Corso di Laurea in Ingegneria dell'Informazione

Tesina

Teoria delle curve algebriche

Laureando:
Alvise Vitturi

Relatore:
Prof. Ezio Stagnaro

27 settembre 2010
A.A. 2009/2010

Indice

Prefazione

L'obbiettivo di questa tesi coincide con lo sviluppo di un mio interesse specifico nei confronti del percorso metodologico proprio della geometria algebrica nel ventesimo secolo. Studiosi quali Federigo Enriques,Guido Castelnuovo hanno, infatti, perfezionato la geometria di fine Ottocento che aveva raggiunto il suo apice speculativo con la Scuola Italiana di Geometria. La soluzione di alcuni problemi si era fermata ad un ambito meramente intuitivo e, perciò, vi era la necessità di una formalizzazione rigorosa e moderna. Già agli inizi del XX secolo, Federigo Enriques negava, in virtù della immane somma degli acquisti fatti, la possibilità di dominare l'intera materia con una sola veduta. Tuttavia, egli poteva parlare della geometria algebrica come di una *dottrina qualitativa delle equazioni e delle funzioni algebriche,..., ove confluiscono il metodo delle coordinate, il metodo delle proiezioni e tutti i diversi ordini di concetti suggeriti dallo studio delle curve.* Lo sviluppo della mia tesi inoltre, prende in considerazione l'utilizzo di metodi di algebra commutativa e dei concetti introduttivi di topologia affinati successivamente. Considero questa disciplina una materia fertile da cui non è stato ottenuto il massimo rendimento, e ricca di applicazioni, come la Teoria dei Codici, e la Teoria dei Sistemi.

Capitolo 1

Concetti introduttivi

Le dimostrazioni riguardo a questo capitolo introduttivo sono rimandate alla bibliografia cfr. [3].

1.1 Gruppi

Definizione 1.1.1. Un' operazione su E è una applicazione $\varphi : E^2 \to E$.

Definizione 1.1.2. Sia definita su E un'operazione φ. Denoteremo $\varphi((a, b))$ con $a \circ b$. Un elemento $e \in E$ tale che

$$e \circ a = a \circ e = a, \forall a \in E,$$

si chiama identità rispetto all'operazione φ.

Definizione 1.1.3. Sia definita su E un' operazione φ e supponiamo che E possegga una identià rispetto a φ. Se a' e a sono due elementi di E tali che

$$a \circ a' = a' \circ a = e,$$

allora a' si chiama inverso di a rispetto all'operazione φ.

Definizione 1.1.4. Su un insieme G sia definita un operazione φ e dentotiamo $\varphi((a, b)) = a \circ b$. G si dice gruppo e si denota $(G, \circ)$ se valgono le seguenti propietà (assiomi di gruppo) :

G1. $(a \circ b) \circ c = a \circ (b \circ c)$, $\forall\ a, b, c \in G$

G2. $\exists\ e \in G \mid \forall\ a \in G$ si abbia $e \circ a = a$

G3. $\forall\ a \in G\ \exists\ a' \in G \mid a' \circ a = e$, dove e è l'elemento la cui esistenza è assicurata da G2.

1.2 Sottogruppi

Sia H un sottoinsieme di G e che $(G, \circ)$ sia un gruppo

Definizione 1.2.1. Il sottoinsieme H di G si dice sottogruppo se H è gruppo con l'operazione ristretta su G.

Proposizione 1.1. *$H \subseteq G$ è sottogruppo $(G, \circ)$ se e solo se valgono le seguenti propietà:*

1. *$\forall\ x, y \in H$ si ha $x \circ y \in H$;*
2. *l'identità di G appartiene ad H;*
3. *$\forall\ x \in H$, l'inverso x' di x appartiene ad H;*

1.3 Gruppi quoziente

Definizione 1.3.1. Sia H un sottogruppo di $(G, \circ)$. L'insieme $a \circ H = \{a \circ x \mid x \in H\}$ si chiama laterale sinistro di H individuato da $a \in G$. Definizione analoga per il laterale destro.

Definizione 1.3.2. Sia I un insieme, con il termine partizione di I si intende una qualsiasi famiglia $\{I_j\}_{j \in J}$ di $\mathcal{P}(I)$ che verifica le seguenti propietà

1. $\bigcup_{j \in J} I_j = I$
2. $I_{j_1} \bigcap I_{j_2} = \emptyset$ se $j_1 \neq j_2$

con J l'insieme degli indici della famiglia.

Proposizione 1.2. *Sia H un sottoinsime di G. Si ha che l'insieme delle classi laterali di H formano una partizione di G.*

Definizione 1.3.3. Se S è un insieme e se $\mathcal{P} = \{S_j\}_{j \in J}$ una partizione di S, si chiama insieme quoziente di S rispetto a $\mathcal{P}$ e si denota con $S/\mathcal{P}$.

Notazione 1.1. Per l'insieme delle classi laterali di un sottogruppo H di G si userà questa scrittura G/H.

Il modo più naturale per dotare l'insieme quoziente G/H di struttura di gruppo sarebbe quello di definire l'operazione $\square$ su G/H in questo modo:

$$(a \circ H) \square (b \circ H) = (a \circ b) \circ H$$

questa definizione però in generale non è ben posta. Bisogna infatti verificare che non dipenda dai rappresentanti scelti. Più precisamente dobbiamo verificare che se $a \circ H = a_1 \circ H$ e $b \circ H = b_1 \circ H$ allora $(a \circ H) \square (b \circ H) = (a \circ b) \circ H = (a_1 \circ H) \square (b_1 \circ H) = (a_1 \circ b_1) \circ H$.

Definizione 1.3.4. Sia H sottogruppo di $(G, \circ)$, H si dice sottogruppo invariante o normale se

$$a \circ H = H \circ a, \forall a \in G$$

È facile dimostrare che nel caso di sottogruppi normali o invarianti l'operazione $\square$ è ben posta e $(G/H, \square)$ verifica gli assiomi di gruppo.

1.4 Omomorfismi di gruppi

Siano $(G_1, \circ)$ e $(G_2, \diamond)$ due gruppi.

Definizione 1.4.1. Un'applicazione $\varphi : G_1 \to G_2$ si dice omomorfismo se:

$$\varphi(a \circ b) = \varphi(a) \diamond \varphi(b)$$

Se inoltre è suriettiva e iniettiva si chiama isomorfismo.

Definizione 1.4.2. Sia $\varphi : G_1 \to G_2$ un'omomorfismo di gruppi. L'insieme degli elementi di G_1 la cui immagine tramite φ è e_2, si chiama nucleo o kernel di φ e si indica con Ker φ. In simboli:

$$Ker\varphi = \{a \in G_1 \mid \varphi(a) = e_2\}$$

Proposizione 1.3. *Sia φ un'omomorfismo. Valgono le seguenti proposizioni:*

1. *$Ker\ \varphi$ è sottogruppo di G_1 e $Im\ \varphi$ è sottogruppo di G_2.*
2. *$Ker\ \varphi = e_1 \Leftrightarrow \varphi$ è iniettiva.*
3. *$Ker\ \varphi$ è sottogruppo invariante.*

L'ultima proposizione ci permette di costruire tale gruppo quoziente $(G/Ker\varphi, \square)$.

