Leftarrow$ *i)* Se vale *ii)* allora data una successione crescente $x_1 \leq x_2 \leq \dots$ l'insieme $\{x_m\}_{m\geq 1}$ ha un elemento massimale, dunque la successione è stazionaria. □

Sia M un A-modulo, consideriamo allora Σ l'insieme dei suoi A-sottomoduli. Se Σ è parzialmente ordinato mediante la relazione $\subseteq$ la *i)* prende il nome di *condizione sulle catene ascendenti* (*a.c.c.* in breve) e la *ii)* prende il nome di *condizione massimale*. Se ordiniamo invece Σ mediante la relazione $\supseteq$ la *i)* è la *condizione sulle catene discendenti* (*d.c.c.* in breve) e la *ii)* è la *condizione minimale*.

DEFINIZIONE 3.24. Un A-modulo M si dice *noetheriano* se l'insieme degli A-sottomoduli di M soddisfa una o l'altra delle due condizioni equivalenti:

i) condizione sulle catene ascendenti;
ii) condizione massimale.

Si dice invece *artiniano* se l'insieme degli A-sottomoduli di M soddisfa una o l'altra delle due condizioni equivalenti:

i) condizione sulle catene discendenti;
ii) condizione minimale.

Esempio 3.25. 1) Un gruppo abeliano finito (come $\mathbb{Z}$-modulo) soddisfa sia la a.c.c. che la d.c.c..
2) L'anello $\mathbb{Z}$ come modulo su sé stesso soddisfa la a.c.c ma non la d.c.c.. Infatti, se $a \in \mathbb{Z} \setminus \{0, +1, -1\}$, si ha $(a) \supsetneq (a^2) \supsetneq (a^3) \supsetneq \dots$ non è stazionaria.
3) L'anello $\mathbb{K}[x]$ soddisfa la a.c.c. (poiché PID) ma non la d.c.c. sugli ideali (che sono suoi sottomoduli). Ad esempio $(x) \supsetneq (x^2) \supseteq \dots$ non è stazionaria.

Nel caso di moduli noetheriani, questi possono essere caratterizzati mediante una terza condizione.

Proposizione 3.26. Un A-modulo M è noetheriano se e solo se ogni suo A-sottomodulo è finitamente generato.

Dimostrazione. ($\Rightarrow$) Sia N un sottomodulo di M e sia Σ l'insieme di tutti i sottomoduli finitamente generati di N. Allora Σ è non vuoto poiché $0 \in \Sigma$ e pertanto possiede un elemento massimale N_0. Se $N \neq N_0$ allora consideriamo il sottomodulo $N_0 + Ax$ con $x \in N \setminus N_0$. Esso è finitamente generato e contiene strettamente N_0, si ottiene così una contraddizione. Dunque $N = N_0$ e pertanto è finitamente generato.

($\Leftarrow$) Sia $M_1 \subseteq M_2 \subseteq \dots$ una catena ascendente di sottomoduli di M. Allora $N = \sum_{n\geq 1} M_n$ è un sottomodulo di M, dunque è generato da un numero finito di elementi $x_1, \dots, x_r$. Supponiamo che $x_i \in M_{n_i}$ e poniamo $n = \max_{1\leq i\leq r} n_i$; allora ciascun $x_i \in M_n$ dunque $M_n = N$ e la catena è stazionaria. □

A seguito di questa proposizione possiamo in un qualche senso privilegiare la noetherianità di un modulo, poiché questa garantisce la veridicità di molti teoremi ad esempio del capitolo precedente.

Proposizione 3.27. Sia $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ una successione esatta di A-moduli. Allora:

i) M è noetheriano se e solo se M' ed M'' sono noetheriani;
ii) se M è finitamente generato allora M'' è finitamente generato. Se M' ed M'' sono finitamente generati lo è anche M.
iii) M è artiniano se e solo se M' ed M'' sono artiniani.

Dimostrazione. La dimostrazione procede allo stesso modo nel caso i) e nel caso iii).

i) ($\Rightarrow$) Una catena di sottomoduli di M' (o di M'') dà origine ad una catena in M, dunque è stazionaria.

($\Leftarrow$) Consideriamo adesso una catena $(L_n)_{n\geq 1}$ in M, questa da origine a due catene $(\alpha^{-1}(L_n))_{n\geq 1}$ in M' e $(\beta(L_n))_{n\geq 1}$. Per n abbastanza grande entrambe le due catene sono stazionarie e dunque è stazionaria anche la catena $(L_n)_{n\geq 1}$.

ii) Se M è finitamente generato con generatori $x_1, \dots, x_n$ allora $\beta(x_1), \dots, \beta(x_n)$ generano M''. Stante i) se M' ed M'' sono finitamente generati sono noetheriani, dunque M è noetheriano ed è finitamente generato. □

Corollario 3.28. Siano $M_1, \dots, M_n$ A-moduli noetheriani (risp. artiniani), tale risulta $\oplus_{i=1}^n M_i$.

Dimostrazione. Per induzione su $n \geq 2$ si applica la proposizione precedente alla successione esatta corta

$$0 \to M_n \hookrightarrow \oplus_{i=1}^n M_i \twoheadrightarrow \oplus_{i=1}^{n-1} M_i \to 0$$

dove $M_n \hookrightarrow \oplus_{i=1}^n M_i$ è la mappa $x \mapsto (0, \dots, 0, x)$ ed $\oplus_{i=1}^n M_i \twoheadrightarrow \oplus_{i=1}^{n-1} M_i$ è la proiezione sui primi $n-1$ fattori. □

Proposizione 3.29. Sia M un A-modulo noetheriano e sia S una parte moltiplicativa di A. Allora $S^{-1}M$ è un $S^{-1}A$-modulo noetheriano.

DIMOSTRAZIONE. Abbiamo mostrato come i sottomoduli del modulo delle frazioni $S^{-1}M$ siano tutti moduli estesi. Allora se M è noetheriano ogni suo sottomodulo N è finitamente generato e così risulta $S^{-1}N$ come sottomodulo di $S^{-1}A$. □

OSSERVAZIONE 3.30. Un anello A si dice *noetheriano* (risp. *artiniano*) se risulta tale come A-modulo, ossia, se soddisfa la a.c.c. (risp. d.c.c.) sugli ideali.

PROPOSIZIONE 3.31. Sia A un anello noetheriano (risp. artiniano), M un A-modulo finitamente generato. Allora M è noetheriano (risp. artiniano).

DIMOSTRAZIONE. Se M è finitamente generato sappiamo che è quoziente di A^n per qualche n. Poiché A è noetheriano (risp. artiniano), tale è $A^{\oplus n}$. Dato che M è finitamente generato sappiamo che è isomorfo ad un quoziente di $A^{\oplus n}$, cioè esiste $p\colon A^{\oplus n} \twoheadrightarrow M$ suriettiva. Dunque considerando la successione esatta corta

$$0 \to \ker p \to A^{\oplus n} \xrightarrow{p} M \to 0$$

con segue che M è noetheriano (risp. artiniano) per la Proposizione 3.27. □

È chiaro sin dal primo capitolo, come l'anello per noi di maggior interesse sia quello dei polinomi. Riguardo alla noetherianità di tale anello vi è un importante risultato.

TEOREMA 3.32 (Teorema della base di Hilbert). Sia A un anello noetheriano. Allora $A[x]$ è un anello noetheriano.

DIMOSTRAZIONE. Sia $I \subseteq A[x]$ vogliamo mostrare che questo è finitamente generato. Scegliamo una sequenza di polinomi $f_1, f_2, \dots$ in I come segue: prendiamo f_1 un polinomio non nullo di grado minimo in I. Per ogni $i \geq 1$, scegliamo f_{i+1} un polinomio non nullo di grado minimo tra quelli che stanno in I ma non in $(f_1, \dots, f_i)$. Se $I = (f_1, \dots, f_i)$, abbiamo finito. Consideriamo a_j il coefficiente direttore di f_j. Dato che A è noetheriano allora l'ideale $J = (a_1, a_2, \dots)$ è finitamente generato. Possiamo dunque scegliere tali generatori tra gli a_j stessi. Consideriamo m il più piccolo intero positivo tale che $a_1, \dots, a_m$ generano J. Mostriamo che $I = (f_1, \dots, f_m)$. Se così non fosse, allora dovremo scegliere f_{m+1}. Possiamo scrivere dunque $a_{m+1} = \sum_{i=1}^{m} u_i a_i$ con $u_i \in A$ per ogni i. Dato che, per come sono stati scelti, il grado di f_{m+1} è maggiore o uguale del grado degli $f_1, \dots, f_m$ possiamo definire un polinomio

$$g = \sum_{i=1}^{m} u_i f_i x^{\deg f_{m+1} - \deg f_i} \in (f_1, \dots, f_m).$$

Tale polinomio g ha lo stesso grado di f_{m+1} e lo stesso coefficiente direttore. Dunque il polinomio $f_{m+1} - g \in I \setminus (f_1, \dots, f_m)$ con grado strettamente minore di f_{m+1} contraddicendo la sua scelta. Dunque $I = (f_1, \dots, f_m)$ è finitamente generato, cioè $A[x]$ è noetheriano. □

Adesso che abbiamo dato delle condizioni di finitezza alle successioni di sottomoduli di un A-modulo M possiamo definire e trattare la sua lunghezza.

DEFINIZIONE 3.33. Un A-modulo M si dice *semplice* se è non nullo e i suoi unici A-sottomoduli sono 0 ed M stesso.

LEMMA 3.34. Sia A un anello e $I, J \subseteq A$ ideali. Allora A/I e A/J sono isomorfi come A-moduli se e solo se $I = J$.

DIMOSTRAZIONE. ($\Leftarrow$) Ovvio.

($\Rightarrow$) Osserviamo che $\mathrm{Hom}_A(A, M) \cong M$ tramite la mappa $f \mapsto f(1)$. Se $I \subseteq A$ è un ideale abbiamo che $\mathrm{Hom}_A(A/I, M) \cong \{f \in \mathrm{Hom}_A(A, M) \mid \ker f \supseteq I\} \cong \{x \in M \mid \mathrm{Ann}_A(x) \supseteq I\}$ per l'osservazione precedente. Allora si ha che $\mathrm{Hom}_A(A/I, A/J) \cong \{x \in A/J \mid \mathrm{Ann}_A(x) \supseteq I\} \cong \{a + J \in A/J \mid a \in A, (J : a) \supseteq I\}$ con I e J ideali di A. Sia allora $\Psi\colon A/I \to A/J$ isomorfismo di A-moduli. Per quanto detto esiste $a \in A$ tale che $(J : a) \supseteq I$ e $\Psi(c + I) = ac + J$. Analogamente esiste $b \in A$ tale che $(I : b) \supseteq J$ e $\Psi^{-1}(a + J) = ba + J$.

Si ha dunque che $a + J = bca + J$ e dunque $bc - 1 \in J$. Pertanto, sia $x \in I \subseteq (J : a)$ abbiamo che $ax \in J$ e dunque $abx \in J$. Allora $x = abx - (ab - 1)x \in J$; dunque $I \subseteq J$. Analogamente si ha l'altra inclusione. □

PROPOSIZIONE 3.35. Sia A anello. Allora esiste una corrispondenza biunivoca tra $\mathrm{Specm}(A)$ e gli A-moduli semplici a meno di isomorfismo.

DIMOSTRAZIONE. Sia M un A-modulo semplice. Sia $x \in M$ non nullo. Allora consideriamo la mappa $\Phi\colon A \to M$ definita da $a \mapsto ax$. Abbiamo che tale mappa è suriettiva poiché $\operatorname{im}\Phi = Ax \subseteq M$ è un sottomodulo non nullo di M che è semplice; dunque $\operatorname{im}\Phi = M$. Per il primo teorema di omomorfismo si ha che $A/\ker\Phi \cong M$. $\ker\Phi = \mathrm{Ann}_A(x)$ che dobbiamo mostrare essere massimale. Se così non fosse avremo $\mathfrak{m} \supsetneq \mathrm{Ann}_A(x)$ ideale massimale e dunque $A/\mathrm{Ann}_A(x) \supsetneq \mathfrak{m}/\mathrm{Ann}_A(x) \supsetneq 0$; il che è assurdo. Siano adesso $\mathfrak{m}$ e $\mathfrak{n}$ ideali massimali tali che $A/\mathfrak{m} \cong A/\mathfrak{n}$ segue dal Lemma precedente che $\mathfrak{m} = \mathfrak{n}$. □

Sia M un A-modulo. Una *catena* di sottomoduli di M è una successione $(M_i)_{0\leq i\leq n}$ di sottomoduli di M tale che

$$M = M_0 \supsetneq M_1 \supsetneq \ldots \supsetneq M_{n-1} \supsetneq M_n = 0.$$

La *lunghezza* di una catena è l'intero non negativo n. Una *serie di composizione* di M è una catena massimale; cioè ciascun quoziente M_i/M_{i+1}, detto *fattore di composizione*, è un A-modulo semplice per ogni $0 \leq i \leq n-1$.

DEFINIZIONE 3.36. Sia M un A-modulo, denotiamo con $\mathrm{length}_A M$ la lunghezza minima di una serie di composizione di M. $\mathrm{length}_A M$ si dice la *lunghezza* di M. Poniamo $\mathrm{length}_A(M) = \infty$ se M non possiede serie di composizione.

PROPOSIZIONE 3.37. Sia A un anello e sia M un A-modulo di lunghezza finita. Sia $M' \subsetneq M$ un A-sottomodulo. Allora M' è un A-modulo di lunghezza finita e $\mathrm{length}_A M' < \mathrm{length}_A M$.

DIMOSTRAZIONE. Data una serie di composizione per M

$$M = M_0 \supsetneq M_1 \supsetneq \ldots \supsetneq M_n = 0$$

vogliamo mostrare che da

$$M' = M_0 \cap M' \supseteq \ldots \supseteq M_n \cap M' = 0$$

può essere estratta una serie di composizione per M'.

Si ha che $(M' \cap M_i)/(M' \cap M_{i+1}) \cong ((M' \cap M_i) + M_{i+1})/M_{i+1}$ e pertanto è contenuto in M_i/M_{i+1} che è semplice; dunque $(M' \cap M_i)/(M' \cap M_{i+1}) \cong M_i/M_{i+1}$ oppure è nullo. Vogliamo allora mostrare che $(M' \cap M_i)/(M' \cap M_{i+1}) \cong M_i/M_{i+1}$ non può accadere per ogni indice i. Supponiamo per assurdo che ciò si verifichi e proviamo per induzione discendente su i che $M' \supseteq M_i$ per ogni i. Il passo base dell'induzione è ovvio poiché $M_n = 0$. Supponiamo per induzione che $M' \supseteq M_{i+1}$, dunque è chiaro che $M' \cap M_i = (M' \cap M_i) + M_{i+1} = M_i$ per la nostra ipotesi di assurdo; segue perciò che $M' \supseteq M_i$. Allora per induzione si ha che $M \subseteq M'$; ma ciò è assurdo poiché avevamo supposto M' un sottomodulo proprio di M. Segue che la catena $M' = M' \cap M_0 \supseteq \ldots \supseteq M' \cap M_{n-1} \supseteq M' \cap M_n = 0$ può essere modificata omettendo i termini tali per cui $M' \cap M_i = M' \cap M_{i+1}$, ottenendo così una serie di composizione per M' di lunghezza strettamente minore di n. Dato che il processo può essere fatto per ogni serie di composizione per M segue che $\mathrm{length}_A M' < \mathrm{length}_A M$. □

Al fine di mostrare la buona positura di tale definizione enunciamo e mostriamo il seguente teorema.

TEOREMA 3.38 (Teorema di Jordan-Hölder). Siano A un anello ed M un A-modulo.

I) Se M ha una serie di composizione di lunghezza finita $M = M_0 \supsetneq M_1 \supsetneq \ldots \supsetneq M_n = 0$ di lunghezza n, allora:

i) ogni altra serie di composizione ha lunghezza n;
ii) ogni catena di sottomoduli di M ha lunghezza minore od uguale ad n;
iii) la somma delle mappe naturali $M \to M_{\mathfrak{p}}$, con $\mathfrak{p} \in \operatorname{Spec}(A)$, dà un isomorfismo di A-moduli $M \cong \oplus_{\mathfrak{p}} M_{\mathfrak{p}}$, dove la sommatoria varia tra gli ideali massimali p tali che $M_i/M_{i+1} \cong A/\mathfrak{p}$ per qualche i. Il numero degli M_i/M_{i+1} isomorfi ad $A/\mathfrak{p}$ è la lunghezza di $M_{\mathfrak{p}}$ come $A_{\mathfrak{p}}$-modulo, e ciò non dipende dalla serie di composizione scelta.

II) M possiede una serie di composizione di lunghezza finita se e solo se M è un A-modulo artiniano e noetheriano.