Teorema 1.1. *Un'omomorfismo $\varphi : G_1 \to G_2$ individua un isomorfismo:*

$$\overline{\varphi} : G_1/Ker\varphi \to Im\varphi$$

Definizione 1.4.3. Sia G un gruppo e H un suo sottogruppo, l'applicazione:

$$\pi : G \to G/H$$

si chiama proiezione canonica sul quoziente.

Tutto questo permette la seguente scomposizione detta anche decomposizione canonica:

$$\begin{array}{ccc} G_1 & \xrightarrow{\varphi} & G_2 \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle i} \\ G_1/Ker\varphi & \xrightarrow[\overline{\varphi}]{} & Im\varphi \end{array}$$

1.5 Anelli

In questa sezione viene introdotta una nuova struttura algebrica che arricchisce quella di gruppo, per poter poi definire i polinomi.

Definizione 1.5.1. Un'insieme A su cui sono definite due operazioni $+$ e $\cdot$ $(A, +, \cdot)$ si dice anello se (assiomi di anello):

A1. A è un gruppo commutativo rispetto all'addizione.

A2. se $a, b, c \in A$, $\Rightarrow a(bc) = (ab)c$.

A3. se $a, b, c \in A$, $\Rightarrow a(b + c) = ab + ac$ e $(b + c)a = ba + ca$.

Definizione 1.5.2. Un sottoinsieme B di A si dirà sottoanello se è anello con l'operazione di A ristretta a B.

Definizione 1.5.3. Un anello A si dice anello con identità o anello unitario se:

A4. $\exists\ 1 \in A \mid a \cdot 1 = 1 \cdot a = a, \forall\ a \in A$

l'elemento 1 si chiama anche identità.

Definizione 1.5.4. Un elemento $a \in A$ si dice divisore dello zero in A se $\exists$ un elemeto $b \neq 0 \in A \mid a \cdot b = 0 \vee b \cdot a = 0$. Lo zero si dice divisore improprio, tutti gli altri sono propri.

Definizione 1.5.5. Un anello A si dice dominio di integrità se non possiede divisori propri dello zero.

Definizione 1.5.6. Un anello K commutativo si dice campo se (assiomi di campo):

K1. K ha almeno due elementi.

K2. K ha un' identità.

K3. Ogni elemento di K diverso da zero possiede inverso.

Definizione 1.5.7. Siano A_1 e A_2 anelli. Una applicazione $\varphi : A_1 \to A_2$ è omomorfismo di anelli se valgono le seguenti:

1. $\forall\ a, b \in A\ \varphi(a +_{A_1} b) = \varphi(a) +_{A_2} \varphi(b)$.
2. $\forall\ a, b \in A\ \varphi(a \cdot_{A_1} b) = \varphi(a) \cdot_{A_2} \varphi(b)$.
3. Se A_1 e A_2 sono anelli unitari allora deve essere che $\varphi(1_{A_1}) = 1_{A_2}$.

1.6 Ideali(paragrafo introduttivo)

Definizione 1.6.1. Un sottoanello I di A si dice ideale sinistro se $\forall\ x \in I$ e $\forall\ a \in A$ si ha $a \cdot x \in I$ (analogo per quello destro). Un sottoanello I di A si dice ideale bilatero se è sia ideale sinistro che destro.

Proposizione 1.4. *$I \neq \emptyset$ un sottoinsieme di A. I è ideale sinistro (destro) di $A \Leftrightarrow$*

1. *$\forall\ x, y \in I$ si ha $x - y \in I$.*
2. *$\forall\ x \in I$ e $\forall a \in A$ si ha $a \cdot x \in I$.*

Definizione 1.6.2. Un ideale I di un anello A si dice primo se

$$x \cdot y \in I \Rightarrow x \in I \vee y \in I$$

Definizione 1.6.3. Un ideale sinistro I di un anello A di dice massimale se per ogni ideale sinistro $J \supset I$ si ha $I = J$ oppure $J = A$. Analogamente per quello destro.

Definizione 1.6.4. Sia A un dominio di integrità con identità e I un suo ideale. Si dice che I è generato dagli elementi $a_1, ...a_n$ e si scrive $I = (a_1, ...a_n)$ se $I = \{a_1x_1 + \cdots a_nx_n$ al variare degli $x_i \in A\}$. Nel caso in cui un ideale possa essere generato da un singolo generatore, tale ideale prende il nome di ideale principale.

Definizione 1.6.5. Un anello A dove ogni ideale è un ideale principale si chiama anello ad ideali principali PID.

1.7 Anelli quoziente

Estenderemo per gli anelli quanto fatto riguardo ai gruppi, cioè definiremo un'ulteriore operazione $\otimes$ sul gruppo quoziente definito precedentemente per renderlo un anello. Siano $(A, +, \cdot)$ anello e B sottoanello. Si ha che B è commutativo rispetto alla somma, pertanto invariante perciò ha senso considerare il gruppo $(A/B, \oplus)$. Per dotare A/B di struttura di anello definiamo l'operazione $\otimes$ nel modo più naturale ancora una volta

$$(a + B) \otimes (b + B) = (a \cdot b) + B$$

Bisogna ovviamente dimostrare che tale operazione non dipende dai rappresentanti. Se B è un ideale bilatero si può verificare facilmente che $\otimes$ è ben posta.

1.8 Polinomi

In questo paragrafo con A si denoterà sempre un anello unitario e con B un suo sottoanello.

Definizione 1.8.1. Un elemento $X \in A$ si dice trascendente su B se $\forall\ n \in N$ da

$$a_0 + a_1X + \cdots\cdots + a_nX^n = 0, con\ a_i \in B\ \forall i\ si\ ha\ a_0 = a_1 = \cdots = a_n = 0$$

Si dice algebrico se non è trascendente. L'elemento trascendente prende spesso il nome di indeterminata o variabile.

Definizione 1.8.2. Partendo da un elemento di un anello commutativo A trascendente su un suo sottoanello B si può considerare l'insieme:

$$B[X] \doteq \{a_0 + a_1X + \cdots\cdots + a_nX^n, con\ a_i \in B\ \forall i\}$$

Tale insieme con le operazioni in A è un anello che chiameremo anello dei polinomi nell'elemento trascendente X.

Osservazione 1.1. Per definire i polinomi abbiamo usato un anello e un suo sottoanello entrambi commutativi, la definizione data sopra si può estendere anche al caso non commutativo. Così facendo tale proprietà viene persa se anche il sottoanello non verifica la proprietà commutativa.

Si può costruire un anello dei polinomi partendo da un solo anello B sfruttando il concetto di isomorfismo. Il modo di definire tale anello è il seguente: Consideriamo tale insieme:

$$A_1 \doteq \{f \in l_f \mid f(n) \neq 0\ per\ un\ numero\ finito\ di\ n\ \in N\}$$

dove con l_f indico l'insieme delle successioni con codominio B.