DIMOSTRAZIONE. I) *i*) Sia

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \ldots \supsetneq M_{n-1} \supsetneq M_n = 0 \tag{1}$$

una serie di composizione per M e consideriamo un'altra serie di composizione

$$M = N_0 \supsetneq N_1 \supsetneq \ldots \supsetneq N_m = 0. \tag{2}$$

Mostriamo per induzione su n che $n = m$. Per il passo base con $n = 1$ si ha che M è un A-modulo semplice e dunque $m = 1 = n$. Sia adesso $n > 1$. Se $M_1 = N_1 = N$ otteniamo dalle due serie di composizione per M due serie di composizione $N = M_1 \supsetneq \ldots \supsetneq M_n = 0$ e $N = N_1 \supsetneq \ldots \supsetneq N_m = 0$. Applicando l'ipotesi induttiva si ha che $n - 1 = m - 1$ e dunque $n = m$. Se $M_1 \neq N_1$ questi sono massimali per definizione di serie di composizione e dunque $M_1 + N_1 = M$. Otteniamo dunque per i teoremi di isomorfismo che $M/M_1 \cong N_1/(M_1 \cap N_1)$ e $M/N_1 \cong M_1/(M_1 \cap N_1)$. Poniamo dunque $D = M_1 \cap N_1$. Per la Proposizione 3.37 D ammette una serie di composizione $D = D_0 \supsetneq \ldots \supsetneq D_t = 0$. Tale serie può essere estesa a due serie di composizione per M ottenendo

$$M \supsetneq M_1 \supsetneq D \supsetneq \ldots \supsetneq 0 \tag{3}$$

$$M \supsetneq N_1 \supsetneq D \supsetneq \ldots \supsetneq 0. \tag{4}$$

Troncando la prima di queste ad M_1 possiamo applicare l'ipotesi induttiva tra (1) e (3) ed ottenere così che $t+1 = n-1$ e dunque $n = t+2$. Ripetendo lo stesso ragionamento tra (2) e (4) troncando ad N_1 (applicando l'ipotesi induttiva su $t + 1 = n - 1 < n$) si ottiene che $t+1 = m-1$ e dunque $m = t+2$. Si è dunque mostrato che $n = t+2 = m$ ed è ben posta dunque $\operatorname{length}_A M$ come la lunghezza di una – e quindi qualsiasi – serie di composizione per M.

ii) Sia $M = N_0 \supsetneq N_1 \supsetneq \ldots \supsetneq N_k$ una catena di sottomoduli. Mostriamo per induzione su $\operatorname{length}_A M$ che $k \leq \operatorname{length}_A M$. Ancora è ovvio se $\operatorname{length}_A M = 0$, dato che $M = 0$. Per la Proposizione 3.37 abbiamo che $\operatorname{length}_A N_1 < \operatorname{length}_A M$; dunque per ipotesi induttiva abbiamo che $k - 1 \leq \operatorname{length}_A N_1$. dato che $\operatorname{length}_A N_1 < \operatorname{length}_A M$ si ha che $k \leq \operatorname{length}_A M$.

iii) Per il Corollario 3.22 è sufficiente mostrare che tale mappa è un isomorfismo dopo aver localizzato ad ogni ideale massimale m di A. A tal fine studiamo cosa succede alla localizzazione di un modulo di lunghezza finita. Nel caso in cui $\operatorname{length}_A M = 1$, ciò è banale poiché M è semplice e dunque $M \cong A/\operatorname{Ann}(M)$. Se $\operatorname{Ann}(M) = \mathfrak{m}$ allora, dato che $A/\mathfrak{m}$ è un campo, gli elementi non in $\mathfrak{m}$ sono invertibili in $A/\mathfrak{m}$; dunque $(A/\mathfrak{m})_{\mathfrak{m}} = A/\mathfrak{m}$. D'altra parte se $\operatorname{Ann}(M) \neq \mathfrak{m}$, allora dato che $\operatorname{Ann}(M)$ è massimale, si ha che $\operatorname{Ann}(M) \nsubseteq \mathfrak{m}$ e perciò $\operatorname{Ann}(M)_{\mathfrak{m}} = A_{\mathfrak{m}}$ dato che $\operatorname{Ann}(M)_{\mathfrak{m}}$ è un ideale di $A_{\mathfrak{m}}$ che contiene un invertibile. Avendo mostrato che la localizzazione commuta con i quozienti si ha che $(A/\operatorname{Ann}(M))_{\mathfrak{m}} = A_{\mathfrak{m}}/\operatorname{Ann}(M)_{\mathfrak{m}} = 0$. Segue dunque in particolare che se $\mathfrak{p}$ e $\mathfrak{p}'$ sono due distinti ideali primi di A e $\operatorname{length}_A M = 1$, allora $(M_{\mathfrak{p}})_{\mathfrak{p}'} = 0$. Tornando al caso generale, supponiamo che M sia un modulo di lunghezza finita $\operatorname{length}_A M = n < \infty$. La serie di composizione per M localizza ad una catena

di sottomoduli

$$M_{\mathfrak{m}} \supsetneq (M_1)_{\mathfrak{m}} \supsetneq \ldots \supsetneq (M_n)_{\mathfrak{m}} = 0.$$

Dato che i fattori di composizione M_i/M_{i+1} hanno lunghezza 1, per quanto detto sopra si ha che $(M_i/M_{i+1})_{\mathfrak{m}} = M_i/M_{i+1}$ se $\mathfrak{m} = \mathrm{Ann}(M_i/M_{i+1})$ ed $(M_i/M_{i+1})_{\mathfrak{m}} = 0$ altrimenti. Allora $M_{\mathfrak{m}}$ ha una serie di composizione finita corrispondente alla sottoserie di M ottenuta mantenendo solo i sottomoduli $(M_i)_{\mathfrak{m}}$ tali che $M_i/M_{i+1} \cong A/\mathfrak{m}$. In particolare dunque se nessuno dei fattori di composizione M_i/M_{i+1} è isomorfo ad $A/\mathfrak{m}$, allora $M_{\mathfrak{m}} = 0$; dunque se $\mathfrak{m}$ ed $\mathfrak{m}'$ sono ideali massimali distinti allora $(M_{\mathfrak{m}})_{\mathfrak{m}'} = 0$. Considerando adesso allora la mappa $\varphi\colon M \to \oplus_{\mathfrak{p}} M_{\mathfrak{p}}$, somma delle mappe di localizzazione, con $\mathfrak{p}$ che varia tra gli ideali massimali tali che ci sono fattori di composizione $M_i/M_{i+1} \cong A/\mathfrak{p}$. Da quanto mostrato sopra segue che possiamo senza problemi estendere la somma a tutti gli ideali massimali; i nuovi termini sono tutti nulli. Per ogni ideale massimale $\mathfrak{m}$ ed ogni modulo M abbiamo che $(M_{\mathfrak{m}})_{\mathfrak{m}} = M_{\mathfrak{m}}$, dunque la mappa identità fa parte della localizzazione della mappa φ:

$$\varphi_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to (\oplus_{\mathfrak{p}\in \mathrm{Specm}(A)} M_{\mathfrak{p}})_{\mathfrak{m}} = \oplus_{\mathfrak{p}\in \mathrm{Specm}(A)} (M_{\mathfrak{p}})_{\mathfrak{m}}.$$

Ma se $\mathfrak{p} \neq \mathfrak{m}$ ed M ha lunghezza finita, abbiamo mostrato che $(M_{\mathfrak{p}})_{\mathfrak{m}} = 0$. Dunque $\varphi_{\mathfrak{m}}$ è la mappa identità per ogni ideale massimale $\mathfrak{m}$. Segue dunque che φ è un isomorfismo.

II) ($\Leftarrow$) Innanzitutto supponiamo che M sia artiniano e noetheriano. Dalla a.c.c. sui sottomoduli possiamo prendere un sottomodulo proprio massimale M_1 di M, un sottomodulo proprio massimale M_2 di M_1 e così via. Dalla d.c.c. questa successione di sottomoduli termina quando qualche $M_n = 0$. In questo caso abbiamo trovato $M = M_0 \supsetneq M_1 \supsetneq \ldots \supsetneq M_n = 0$ una serie di composizione per M.

($\Rightarrow$) Abbiamo per I) che $\mathrm{length}_A M$ fornisce un *upper bound* per tutte le catene di A-sottomoduli di M e dunque M rispetta sia la a.c.c. che la d.c.c.; cioè è sia artiniano che noetheriano.

□

Proposizione 3.39. Sia A un anello e M un A-modulo. Sia $\mathfrak{m} \in \mathrm{Specm}(A)$. Allora l'omomorfismo di localizzazione $M \to M_{\mathfrak{m}}$ è un isomorfismo se $\mathfrak{m} \subseteq \sqrt{\mathrm{Ann}(M)}$.

Dimostrazione. Usiamo la proprietà locale 3.22 sull'omomorfismo di localizzazione $f\colon M \to M_{\mathfrak{m}}$. Sia $\mathfrak{n} \in \mathrm{Specm}(A)$.

- Se $\mathfrak{n} = \mathfrak{m}$ si ha che $(M_{\mathfrak{m}})_{\mathfrak{m}} = M_{\mathfrak{m}}$ e dunque $f_{\mathfrak{m}}$ è l'identità.
- Se $\mathfrak{m} \neq \mathfrak{n}$, allora esiste $x \in \mathfrak{m}$ tale che $x \notin \mathfrak{n}$. Per ipotesi esiste $k \in \mathbb{Z}_{>0}$ tale che $x^k M = 0$. Dunque per la Proposizione 3.15 $M_{\mathfrak{n}} = 0$. Sapendo che $(M_{\mathfrak{m}})_{\mathfrak{n}} = 0$ si ha che $f_{\mathfrak{n}}$ è l'unico omomorfismo tra moduli nulli.

Dunque $M \cong M_{\mathfrak{m}}$. □

Consideriamo adesso il caso particolare dei moduli sopra un campo $\mathbb{K}$, cioè i $\mathbb{K}$-spazi vettoriali.

Proposizione 3.40. Sia V un $\mathbb{K}$-spazio vettoriale. Allora le seguenti condizioni sono equivalenti:

i) dimensione finita;
ii) lunghezza finita;
iii) a.c.c.;
iv) d.c.c..

Inoltre se una – e quindi tutte – tra le seguenti condizioni è rispettata, la dimensione coincide con la lunghezza.

Dimostrazione. *i*) implica *ii*) è ovvia in quanto la dimensione da una maggiorazione sulla lunghezza delle catene. Dal Teorema 3.38 segue inoltre che *ii*) implica sia *iii*) che *iv*).

Mostriamo adesso sia che *iii*) e *iv*) implicano *i*). Se per assurdo V non avesse dimensione finita allora avremmo una successione infinita di elementi linearmente indipendenti $\{x_n\}_{n\geq 1}$. Sia U_n (risp. V_n) il sottospazio vettoriale generato da $x_1, \ldots, x_n$ (risp. $x_{n+1}, x_{n+2} \ldots,$). Allora la successione $\{U_n\}_{n\geq 1}$ (risp. $\{V_n\}_{n\geq 1}$) è infinita e strettamente crescente (risp. decrescente) e non vale l'a.c.c. (risp. d.c.c.); e questo è assurdo. □

Vediamo adesso un raffinamento delle condizioni sulla finitezza della lunghezza di un modulo se l'anello è noetheriano.

PROPOSIZIONE 3.41. Sia A un anello noetheriano e sia M un A-modulo finitamente generato. Allora sono equivalenti le seguenti:

i) M ha lunghezza finita;
ii) M è un A-modulo artiniano;
iii) $\operatorname{Supp}(M) \subseteq \operatorname{Specm}(A)$.

DIMOSTRAZIONE. L'equivalenza dei primi due punti segue dal Teorema 3.38 e dalla Proposizione 3.31. Per il punto *iii*) [**Eis95**, pag. 77, Corollario 2.17]. □

Grazie alla proposizione precedente abbiamo il seguente risultato che lega la noetherianità e l'artinianità per gli anelli.

PROPOSIZIONE 3.42. Sia A un anello. Allora A è artiniano se e solo se A è noetheriano e $\dim A = 0$.

DIMOSTRAZIONE. ($\Leftarrow$) Segue immediatamente dalla proposizione precedente poiché se $\dim A = 0$ allora tutti gli ideali primi sono massimali e dunque la condizione *iii*) su $\operatorname{Supp} A$ è tautologicamente verificata, A è finitamente generato su A e dunque A è artiniano.
($\Rightarrow$) Vedi [**AM16**, pag. 135, Teorema 8.5]. □

3.4. Prodotto tensoriale e potenza esterna

Dedichiamo quest'ultima sezione del capitolo allo studio di un'importante costruzione dell'algebra commutativa: il prodotto tensoriale. In particolare da questo ricaveremo poi un oggetto a noi più utile: la potenza esterna.

La costruzione del prodotto tensoriale risponde alla risoluzione universale di un problema di fattorizzazioni di mappe. In particolare ci chiediamo se ogni mappa A-bilineare dal prodotto di due moduli in un terzo modulo possa essere sempre fattorizzata tramite una mappa A-bilineare su di un oggetto ed una mappa A-lineare da quest'ultimo al codominio della mappa A-bilineare iniziale. Abbiamo già incontrato un problema di questo tipo nella costruzione dell'anello delle frazioni relativo ad una parte moltiplicativa.

DEFINIZIONE 3.43. Siano M_1, M_2 ed N tre A-moduli. $\beta\colon M_1 \times M_2 \to M$ si dice A-*bilineare* se, per ogni $x_1, y_1 \in M_1$, $x_2, y_2 \in M_2$ e $\lambda \in A$ vale che

$$\begin{aligned}\beta(x_1 + y_1, x_2) &= \beta(x_1, x_2) + \beta(y_1, x_2),\\ \beta(x_1, x_2 + y_2) &= \beta(x_1, x_2) + \beta(x_1, y_2),\\ \beta(\lambda x_1, x_2) &= \beta(x_1, \lambda x_2) = \lambda\beta(x_1, x_2).\end{aligned}$$

Siano dunque due A-moduli M_1, M_2 e consideriamo l'A-modulo libero con base le coppie ordinate $(x, y) \in M_1 \times M_2$, $C = A^{(M_1 \times M_2)}$. Sia adesso D il suo A-sottomodulo generato dagli elementi dei tipi seguenti:

$$\begin{aligned}&(x_1 + x_2, y) - (x_1, y) - (x_2, y),\\ &(x, y_1 + y_2) - (x, y_1) - (x, y_2),\\ &(\lambda x, y) - (x, \lambda y),\\ &\lambda \cdot (x, y) - (\lambda x, y)\end{aligned}$$

con $x, x_1, x_2 \in M_1$, $y, y_1, y_2 \in M_2$ e $\lambda \in A$.

DEFINIZIONE 3.44. Il *prodotto tensoriale* di due A-moduli M_1 ed M_2, denotato come $M_1 \otimes_A M_2$ (o più brevemente $M_1 \otimes M_2$ quando non c'è possibilità di incomprensione), è l'A-modulo quoziente C/D. Dati due elementi $x \in M_1$ ed $y \in M_2$ l'elemento che è immagine di $(x, y) \in C$ viene denotato come $x \otimes y$ ed è chiamato il *prodotto tensoriale* di x ed y.

Abbiamo dunque una mappa canonica $\Phi\colon M_1 \times M_2 \to M_1 \otimes M_2$ definita come $(x, y) \mapsto x \otimes y$. Si osserva facilmente come questa sia un mappa A-bilineare di moduli. Come preannunciato il prodotto tensoriale insieme alla sua mappa canonica risponde al problema universale di fattorizzazione delle forme A-bilineari.

TEOREMA 3.45 (Proprietà universale del prodotto tensoriale). Siano M_1, M_2 ed N tre A-moduli.

1) Sia $f\colon M_1 \otimes_A M_2 \to N$ A-lineare. La mappa $f \circ \Phi$ da $M_1 \times M_2$ in N è A-bilineare.
2) Sia $\beta\colon M_1 \times M_2 \to N$ una mappa A-bilineare. Allora esiste un'unica mappa A-lineare $g\colon M_1 \otimes_A M_2 \to N$ tale che $\beta = g \circ \Phi$.

Abbiamo dunque un isomorfismo canonico tra gli A-moduli $\mathrm{Bil}_A(M_1, M_2; N)$ delle forme A-bilineari e $\mathrm{Hom}_A(M_1 \otimes_A M_2, N)$.

DIMOSTRAZIONE. 1) Siano $x, x_1, x_2 \in M_1$, $y, y_1, y_2 \in M_2$ e $\lambda \in A$ allora $f(x \otimes (y_1 + y_2)) = f(x \otimes y_1 + x \otimes y_2) = f(x \otimes y_1) + f(x \otimes y_2)$ (analogamente $f((x_1 + x_2) \otimes y) = f(x_1 \otimes y) + f(x_2 \otimes y)$) ed $f(\lambda x \otimes y) = f(x \otimes \lambda y) = f(\lambda(x \otimes y)) = \lambda f(x \otimes y)$.