Notazione 1. Un elemento di A_1 lo indicheremo in tal modo $(a_0, a_1, \cdots, a_n, \cdots)$

Su A_1 definiamo le seguenti due operazioni che chiameremo rispettivamente somma e prodotto. La somma:

$$(a_0, a_1, \cdots, a_n, \cdots) + (b_0, b_1, \cdots, b_n, \cdots) = (a_0 + b_0, a_1 + b_1, \cdots, a_n + b_n, \cdots)$$

Il prodotto detto anche prodotto di cauchy :

$$(a_0, a_1, \cdots, a_n, \cdots) \cdot (b_0, b_1, \cdots, b_n, \cdots) = (c_0, c_1, \cdots, c_n, \cdots)$$

con

$$\begin{aligned} c_0 &= a_0 \cdot_B b_0 \\ c1 &= a_1 \cdot_B b_0 + a_0 \cdot_B b_1 \\ c_{n+m} &= \sum_{i=0}^{n+m} a_i \cdot_B b_{n+m-i} \end{aligned}$$

Con tali operazioni verifica gli assiomi di anello. Inoltre si può facilmente vedere che l'elemento $(0, 1, 0, 0, 0, \cdots, 0, \cdots)$ è trascendete su B ed inoltre esiste un isomorfismo tra B e un sottoinsieme di A_1 che chiameremo B_1.

Notazione 1. Identificando B con il suo insieme isomorfo B_1 possiamo scrivere $B[X]$ al posto di $B_1[X]$.

Osservazione 1.2. Quanto detto si può ripetere più volte in modo da ottenere un anello di polinomi a più variabili. Si parte da un anello B, si trova un elemento trascendente X oppure si applica il procedimento sopra esposto e si ottiene un anello $B[X]$. $B[X]$ è un nuovo anello e si ripete; cioè si trova un elemento Y e si ottiene $(B[X])[Y]$ che si scrive anche $B[X, Y]$.

1.9 Polinomi omogenei

Definizione 1.9.1. Un polinomio $P \in B[X_1, ..., X_n]$ si dice omogeneo se tutti i coefficienti sono nulli tranne quelli relativi a monomi di un solo grado d. Se $d = 1$ si dice anche polinomio omogeneo lineare.

Proposizione 1.5. *Ogni polinomio $P \in B[X_1, ..., X_n]$ ha un' unica scrittura $P = P_0 + P_1 + \cdots + P_d$ dove P_i sono tutti polinomi omogenei di grado i.*

Da un polinomio omogeneo P di $B[X_1, ..., X_n]$, si può definire un nuovo polinomio $P_* = P(X_1, X_2, ..., X_{n-1}, 1)$ chiamato il suo polinomio deomogeneizzato. Viceversa da un polinomio F di $B[X_1, ..., X_n]$ con $F = F_0 + F_1 + \cdots + F_d$ si definisce un nuovo polinomio in $F^* = X_{n+1}^d F_0 + X_{n+1}^{d-1} F_1 + \cdots + F_d = X_{n+1}^d F(\frac{X_1}{X_{n+1}}, \frac{X_2}{X_{n+1}}, ..., \frac{X_n}{X_{n+1}})$ chiamato il suo polinomio omogeneo. Quanto fatto si può fare rispetto a tutte le variabili.

Proposizione 1.6. *Sono vere le seguenti affermazioni:*

1. $(FG)_* = F_* G_*$; $(FG)^* = F^* G^*$.
2. *Se r è l'esponente massimo di X_{n+1} che divide F, allora $X_{n+1}^r (F_*)^* = F$; $(F^*)_* = F$.*
3. $(F + G)_* = F_* + G_*$; $X_{n+1}^t (F + G)^* = X_{n+1}^r F^* + X_{n+1}^s G^*$, *dove* $r = deg(G)$, $s = deg(F)$, *e* $t = r + s - deg(F + G)$.

Osservazione 1.3. Sia $V(d, n)$ l'iniseme (spazio vettoriale) fatto da tutte le forme di $K[X_1, ..., X_n]$ di grado n. Si può facilmente verificare che l'insieme:

$$B \doteq \{A_{i,j} \mid i + j\}.$$

con $A_{i,j} = L_1 L_2 \cdot ..... \cdot L_i \cdot M_1 M_2 \cdot ..... \cdot M_j$ e $L_1, L_2, ...$ e $M_1, M_2, ...$ ennuple di forme lineari (di grado uno), forma una base di $V(d, n)$.

1.10 Anelli UFD

Diamo innanzitutto qualche definizione riguardo alla divisibilità in un anello A qualsiasi.

Definizione 1.10.1. Sia A un anello e $a, b \in A$. Si dice che b divide a in simboli $b \mid a$ se esiste $c \in A$ con $a = b \cdot c$. Noi chiamiamo $a, b \in A$ associati se esiste un unità $u \in A$ con $a = b \cdot u$. Se $a, b \in A$, allora $d \in A$ è chiamato massimo comun divisore, oppure mcd, di a e b se si hanno le seguenti due propietà:

1. $d \mid a$ e $d \mid b$.
2. quando $d' \mid a$ e $d' \mid b$ per qualche $d' \in A$, allora $d' \mid d$, ogni divisore comune divide d.

Definizione 1.10.2. Sia A un anello commutativo con identità e dominio di integrità, un elemento a non unità si dice primo se l'ideale generato da a scritto (a) è primo.

Un unità u divide ogni elemento $a \in A$. Gli elementi associati e le unità sono anche chiamati divisori impropri. Diamo ora la seguente importante definizione:

Definizione 1.10.3. Un dominio di integrità A è un anello a fattorizzazione unica se soddisfa le seguenti condizioni:

UF1. Ogni non unità di A si può scrivere come prodotto finito di elementi irriducibili.

UF2. La fattorizzazione è unica a meno dell'ordine e delle unità.

Di importanza fondamentale è tale teorema che ci permetterà di semplificare l' mcd(mcm) nel caso di anelli UFD.

Teorema 1.2. *Per un anello A che possiede UF1, la condizione UF2 è equivalente alla seguente condizione:*

UF3. *Se p è un elemento irruducibile di A, allora p è un elemento primo.*

Proposizione 1.7. *Se $p \in A$ è elemento primo, allora p è irrudicibile.*

Queste due proposizioni ci fanno capire l'equivalenza tra primo e irriducibile (solo UFD). Inoltre come già anticipato si può facilmente vedere che definendo l'mcd come il prodotto degli elementi irriducibili in comune tale definizione verifica le due propietà per l'mcd. Pertanto in un anello UFD si possono sfruttare tali due fatti.

Teorema 1.3. *A fattoriale $\Rightarrow A[X]$ fattoriale, dove $A[X]$ è l'anello dei polinomi.*

Dimostrazione. Cfr. [4] □

Corollario 1.1. *A fattoriale $\Rightarrow A[X_1, X_2, ..., X_n]$ è fattoriale.*

Teorema 1.4. *Un anello A ad ideali principali è fattoriale e ogni ideale primo è massimale.*

1.11 A-moduli

Sia A un anello.

Definizione 1.11.1. Un $A-modulo$ è una coppia (A, M) dove M è un gruppo commutativo ed inoltre è defintita un operazione esterna $\cdot_e : A\text{x}M \to M$ che verifica:

1. $(a+b)m = am + bm \ \forall a, b \in A$ e $\forall m \in M$.
2. $a \cdot_e (m+n) = am + an \ \forall a \in A$ e $\forall m, n \in M$.
3. $(ab) \cdot_e m = a \cdot_e (b \cdot_e m) \ \forall a, b \in A$ e $\forall m \in M$.
4. $1_A \cdot_e m = m \ \forall m \in M$.

N.B 1.1. Anche per gli $A-moduli$ esiste il concetto di omomorfismo, bisogna aggiungere:

$$\varphi(am) = a \cdot_e \varphi(m) \ \forall a \in A, m \in M.$$

Se N è un sottomodulo di un modulo A, il gruppo quoziente M/N si rende un A modulo nel seguente modo: se $\overline{m}$ è il laterale contenente m, e $a \in A$ si definisce $a\overline{m} = \overline{am}$. È facile verificare che le quattro propietà di cui sopra sono soddisfatte.

1.11.1 Sequenze esatte

Definizione 1.11.1. Siano $\varphi' : M' \to M$ e $\varphi'' : M \to M''$ due omomorfismi di $A - moduli$. Si dice che:

$$M' \to M \to M''$$

è esatta se $Im(\varphi') = Ker(\varphi'')$.

Se $\varphi_i : M_i \to M_{i+1}$ sono omomorfismi di $A - moduli$, noi diciamo che la sequenza:

$$M_1 \to M_2 \to \cdots \to M_{n+1}$$

è esatta se $Im(\varphi_i) = Ker(\varphi_{i+1})$.

Osservazione 1.4. Si noti che esiste un unico omomorfismo di $A - moduli$ tra l'$A - modulo$ 0 e tutti gli altri $A - moduli$.

Capitolo 2

Ideali

Anche in questo capitolo le dimostrazioni non vengono riportate ma riferite alla bibliografia.

2.1 Anelli Noetheriani

Definizione 2.1.1. Un ideale I di A si dice finitamente generato se esiste un numero finito di elementi di A $\{a_0, ...a_n\}$ tali che $I = (a_0, ..., a_n)$.

Osservazione 2.1. L' enupla di generatori per un ideale I non è unica come non è unico il numero di elementi che possono generarlo.

Definizione 2.1.2. Una successione di ideali di A $\{I_j\}$, con $j \in N$ si dice crescente se:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq ..... \subseteq I_n \subseteq .....$$

Una successione di ideali si dice stazionaria se:

$$\exists n \in N \mid I_1 \subseteq I_2 \subseteq I_3..... \subseteq I_n = I_{n+1} = ...$$

Definizione 2.1.3. Un anello A si dice noetheriano se ogni ideale I di A è finitamente generato.

Un teorema di fondamentale importanza riguardo agli ideali è il teorema della base di Hilbert.

Teorema 2.1. *Se A è un anello noetheriano, allora lo è anche qualsiasi anello di polinomi in un numero finito di variabili.*

Dimostrazione. Cfr. [2]. □

Corollario 2.1. *$K[X_1, ..., X_n]$ è noetheriano $\forall$ campo K.*

2.2 Operazioni sugli ideali

Sia A un anello. Noi definiremo tre operazioni sull'insieme degli ideali di A. L'intersezione (già definita perchè corrisponde all'intersezione tra insiemi), la somma e il prodotto

Definizione 2.1. Siano I_1 e I_2 due ideali di un anello A, si definisce la loro somma $I_1 + I_2$ come l'insieme di tutti gli elementi con questa forma $x + y$ con $x \in I_1$ e $y \in I_2$.

Osservazione 2.2. L'insieme somma definto precedentemente è un ideale perchè si vede facilmente che verifica 1.4.

Per il prodotto si sfrutta l'operazione somma appena definita.

Definizione 2.2. Dati I_1 e I_2 si definisce prodotto $I_1 \cdot I_2$ l'insieme:

$$\{x_1y_1 + \cdots x_ny_n \mid x_i \in I_1, y_j \in I_2\}$$

Ora definiamo il radicale di un ideale.

Definizione 2.3. Sia I un ideale di A, si definisce radicale di I l'ideale (si verifica facilmente che è un ideale):

$$\sqrt{I} \doteq \{a \in A \mid \exists\, n > 0 \,:\, a^n \in I\}$$

2.3 Ideali estesi e contratti

In questo paragrafo vogliamo studiare il comportamento degli ideali di due anelli A_1 e A_2 per mezzo dell'azione di un omomorfismo $\varphi : A_1 \to A_2$. Si può verificare che se I_2 è un ideale di A_2 la controimmagine per mezzo di φ è un ideale di A_1. Invece se I_1 è ideale di A_1, in generale non è vero che la sua immagine è un ideale di A_2.

Dato un ideale I_1, vogliamo associare a $\varphi(I_1)$ un ideale, o meglio il più piccolo ideale che contiene l'immagine, che chiameremo ideale esteso. Diamo pertanto la seguente definizione:

Definizione 2.3.1. Sia I_1 un ideale di A_1, definiamo ideale esteso di I_1 l'ideale:

$$I_1^e \doteq \{\sum_i x_i' \cdot b_i \; con \; x_i' \in \varphi(I_1) \; e \; b_i \in A_2\}.$$

Si verifica facilmete che tale insieme è un ideale, quindi la definizione è ben posta.

Definizione 2.3.2. Sia I_2 un ideale di A_2, l'ideale:

$$I_2^c \doteq \varphi^{-1}(I_2).$$

lo chiameremo ideale contratto.

Proposizione 2.1. *Sia φ omomorfismo come sopra:*

1. $I_1 \subseteq I_1' \Rightarrow I_1^e \subseteq I_1'^e$, $I_2 \subseteq I_2' \Rightarrow I_2^c \subseteq I_2'^c$.
2. $(I_1^e)^c \supseteq I_1$, $(I_2^c)^e \subseteq I_2$.
3. $(I_1 + I_1')^e = I_1^e + I_1'^e$, $(I_2 + I_2')^c \supseteq I_2^c + I_2'^c$.
4. $(I_1 \cap I_1')^e \subseteq I_1^e \cap I_1'^e$, $(I_2 \cap I_2')^c = I_2^c \cap I_2'^c$.
5. $(I_1 \cdot I_1')^e = I_1^e \cdot I_1'^e$, $(I_2 \cdot I_2')^c \supseteq I_2^c \cdot I_2'^c$.
6. $(\sqrt{I_1})^e \subseteq (\sqrt{I_1^e})$, $(\sqrt{I_2})^c = (\sqrt{I_2^c})$.

Dimostrazione. Cfr. [4]. □

Osservazione 2.3. Da un anello A dominio, si possono costruire le frazioni partendo da un sottoinsieme S di $A - \{0\}$ moltiplicativamente chiuso che si indicherà con $S^{-1}A$, dove al denominatore compaiono solo gli elementi di S. Cambiando la definizione della relazione di equivalenza che definisce le frazioni si può generalizzare anche ai non domini di integrità cfr. [4].

Si hanno le seguenti proposizioni:

Proposizione 2.2. *$\varphi : A \to S^{-1}A$,$1 \in S$ si ha:*

1. *Ogni ideale di $S^{-1}A$ è del tipo I^e con I ideale di A.*
2. *Nella prima della 4 di 2.1, vale l'uguaglianza.*
3. *Nella prima della 6 di 2.1, vale l'uguaglianza.*

I vari corollari:

Corollario 2.1. *A noetheriano $\Rightarrow$ $S^{-1}A$ noetheriano.*

Corollario 2.2. *Sia I ideale di A. Allora $I^e \neq S^{-1}A \Leftrightarrow I \cap S = \emptyset$.*

Questi risultati saranno utili nel capitolo 3 quando si parlerà di molteplicità di intersezione e di anelli locali.