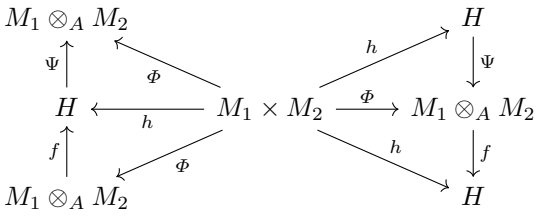
2) La mappa A-bilineare β si estende naturalmente ad una mappa A-lineare $\overline{\beta}\colon C \to N$. Per le proprietà di A-bilinearità inoltre questa è nulla sugli elementi che generano D, dunque su tutto D. Dunque per la proprietà universale del quoziente esiste una mappa A-lineare $g\colon M_1 \otimes_A M_2 \to N$ tale che, indicando con $p\colon C \to M_1 \otimes_A M_2$ la mappa al quoziente, $\overline{\beta} = g \circ p$. Tale g è unica poiché $M_1 \otimes_A M_2$ è generato dagli $x \otimes y$. Abbiamo dunque che $\beta = g \circ \Phi$. □

COROLLARIO 3.46. Siano M_1, M_2 due A-moduli. Sia H un A-modulo ed $h\colon M_1 \times M_2 \to H$ una mappa A-bilineare tale che:

i) H è generato da $h(M_1 \times M_2)$ come A-modulo;
ii) per ogni A-modulo N e per ogni mappa A-bilineare $\beta\colon M_1 \times M_2 \to N$, esiste una mappa A-lineare $g\colon H \to N$ tale che $\beta = g \circ h$.

Allora esiste un unico isomorfismo di A-moduli $\Psi\colon M_1 \otimes_A M_2 \to H$ tale che $h = \Psi \circ \Phi$.

DIMOSTRAZIONE. Questa è una conseguenza diretta dell'esistenza ed unicità del prodotto tensoriale dovuta all'analisi del seguente diagramma commutativo:



Concentriamoci sul ramo destro del diagramma: per le proprietà di (H, h) essendo Φ bilineare esiste $\Psi\colon H \to M_1 \otimes_A M_2$ ed analogamente per $(M_1 \otimes_A M_2, \Phi)$ essendo h bilineare esiste $f\colon M_1 \otimes_A M_2 \to H$ che fanno commutare il lato destro del diagramma. Poiché commutano i due triangoli a destra commuta anche il triangolo di destra esterno considerando la composizione $f \circ \Psi$. Anche la mappa id_H fa commutare il diagramma pertanto $\mathrm{id}_H \circ h = h = (f \circ \Psi) \circ h$; dunque $f \circ \Psi$ coincide con id_H su $h(M_1 \times M_2)$. $h(M_1 \times M_2)$ genera H per ipotesi e dunque $f \circ \Psi = \mathrm{id}_H$. Applicando lo stesso ragionamento al lato sinistro applicando Φ a se stessa si ottiene anche che $\Psi \circ f = \mathrm{id}_{M_1 \otimes_A M_2}$; dunque $f = \Psi^{-1}$ e Ψ è l'isomorfismo cercato. □

A seguito una carrellata di proprietà del prodotto tensoriale che seguono direttamente dalla sua proprietà universale. Siano M, N, P A-moduli allora esistono isomorfismi canonici:

(i) $M \otimes N \to N \otimes M$ definito da $x \otimes y \mapsto y \otimes x$.
(ii) $(M \otimes N) \otimes P \to M \otimes (N \otimes P)$ definito da $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$.
(iii) $A \otimes M \to M$ definito da $a \otimes x \mapsto ax$.
(iv) $A/I \otimes_A M \cong M/IM$, con $I \subseteq A$ ideale, definito da $(a + I) \otimes x \mapsto ax + IM$.
(v) $A/I \otimes_A A/J \cong A/(I+J)$, con $I, J \subseteq A$ ideali, definito da $(a+I)\otimes(b+J) \mapsto ab+I+J$.

Osservazione 3.47. Abbiamo già visto come avendo un omomorfismo di anelli $f\colon A \to B$ potessimo definire una struttura di A-modulo su di un B-modulo M tramite restrizione degli scalari. Grazie al prodotto tensoriale possiamo costruire un B-modulo a partire da un A-modulo M. Sappiamo già che per restrizione degli scalari B può essere considerato come un A-modulo. Allora esiste unico il prodotto tensoriale $M_B = B \otimes_A M$ su cui può essere definita una struttura di B-modulo come $b(b' \otimes x) = bb' \otimes x$ per ogni $b, b' \in B$ e per ogni $x \in M$. Il B-modulo M_B si dice ottenuto da M per *estensione degli scalari*.

Il prodotto tensoriale gode di proprietà funtoriali, nel senso che dati M_1, M_2 ed N_1, N_2 A-moduli con $u\colon M_1 \to N_1$ e $v\colon M_2 \to N_2$ omomorfismi di A-moduli si verifica facilmente che la mappa $(x, y) \mapsto u(x) \otimes v(y)$ è A-bilineare, dunque per la proprietà universale del prodotto tensoriale esiste ed è unica la mappa A-lineare $w\colon M_1 \otimes M_2 \to N_1 \otimes N_2$ tale che $w(x \otimes y) = u(x) \otimes v(y)$ per ogni $x \in M_1,\ y \in M_2$. Tale mappa viene denotata con $u \otimes v$ ed è chiamata il *prodotto tensoriale* delle mappe u e v.

Tale costruzione dà una mappa A-bilineare canonica

$$\mathrm{Hom}_A(M_1, N_1) \times \mathrm{Hom}_A(M_2, N_2) \to \mathrm{Hom}_A(M_1 \otimes_A M_2, N_1 \otimes_A N_2).$$

Per la proprietà universale del prodotto tensoriale dunque esiste ed è unica una mappa A-lineare

$$\mathrm{Hom}_A(M_1, N_1) \otimes_A \mathrm{Hom}_A(M_2, N_2) \to \mathrm{Hom}_A(M_1 \otimes_A M_2, N_1 \otimes_A N_2)$$

che associa ad ogni elemento $u \otimes v$ del prodotto tensoriale la mappa A-lineare $u \otimes v\colon M_1 \otimes M_2 \to N_1 \otimes N_2$. Inoltre, siano M_3, N_3 due A-moduli, $u'\colon M_2 \to M_3$ e $v'\colon N_2 \to N_3$ due mappe A-lineari segue che

$$(u' \circ u) \otimes (v' \circ v) = (u' \circ v') \otimes (u \circ v).$$

Osservazione 3.48. Il prodotto tensoriale di due moduli non nulli può essere nullo. Prendiamo ad esempio i due Z-moduli $\mathbb{Z}/3\mathbb{Z}$ e $\mathbb{Z}/2\mathbb{Z}$: in $\mathbb{Z}/3\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ si ha

$$x \otimes y = 3(x \otimes y) - 2(x \otimes y) = (3x) \otimes y - x \otimes (2y) = 0$$

per ogni $x \in \mathbb{Z}/3\mathbb{Z}$ ed $y \in \mathbb{Z}/2\mathbb{Z}$.

Siano adesso $(M_\alpha)_{\alpha\in\Lambda}$ ed $(N_\beta)_{\beta\in B}$ due famiglie di A-moduli e poniamo $M = \prod_{\alpha\in\Lambda} M_\alpha$ ed $N = \prod_{\beta\in B} N_\beta$. Abbiamo una mappa A-bilineare

$$\begin{aligned} f\colon M \times N &\to \prod_{(\alpha,\beta)\in\Lambda\times B} (M_\alpha \otimes N_\beta) \\ ((x_\alpha)_{\alpha\in\Lambda}, (y_\beta)_{\beta\in B}) &\mapsto (x_\alpha \otimes y_\beta) \end{aligned}$$

Dunque per la proprietà universale del prodotto tensoriale abbiamo una mappa A-lineare $(\prod_{\alpha\in\Lambda} M_\alpha) \otimes (\prod_{\beta\in B} N_\beta) \to \prod_{(\alpha,\beta)\in\Lambda\times B}(M_\alpha \otimes N_\beta)$ definita come $(x_\alpha)_{\alpha\in\Lambda} \otimes (y_\beta)_{\beta\in B} \mapsto (x_\alpha \otimes y_\beta)$. Tale mappa non è in generale né iniettiva né suriettiva. Consideriamo adesso $\oplus_{\alpha\in\Lambda} M_\alpha$ ed $\oplus_{\beta\in B} N_\beta$. Le due immersioni $\oplus_{\alpha\in\Lambda} M_\alpha \hookrightarrow \prod_{\alpha\in\Lambda} M_\alpha$ e $\oplus_{\beta\in B} N_\beta \hookrightarrow \prod_{\beta\in B} N_\beta$ definiscono una mappa A-lineare $(\oplus_{\alpha\in\Lambda} M_\alpha) \otimes (\oplus_{\beta\in B} N_\beta) \to (\prod_{\alpha\in\Lambda} M_\alpha) \otimes (\prod_{\beta\in B} N_\beta)$. Post-componendo tale mappa con f si ottiene una mappa

$$\begin{aligned} (\oplus_{\alpha\in\Lambda} M_\alpha) \otimes (\oplus_{\beta\in B} N_\beta) &\to \prod_{(\alpha,\beta)\in\Lambda\times B} (M_\alpha \otimes N_\beta) \\ (x_\alpha)_{\alpha\in\Lambda} \otimes (y_\beta)_{\beta\in B} &\mapsto (x_\alpha \otimes y_\beta) \end{aligned}$$

che diventa una mappa A-lineare $g\colon (\oplus M_\alpha)\otimes(\oplus N_\beta)\to\oplus(M_\alpha\otimes N_\beta)$. La mappa g è un isomorfismo di A-moduli. Possiamo difatti costruirne un'inversa esplicita. Costruiamo la funzione inversa sulle componenti. Per ogni $\alpha\in\Lambda$ abbiamo l'inclusione $i_\alpha\colon M_\alpha\hookrightarrow\oplus M_\alpha$ e per ogni $\beta\in B$ l'inclusione $j_\beta\colon N_\beta\hookrightarrow\oplus N_\beta$. Consideriamo allora per ogni $(\alpha,\beta)\in\Lambda\times B$ la mappa prodotto tensoriale $h_{\alpha,\beta}=i_\alpha\otimes j_\beta$ e poniamo dunque $h=\oplus h_{\alpha,\beta}$. Osserviamo che le composizioni $g\circ h$ ed $h\circ g$ sono l'identità sui generatori; dunque per A-linearità lo sono su tutto $(\oplus M_\alpha)\otimes(\oplus N_\beta)$ e $\oplus(M_\alpha\otimes N_\beta)$.

Corollario 3.49. Siano M ed N A-moduli liberi, allora il prodotto tensoriale $M\otimes_A N$ è ancora un A-modulo libero.

Dimostrazione. Poiché M ed N sono A-moduli liberi allora $M\cong A^{\oplus m}$ ed $N\cong A^{\oplus n}$ per qualche $n,m\in\mathbb{Z}_{\geq 0}$. Si ha pertanto che $M\otimes N=A^{\oplus n}\otimes A^{\oplus n}\cong A^{\oplus mn}$. □

Corollario 3.50. Siano M ed N due A-moduli finitamente generati, allora $M\otimes_A N$ è finitamente generato.

Dimostrazione. Dato che M ed N sono finitamente generati allora esistono due omomorfismi di A-moduli suriettivi $f\colon A^{\oplus m}\twoheadrightarrow M$ e $g\colon A^{\oplus n}\twoheadrightarrow N$ per qualche $n.m\in\mathbb{Z}_{\geq 0}$. Allora la mappa prodotto tensoriale $f\otimes g\colon A^{\oplus m}\otimes A^{\oplus n}\to M\otimes N$ è ancora suriettiva. Per il Corollario 3.49 segue che anche $M\otimes N$ è finitamente generato. □

Avendo adesso ben chiara la costruzione e le proprietà basilari del prodotto tensoriale possiamo passare ad un'altra costruzione per avvicinarci ulteriormente al nostro scopo.

Definizione 3.51. Sia A un anello commutativo unitario ed M un A-modulo. Per ogni $n\geq 0$ definiamo la *n-esima potenza tensoriale* di M come l'A-modulo $T^n(M)=M^{\otimes n}$. Poniamo poi $T^1(M)=M$ e $T^0(M)=A$.

Denotiamo con $T(M)$ l'A-modulo $\oplus_{n\geq 0}T^n(M)$. Possiamo definire su tale modulo una struttura di algebra $\mathbb{N}$-graduata definendo per ogni coppia ordinata di interi non negativi p,q l'omomorfismo di A-moduli

$$m_{p,q}\colon T^p(M)\otimes T^q(M)\to T^{p+q}(M).$$

Per $p,q>0$, $m_{p,q}$ è l'isomorfismo dato dall'associatività del prodotto tensoriale, mentre per $p=0$ (risp. $q=0$) $m_{0,q}$ (risp. $m_{p,0}$) è l'isomorfismo canonico di $A\otimes T^q(M)$ in $T^q(M)$ (risp. di $T^p(M)\otimes A$ in $T^p(M)$). Siano dunque $x_i\in M$ ed $a\in A$,

$$\begin{gathered}(x_1\otimes\ldots\otimes x_p)\cdot(x_{p+1}\otimes\ldots\otimes x_{p+q})=x_1\otimes\ldots\otimes x_p\otimes x_{p+1}\otimes\ldots\otimes x_{p+q};\\ a\cdot(x_1\otimes\ldots\otimes x_p)=a(x_1\otimes\ldots\otimes x_p).\end{gathered}\tag{5}$$

Si verifica dunque facilmente che la moltiplicazione così definita è associativa ed ha elemento neutro $1\in T^0(M)=A$.

Definizione 3.52. Sia M un A-modulo. L'*algebra tensoriale* di M, denotata con $T(M)$, è l'algebra $\oplus_{n\geq 0}T^n(M)$ con la moltiplicazione definita come in (5). L'iniezione $\Phi\colon T^1(M)\hookrightarrow T(M)$ definisce l'inclusione canonica di M in $T(M)$.

Anche l'algebra tensoriale ha una proprietà universale.

Teorema 3.53 (Proprietà universale dell'algebra tensoriale). Sia E una A-algebra unitaria ed $f\colon M\to E$ un omomorfismo di A-moduli. Allora esiste ed è unico un omomorfismo di A-algebre $g\colon T(M)\to E$ tale che $f=g\circ\Phi$.

Dimostrazione. Vedi [**Bou74**, pag. 485, Proposizione 1]. □

Osservazione 3.54. Supponiamo che E sia una algebra $\mathbb{Z}$-graduata e supponiamo che $f(M)\subseteq E_1$. Allora segue che $g(T^p(M))\subseteq E_p$ per ogni $p\geq 0$. Dunque g è un omomorfismo di algebre graduate.

Nella dimostrazione della proprietà universale dell'algebra tensoriale è racchiuso un fatto per noi più importante. Iniziamo con l'osservare che per definizione del prodotto in $T(M)$ abbiamo che

$$x_1 \otimes \ldots \otimes x_n = \Phi(x_1) \cdots \Phi(x_n) =: \Phi_n(x_1, \ldots, x_n).$$

Consideriamo adesso un omomorfismo di A-moduli $f\colon M \to N$. Allora per ogni $n > 0$, la mappa $(x_1, \ldots, x_n) \mapsto f(x_1) \cdots f(x_n)$ da $M^{\oplus n}$ ad N è A-multilineare. Ad essa corrisponde dunque un omomorfismo di A-moduli $g_n\colon T^n(M) \to N$ tale che $g_n(x_1 \otimes \ldots \otimes x_n) = f(x_1) \ldots f(x_n)$. Dunque più in generale, sia $f\colon M^{\oplus n} \to N$ una mappa A-multilineare allora esiste ed è unico un omomorfismo di A-moduli $g_n\colon T^n(M) \to N$ tale che $f = g_n \circ \Phi_n$. Ciò si traduce nella proprietà universale della n-esima potenza tensoriale tramite la quale si fattorizzano tutte le mappe A-multilineari $M^{\oplus n} \to N$.

È dall'algebra tensoriale, ed in particolare dalla n-esima potenza tensoriale, che possiamo adesso costruire l'oggetto a noi davvero utile: l'algebra esterna.

Definizione 3.55. Sia M un A-modulo. L'*algebra esterna* di M, denotata come $\bigwedge M$, è il quoziente dell'algebra tensoriale di M tramite l'ideale bilatero $\mathfrak{I}$ generato dagli elementi $x \otimes x$, con $x \in M$.

Osservazione 3.56. Indichiamo con $x_1 \wedge \cdots \wedge x_n \in \bigwedge M$ la classe di equivalenza di $x_1 \otimes \ldots \otimes x_n \in T(M)$. Osserviamo che dalla relazione che definisce l'ideale $\mathfrak{I}$ segue che per ogni $x, y \in M$

$$0 = (x+y) \wedge (x+y) = x \wedge x + x \wedge y + y \wedge x + y \wedge y = x \wedge y + y \wedge x.$$

Cioè $x \wedge y = -y \wedge x$ in $\bigwedge M$.

Dato che l'ideale $\mathfrak{I}$ è generato da termini omogenei di grado 2 risulta un ideale omogeneo. Indichiamo adesso con $\mathfrak{I}_n = \mathfrak{I} \cap T^n(M)$, che risulta essere un sottomodulo di $T^n(M)$. Allora l'algebra esterna risulta una algebra graduata con componenti omogenee $\bigwedge^n M = T^n(M)/\mathfrak{I}_n$. Osserviamo che $\mathfrak{I}_0 = \mathfrak{I}_1 = 0$; pertanto $\bigwedge^0 = A$ e $\bigwedge^1 M = T^1(M) = M$. Segue dunque un'inclusione canonica $\Psi\colon M \hookrightarrow \bigwedge M$ tramite $\bigwedge^1 M$.