Capitolo 3

Varietà Affini

In questo capitolo si comincia a descrivere la Geometria algebrica partendo proprio dalle strutture algebriche definite nei due capitoli precedenti. Si troverà inoltre uno stretto legame tra ideali e varietà; specialmente nel caso di un campo algebricamente chiuso cfr. appendice A. In tutto il capito con K si intende un campo di caratteristica zero cfr. appendice B.

3.1 Introduzione alle varietà

Definizione 3.1.1. K^n si chiama spazio affine.

Definizione 3.1.2. Un elemento $(a_1, ..., a_n) \in K$ è uno zero del polinomio $P(X_1, ..., X_n)$ se $P(a_1, ..., a_n) = 0$.

Definizione 3.1.3. Se I è un ideale di $K[X_1, ..., X_n]$ si dice zero di I uno zero di tutti i polinomi di I.

Proposizione 3.1. *$(a_1, ..., a_n)$ è zero di $I \Leftrightarrow$ è zero dei generatori di I.*

Definizione 3.1.4. Il luogo degli zeri di un ideale I di $K[X_1, ...X_n]$ si dice varietà algebrica e si indica con $\mathcal{V}(I)$.

Da una varietà V definisco $\mathcal{I}(V)$ come l'insieme dei polinomi che si annullano su V. È facile verificare che tale insieme forma un ideale.

Proposizione 3.2. *Valgono le seguenti affermazioni:*

1. $I_1 \subseteq I_2 \Rightarrow \mathcal{V}(I_1) \supseteq \mathcal{V}(I_2)$.
2. $E_1 \subseteq E_2 \Rightarrow \mathcal{I}(E_1) \supseteq \mathcal{I}(E_2)$.
3. $\mathcal{V}(I_1 + I_2) = \mathcal{V}(I_1) \cap \mathcal{V}(I_2)$.
4. $\mathcal{I}(E_1 \cap E_2) = \mathcal{I}(E_1) \cup \mathcal{I}(E_2)$.
5. $\mathcal{V}(I_1 \cdot I_2) = \mathcal{V}(I_1 \cap I_2) = \mathcal{V}(I_1) \cup \mathcal{V}(_2)$.
6. $E \subseteq \mathcal{V}(\mathcal{I}(E))$.
7. $I \subseteq \mathcal{I}(\mathcal{V}(I))$.
8. $\mathcal{V}(\sqrt{I}) = \mathcal{V}(I)$.
9. $E = \mathcal{V}(\mathcal{I}(E))$ *se E è varietà algebrica.*

Dimostrazione. Cfr. [4]. □

3.2 Varietà Irriducibili

Una varietà può essere l'unione finita di altre varietà. Si può dare la seguente importante definizione:

Definizione 3.2.1. Una varietà $V \subset K^n$ si dice riducibile se $V = V_1 \cup V_2$ dove V_1, V_2 sono varietà in K^n, e $V_i \neq V$, $i = 1, 2$. Altrimenti V si dice irriducibile.

Proposizione 3.3. *Una varietà affine V è irriducibile $\Leftrightarrow$ $\mathcal{I}(V)$ è primo.*

Tale definizione ci permette di trovare una scomposizione in fattori irriducibili per le varietà affini.

Teorema 3.1. *Sia V una varietà di K^n. Allora è rappresentabile come unione finita di varietà irruducibili V_i:*

$$V = V_1 \cup V_2 \cup \cdots \cup V_r$$

Tale rappresentazione è unica a meno dell'ordine, se essa è ridotta o irridondante.

Definizione 3.2.2. Partendo da una qualunque varietà V, si definisce anello delle coordinate affini il seguente anello:

$$\Gamma[V] \doteq K[X_1, ..., X_n]/\mathcal{I}(V).$$

Osservazione 3.1. Nel caso di una varietà algebrica V irriducibile abbiamo già visto che $\mathcal{I}[V]$ è primo pertanto $\Gamma[V]$ è dominio di integrità e si può considerare il suo campo delle frazioni indicato con $\Gamma(V)$ detto anche campo delle funzioni razionali su V cfr. [2].

Prendendo alcuni concetti descritti nell'appendice A, si può ora dare la definizione di dimensione di una varietà.

Definizione 3.2.3. Se V è irriducibile, si chiama dimensione di V il grado di trascendenza di $\Gamma(V)$ ($gr.tr._k\Gamma(V) = dim\, V$). Se V è irriducibile si definisce la sua dimensione come la dimensione massima delle componenti della sua decomposizione ridotta.

Qui un semplice elenco di teoremi che saranno utili riguardo alle varietà del piano.

Teorema 3.2. *Siano F e G due polinomi di $K[X, Y]$ senza fattori in comune ($mcd(F, G) = 1$). Allora $\mathcal{V}((F, G)) = \mathcal{V}((F)) \cap \mathcal{V}((G))$ è un insieme finito di punti.*

Dimostrazione. Cfr. [2]. □

Corollario 3.2.1. *Se F è un polinomio irriducibile $\in K[X, Y]$, e $\mathcal{V}((F))$ è un insieme infinito, allora $\mathcal{I}(\mathcal{V}((F))) = (F)$, e $\mathcal{V}((F))$ è irriducibile.*

Dimostrazione. Se $G \in \mathcal{I}(\mathcal{V}((F)))$, $\mathcal{V}((F, G))$ è un insieme infinito, così F divide G, $G \in F$. La tesi deriva dalla proposizione 3.3. □

Corollario 3.2.2. *Supponiamo K infinito (caratteristica zero). Allora le varietà irriducibili contenute in K^2 sono: K^2, $\emptyset$, i punti, e le varietà irriducibili piane $\mathcal{V}((F))$, dove F è un polinomio irriducibile e $\mathcal{V}((F))$ è infinito.*

Dimostrazione. Sia V una varietà irriducibile di K^2. Se V è finita o $\mathcal{I}(V) = 0$, V va bene. Altrimenti $\mathcal{I}(V)$ contiene un polinomio non costante F; dato che $\mathcal{I}(V)$ è primo, qualche fattore irriducibile appartiene a $\mathcal{I}(V)$, così, possiamo assumere F irriducibile. Allora $\mathcal{I}(V) = (F)$; infatti se $G \in \mathcal{I}(V)$, $G \notin (F)$, allora $V \subset \mathcal{V}((F, G))$ è finito. □

Corollario 3.2.3. *Assumiamo K algebricamente chiuso, $F \in K[X,Y]$. Sia $F = F_1^{n_1} \cdots F_m^{n_m}$ la scomposizione di F nei fattori irriducibili. Allora $\mathcal{V}((F)) = \mathcal{V}((F_1)) \bigcup \cdots \bigcup \mathcal{V}((F_m))$ è la decomposizione in fattori irriducibili di V e $\mathcal{I}(\mathcal{V}((F))) = (F_1 \cdots F_m)$.*

Dimostrazione. Cfr. [2]. □

3.3 Hilbert Nullstellensatz e conseguenze

Ora uno dei più importanti teoremi della geometria algebrica il teorema degli zeri di Hilbert.