Definizione 3.57. Sia M un A-modulo chiamiamo l'*n-esima potenza esterna* di M l'A-modulo $\bigwedge^n M$.

Teorema 3.58 (Proprietà universale dell'algebra esterna). Sia E una A-algebra ed $f\colon M \to E$ un omomorfismo di A-moduli tale che $f(x)^2 = 0$ per ogni $x \in M$. Allora esiste ed è unico un omomorfismo di A-algebre $g\colon \bigwedge M \to E$ tale che $f = g \circ \Psi$.

Dimostrazione. Vedi [**Bou74**, pag. 507, Proposizione 1]. □

Anche in questo caso è racchiuso all'interno della dimostrazione della proprietà universale della potenza esterna ciò che a noi davvero interessa. Poniamo innanzitutto $\Psi_n\colon M^{\oplus n} \to \bigwedge^n M$ come $\Psi_n(x_1 \ldots, x_n) \coloneqq x_1 \wedge \cdots \wedge x_n$.

Lemma 3.59 (Proprietà universale della potenza esterna). Sia A un anello e siano M ed N A-moduli. Sia $f\colon M^{\oplus n} \to N$ una mappa A-alternante. Allora esiste ed è unico l'omomorfismo di A-moduli $g_n\colon \bigwedge^n M \to N$ tale che $f = g_n \circ \Psi_n$.

Dimostrazione. Osserviamo che le mappe A-lineari $\bigwedge^n M \to N$ sono in corrispondenza biunivoca con le mappe A-lineari $T^n(M) \to N$ che si annullano in $\mathfrak{I}_n$ ottenute associando ad ogni $g\colon \bigwedge^n M \to N$ la mappa $f = g \circ p_n$, con $p_n\colon T^n(M) \to T^n(M)/\mathfrak{I}_n = \bigwedge^n M$. Per la proprietà universale della potenza tensoriale sappiamo che esiste ed è unica $f_n\colon T^n(M) \to N$ tale che $f = f_n \circ \Phi_n$. Non resta che mostrare che f_n si annulla su $\mathfrak{I}_n$. Per definizione $f_n(x_1 \otimes \ldots \otimes x_n) = f(x_1, \ldots, x_n)$ che si annulla sugli elementi di $\mathfrak{I}_n$ poiché f è alternante □

Anche la potenza esterna gode di proprietà funtoriali. Sia $u\colon M \to N$ un omomorfismo di A-moduli allora esiste ed è unico l'omomorfismo di A-moduli $\bigwedge^k u\colon \bigwedge^k M \to \bigwedge^k N$ definito come

$$\bigwedge^k u(x_1 \wedge \ldots \wedge x_n) = u(x_1) \wedge \ldots \wedge u(x_n).$$

L'omomorfismo $\bigwedge^k u$ prende dunque il nome di *estensione* di u a $\bigwedge^k M$. Inoltre, siano $u\colon M \to N$ e $v\colon N \to P$ due omomorfismi di A-moduli, allora $\bigwedge^k(v \circ u) = \bigwedge^k v \circ \bigwedge^k u$.

PROPOSIZIONE 3.60. Sia M un A-modulo libero di rango n generato dagli elementi $e_1, \ldots, e_n$. Allora per ogni $k \geq 0$ $\bigwedge^k M$ è un A-modulo libero di rango $\binom{n}{k}$ con base

$$\{e_{i_1} \wedge \cdots \wedge e_{i_k} \mid 1 \leq i_1 \leq \ldots \leq i_k \leq n\}.$$

DIMOSTRAZIONE. Consideriamo innanzitutto $k \geq 1$ dato che il caso $k = 0$ è triviale dato che $\bigwedge^0 M = A$ che è libero di rango 1 e difatti $\binom{n}{0} = 1$. Supponiamo poi $k \leq n$ dato che per $k > n$ si ha che $\binom{n}{k} = 0$; dunque $\bigwedge^k M = 0$ per $k > n$. Consideriamo adesso la mappa $f\colon M^k \to T^k(M)$ definita da

$$(m_1, \ldots, m_k) \mapsto \sum_{\sigma \in \mathfrak{S}_k} \operatorname{sgn}(\sigma) m_{\sigma(1)} \otimes \ldots \otimes m_{\sigma(k)}.$$

Tale mappa è A-alternante, dunque per la proprietà universale della k-esima potenza esterna si ha che esiste ed è unico l'omomorfismo di A-moduli $\varphi_k\colon \bigwedge^k M \to M^{\otimes k}$ definita come

$$\varphi_k(m_1 \wedge \cdots \wedge m_k) = \sum_{\sigma \in \mathfrak{S}_k} \operatorname{sgn}(\sigma) m_{\sigma(1)} \otimes \ldots \otimes m_{\sigma(k)}.$$

Osserviamo che per $k = 1$ tale mappa è l'identità. Dato che gli elementi $e_1, \ldots, e_n$ generano M, allora gli $\binom{n}{k}$ elementi $e_{i_1} \wedge \ldots \wedge e_{i_k}$, con $1 \leq i_1 \leq \ldots \leq i_k \leq n$, generano $\bigwedge^k M$. Vogliamo adesso provare che questi sono linearmente indipendenti: proviamo a tale scopo che φ_k è iniettiva. Sia $w \in \bigwedge^k M$ tale che $\varphi_k(w) = 0$. Scriviamo $w = \sum_{1 \leq i_1 \leq \ldots \leq i_k \leq n} c_{i_1,\ldots,i_k} e_{i_1} \wedge \cdots \wedge e_{i_k}$ con $c_{i_1,\ldots,i_k} \in A$. Dunque dato che $\varphi_k(w) = 0$ abbiamo che

$$\sum_{1 \leq i_1 \leq \ldots \leq i_k \leq n} c_{i_1,\ldots,i_k} \sum_{\sigma \in \mathfrak{S}_k} \operatorname{sgn}(\sigma) e_{\sigma(1)} \otimes \ldots \otimes e_{\sigma(k)} = 0.$$

Scambiando le due sommatorie (ed alleggerendo la notazione sostituendo $c_{i_1,\ldots,i_k}$ con c_I e $e_{\sigma(1)} \otimes \ldots \otimes e_{\sigma(k)}$ con $e_{\sigma(I)}$ con $I \subset \{1, \ldots, n\}$ di cardinalità k) otteniamo che

$$\sum_{\sigma \in \mathfrak{S}_n} \sum_I \operatorname{sgn}(\sigma) c_I e_{\sigma(I)} = 0.$$

Dato che gli $\{e_{\sigma(I)}\}$ sono linearmente indipendenti in $M^{\otimes k}$ segue che i $c_I = 0$; dunque $w = 0$. Allora gli $e_{i_1} \wedge \ldots \wedge e_{i_k}$ sono A-linearmente indipendenti e generano $\bigwedge^k M$. Pertanto abbiamo un isomorfismo $\sum_I Ae_I \to \bigwedge^k M$; dunque $\bigwedge^k M$ è libero di rango $\binom{n}{k}$. □

CAPITOLO 4

Rudimenti di geometria algebrica

Nel capitolo 1 abbiamo parlato nei termini della geometria proiettiva delle ipersuperfici, per poi soffermarci e prendere in esame il caso particolare delle curve algebriche piane. Per dimostrare al meglio il nostro risultato, ci siamo impegnati a sviluppare strumenti più sofisticati di algebra che, come vedremo più avanti, ci consentiranno di legare la molteplicità di intersezione che definiremo in 5 ad una quantità intrinseca alle curve: questi non sono tuttavia gli unici necessari. Dobbiamo trovare un modo per descrivere in modo più preciso i nostri oggetti: questo viene fatto attraverso il linguaggio della geometria algebrica.

Assumiamo per tutto il capitolo $\mathbb{K} = \overline{\mathbb{K}}$. Consideriamo allora $A = \mathbb{K}[x_1, \dots, x_n]$. Sappiamo che, poiché $\mathbb{K}$ è un dominio, ogni polinomio $f \in A$ induce una funzione polinomiale $\mathbb{A}^n_{\mathbb{K}} \to \mathbb{K}$. Ha dunque senso parlare degli zeri di $f \in A$. Allora poniamo $\mathbf{V}(f) = \{p \in \mathbb{A}^n \mid f(p) = 0\}$. Più in generale per ogni sottoinsieme $T \subseteq A$ poniamo

$$\mathbf{V}(T) \coloneqq \{p \in \mathbb{A}^n \mid f(p) = 0 \text{ per ogni } f \in T\}.$$

DEFINIZIONE 4.1. Un sottoinsieme $X \subseteq \mathbb{A}^n$ si dice un *insieme algebrico affine* o *chiuso algebrico affine* se esiste $T \subseteq \mathbb{K}[x_1, \dots, x_n]$ tale che $X = \mathbf{V}(T)$.

OSSERVAZIONE 4.2. Segue dalle definizioni che, sia $T \subseteq \mathbb{K}[x_1, \dots, x_n]$, allora $\mathbf{V}(T) = \mathbf{V}((T))$ con (T) l'ideale generato da T. Allora per il Teorema 3.32 $\mathbf{V}(T)$ si esprime come luogo comune di zeri di un insieme finito di polinomi $f_1, \dots, f_r \in T$.

PROPOSIZIONE 4.3. L'unione di due insiemi algebrici di $\mathbb{A}^n$ è ancora un insieme algebrico. L'intersezione arbitraria di insiemi algebrici di $\mathbb{A}^n$ è ancora un insieme algebrico di $\mathbb{A}^n$. Inoltre $\mathbb{A}^n$ e $\varnothing$ sono insiemi algebrici.

DIMOSTRAZIONE. Vedi [**Har77**, Proposizione 1.1, pag. 2]. □

Grazie alla precedente proposizione possiamo definire una topologia su $\mathbb{A}^n$ i cui aperti sono i complementari degli insiemi algebrici. Tale topologia prende il nome di *topologia di Zariski* su $\mathbb{A}^n_{\mathbb{K}}$.

DEFINIZIONE 4.4. Uno spazio topologico X si dice *irriducibile* se è non vuoto e se non esistono due sottoinsiemi chiusi $Y_1, Y_2 \subsetneq X$ tali che $X = Y_1 \cup Y_2$.

PROPOSIZIONE 4.5. Sia X uno spazio topologico irriducibile, $A \subseteq X$ aperto non vuoto. Allora A è denso ed irriducibile.

DIMOSTRAZIONE. Se per assurdo A non fosse denso allora esisterebbe $U \subseteq X$ aperto non vuoto tale che $A \cap U = \varnothing$. Allora $X = (X \setminus A) \cup (X \setminus U)$: il che è assurdo poiché X irriducibile.

Se per assurdo A non fosse irriducibile, allora esisterebbero due chiusi X_1, X_2 di X tali per cui $A = (X_1 \cap A) \cup (X_2 \cap A)$ e $X_1 \cap A \subsetneq A, X_2 \cap A \subsetneq A$. Allora $X = (X \setminus A) \cup (X_1 \cup X_2)$ e siamo giunti di nuovo ad un assurdo. □

DEFINIZIONE 4.6. Siano $X \subseteq A^n$ e $Y \subseteq A^m$ chiusi di Zariski. Una mappa $f \colon X \to Y$ si dice *polinomiale* se esistono $f_1, \dots, f_m \in \mathbb{K}[x_1, \dots, x_n]$ tali che $f(x) = (f_1(x), \dots, f_m(x))$ per ogni $x \in X$.

Avendo definito i chiusi affini, vogliamo adesso definire una costruzione che sia in un qualche modo inversa. Sia $X \subseteq \mathbb{A}^n$, definiamo l'*ideale* di X in $\mathbb{K}[x_1, \dots, x_n]$ come

$$\mathbf{I}(X) \coloneqq \{f \in \mathbb{K}[x_1, \dots, x_n] \mid f(p) = 0 \text{ per ogni } p \in X\}.$$

Abbiamo adesso due mappe: $\mathbf{V}$ che mappa sottoinsiemi di $\mathbb{K}[x_1, \dots, x_n]$ in insiemi algebrici e $\mathbf{I}$ che mappa sottoinsiemi di $\mathbb{A}^n$ in ideali di $\mathbb{K}[x_1, \dots, x_n]$. Tale corrispondenza può essere arricchita dal seguente teorema.

Teorema 4.7 (Hilbert's Nullstellensatz). Sia $\mathbb{K}$ un campo algebricamente chiuso, sia I un ideale di $\mathbb{K}[x_1, \dots, x_n]$ ed $f \in \mathbb{K}[x_1, \dots, x_n]$ un polinomio che si annulla in ogni punto di $\mathbf{V}(I)$. Allora $f^k \in I$ per qualche $k \in \mathbb{Z}_{>0}$. Equivalentemente $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$.

Dimostrazione. Vedi [**Har77**, Teorema 1.3A, pag. 4]. □

Corollario 4.8. Abbiamo una corrispondenza biunivoca che rovescia le inclusioni tra gli insiemi algebrici di $\mathbb{A}^n$ e gli ideali radicali di $\mathbb{K}[x_1, \dots, x_n]$, data da $X \mapsto \mathbf{I}(X)$ e $I \mapsto \mathbf{V}(I)$.

Dimostrazione. Vedi [**Har77**, Corollario 1.4, pag. 4]. □

Definizione 4.9. Sia $X \subseteq \mathbb{A}^n$ un insieme algebrico. Definiamo il suo *anello delle coordinate affini* $\mathbb{K}[X] \coloneqq \mathbb{K}[x_1, \dots, x_n]/\mathbf{I}(X)$.

Osservazione 4.10. Sia X un chiuso affine vale anche una versione relativa del Nullstellensatz. Definiamo:

- se $Y \subseteq X$ $\mathbf{I}_X(Y) \coloneqq \{\varphi \in \mathbb{K}[X] \mid \text{per ogni } y \in Y \ \varphi(y) = 0\}$;
- se $J \subseteq \mathbb{K}[X]$ ideale, $\mathbf{V}_X(J) \coloneqq \{x \in X \min \text{per ogni } \varphi \in J \ \varphi(x) = 0\}$.

Sia $\mathbb{K} = \overline{\mathbb{K}}$ ed $X \subseteq \mathbb{A}^n$ chiuso affine. Per ogni $J \subseteq \mathbb{K}[X]$ ideale si ha che $\mathbf{I}_X(\mathbf{V}_X(J)) = \sqrt{J}$.

Proposizione 4.11. Sia $\mathbb{K} = \overline{\mathbb{K}}$. Sia $X \subseteq \mathbb{A}^n$ chiuso affine. Allora X è irriducibile se e solo se $\mathbf{I}(X)$ è primo.

Dimostrazione. [**Har77**, Corollario 1.4, pag. 4]. □

Definizione 4.12. Uno spazio topologico X si dice *noetheriano* se rispetta la d.c.c. sui suoi sottoinsiemi chiusi.

Osservazione 4.13. $\mathbb{A}^n$ con la topologia di Zariski è noetheriano. Siano $Y_1 \supseteq Y_2 \supseteq \dots$ una discendente di chiusi. Allora $\mathbf{I}(Y_1) \subseteq \mathbf{I}(Y_2) \subseteq \dots$ è una catena ascendente di ideali in $\mathbb{K}[x_1, \dots, x_n]$ che è noetheriano. Allora $\mathbf{I}(Y_1) \subseteq \mathbf{I}(Y_2) \subseteq \dots$ è stazionaria e dunque lo è anche $Y_1 \supseteq Y_2 \supseteq \dots$.

Proposizione 4.14. Sia X uno spazio topologico noetheriano. Allora ogni sottoinsieme chiuso $Y \subseteq X$ può essere scritto come unione di chiusi irriducibili con la topologia di sottospazio, cioè esistono $Y_1, \dots, Y_n \subseteq Y$ chiusi irriducibili tali che $Y = Y_1 \cup \dots \cup Y_n$.

Se richiediamo che $Y_i \not\supseteq Y_j$ per $i \neq j$, allora gli Y_i sono univocamente determinati e sono detti le *componenti irriducibili* di Y.

Dimostrazione. Vedi [**Har77**, pag. 5, Proposizione 1.5]. □

Vogliamo adesso definire i chiusi di Zariski proiettivi. Sia $f \in \mathbb{K}[x_0, \dots, x_n]$, esso non può essere utilizzato per definire una funzione su $\mathbb{P}^n(\mathbb{K})$. Tuttavia, se f è omogeneo, è ben posto sulle coordinate omogenee dei punti di $\mathbb{P}^n(\mathbb{K})$ l'annullarsi di f; dunque poniamo $\mathbf{V}(f) = \{p \in \mathbb{P}^n(\mathbb{K}) \mid f(p) = 0\}$. Sia più in generale $T \subseteq \mathbb{K}[x_0 \dots, x_n]$ un insieme di elementi omogenei, allora poniamo

$$\mathbf{V}(T) = \{p \in \mathbb{P}^n(\mathbb{K}) \mid f(p) = 0 \text{ per ogni } f \in T\}.$$

Se $I \subseteq \mathbb{K}[x_0, \dots, x_n]$ è un ideale omogeneo definiamo $\mathbf{V}(I) = \mathbf{V}(T)$, con T l'insieme degli elementi omogenei di I. Dato che $\mathbb{K}[x_0, \dots, x_n]$ è noetheriano, si ha che ogni insieme T di elementi omogenei ha un sottoinsieme finito $f_1, \dots, f_r$ tale che $\mathbf{V}(T) = \mathbf{V}(f_1, \dots, f_r)$.

DEFINIZIONE 4.15. Un sottoinsieme $X \subseteq \mathbb{P}^n(\mathbb{K})$ si dice *insieme algebrico proiettivo* o *chiuso algebrico proiettivo* se esiste un sottoinsieme $T \subseteq \mathbb{K}[x_0, \ldots, x_n]$ di elementi omogenei tale che $X = \mathbf{V}(T)$.

PROPOSIZIONE 4.16. L'unione di due insiemi algebrici di $\mathbb{P}^n(\mathbb{K})$ è un insieme algebrico proiettivo di $\mathbb{P}^n(\mathbb{K})$. L'intersezione arbitraria di insiemi algebrici di $\mathbb{P}^n(\mathbb{K})$ è un insieme algebrico di $\mathbb{P}^n(\mathbb{K})$. Inoltre $\mathbb{P}^n(\mathbb{K})$ e $\varnothing$ sono insiemi algebrici proiettivi.

DIMOSTRAZIONE. Confronta Proposizione 4.3. □

Come per lo spazio affine n-dimensionale, stante la proposizione precedente, possiamo definire la *topologia di Zariski* su $\mathbb{P}^n(\mathbb{K})$ prendendo come aperti i complementari degli insiemi algebrici. Sia $X \subseteq \mathbb{P}^n(\mathbb{K})$, definiamo l'*ideale omogeneo* di X in $\mathbb{K}[x_0 \ldots, x_n]$, denotato come $\mathbf{I}(X)$, come l'ideale generato dall'insieme

$$\{f \in \mathbb{K}[x_0, \ldots, x_n] \mid f \text{ è omogeneo e } f(p) = 0 \text{ per ogni } p \in X\}.$$

DEFINIZIONE 4.17. Sia $X \subseteq \mathbb{P}^n(\mathbb{K})$ un insieme algebrico. Definiamo l'*anello delle coordinate omogeneo* di X come $\mathbb{K}[X] \coloneqq \mathbb{K}[x_0, \ldots, x_n]/\mathbf{I}(X)$.

Gli iperpiani standard $H_i = \{[x_0 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{K}) \mid x_i = 0\}$ definiti nel Capitolo 1 risultano facilmente essere chiusi della topologia di Zariski su $\mathbb{P}^n(\mathbb{K})$ $H_i = \mathbf{V}(x_i)$; dunque le carte affini standard $U_i = \{[x_0 \cdots : x_n] \in \mathbb{P}^n(\mathbb{K}) \mid x_i \neq 0\}$ sono aperti di tale topologia. Avevamo anche definito le mappe di immersione $j_i \colon \mathbb{A}^n \to U_i$.

DEFINIZIONE 4.18. Sia X un chiuso affine. Fissata un'immersione di $\mathbb{A}^n$ in $\mathbb{P}^n(\mathbb{K})$ tramite una carta affine, la *chiusura proiettiva* di X, indicata con $\overline{X}$, è la chiusura topologica di X in $\mathbb{P}^n(\mathbb{K})$ dotato della topologia di Zariski.

PROPOSIZIONE 4.19. Consideriamo l'immersione di $\mathbb{A}^n$ in U_0. Sia $X \subseteq \mathbb{A}^n$ un chiuso affine e sia $\mathbf{I}(X)$ l'ideale di X. Allora l'ideale generato dall'omogeneizzazione rispetto alla variabile x_0 di tutti i polinomi di $\mathbf{I}(X)$ è l'ideale omogeneo di $\overline{X}$.

DIMOSTRAZIONE. Vedi [**SKKT00**, Teorema pag. 40]. □

DEFINIZIONE 4.20. Una *varietà quasi-proiettiva* è l'intersezione tra un aperto ed un chiuso di $\mathbb{P}^n(\mathbb{K})$.

DEFINIZIONE 4.21. Siano $X \subseteq \mathbb{P}^n(\mathbb{K})$ ed $Y \subseteq \mathbb{P}^m(\mathbb{K})$ varietà quasi-proiettive. Una mappa $F \colon X \to Y$ si dice un *morfismo* se per ogni punto $p \in X$ esiste un intorno aperto $U \subseteq X$ di p e polinomi omogenei dello stesso grado $F_0, \ldots, F_m \in \mathbb{K}[x_0, \ldots, x_n]$ che non si annullano contemporaneamente su U tali che $F(x) = [F_0(x) : \cdots : F_m(x)]$ per ogni $x \in U$.

Si ottiene quindi la categoria delle varietà quasi-proiettiva.

DEFINIZIONE 4.22. Una *varietà affine* è una varietà quasi-proiettiva isomorfa ad un chiuso algebrico affine.

Una *varietà proiettiva* è una varietà quasi-proiettiva isomorfa ad un chiuso algebrico proiettivo.

OSSERVAZIONE 4.23. È possibile mostrare che se una varietà quasi-proiettiva è isomorfa ad un chiuso proiettivo allora è essa stessa un chiuso proiettivo (vedi [**Sha13**, pag. 49, pag. 57 Teorema 1.10]). Dunque la definizione di varietà proiettiva non amplia la famiglia dei chiusi proiettivi.

Nel caso affine invece abbiamo varietà che non sono essi stessi chiusi affini. Ad esempio $\mathbb{A}^1 \setminus \{0\}$ non è un chiuso affine ma è isomorfo (secondo la Definizione 4.21) a $\mathbf{V}(xy-1) \subseteq \mathbb{A}^2$: è dunque una varietà affine.

OSSERVAZIONE 4.24. Ogni varietà quasi-proiettiva, se dotata della topologia di Zariski come sottospazio dello spazio proiettivo, è uno spazio topologico noetheriano.

DEFINIZIONE 4.25. Sia X una varietà affine. Definiamo l'*anello delle coordinate* di X, denotato con $\mathbb{K}[X]$, come l'anello delle coordinate di un chiuso affine isomorfo ad X.

OSSERVAZIONE 4.26. La Definizione 4.25 di anello delle coordinate per una varietà affine è ben posta poiché si può mostrare che due chiusi affini sono isomorfi se e solo se sono isomorfi i loro anelli delle coordinate. Vedi [**SKKT00**, Teorema pag. 24-26].

DEFINIZIONE 4.27. Sia X una varietà quasi-proiettiva in $\mathbb{P}^n(\mathbb{K})$. Una funzione $f\colon X \to \mathbb{K}$ si dice *regolare in un punto* $p \in X$ se esistono $U \subseteq X$ intorno aperto di x e due polinomi $g, h \in \mathbb{K}[x_0, \ldots, x_n]$ omogenei dello stesso grado tali che per ogni $x \in U$ $h(x) \neq 0$ ed $f(x) = g(x)/h(x)$.

Una funzione $f\colon X \to \mathbb{K}$ si dice *regolare* su X se è regolare in ogni punto di X. Indichiamo con $\mathcal{O}(X)$ la $\mathbb{K}$-algebra delle funzioni regolari su X.

PROPOSIZIONE 4.28. Sia X una varietà quasi-proiettiva su $\mathbb{K}$. Se dotiamo $\mathbb{K}$ della topologia di Zariski, allora $f \in \mathcal{O}(X)$ è continua.

DIMOSTRAZIONE. Poiché in $\mathbb{K}$ i chiusi propri sono insiemi finiti di punti è sufficiente provare che per ogni $\lambda \in \mathbb{K}$ $f^{-1}(\lambda)$ è chiuso in X.

Per ipotesi di regolarità possiamo trovare un ricoprimento aperto $\{U_i\}_i$ e g_i, h_i polinomi omogenei di grado d_i tali che per ogni i vale che per ogni $x \in U_i$ $h_i(x) \neq 0$ ed $f(x) = g_i(x)/h_i(x)$. Allora per ogni i si ha che $f^{-1}(\lambda) \cap U_i = \mathbf{V}(g_i - \lambda h_i) \cap U_i$ chiuso in U_i. Dunque $f^{-1}(\lambda)$ è chiuso in X per ogni $\lambda \in \mathbb{K}$. □

PROPOSIZIONE 4.29. Sia X varietà affine. Sia $f \in \mathcal{O}(X)$ ed $x \in X$ allora esistono $p, q \in \mathbb{K}[X]$ tali che $p(x) \neq 0$ e per ogni $y \in X$ $p(y) \cdot f(y) = q(y)$.

DIMOSTRAZIONE. Senza perdere di generalità possiamo pensare $X \subseteq \mathbb{A}^n$.

Sia $U \subseteq X$ intorno aperto di x, abbiamo $g, h \in \mathbb{K}[x_1, \ldots, x_n]$ tali che per ogni $y \in U$ $h(y) \neq 0$ ed $f(y) = g(y)/h(y)$. Poiché $\mathbb{A}^n$ è noetheriano posso decomporre X in componenti irriducibili $X = X_1 \cup \ldots \cup X_s \cup X_{s+1} \cup \ldots \cup X_k$ tali che per ogni $j \leq s$ $X_j \cap U \neq \varnothing$ e per ogni $j \geq s+1$ $X_j \cap U = \varnothing$.

Su U vale che $hf - g = 0$. Si noti che $g, h \in \mathcal{O}(X)$, quindi $hf - g \in \mathcal{O}(X)$ ed è dunque continua. Osserviamo che poiché $hf - g = 0$ su U, allora per la Proposizione 4.5 $hf - g = 0$ su X_j per ogni $j \leq s$; dunque su $X_1 \cup \ldots \cup X_s$.

Poiché $x \in U$ e $U \cap (X_{s+1} \cup \ldots \cup X_k) = \varnothing$ e $X_{s+1} \cup \ldots \cup X_k$ è un chiuso, esiste $\alpha \in \mathbb{K}[x_1, \ldots, x_n]$ tale che $\alpha \equiv 0$ su $X_{s+1} \cup \ldots \cup X_k$ e $\alpha(x) \neq 0$. Posti $p = \alpha h$ e $q = \alpha g$ si ha la tesi. □

COROLLARIO 4.30. Sia $X \subseteq \mathbb{A}^n$ chiuso affine e sia $f \in \mathcal{O}(X)$. Per ogni $x \in X$ esiste $h_x \in \mathbb{K}[X]$ tale che $h_x(x) \neq 0$ e $h_x f \in \mathbb{K}[X]$.

TEOREMA 4.31. Sia $X \subseteq \mathbb{A}^n$ chiuso affine. Allora $\mathbb{K}[X] = \mathcal{O}(X)$.

DIMOSTRAZIONE. L'inclusione $\mathbb{K}[X] \subseteq \mathcal{O}(X)$ è ovvia. Sia dunque $f \in \mathcal{O}(X)$. Per il Corollario 4.30 per ogni $x \in X$ esiste $h_x \in \mathbb{K}[X]$ tale che $h_x(x) \neq 0$ ed $h_x f \in \mathbb{K}[X]$.

Sia allora $J = (h_x)_{x \in X}$ l'ideale generato in $\mathbb{K}[X]$. Abbiamo che $\mathbf{V}_X(J) = \varnothing$ e dunque per l'Osservazione 4.10 abbiamo che $1 \in J$. Allora $1 = \sum_{i=1}^t \beta_i h_{x_i}$ con $h_{x_i} \in J$ e $\beta_i \in \mathbb{K}[X]$. Allora $f = 1 \cdot f = \sum_{i=1}^t \beta_i (h_{x_i} f)$; dunque $f \in \mathbb{K}[X]$. □

DEFINIZIONE 4.32. Sia $X \subseteq \mathbb{A}^n$ chiuso affine ed $f \in \mathbb{K}[X]$. Allora $X \setminus \mathbf{V}(f) : X_f$ si dice *aperto principale* ed è un aperto affine di X.

LEMMA 4.33. Sia $X \subseteq \mathbb{A}^n$ ed $f \in \mathbb{K}[X]$. Allora l'aperto principale X_f è una varietà affine con anello delle coordinate $\mathbb{K}[X_f] \cong \mathbb{K}[X]_f$.

DIMOSTRAZIONE. Vedi [**SKKT00**, pag. 52-53]. □

COROLLARIO 4.34. Sia X varietà quasi-proiettiva. Allora gli aperti affini sono una base per la topologia di Zariski su X.

DIMOSTRAZIONE. Vedi [**SKKT00**, pag. 54] □

DEFINIZIONE 4.35. Siano X una varietà quasi-proiettiva ed $x \in X$ un punto. Definiamo l'*anello dei germi delle funzioni regolari attorno ad* x, denotato con $\mathcal{O}_{X,x}$, come l'anello delle coppie ordinate (U, f) dove $U \subseteq X$ è un intorno aperto di x ed $f \in \mathcal{O}(U)$ modulo la relazione di equivalenza data da

$(U, f) \sim (V, g)$ se e solo se esiste $W \subseteq U \cap V$ aperto tale che $f_{|W} \equiv g_{|W}$ ed $x \in W$.

OSSERVAZIONE 4.36. Sia X varietà quasi-proiettiva ed $x \in X$, $\mathcal{O}_{X,x}$ è un anello locale con ideale massimale $\mathfrak{m}_x \coloneqq \{[(U, f)] \in \mathcal{O}_{X,x} \mid f(x) = 0\}$.

OSSERVAZIONE 4.37. Sia X varietà quasi-proiettiva ed $U \subseteq X$ aperto, allora per ogni $x \in U$ si ha un isomorfismo naturale $\mathcal{O}_{X,x} \cong \mathcal{O}_{U,x}$.

TEOREMA 4.38. Siano $\mathbb{K} = \overline{\mathbb{K}}$, X varietà affine ed $x \in X$. Posto $\mathscr{M} \coloneqq \{f \in \mathcal{O}(X) \mid f(x) = 0\} \in \operatorname{Specm}(\mathcal{O}(X))$ si ha che $\mathcal{O}_{X,x} \cong \mathcal{O}(X)_{\mathscr{M}}$.

DIMOSTRAZIONE. Sia $j \colon \mathcal{O}(X) \to \mathcal{O}_{X,x}$ l'omomorfismo naturale che manda una funzione regolare nel suo germe. Osserviamo che per ogni $f \in \mathcal{O}(X) \setminus \mathscr{M}$, $[(X, f)]$ è invertibile in $\mathcal{O}_{X,x}$. Questo poiché $f(x) \neq 0$ e dunque è ben definita e regolare $1/f$ in un intorno $U \subseteq X$ di x ed è l'inversa di $[(X, f)] = [(U, f_{|U})]$. Allora per la proprietà universale delle localizzazioni 3.5 esiste ed è unico $\tilde{j} \colon \mathcal{O}(X)_{\mathscr{M}} \to \mathcal{O}_{X,x}$ tale che, posto $f \colon \mathcal{O}(X) \to \mathcal{O}(X)_{\mathscr{M}}$ l'omomorfismo di localizzazione, $\tilde{j} \circ f = j$.

Vogliamo mostrare che $\tilde{j}$ è un isomorfismo. Sia $f/g \in \ker \tilde{j}$, allora $j(f) = 0$. Esiste dunque un introno $U \subseteq X$ aperto di x tale per cui $f_{|U} \equiv 0$. Sia $X = X_1 \cup \ldots X_s \cup X_{s+1} \cup \ldots X_k$ scomposizione in componenti irriducibili per X tale che $p \in X_j$ per ogni $j \leq s$ e $p \notin X_j$ per ogni $j \geq s + 1$ si ha, come nel Corollario 4.30, che $f_{|X_j} \equiv 0$ per ogni $j \leq s$. Poiché $p \notin X_{s+1} \cup \ldots \cup X_k$ si ha per il Nullstellensatz relativo 4.10 che $\mathscr{M} \not\supseteq \mathbf{I}_X(X_{s+1} \cup \ldots \cup X_k)$. Allora esiste $t \in \mathbf{I}_X(X_{s+1} \cup \ldots \cup X_k) \setminus \mathscr{M}$ tale che $t_{|X_{s+1} \cup \ldots \cup X_k} \equiv 0$. Allora $ft \equiv 0$ su X e dunque $f = 0$ in $\mathcal{O}(X)_{\mathscr{M}}$.

Sia $f = [(U, \varphi)] \in \mathcal{O}_{X,x}$. Poiché gli aperti principali sono una base per la topologia di X troviamo $b \in \mathbb{K}[X]$ tale che $x \in X_b \subseteq U$, allora $\varphi_{|X_b} \in \mathcal{O}(X_b) \cong \mathbb{K}[X]_b$ e dunque esiste $a \in \mathbb{K}[X]$ tale che $\varphi_{|X_b} = a/b^k$ su X_b. Allora $f = [(X_b, a/b^k)]$ e $a/b^k \in \mathcal{O}(X)_{\mathscr{M}}$ perché $b(x) \neq 0$. □

CAPITOLO 5

Teorema di Bézout

5.1. Risultante e molteplicità di intersezione

Dato un dominio a fattorizzazione unica (UFD) D vogliamo determinare delle condizioni tramite le quali stabilire se due polinomi in $D[x]$ hanno dei fattori comuni non costanti.

LEMMA 5.1. Sia D un UFD e siano $f, g \in D[x]$ due polinomi di gradi rispettivamente n ed m. Allora f e g possiedono un fattore comune non costante se e solo se esistono $a, b \in D[x]$ tali che $\deg a < \deg f$, $\deg b < \deg g$ e $bf = ag$.