Teorema(Nullstellensatz) 3.3. *Se K è algebricamente chiuso si ha che $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$.*

Ora i più importanti corollari del Nullstellensatz.

Corollario 3.1. *Se I è ideale primo di $K[X_1, ..., X_n]$ allora $\mathcal{I}(\mathcal{V}(I)) = I$.*

Corollario 3.2. *Esiste una corrispondenza biunivoca tra varietà irriducibili e ideali primi.*

Corollario 3.3. *Sia $F \in K[X_1, ..., X_n]$, $F = F_1^{n_1} \cdots F_s^{n_s}$ la scomposizione in fattori irriducibili di F. Allora $\mathcal{V}((F)) = \mathcal{V}((F_1)) \cap ..... \cap \mathcal{V}((F_s))$ è la decomposizione ridotta, e $\mathcal{I}(\mathcal{V}(F)) = (F_1 \cdots F_r)$. C'è pertanto una corrispondenza biunivoca tra polinomi irriducibili e ipersuperficii (varietà di dimensione n-1).*

3.3.1 Esempi elementari

Ora un esempio importante che sfrutta i teoremi fin qui elencati.

Esempio 3.1. Partiamo da un punto $P = (a_1, ..., a_n) \in K[X_1, ..., X_n]$, abbiamo che $\mathcal{I}(P) \supseteq I = (X_1 - a_1, ..., X_n - a_n)$. L' ideale I è massimale perchè l'insieme $\Gamma(V) = K[X_1, ..., X_n]/\mathcal{I}(P) \cong K$ pertanto o $\mathcal{I}(P) = I$ o coincide con tutto l'anello dei polinomi. Dal corollario uno segue che $\mathcal{I}(P) = I$. Si può verificare anche il viceversa cioè si parte da un ideale massimale I e si dimostra che $\mathcal{V}(I)$ è un punto. In sostanza esiste una corrispondenza biunivoca tra ideali massimali e punti.

Il secondo esempio consiste in un semplice esercizio.Tale esercizio ha lo scopo di mostrare il modo di procedere (nei casi più banali) per quanto riguarda un campo algebricamente chiuso.

Esempio 3.2. Si consideri il polinomio il polinomio $P(X,Y) = Y - X^2$ in $K[X,Y]$ con K algebricamente chiuso (ad esempio i numeri complessi). Vogliamo capire il suo grafico nel piano (disegno solo la parte reale intendendo $K = \mathcal{C}$). Le sue componenti irriducibili(nel caso non lo fosse), la sua dimensione ecc ecc. Innanzitutto si calcola $\mathcal{V}((P))$, nel nostro caso $\mathcal{V}((P)) = \{(x,y) \mid y = x^2\}$.
Per vedere se il nostro polinomio è irriducibile basta dimostrare che l'ideale da lui generato (P) è primo. Per questo ci viene in soccorso un isomorfismo $A[X]/(X-a) \cong A$ che nel nostro caso diventa $(K[X])[Y]/(Y - X^2) = K[X,Y]/(Y - X^2) \cong K[X]$ che ci permette di affermare che (P) è primo. Si usa il teorema degli zeri di Hilbert per calcolare l'anello delle coordinate affini per cui si ottiene $\Gamma(V) = K[X_1, ..., X_n]/\mathcal{I}(\mathcal{V}((P))) = K[X_1, ..., X_n]/(P) \cong K[X]$.
Abbiamo così visto che $\mathcal{V}((P))$ è irriducibile, ha dimensione uno ed il suo grafico vedi sopra.

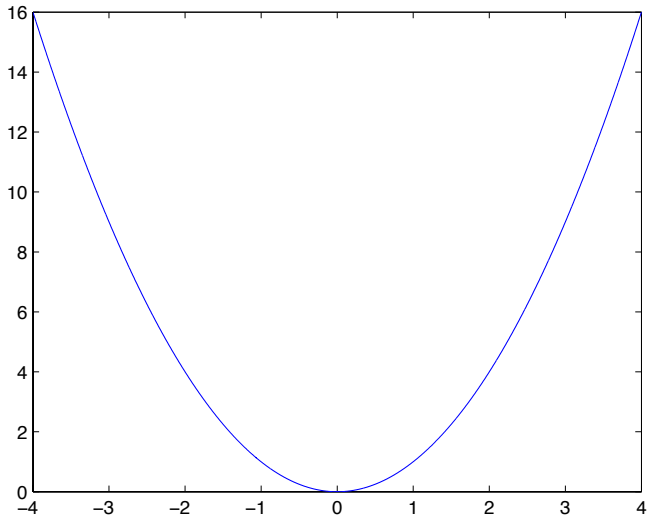


Figura 3.1: Varietà affine dell'ideale $(Y - X^2)$.

3.4 Anelli locali e anelli DVR

Sappiamo che $\Gamma(V)$ è un campo (V irriducibile) e che un suo elemento è chiamato funzione razionale su V. Se f è una funzione razionale su V, $P \in V$ noi diciamo che f è definita su P se per qualche $a, b \in \Gamma(V)$, $f = a/b$ e $b(P) \neq 0$.

Lemma 3.1. *Le seguenti condizioni in un anello A sono equivalenti:*

1. *L'insieme delle non unità in A formano un ideale.*
2. *A ha un unico ideale massimale che contiene ogni ideale proprio di A.*

Un anello A che verifica tali propietà si chiama anello locale.

Esempio importante di anello locale:

Definizione 3.4.1. Sia $P \in V$. Noi definiamo $\mathcal{O}_P(V)$ l'insieme delle funzioni razionali su V che sono definite in P.

Proposizione 3.4. *$\mathcal{O}_P(V)$ è un anello locale notheriano.*

Osservazione 3.2. L'insieme:

$$M_P(V) \doteq \{f \in O_P(V) \mid f(P) = 0\}$$

è chiamato l'ideale massimale di V su P (è massimale su $\mathcal{O}_P$).

Proposizione 3.5. *Sia A un anello che non è un campo. Allora sono equivalenti:*

1. *A è notheriano e locale, e l'ideale massimale è principale.*
2. *Esiste un' elemento irriducibile $t \in A$ per cui ogni elemento $a \in A$ può essere scritto in modo unico nella forma $a = ut^n$, u unità in A, n un numero intero non negativo.*

Un'anello A che verifica le condizioni della proposizione precedente è chiamato un anello a valutazione discreta scritto DVR .Un' elemento t che verifica la 2. Si dice parametro uniformizzante; inoltre ogni altro parametro uniformizzante t' è tale per cui $t' = ut$ con u unità.

3.5 Sottovarietà semplici e singolari

Da qui in avanti si considererà K algebricamente chiuso; se K non algebricamente chiuso vanno apportate alcune modifiche e qualche teorema non è più vero.
Vogliamo dare una caratterizzazione alle curve del piano. Prima di fare questo diamo le definizioni più generali per poi, poterci limitare al caso bidimensionale (più facile da trattare).