DIMOSTRAZIONE. Supponiamo che f e g abbiano un fattore in comune non costante h, allora abbiamo che $f = ah$ e $g = bh$ con $\deg a < \deg f$ e $\deg b < \deg g$. Pertanto $bf = ag$. Viceversa supponiamo che esistano $a, b \in D[x]$ come nell'enunciato. Allora dall'uguaglianza $bf = ga$, poiché $\deg a < \deg f$ uno dei fattori non costanti di g deve dividere f e dunque f e g hanno un fattore in comune non costante. □

Il lemma precedente fornisce sì una condizione necessaria e sufficiente per stabilire se due polinomi abbiano un fattore comune non costante, tuttavia tale condizione non è facilmente applicabile. Il lemma precedente sarà tuttavia il risultato cardine che legherà la costruzione che verrà a seguire con il nostro obiettivo.

DEFINIZIONE 5.2. Sia A un anello e siano $f, g \in A[x]$ polinomi di gradi rispettivamente n ed m. Supponiamo f e g della forma seguente:

$$f = a_n + a_{n-1}x + \ldots + a_0x^n;$$
$$g = b_m + b_{m-1}x + \ldots + b_0x^m$$

con $a_0, \ldots, a_n, b_0, \ldots, b_m \in A$ e $a_0, b_0 \neq 0$. Costruiamo allora la *matrice di Sylvester* dei polinomi f e g (di tipo (n, m))

$$Syl_{n,m}(f,g) \coloneqq \begin{pmatrix} a_n & a_{n-1} & \cdots & \cdots & a_0 & 0 & \cdots & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & \cdots & a_0 & 0 \\ 0 & \cdots & \cdots & 0 & a_n & a_{n-1} & \cdots & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & \cdots & b_0 & 0 & & \cdots & 0 \\ 0 & b_m & b_{m-1} & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & b_m & b_{m-1} & \cdots & \cdots & b_0 & 0 \\ 0 & \cdots & \cdots & 0 & b_m & b_{m-1} & \cdots & \cdots & b_0 \end{pmatrix} \in \mathrm{M}_{n+m}(A),$$

con i coefficienti di f sulle prime m righe e quelli di g nelle successive n. Definiamo poi il *risultante di tipo* (n, m) dei polinomi f e g come $\mathrm{Res}_{n,m}(f, g) \coloneqq \det(Syl_{n,m}(f, g))$.

OSSERVAZIONE 5.3. Nella definizione della matrice di Sylvester e del risultante la specifica del tipo (n, m) non è superflua. Difatti f e g possono essere considerati anche come polinomi di gradi rispettivamente maggiori uguali ad n ed m con coefficienti nulli; consideriamo il caso in cui questi sono $n' > n$ ed $m' > m$. In questo caso la matrice di Sylvester di tipo (n', m') sarà di dimensione $n' \times m'$ ed il corrispondente risultante sarà certamente nullo.

NOTA 5.4. Da qui in poi $\mathrm{Res}(f,g)$ e $Syl(f,g)$ staranno ad indicare risultante e matrice di Sylvester di tipo (n,m) con $n = \deg f$ ed $m = \deg g$.

Come il risultante sia collegato alla fattorizzazione di due polinomi è chiarito dal seguente risultato.

PROPOSIZIONE 5.5. Sia D un UFD e siano $f, g \in D[x]$ come sopra. Allora f e g hanno un fattore comune non costante se e solo se $\mathrm{Res}(f,g) = 0$.

DIMOSTRAZIONE. ($\Rightarrow$) Supponiamo che f e g abbiano un fattore comune non costante. Allora per il lemma precedente esistono $a, b \in D[x]$ tali che $bf = ag$ con $\deg a < \deg f, \deg b < \deg g$. Tali a e b sono della forma

$$\begin{aligned} a &= -\alpha_{n-1} - \alpha_{n-2}x - \ldots - \alpha_0 x^{n-1}; \\ b &= \beta_{m-1} + \beta_{m-2}x + \ldots + \beta_0 x^{m-1} \end{aligned} \tag{6}$$

con $\alpha_j, \beta_k \neq 0$ per qualche j e k. L'identità $bf = ag$ allora termine a termine si legge come

$$\begin{aligned} a_n\beta_{m-1} &= -b_m\alpha_{n-1}; \\ a_n\beta_{m-2} + a_{n-1}\beta_{m-1} &= -b_m\alpha_{n-2} - b_{m-1}\alpha_{m-1}; \\ &\vdots \\ a_0\beta_0 &= -b_0\alpha_0. \end{aligned} \tag{7}$$

Tali definiscono l'esistenza di una soluzione non banale del sistema lineare con matrice associata la trasposta della matrice $Syl_{n,m}(f,g)$; dunque l'annullarsi del risultante.

($\Leftarrow$) Supponiamo che $\mathrm{Res}(f,g) = 0$. Allora il sistema lineare con matrice associata $Syl(f,g)^T$ ha una soluzione nelle incognite $\beta_{m-1}, \ldots, \beta_0, \alpha_{n-1}, \ldots, \alpha_0$ come in (7). Segue dunque che i polinomi a e b con coefficienti la soluzione trovata costruiti come in (6) soddisfano l'identità $bf = ag$. Ancora per il Lemma 5.1 i polinomi f e g hanno un fattore in comune non costante. □

Nel caso dunque di un campo algebricamente chiuso $\mathbb{K}$, abbiamo trovato una facile condizione necessaria e sufficiente affinché due polinomi $f, g \in \mathbb{K}[x]$ abbiano una radice in comune. Supponiamo adesso di prendere due polinomi $F, G \in A[x_1, \ldots, x_n]$, per $n \geq 2$. Questi possono essere considerati come polinomi in una sola delle variabili, senza perdere di generalità consideriamo x_n, i cui coefficienti sono polinomi nelle restanti $x_1, \ldots, x_{n-1}$. Ponendo rispettivamente n ed m i loro gradi rispetto la variabile x_n, scriviamo dunque

$$\begin{aligned} F &= A_n + A_{n-1}x_n + \ldots + A_0 x_n^n; \\ G &= B_m + B_{m-1}x_n + \ldots + B_0 x_n^m \end{aligned}$$

con $A_n, \ldots, A_0, B_m, \ldots, B_0 \in A[x_1, \ldots, x_{n-1}]$ con $A_0, B_0 \neq 0$. Possiamo dunque definire il risultante dei due polinomi.

DEFINIZIONE 5.6. Sia A anello e siano $F, G \in A[x_1, \ldots, x_n]$ polinomi come sopra. Poniamo il *risultante di F e G rispetto ad x_n*, indicato con $\mathrm{Res}(F, G; x_n)$, come il determinante della *matrice di Sylvester di F e G rispetto x_n*

$$Syl(F,G;x_n) \coloneqq \begin{pmatrix} A_n & A_{n-1} & \cdots & \cdots & A_0 & 0 & \cdots & \cdots & 0 \\ 0 & A_n & A_{n-1} & \cdots & \cdots & A_0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & A_n & A_{n-1} & \cdots & \cdots & A_0 & 0 \\ 0 & \cdots & \cdots & 0 & A_n & A_{n-1} & \cdots & \cdots & A_0 \\ B_m & B_{m-1} & \cdots & \cdots & B_0 & 0 & & \cdots & 0 \\ 0 & B_m & B_{m-1} & \cdots & \cdots & B_0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & B_m & B_{m-1} & \cdots & \cdots & B_0 & 0 \\ 0 & \cdots & \cdots & 0 & B_m & B_{m-1} & \cdots & \cdots & B_0 \end{pmatrix}$$

.

OSSERVAZIONE 5.7. Dati $F, G \in A[x_1, \ldots, x_n]$ come sopra. Osserviamo che in questo caso i coefficienti della matrice di Sylvester di F e G sono polinomi nelle $x_1, \ldots, x_{n-1}$ e pertanto $\mathrm{Res}(F, G; x_n) \in A[x_1, \ldots, x_{n-1}]$.

PROPOSIZIONE 5.8. Sia A un anello e siano $F, G \in A[x_1, \ldots, x_n]$, omogenei rispettivamente di grado n ed m,

$$F = A_n + A_{n-1}x_n + \ldots + A_0 x_n^n;$$
$$G = B_m + B_{m-1}x_n + \ldots + B_0 x_n^m$$

con $A_n, \ldots, A_0, B_m, \ldots, B_0 \in D[x_1, \ldots, x_{n-1}]$ omogenei nelle $x_1, \ldots, x_{n-1}$ di gradi $\deg A_k = k$ e $\deg B_j = j$ ed $A_0, B_0 \neq 0$. Allora $\mathrm{Res}(F, G; x_n)$ è omogeneo di grado nm.

DIMOSTRAZIONE. Poniamo $x = (x_1, \ldots, x_{n-1})$ ed abbiamo dunque per l'omogeneità degli A_k e dei B_j

$$\mathrm{Res}(F, G; x_n)(tx) =$$
$$= \det \begin{pmatrix} t^n A_n & t^{n-1}A_{n-1} & \cdots & A_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & t^n A_n & t^{n-1}A_{n-1} & \cdots & A_0 & 0 \\ 0 & \cdots & 0 & t^n A_n & t^{n-1}A_{n-1} & \cdots & A_0 \\ t^m B_m & t^{m-1}B_{m-1} & \cdots & B_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & t^m B_m & t^{m-1}B_{m-1} & \cdots & B_0 & 0 \\ 0 & \cdots & 0 & t^m B_m & t^{m-1}B_{m-1} & \cdots & B_0 \end{pmatrix}.$$

Moltiplicando allora la i-esima riga del blocco superiore per t^{m-i+1} e la j-esima riga del blocco inferiore per t^{n-j+1} otteniamo, sviluppando poi per multilinearità del determinante sulle colonne, $t^p \mathrm{Res}(F, G; x_n)(tx) = t^q \mathrm{Res}(F, G; x_n)(x)$ dove $p = m + (m-1) + \ldots + 1 + n + (n-1) + \ldots + 1$ e $q = (n+m) + (n+m-1) + \ldots + 1$. Otteniamo allora $\mathrm{Res}(F, G; x_n)(tx) = t^{q-p} \mathrm{Res}(F, G; x_n)(x) = t^{nm} \mathrm{Res}(F, G; x_n)$. Dunque $\mathrm{Res}(F, G; x_n)$ è omogeneo di grado nm. □

Anche nel caso di polinomi in più variabili il risultante fornisce una condizione necessaria e sufficiente affinché questi abbiano un fattore comune.

PROPOSIZIONE 5.9. Sia D un UFD e siano $F, G \in D[x_1, \ldots, x_n]$ omogenei di gradi rispettivamente n ed m. Supponiamo che $F(0, \ldots, 0, 1), G(0, \ldots, 0, 1) \neq 0$. Allora F e G hanno un fattore comune omogeneo non costante se e solo se $\mathrm{Res}(F, G; x_n) = 0$.

DIMOSTRAZIONE. Dato che D è un UFD allora anche $D[x_1, \ldots, x_{n-1}]$ è un UFD. Per la proposizione precedente allora abbiamo che F e G hanno un fattore in comune visti come polinomi in x_n a coefficienti in $D[x_1, \ldots, x_{n-1}]$, ma ciò è equivalente al fatto che F e G abbiano un fattore comune come polinomi nelle $x_1, \ldots, x_n$ a coefficienti in D. Poiché fattori di polinomi omogenei sono omogenei la prova si chiude. □

OSSERVAZIONE 5.10. Siano $F, G \in A[x_1, \ldots, x_n]$ polinomi omogenei e sia $c = (c_1, \ldots, c_{n-1}) \in A^{n-1}$ tale che $F(c, 1), G(c, 1) \neq 0$. Abbiamo osservato come $\mathrm{Res}(F, G; x_n)$ sia un polinomio nelle $x_1, \ldots, x_{n-1}$. Abbiamo pertanto la cosiddetta *proprietà di specializzazione* del risultante $\mathrm{Res}(F, G; x_n)(c) = \mathrm{Res}(F(c, x_n), G(c, x_n))$.

Nel capitolo 1 abbiamo visto come definire la molteplicità di intersezione di una ipersuperficie con una retta. Nel caso di $\mathbb{P}^2(\mathbb{K})$ questo equivale all'intersezione di due curve algebriche piane proiettive nel caso particolare in cui una di queste due sia una retta: avendo definito il risultante possiamo adesso considerare il caso generale tra due curve di qualsivoglia grado.

DEFINIZIONE 5.11. Siano $\mathcal{C}$ e $\mathcal{D}$ due curve algebriche in $\mathbb{P}^2(\mathbb{K})$ definite dai polinomi F e G e sia $p = [p_0 : p_1 : p_2] \in \mathcal{C} \cap \mathcal{D}$. Scegliamo un sistema di coordinate omogenee per il quale $[0 : 0 : 1] \notin \mathcal{C} \cup \mathcal{D}$ e che p sia l'unico punto di $\mathcal{C} \cap \mathcal{D}$ sulla retta congiungente p e $[0 : 0 : 1]$. Definiamo la *molteplicità di intersezione di $\mathcal{C}$ e $\mathcal{D}$ in p* come la molteplicità di $[p_0 : p_1]$ come radice omogenea di $\mathrm{Res}(F, G; x_2)$ e la denotiamo con $I(\mathcal{C}, \mathcal{D}, p)$.

OSSERVAZIONE 5.12. 1) Se $p \notin \mathcal{C} \cap \mathcal{D}$ poniamo $I(\mathcal{C}, \mathcal{D}, p) = 0$.
2) Se $\mathcal{C}$ e $\mathcal{D}$ hanno una componente comune allora dallo studio del risultante sappiamo che $Res(F, G; x_2) = 0$ e dunque poniamo $I(\mathcal{C}, \mathcal{D}, p) = \infty$ nei punti p che appartengono a tale componente.

La Definizione 5.11 di molteplicità di intersezione tra curve piane proiettive è data prendendo un opportuno sistema di coordinate omogenee. Nonostante ciò questa è una buona definizione, come verrà dimostrato nella Sezione 5.2.

OSSERVAZIONE 5.13. La molteplicità di intersezione può essere calcolata anche in carte locali. Supponiamo $p \in U_o$ e consideriamo adesso f e g i polinomi ottenuti deomogeneizzando F e G rispetto alla variabile x_0. Avendo supposto che $[0 : 0 : 1] \notin \mathcal{C} \cup \mathcal{D}$, ciò si traduce nel fatto che f e g hanno lo stesso grado di F e G. Per quanto visto sulle proprietà di specializzazione del risultante si ha che $Res(F, G; x_2)(1, x_1) = Res(f, g; x_2)(x_1)$ e dunque la molteplicità di intersezione di due curve un punto p può essere calcolata in coordinate locali.

5.2. Teorema di Bézout

Vogliamo adesso utilizzare le teoria sviluppata dell'algebra commutativa e gli invarianti della geometria algebrica per mostrare la buona positura della definizione di molteplicità di intersezione e che questa è invariante per cambi di coordinate lineari di $\mathbb{P}^2(\mathbb{K})$.

PROPOSIZIONE 5.14. Siano $\mathbb{K}$ un campo, $(A, \mathfrak{m})$ anello locale, A una $\mathbb{K}$-algebra. Sia M un A-modulo. Supponiamo che $A/\mathfrak{m}$ sia un'estensione di campo finita di $\mathbb{K}$. Allora M ha lunghezza finita come A-modulo se e solo se M ha dimensione finita come $\mathbb{K}$-spazio vettoriale. Se tali condizioni sono verificate allora $\dim_{\mathbb{K}} M = [A/\mathfrak{m} : \mathbb{K}] \cdot \mathrm{length}_A M$.

DIMOSTRAZIONE. ($\Rightarrow$) Sia $M = M_0 \supsetneq M_1 \supsetneq \ldots \supsetneq M_r = 0$ una serie di composizione per M si ha che $M_{i-1}/M_i \cong A/\mathfrak{m}$ per ogni $1 \leq i \leq r$ per la Proposizione 3.35. Allora $\dim_{\mathbb{K}} M = \sum_{i=1}^{r} \dim_{\mathbb{K}} M_{i-1}/M_i = \mathrm{length}_A M \cdot \dim_{\mathbb{K}} A/\mathfrak{m} = [A/\mathfrak{m} : \mathbb{K}] \cdot \mathrm{length}_A M$.
($\Leftarrow$) Se M è un $\mathbb{K}$-spazio vettoriale di dimensione finita allora ha anche lunghezza finita per la proposizione 3.40. Dato che gli A-sottomoduli di M sono $\mathbb{K}$-sottospazi vettoriali, M ha lunghezza finita anche come A-modulo. □

Dobbiamo adesso introdurre una nuova famiglia di anelli ed elencare brevemente alcune loro caratteristiche.

DEFINIZIONE 5.15. Sia $\mathbb{K}$ un campo. Una *valutazione discreta* su $\mathbb{K}$ è un'applicazione suriettiva $\nu\colon \mathbb{K}^* \to \mathbb{Z}$ tale che
1) $\nu(xy) = \nu(x) + \nu(y)$, ossia è un omomorfismo suriettivo di gruppi[1];
2) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$.
$\{x \in \mathbb{K}^* \mid \nu(x) \geq 0\} \cup \{0\}$ è un anello, chiamato l'*anello di valutazione* di ν.

OSSERVAZIONE 5.16. Talvolta conviene estendere la valutazione a tutto $\mathbb{K}$ come $\nu(0) = \infty$.

ESEMPIO 5.17. Gli esempi chiave sono i seguenti.

[1] In questo caso da $\nu(xy) = \nu(x)+\nu(y)$ segue che $\nu(1) = 0$. Questo poiché $\nu(1) = \nu(1 \cdot 1) = \nu(1)+\nu(1) = 2\nu(1)$.

1) Consideriamo $\mathbb{K} = \mathbb{Q}$. Fissato un numero primo $p \in \mathbb{Z}$ arbitrario ogni elemento $x \in \mathbf{Q}$ può essere scritto come $x = (p^n a)/b$ con $a, b \in \mathbb{Z}$ primi rispetto a p e $b \neq 0$. Definiamo dunque $\nu_p(x) = n$. L'anello di valutazione di ν è dunque $\mathbb{Z}_{(p)}$.
2) Sia adesso $\mathbb{K}(x)$ il campo delle funzioni razionali a coefficienti in $\mathbb{K}$ in una indeterminata. Prendiamo adesso un polinomio irriducibile $f \in \mathbb{K}[x]$. Si ha che ogni elemento $a/b \in \mathbb{K}(x)$ può essere scritto come $f^k g/h$ con $f \nmid g, h$ e $k \in \mathbb{Z}$: poniamo dunque $\nu_f(f^k g/h) = k$. Abbiamo in questo caso che l'anello di valutazione di ν_f è $\mathbb{K}[x]_{(f)}$. Caso particolare di questo è $f(x) = x - \lambda$ con $\lambda \in \mathbb{K}$: in questo caso ν_λ rappresenta la molteplicità di λ come zero/polo di un elemento $\varphi \in \mathbb{K}(x)$.

Definizione 5.18. Un dominio A prende il nome di *anello di valutazione discreta* (DVR) se esiste una valutazione discreta ν del suo campo delle frazioni $\mathrm{Frac}(A)$ tale che A è l'anello di valutazione di ν.

Proposizione 5.19. Sia A un DVR, allora A è locale con unico ideale massimale $\mathfrak{m} = \{x \in \mathrm{Frac}(A) \mid \nu(x) > 0\}$.

Dimostrazione. Vedi [**AM16**, pag. 101, Proposizione 5.18]. □

Teorema 5.20. Sia $(A, \mathfrak{m})$ un dominio noetheriano locale. Allora le seguenti condizioni sono equivalenti:

i) A è un dominio a valutazione discreta;
ii) $\mathfrak{m}$ è un ideale principale e non è zero;
iii) A è un PID e non è un campo;
iv) esiste $t \in A$, detto *uniformizzante*, tale che tutti gli ideali non nulli di A appartengono alla catena $A \supsetneq (t) \supsetneq (t^2) \supsetneq \ldots$;
v) esiste $t \in A \setminus \{0\}$, $t \notin A^*$ tale che per ogni $a \in A$ esiste $u \in A^*$ ed $m \in \mathbf{N}$ tale che $a = ut^m$.

Dimostrazione. Vedi [**AM16**, pag. 142, Proposizione 9.2]. □

Proposizione 5.21. Sia A un DVR e sia $\nu \colon A \to \mathbb{N} \cup \{\infty\}$ la sua valutazione. Per ogni $a \in A$ si ha che $\mathrm{length}_A A/(a) = \nu(a)$.

Dimostrazione. Sia $t \in A$ uniformizzante di A e sia dunque $\mathfrak{m} = At$ l'ideale massimale di A. Dato che per ogni $a \in A$ esiste $u \in A^*$ ed $n \in \mathbf{N}$ tale che $a = ut^n$ si ha che $\nu(a) = n$ e $(a) = \mathfrak{m}^n$. Abbiamo pertanto che

$$A/(a) \supseteq \mathfrak{m}/\mathfrak{m}^n \supseteq \mathfrak{m}^2/\mathfrak{m}^n \supseteq \ldots \supseteq \mathfrak{m}^{n-1}/\mathfrak{m}^n \supseteq 0$$

è una serie di composizione per $A/(a)$ dato che per ogni i si ha $(\mathfrak{m}^i/\mathfrak{m}^n)/(\mathfrak{m}^{i+1}/\mathfrak{m}^n) \cong \mathfrak{m}^i/\mathfrak{m}^{i+1}$ per i teoremi di omomorfismo e $\mathfrak{m}^i/\mathfrak{m}^{i+1} \cong A/\mathfrak{m}$ tramite la mappa $a+\mathfrak{m} \mapsto at^i+\mathfrak{m}^i$. Dunque $\mathrm{length}_A A/(a) = n = \nu(a)$. □

Per la prova del prossimo risultato è necessario il seguente lemma.

Lemma 5.22 (Forma normale di Smith). Sia A un PID e sia $P \in \mathrm{M}_{n,m}(A)$ di rango $r \geq 0$. Allora esistono $H \in \mathrm{GL}_n(A)$ e $K \in \mathrm{GL}_m(A)$ tali che $HPK = \left(\begin{smallmatrix} D_r & 0 \\ 0 & 0 \end{smallmatrix}\right)$, dove $D_r \in \mathrm{M}_r(A)$ diagonale con elementi $d_1, \ldots, d_r \in A \setminus \{0\}$.

Dimostrazione. Vedi [**Hun74**, pag. 339, Proposizione 2.11]. □

Proposizione 5.23. Sia A un DVR con valutazione ν. Sia M un A-modulo libero di rango finito e sia $\Phi \colon M \to M$ un omomorfismo di A-moduli. Allora $\mathrm{length}_A \operatorname{coker} \Phi = \mathrm{length}_A A/(\det(\Phi))$.

Dimostrazione. Sia $n = \mathrm{rank}_A M$, allora Φ è rappresentata da una matrice $n \times n$ a coefficienti in A. Poiché A è un PID per il Teorema 5.20 allora per la forma normale di Smith (Lemma 5.22) esistono P, $Q \in \mathrm{GL}_n(A)$ tali che $P\Phi Q$ è una matrice diagonale D con

elementi diagonali $a_1, \dots, a_n$. Si ha dunque che $\operatorname{coker} \Phi \cong \operatorname{coker} D = A/(a_1) \oplus \dots \oplus A/(a_n)$. Sia ν la valutazione discreta di A, allora per la Proposizione 5.21

$$\begin{aligned}\operatorname{length}_A \operatorname{coker} \Phi &= \sum_{i=1}^{n} \operatorname{length}_A A/(a_i) = \sum_{i=1}^{n} \nu(a_i) = \\ &= \nu(a_1 \cdots a_n) = \nu(\det \Phi) = \operatorname{length}_A A/(\det \Phi).\end{aligned}$$

□

Osservazione 5.24. Sia A un anello, consideriamo l'anello dei polinomi $A[x]$. Siano $f,\ g \in A[x]$ di gradi rispettivamente n ed m. Tali possono essere visti come elementi di $A[x]_{\leq n+m-1}$, che è un A-modulo libero di rango $n+m$ con base $\{x^{n+m-1}, \dots, x, 1\}$. Allora $\bigwedge_A^{n+m} A[x]_{\leq n+m-1}$ è libero di rango 1 generato da $x^{n+m-1} \wedge \dots \wedge x \wedge 1$ stante la Proposizione 3.60. In $\bigwedge_A A[x]_{\leq n+m-1}$ si ha pertanto che

$$x^{m-1} f \wedge \dots \wedge xf \wedge f \wedge x^{n-1} g \wedge \dots \wedge xg \wedge g = Res(f,g) x^{n+m-1} \wedge \dots \wedge x \wedge 1.$$

Difatti osserviamo che $x^i f = a_0 x^{i+n} + \dots + a_{n-1} x^{i+1} + a_n x^i$ e $x^j g = b_0 x^{j+m} + \dots + b_{m-1} x^{j+1} + b_m x^j$. Sfruttando le proprietà di multilinearità ed alternanza della potenza esterna possiamo sviluppare il membro di sinistra ed ottenere dunque il membro di destra.

Proposizione 5.25. Sia A un anello e siano $f,\ g \in A[x]$ di gradi rispettivamente n ed m. Supponiamo il coefficiente direttore di f sia invertibile in A. Allora $A[x]/(f)$ è un A-modulo libero di rango n e $\operatorname{Res}(f,g)$ è il determinante dell'omomorfismo di A-moduli $A[x]/(f) \xrightarrow{\cdot g} A[x]/(f)$ dato dalla moltiplicazione per g a meno di associati.

Dimostrazione. Poniamo $f = a_0 x^n + \dots + a_n$. Consideriamo la base di $A[x]/(f)$ come A-modulo data da $\mathcal{B} = \{x^{n-1}, \dots, x, 1\}$. Dato che $a_0 \in A^*$ è invertibile è possibile la divisione euclidea e dunque $g x^i = q_i f + r_i$ per ogni $0 \leq i \leq n-1$ con $r_i = r_{i,0} x^{n-1} + \dots r_{i,n-1} x + r_{i,n-1}$ con $r_{i,j} \in A$. Abbiamo allora che il nostro omomorfismo rispetto alla base $\mathcal{B}$ in arrivo e partenza risulta essere

$$M = \begin{pmatrix} r_{n-1,n-1} & \dots & r_{1,n-1} & r_{0,n-1} \\ r_{n-1,n-2} & \dots & r_{1,n-2} & r_{0,n-2} \\ \vdots & & & \vdots \\ r_{n-1,1} & \dots & r_{1,1} & r_{0,1} \\ r_{n-1,0} & \dots & r_{1,0} & r_{0,0} \end{pmatrix}.$$

Per l'osservazione precedente abbiamo perciò in $\bigwedge_A^{n+m} A[x]_{\leq n+m-1}$

$$\begin{aligned}\operatorname{Res}(f,g) x^{n+m-1} \wedge \dots \wedge x \wedge 1 &= x^{m-1} f \wedge \dots \wedge yf \wedge f \wedge x^{n-1} g \wedge \dots \wedge xg \wedge g = \\ &= x^{m-1} f \wedge \dots \wedge yf \wedge f \wedge (q_{n-1} f + r_{n-1}) \wedge \dots \wedge (q_1 f + r_1) \wedge (q_0 f + r_0) = \\ &= x^{m-1} f \wedge \dots \wedge yf \wedge f \wedge r_{n-1} \wedge \dots \wedge r_1 \wedge r_0 = \\ &= x^{m-1} f \wedge \dots \wedge yf \wedge f \wedge \det(M) x^{n-1} \wedge \dots \wedge x \wedge 1 = \\ &= \det(M) x^{m-1} f \wedge \dots \wedge yf \wedge f \wedge x^{n-1} \wedge \dots \wedge x \wedge 1 = \\ &= \det(M) \det \begin{pmatrix} a_0 & a_1 & \dots & a_n & & \\ & \ddots & & & \ddots & \\ & & a_0 & a_1 & \dots & a_n \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix} x^{n+m-1} \wedge \dots \wedge x \wedge 1 = \\ &= \det(M) a_0^m x^{n+m-1} \wedge \dots \wedge x \wedge 1.\end{aligned}$$

Dunque poiché $\bigwedge_A^{n+m} A[x]_{\leq n+m-1}$ è libero di rango uno per la Proposizione 3.60 si ha che $\operatorname{Res}(f,g) = \det(M) a_0^m$. □

Al fine di mostrare l'ultimo risultato è necessaria la seguente proposizione legata all'isomorfismo di localizzazioni di un modulo.

PROPOSIZIONE 5.26. Sia A un anello ed M un A-modulo. Siano S e T parti moltiplicative di A tali che $S \subseteq T$. Sia $\Phi\colon S^{-1}M \to T^{-1}M$ omomorfismo di A-moduli dato da $m/s \mapsto m/s$. Supponiamo che per ogni $\mathfrak{p} \in \operatorname{Spec}(A)$ tale che $\mathfrak{p} \in \operatorname{Supp}(M)$ e $\mathfrak{p} \cap S = \varnothing$ si ha che $\mathfrak{p} \cap T = \varnothing$. Allora Φ è un isomorfismo.

DIMOSTRAZIONE. Osserviamo che Φ è anche un omomorfismo di $S^{-1}A$-moduli dato che $S \subseteq T$ e dunque usiamo la proprietà locale 3.22 per l'anello $S^{-1}A$. Per la Proposizione 3.7 sappiamo che gli ideali primi in $S^{-1}A$ sono tutti ideali estesi e sono in corrispondenza biunivoca con gli ideali primi di A che non incontrano S. Abbiamo dunque due casi:

- se $\mathfrak{p} \cap T = \varnothing$ allora si ha anche che $\mathfrak{p} \cap S = \varnothing$. Si ha dunque che $(S^{-1}M)_{\mathfrak{p}}$ e $(T^{-1}M)_{\mathfrak{p}}$ sono entrambi $M_{\mathfrak{p}}$, perciò $\Phi_{\mathfrak{p}}$ è l'identità su $M_{\mathfrak{p}}$;
- se $\mathfrak{p} \cap T \neq \varnothing$ e $\mathfrak{p} \cap S = \varnothing$ si deve avere che $M_{\mathfrak{p}} = 0$ per ipotesi. Dunque $\Phi_{\mathfrak{p}}$ è in questo caso l'unico omomorfismo tra i moduli nulli, che è un isomorfismo.

Ciò prova che Φ è un isomorfismo. □

TEOREMA 5.27 (Invarianza della molteplicità di intersezione). Sia $\mathbb{K} = \overline{\mathbb{K}}$ campo. Siano $\mathcal{C}$ e $\mathcal{D}$ due curve algebriche in $\mathbb{P}^2(\mathbb{K})$ e sia $p \in \mathcal{C} \cap \mathcal{D}$. Siano $F, G \in \mathbb{K}[x_0, x_1, x_2]$ tali che $\mathcal{C} = \mathbf{V}(F)$ e $\mathcal{D} = \mathbf{V}(G)$ ed f e g equazioni locali rispettivamente di $\mathcal{C}$ e $\mathcal{D}$. Allora $I(\mathcal{C}, \mathcal{D}, p) = \dim_{\mathbb{K}} \mathcal{O}_{\mathbb{P}^2(\mathbb{K}),p}/(f, g)$.

DIMOSTRAZIONE. Grazie alla Proposizione 1.22 possiamo scegliere un sistema di coordinate omogenee tale che $[0 : 0 : 1] \notin \mathcal{C} \cup \mathcal{D}$ e che tutte le rette passanti per $[0 : 0 : 1]$ incontrano al massimo un solo punto di $\mathcal{C} \cap \mathcal{D}$ e tale che la retta di equazione $x_0 = 0$ non incontri punti di $\mathcal{C} \cap \mathcal{D}$.

Possiamo dunque deomogeneizzare rispetto alla variabile x_0 i polinomi F e G senza perdita di grado con coordinate affini $x = x_1/x_0$ ed $y = x_2/x_0$. Otteniamo pertanto $f = a_0y^n + \ldots + a_{n-1}y + a_n$ e $g = b_0y^m + \ldots + b_{m-1}y + b_m$ con $a_i,\ b_j \in \mathbb{K}[x]$ di gradi rispettivamente i e j e $a_0, b_0 \neq 0$. Si consideri $\operatorname{Res}(f, g; y)$ che risulta essere il deomogeneizzato rispetto ad x_0 di $\operatorname{Res}(F, G; x_2)$. Avendo supposto che la retta di equazione $x_0 = 0$ non incontri punti nell'intersezione delle due curve si ha che le radici di $\operatorname{Res}(f, g; y)$ sono in biezione con quelle di $\operatorname{Res}(F, G; x_2)$ per la Proposizione 1.4. Sia $\lambda \in \mathbb{K}$ una radice di $\operatorname{Res}(f, g; y)$ e sia $p_\lambda \in \mathcal{C} \cap \mathcal{D}$ il punto corrispondente. Sia poi $\nu_\lambda\colon \mathbb{K}(x) \to \mathbb{Z} \cup \{\infty\}$ la valutazione relativa a λ con anello di valutazione $A = \mathbb{K}[x]_{(x-\lambda)} = \{\varphi \in \mathbb{K}(x) \mid \nu_\lambda(\varphi) \geq 0\} \cong \mathcal{O}_{\mathbb{A}^1,\lambda}$, dove l'isomorfismo è dato dal Teorema 4.38. Per definizione A è un DVR. Consideriamo poi $\psi\colon A[y]/(f) \to A[y]/(f)$ l'omomorfismo di A-moduli dato dalla moltiplicazione per g. Si ha dunque che

$$\begin{aligned} I(\mathcal{C}, \mathcal{D}, p) = \nu_\lambda(Res(f, g; y)) = \nu_\lambda(\det \psi) = \operatorname{length}_A A/(\det \psi) = \\ = \operatorname{length}_A \operatorname{coker}(\psi) = \operatorname{length}_A A[y]/(f, g) = \dim_{\mathbb{K}} A[y]/(f, g). \end{aligned}$$

dove la prima uguaglianza è per definizione, la seconda segue dalla Proposizione 5.25, la terza dalla Proposizione 5.21, la quarta per la Proposizione 5.23. Osservando che $\operatorname{coker}(\psi) = (A[y]/(f))/(g) \cong A[y]/(f, g)$, l'ultima uguaglianza segue per la Proposizione 5.14 poiché $(A, (x - \lambda))$ è una $\mathbb{K}$-algebra locale e $[A/(x - \lambda) : \mathbb{K}] = 1$ poiché $A/(x - \lambda) = (\mathbb{K}[x]/(x - \lambda))_{(x-\lambda)}$ per la Proposizione 3.14 e dato che $\operatorname{Ann}(\mathbb{K}[x]/(x - \lambda)) = (x - \lambda)$ si ha per la Proposizione 3.39 l'isomorfismo $(\mathbb{K}[x]/(x - \lambda))_{(x-\lambda)} \cong \mathbb{K}[x]/(x - \lambda) \cong \mathbb{K}$.