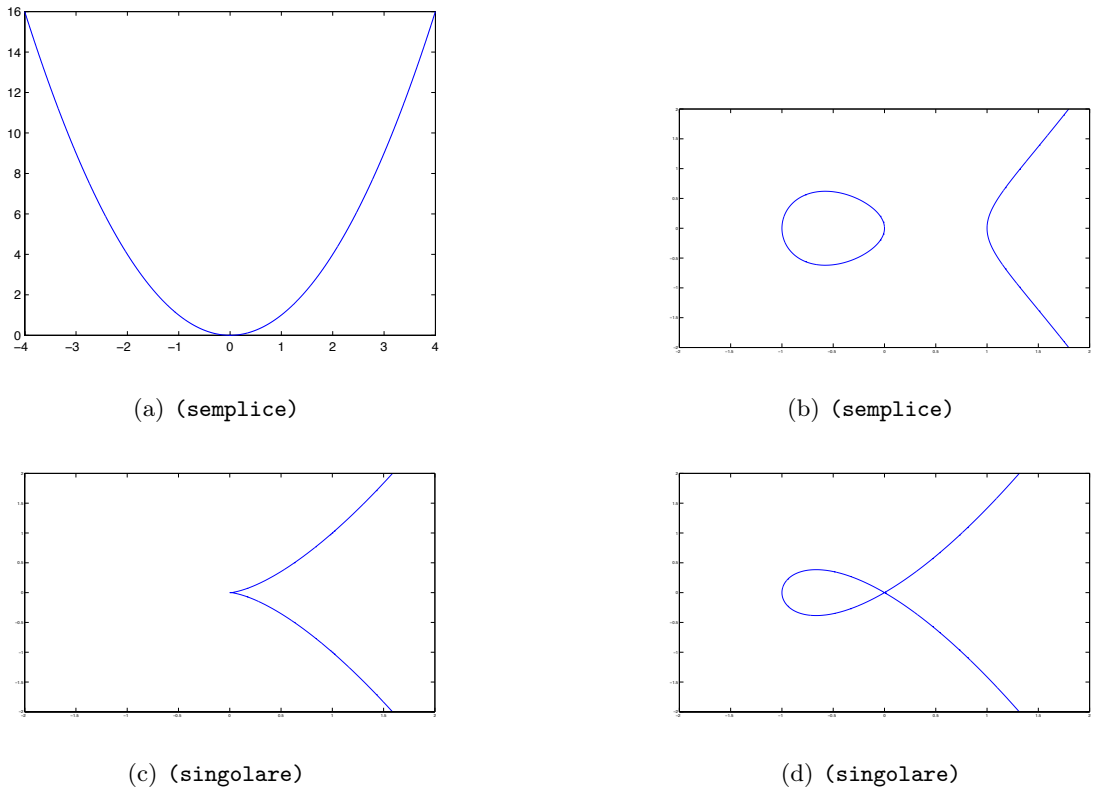
Definizione 3.5.1. Un sottoinsieme W di V si dice sottovarietà algebrica di V se W è una varietà algebrica.

Sia W sottovarietà irriducibile di V e sia $\mathcal{I}(W)$ l'ideale definito da W. La proiezione $\pi(\mathcal{I}(W))$ è ideale di $\Gamma[V]$ e, poichè $\mathcal{I}(W)$ primo lo è anche la sua proiezione. Possiamo considerare l'anello delle frazioni di $\Gamma[V]$ rispetto all'insieme moltiplicativamente chiuso $\Gamma[V] - \pi(\mathcal{I}(W)$. In simboli:

$$K[X_1, ..., X_n] \to \Gamma[V] \to \Gamma[V]_{\Gamma[V]-\pi(\mathcal{I}(W)}$$

dove $\Gamma[V]_{\Gamma[V]-\pi(\mathcal{I}(W)}$ è anello locale con $\pi^e(\mathcal{I}(W)) = \mathcal{M}$ è il suo ideale massimale.

Definizione 3.5.2. La sottovarietà irriducibile W di V si dice semplice su V se l'ideale massimale $\mathcal{M}$ può essere generato da un numero di elementi pari a $dimV - dimW$. In caso contrario si dice singolare.



(a) `(semplice)` (b) `(semplice)`

(c) `(singolare)` (d) `(singolare)`

Figura 3.2: Vari esempi di varietà aventi $P = (0, 0)$ come sottovarietà.

La definizione appena data diventa più facile se V varietà di dimensione uno del piano e W è un punto $\in V$ (assumendo K algebricamente chiuso) (fino alla fine del paragrafo parliamo di varietà del piano).

Definizione 3.5.3. Sia $\mathcal{V}(F)$ una curva, $P = (a, b)$. P è chiamato un punto semplice (sottovarietà semplice) se $F_X(P) \neq 0$ o $F_Y(P) \neq 0$. La curva $F_X(P)(X - a) + F_Y(P)(Y - b)$ viene detta linea tangente (nel caso di P semplice). Un punto che non è semplice viene detto singolare. In realtà anche questa definizione può essere data in senso generale e coincide con quella sopra.

Si può notare che i polinomi omogenei di grado uno dei primi due esempi sono le rette tangenti alle due curve. Noi vogliamo estendere tale fatto, con delle opportune modifiche, anche nel caso di curve singolari in un punto P. Sia $\mathcal{V}((F))$ una curva, $P = (0, 0)$. Possiamo scrivere $F = F_m + ... + F_n$, dove F_i è un polinomio omogeneo di grado i con $F_m \neq 0$.

Definizione 3.5.4. Si definisce m la molteplicità di $\mathcal{V}((F))$ su $P = (0, 0)$, e si scrive $m = m_P(F)$.

F_m è una forma in due variabili, per quanto detto nel capitolo dei polinomi omogenei si ha che:

$$F_m = \prod L_i^{r_i}$$

dove L_i sono rette distinte chiamate rette tangenti ad F nel punto $P = (0, 0)$. Il punto $P = (0, 0)$ si dice un punto multiplo ordinario se tutte le tangenti hanno come molteplicità $r_i = 1$.

Definizione 3.5.5. Sia $\mathcal{V}((F)) \in K[X, Y]$ e $P = (a, b)$ un punto. Si definisce la molteplicità di $\mathcal{V}((F))$ su P come la molteplicità di $\mathcal{V}((F^T))$ con $F^T(X, Y) = F(X + a, Y + a)$ su $(0, 0)$.

3.5.1 Molteplicità e anelli locali

In questa sezione si elencheranno dei risultati che legano la molteplicità di una varietà irriducibile $\mathcal{V}((F))$ con l'anello locale $\mathcal{O}_P(V)$.

Teorema 3.4. *P è un punto semplice di $\mathcal{V}((F))$ se e solo se $\mathcal{O}_P(V)$ è un DVR. In questo caso se $L = a + bX + cY$ è una retta passante per P che non è tangente ad $\mathcal{V}((F))$ in P, allora l'immagine l di L su $\mathcal{O}_P(V)$ è un parametro uniformizzante di $\mathcal{O}_P(V)$.*

Aggiungiamo una proposizione riguardo alle sequenze del capitolo uno perchè abbiamo ora gli strumenti per farlo:

Proposizione 3.6. *Sia A un anello DVR e K un suo sottoanello che è campo isomorfo a A/M dove M è l'ideale massimale del DVR allora:*

1. *$dim_K(M^n/M^{n+1}) = 1$.*
2. *$dim_K(A/M^n) = n \; \forall n > 0$.*
3. *Sia $z \in A$ si ha che $ord(z) = n$ se $(z) = M^n$.*

Dove con $ord(z)$ si intende l'esponente da dare al parametro uniformizzante per ottenere z in simboli $z = ut^n$.