Non resta che mostrare che $\dim_{\mathbb{K}} A[y]/(f, g) = \dim_{\mathbb{K}} \mathcal{O}_{\mathbb{P}^2(\mathbb{K}),p}/(f, g)$; mostriamo che i due $\mathbb{K}[x, y]$-moduli sono isomorfi. Poiché la retta di equazione $x_0 = 0$ non contiene punti di $\mathcal{C} \cap \mathcal{D}$ abbiamo che $p \in U_0$ e dunque $\mathcal{O}_{\mathbb{P}^2(\mathbb{K}),p} = \mathcal{O}_{U_0,p}$. Tuttavia sappiamo che $U_0 \cong \mathbb{A}^2$ e dunque per il Teorema 4.38 abbiamo che $\mathcal{O}_{U_0,p} \cong \mathcal{O}_{\mathbb{A}^2,p} \cong \mathbb{K}[x, y]_{(x-\lambda,y-\mu)}$ con (λ, μ) le coordinate affini in U_0 di p. Osserviamo che $A[y] = \mathbb{K}[x]_{(x-\lambda)}[y] = S^{-1}\,\mathbb{K}[x, y]$ con $S = \mathbb{K}[x] \setminus (x-\lambda)$ parte moltiplicativa di $\mathbb{K}[x]$ e $\mathbb{K}[x, y]$. Ricordando la Proposizione 3.14 abbiamo che quozienti commutano con la costruzione dei moduli di frazioni e dunque mostriamo che

$S^{-1}(\mathbb{K}[x,y]/(f,g))$ è isomorfo a $(\mathbb{K}[x,y]/(f,g))_{(x-\lambda,y-\mu)}$. Indicando con $\mathfrak{m} = (x-\lambda, y-\mu)$ e $T = \mathbb{K}[x,y] \setminus \mathfrak{m}$ si ha che $(\mathbb{K}[x,y]/(f,g))_{(x-\lambda,y-\mu)} = T^{-1}(\mathbb{K}[x,y]/(f,g))$ ed applichiamo la Proposizione 5.26 al $\mathbb{K}[x,y]$-modulo $M = \mathbb{K}[x,y]/(f,g)$ con le parti moltiplicative $S \subseteq T$. Sia $\mathfrak{p} \in \operatorname{Spec}(\mathbb{K}[x,y])$ tale che $\mathfrak{p} \cap S = \varnothing$ e tale che $M_{\mathfrak{p}} \neq 0$, cioè $\mathfrak{p} \in \operatorname{Supp}(M)$. Dalla Proposizione 3.16 abbiamo che $\mathfrak{p} \in \operatorname{Supp}(M)$ se e solo se $\mathfrak{p} \supseteq \operatorname{Ann}(M) = (f,g)$. Avendo che $\operatorname{height}(f,g) = 2$ segue che $\operatorname{height}\mathfrak{p} \geq 2$; dunque $\mathfrak{p}$ è massimale dato che $\dim \mathbb{K}[x,y] = 2$. Dall'inclusione $\mathfrak{p} \supseteq (f,g)$ segue poi che $\mathbb{V}(\mathfrak{p}) \subseteq \mathbb{V}(f,g) = \{p_1, \ldots, p_N\}$. Allora si ha che $\mathfrak{p} = (x-a, y-b)$ ove $(a,b) \in \mathbb{V}(f,g)$. Avendo che $\mathfrak{p} \cap S = \varnothing$ segue che $\mathfrak{p} \cap \mathbb{K}[x] \subseteq (x-\lambda)\,\mathbb{K}[x,y]$; tuttavia $x - a \in \mathfrak{p} \cap \mathbb{K}[x] \subseteq (x-\lambda)\,\mathbb{K}[x,y]$ e dunque $a = \lambda$. Stante ciò sappiamo che $\mathfrak{m}$ corrisponde al punto di $\mathcal{C} \cap \mathcal{D}$ di coordinate affini (λ, μ). Ma se $\mathfrak{p}$ corrisponde ad uno dei punti di $\mathcal{C} \cap \mathcal{D}$ ed abbiamo mostrato che $a = \lambda$ poiché sulla retta $x = \lambda$ c'è solo un punto di $\mathcal{C} \cap \mathcal{D}$ segue che anche $b = \mu$ e dunque $\mathfrak{p} = \mathfrak{m}$ e dunque tautologicamente $\mathfrak{p} \cap T = \varnothing$ e sono verificate le ipotesi della Proposizione 5.26. Pertanto $S^{-1}M \cong T^{-1}M$, cioè $A[y]/(f,g) \cong \mathcal{O}_{\mathbb{P}^2(\mathbb{K}),p}/(f,g)$ e dunque $I(\mathcal{C},\mathcal{D},p) = \dim_{\mathbb{K}} A[y]/(f,g) = \dim_{\mathbb{K}} \mathcal{O}_{\mathbb{P}^2(\mathbb{K}),p}/(f,g)$. □

Corollario 5.28. La Definizione 5.11 è ben posta.

Corollario 5.29. Sia $\mathbb{K} = \overline{\mathbb{K}}$ campo. Siano $\mathcal{C}$ e $\mathcal{D}$ due curve algebriche di $\mathbb{P}^2(\mathbb{K})$, $p \in \mathcal{C} \cap \mathcal{D}$ e g proiettività di $\mathbb{P}^2(\mathbb{K})$. Allora $I(\mathcal{C},\mathcal{D},p) = I(g(\mathcal{C}), g(\mathcal{D}), g(p))$.

Possiamo adesso mostrare il Teorema di Bézout.

Teorema 5.30 (Teorema di Bézout). Sia $\mathbb{K} = \overline{\mathbb{K}}$. Siano $\mathcal{C}$ e $\mathcal{D}$ due curve algebriche in $\mathbb{P}^2(\mathbb{K})$ di gradi rispettivamente n ed m senza componenti comuni. Allora

$$\sum_{p \in \mathcal{C} \cap \mathcal{D}} I(\mathcal{C},\mathcal{D},p) = nm$$

.

Dimostrazione. Per la Proposizione 1.22 possiamo scegliere un sistema di coordinate omogenee tale che $[0:0:1] \notin \mathcal{C} \cup \mathcal{D}$ e che nessuna retta passante per $[0:0:1]$ contenga più di un punto di $\mathcal{C} \cap \mathcal{D}$; in altri termini che $[0:0:1] \notin \mathcal{C} \cup \mathcal{D} \cup \bigcup_{p,q \in \mathcal{C} \cap \mathcal{D}} L(p,q)$ senza alterare l'indice della molteplicità di intersezione per il Teorema 5.27. Siano poi $F, G \in \mathbb{K}[x_0, x_1, x_2]$ polinomi omogenei rappresentanti rispettivamente $\mathcal{C}$ e $\mathcal{D}$. Poiché $\mathcal{C}$ e $\mathcal{D}$ non hanno componenti in comune, ricordiamo che $\operatorname{Res}(F, G; x_2) \in \mathbb{K}[x_0, x_2]$ è un polinomio omogeneo non nullo di grado nm e dunque per il Teorema 1.35 ha esattamente nm radici omogenee contate con molteplicità essendo $\mathbb{K} = \overline{\mathbb{K}}$. Vogliamo adesso mostrare che le radici in $\mathbb{P}^1(\mathbb{K})$ di $\operatorname{Res}(F, G; x_2)$ sono in corrispondenza biunivoca con i punti di $\mathcal{C} \cap \mathcal{D}$ tramite la proiezione dal punto $[0:0:1]$ sull'iperpiano standard H_2. Osserviamo che identificando l'iperpiano standard H_2 con $\mathbb{P}^1(\mathbb{K})$ abbiamo che $\pi([x_0 : x_1 : x_2]) = [x_0 : x_1]$, con π la proiezione. Sia $[a_0 : a_1]$ una radice omogenea di $\operatorname{Res}(F, G; x_2)$. Per la proprietà di specializzazione del risultante 5.10 ciò implica che i polinomi $F(a_0, a_1, x_2)$ e $G(a_0, a_1, x_2)$ hanno una radice in comune per la Proposizione 5.5 poiché il campo è algebricamente chiuso; dunque esiste $a_2 \in \mathbb{K}$ tale che $F(a_0, a_1, a_2) = G(a_0, a_1, a_2) = 0$, cioè $[a_0 : a_1 : a_2] \in \mathcal{C} \cap \mathcal{D}$. Dall'ipotesi fatta sul sistema di coordinate omogenee si ha dunque la bigezione tra le radici omogenee di $\operatorname{Res}(F, G; x_2)$ ed i punti di $\mathcal{C} \cap \mathcal{D}$. Sia allora $p = [p_0 : p_1 : p_2] \in \mathcal{C} \cap \mathcal{D}$: avendo definito $I(\mathcal{C},\mathcal{D},p)$ come la molteplicità di $[p_0 : p_1]$ come radice omogenea di $\operatorname{Res}(F, G; x_2)$ si ha la tesi per il Teorema 1.35. Sia infatti $p = [p_0 : p_1 : p_2] \in \mathcal{C} \cap \mathcal{D}$ denotiamo con m_p la molteplicità della corrispondente radice omogenea $[p_0 : p_1]$ di $\operatorname{Res}(F, G; x_2)$; segue che

$$nm = \sum_{p \in \mathcal{C} \cap \mathcal{D}} m_p = \sum_{p \in \mathcal{C} \cap \mathcal{D}} I(\mathcal{C},\mathcal{D},p).$$

□

Esempio 5.31. Sia $\mathbb{K} = \mathbb{C}$. Consideriamo le curve in $\mathbb{P}^2(\mathbb{K})$ $\mathcal{C} = \overline{\mathbb{V}(y - x^2)}$ e $\mathcal{D} = \overline{\mathbb{V}(x(y - x^3))}$ dove identifichiamo $\mathbb{A}^2$ con la carta U_0. Si osserva facilmente che $\mathcal{C}$ e $\mathcal{D}$ non hanno componenti in comune avendo dato i polinomi che le descrivono già fattorizzati in

termini irriducibili ed è dunque applicabile il Teorema di Bézout. Troviamo i punti di intersezione delle due curve. I punti di intersezione all'infinito sono dati dal sistema

$$\begin{cases} x_1^2 = 0 \\ x_1^4 = 0 \end{cases}$$

la cui unica soluzione è data dal punto $[0:0:1]$.

I punti di intersezione nella parte affine sono invece dati dalle soluzioni del sistema

$$\begin{cases} x_2 - x_1^2 = 0 \\ x_1 x_2 - x_1^4 = 0 \end{cases} \iff \begin{cases} x_2 = x_1^2 \\ x_1^3 - x_1^4 = 0 \end{cases} \iff \begin{cases} x_2 = x_1^2 \\ x_1^3(1 - x_1) = 0 \end{cases}$$

da cui le soluzioni $[1:0:0]$ e $[1:1:1]$.

Calcoliamo adesso le molteplicità di intersezione tra $\mathcal{C}$ e $\mathcal{D}$ in tali punti come indicato dal Teorema 5.27.

Iniziamo da $p_0 = [1:0:0]$. Nella carta U_0 identificata con $\mathbb{A}^2$ diamo le coordinate affini $x = x_1/x_0, y = x_2/x_0$. In tale carta abbiamo equazioni locali $f_0 = y - x^2$ e $g_0 = x(y - x^3)$ e calcoliamo dunque la dimensione di $\mathbb{C}[x,y]_{(x,y)}/(f_0, g_0)$. In $\mathbb{C}[x,y]_{(x,y)}$ abbiamo che

$$(f_0, g_0) = (y - x^2, x(y - x^3)) = (y - x^2, x(x^2 - x^3)) = (y - x^2, x^3(1 - x)) = (y - x^2, x^3)$$

poiché $1 - x$ è invertibile in $\mathbb{C}[x,y]_{(x,y)}$. Per la Proposizione 3.14 $\mathbb{C}[x,y]_{(x,y)}/(y - x^2, x^3) \cong (\mathbb{C}[x,y]/(y - x^2, x^3))_{(x,y)}$. Osserviamo che $\sqrt{\mathrm{Ann}(\mathbb{C}[x,y]/(y - x^2, x^3))} = (x,y)$ e dunque per la Proposizione 3.39 abbiamo che $(\mathbb{C}[x,y]/(y - x^2, x^3))_{(x,y)}) \cong \mathbb{C}[x,y]/(y - x^2, x^3) \cong \mathbb{C}[x]/(x^3)$ che ha dimensione 3 su $\mathbb{C}$. Allora $I(\mathcal{C}, \mathcal{D}, p) = 3$.

Prendiamo adesso in considerazione $p_1 = [0:0:1]$ che corrisponde al punto $(0,0)$ nella carta U_2 con coordinate affini $u = x_0/x_2, v = x_1/x_2$. In questa carta abbiamo equazioni locali $f_1 = u - v^2$ e $g_1 = u^2 v - v^4$. In $\mathbb{C}[u,v]_{(u,v)}$ abbiamo come nel caso precedente che

$$(f_1, g_1) = (u - v^2, (u^2 - v^3)v) = (u - v^2, (v^4 - v^3)v) = (u - v^2, (v - 1)v^4) = (u - v^2, v^4).$$

Ragionando come nel caso precedente si ottiene che $\mathbb{C}[u,v]_{(u,v)}/(u - v^2, v^4) \cong \mathbb{C}[v]/(v^4)$ che ha dimensione 4. Allora $I(\mathcal{C}, \mathcal{D}, p_1) = 4$.

Consideriamo adesso l'ultimo punto $p_2 = [1:1:1]$. Utilizziamo come per il punto p_0 la carta U_0 con coordinate x ed y dove avevamo le equazioni locali f_0 e g_0. In questo caso il punto p_2 corrisponde al punto $(1,1)$ e si ha in $\mathbb{C}[x,y]_{(x-1,y-1)}$ che

$$\begin{aligned}(f_0, g_0) &= (y - x^2, x(y - x^3)) = (y - x^2, y - x^3) = (y - x^2, x^2 - x^3) = \\ &= (y - x^2, x^2(1 - x)) = (y - x^2, 1 - x) = (y - x^2, 1 - x) = (x - 1, y - 1)\end{aligned}$$

poiché in questo caso sono invertibili x e dunque x^2. Di nuovo per la Proposizione 3.14 si ha $\mathbb{C}[x,y]_{x-1,y-1}/(x-1, y-1) \cong (\mathbb{C}[x,y]/(x-1, y-1))_{(x-1,y-1)}$ e poiché $\mathrm{Ann}(\mathbb{C}[x,y]/(x - 1, y-1)) = (x-1, y-1)$ si ha che $(\mathbb{C}[x,y]/(x-1, y-1))_{(x-1,y-1)} \cong \mathbb{C}[x,y]/(x-1, y-1) \cong \mathbb{C}$. Allora $I(\mathcal{C}, \mathcal{D}, p_2) = 1$.

Abbiamo che $\deg \mathcal{C} = \deg F = 2$ e $\deg \mathcal{D} = \deg G = 4$ e pertanto è facile verificare il teorema di Bézout poiché $2 \cdot 4 = 8 = 3 + 4 + 1$.

Bibliografia

[AM16] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, economy edition, 2016. For the 1969 original see [MR0242802].

[Bou74] Nicolas Bourbaki. *Elements of mathematics. Algebra, Part I: Chapters 1-3*. Hermann, Paris; Addison-Wesley Publishing Co., Reading, MA, 1974. Translated from the French.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[FFP16] Elisabetta Fortuna, Roberto Frigerio, and Rita Pardini. *Projective geometry*, volume 104 of *Unitext*. Springer, [Cham], italian edition, 2016. Solved problems and theory review, La Matematica per il 3+2.

[Har77] Robin Hartshorne. *Algebraic geometry*, volume No. 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1977.

[Hun74] Thomas W. Hungerford. *Algebra*. Holt, Rinehart and Winston, Inc., New York-Montreal, Que.-London, 1974.

[Kir92] Frances Kirwan. *Complex algebraic curves*, volume 23 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1992.

[Ser00] Edoardo Sernesi. *Geometria 1: programma di matematica fisica elettronica*. Bollati Boringhieri, 2000.

[Sha13] Igor R. Shafarevich. *Basic algebraic geometry. 1*. Springer, Heidelberg, third edition, 2013. Varieties in projective space.

[SKKT00] Karen E. Smith, Lauri Kahanpää, Pekka Kekäläinen, and William Traves. *An invitation to algebraic geometry*. Universitext. Springer-Verlag, New York, 2000.