Abbiamo inserito tale proposizione qui perchè $\mathcal{O}_P(V)$ è un $K - modulo$ ed inoltre si può dimostrare che:

Teorema 3.5. *Sia P un punto di una curva irriducibile F. Allora $m_P(F) = dim_K(M_P)^n/M_P)^{n+1}$ per un numero n sufficientemente grande. In particolare la molteplicità di F in P dipende solo dall' anello locale.*

Dimostrazione. Cfr. [2]. □

Osservazione 3.3. Se $\mathcal{O}_P(\mathcal{V}(F))$ è DVR abbiamo dal teorema 3.5 che P è punto semplice.In realtà (nel caso F irriducibile) è vero anche l'implicazione opposta cosa che sarà sfruttata per la molteplicità di intersezione.

Osservazione 3.4. La funzione *ord* usata in 3.6 può essere estesa anche al campo delle frazioni del DVR e, cosa più importante è indipendente dalla scelta del parametro uniformizzante.

3.6 Molteplicità di intersezione

Sfruttando quanto già anticipato nel paragrafo 3.5 si può dare la seguente definizione: Sia V una varietà algebrica , H un ipersuperficie di K^n, definita da (F), che incontra V in una sottovarietà irriducibile e semplice W (serve per DVR).

Definizione 3.6.1. Si definisce molteplicità di intersezione di V (irriducibile) e H lungo W, e si indica con $I(W, V \cap H)$ il numero intero positivo o nullo così definito: sappiamo che l'anello delle frazioni di $\Gamma[V]$ rispetto all'insieme moltiplicativamente chiuso $\Gamma[V] - \pi(\mathcal{I}(W)$ è DVR, pertanto il suo ideale massimale $(M) = (t)$; se H è definita da un polinomio $F \in K[X_1, ..., X_n]$. Così nel DVR si ha $\pi(P) = ut^m$ perchè appartiene al DVR,

$$I(W, V \cap H) = m$$

Questa definizione va bene tranne nel caso in cui V e H hanno una componente in comune che si interseca in W, in tale caso la molteplicità è infinito.

Prima di proseguire bisogna definire il concetto di mappa polinomiale e di cambiamento di coordinate:

Definizione 3.6.2. Siano $V \subset K^n$, $W \subset K^m$. Una funzione $\varphi : V \to W$ è chiamata mappa polinomiale se esistono dei polinomi $T_1, ..., T_m \in K[X_1, ..., X_n]$ per cui

$$\varphi(a_1, ..., a_n) = (T_1(a_1, ..., a_n), ..., T_m(a_1, ..., a_n)) \; \forall \; ((a_1, ..., a_n)) \in V.$$

Definizione 3.6.3. Un cambiamento di coordinate affine su K^n è una mappa polinomiale $T = (T_1, ..., T_m) : K^n \to K^n$ dove ogni polinomio ha grado uno e la funzione è suriettiva e iniettiva.

Se ci limitiamo a considerare varietà di K^2 (K algebricamente chiuso) di dimensione uno che si incontrano su un punto P possiamo definire la molteplicità di intersezione come quel numero che soddisfa i seguenti assiomi:

1. $I(P, F \cap G)$ è un intero non negativo $\forall$ F, G se F, G si intersecano propriamente in P. Infinito in caso contrario (propriamente significa che non hanno componenti in comune che si intersecano su P).

2. $I(P, F \cap G) = 0$ se e solo se $P \notin F \cap G. I(P, F \cap G)$ dipende solo dalle componenti di F e G che passano su P.

3. Se T è un cambiamento affine di coordinate su K^2, e $T(Q) = P$, allora $I(Q, F^T \cap G^T) = I(P, F \cap G)$.

4. $I(P, F \cap G) = I(P, G \cap F)$.

5. $I(P, F \cap G) \geq m_P(F) m_P(G)$, lcon l'uguaglianza che si verifica se e solo se F e G non hanno tangenti in comune.

6. Se $F = \prod F_i^{r_i}$, e $G = \prod G_j^{s_j}$, allora $I(P, F \cap G) = \sum_{i,j} r_i s_j I(P, F_i \cap G_j)$.
7. $I(P, F \cap G) = I(P, F \cap G + AF) \ \forall \ A \in K[X, Y]$.

Teorema 3.6. *Esiste un'unico numero che verifica gli assiomi di cui sopra $I(P, \mathcal{V}((F)) \cap \mathcal{V}((G)))$ definito per ogni F, G, P. È dato da:*

$$I(P, \mathcal{V}(F) \cap \mathcal{V}(G)) = dim_k(\mathcal{O}_P(A^2)/(F, G))$$

N.B 3.1. La moltiplicità di intersezione definita nel caso generale ha bisogno di V e W irriducibili. Invece la seconda, parla solo di punti. Comunque dove sono definite entrambe coincidono.

N.B 3.2. Abbiamo sfruttato (per le varietà del piano) i teoremi del paragrafo riguardo alle varietà irriducibili perchè ci permettono, di identificare una varietà con un polinomio (a meno di fattori unità), nel caso di K algebricamente chiuso.

Ci sono delle proprietà importanti che possono essere immediatamente dimostrate; le altre le vedremo più avanti. Il primo ci permette di capire il legame con l'anello DVR della prima definizione che coincide con $\mathcal{O}_P(\mathcal{V}(F))$ (si riprende dall'osservazione 3.3).

Teorema 3.7. Se P è un punto semplice, allora:

$$I(P, F \cap G) = ord_P^F(G).$$

Si è assunto F irriducibile perchè se non lo fosse, si può scomporlo, ed esiste una sola componente (presente una sola volta) che interseca P visto che P è semplice.

Teorem 3.8. Se F e G sono privi di componenti in comune, allora

$$I(P, F \cap G)$$

Un esempio di calcolo della molteplicità di intersezione:

Esempio 3.3. Calcoliamo la molteplicità di intersezione con $V = \mathcal{V}((Y - X^2))$ $F = X^2 + Y^2 - Y$ sopra la varietà irriducibile $P = \{(0, 0)\}$. Abbiamo che:

$$K[X, Y] \to K[X, Y]/\mathcal{I}(V) = K[X, Y]/(Y - X^2) = K[\overline{X}, \overline{Y}]$$

con $W = (0, 0) = \mathcal{V}((X, Y))$. Sapendo che $\overline{Y} = \overline{X^2}$ si ha che $\mathcal{M} = (\overline{X}, \overline{Y}) = (\overline{X})$ e che il parametro uniformizzante è $t = \overline{X}$.

$$\overline{F} = \overline{X^2} + \overline{Y^2} - \overline{Y} = \overline{X^2} + \overline{X^4} - \overline{X^2} = \overline{X^4}$$

pertanto la molteplicità di intersezione è $m = 4$. Eseguiamo il calcolo utilizzando la definizione per le curve del piano. La prova dell' unicità ci ha dato un metodo costruttivo per portarci a un caso più facile da trattare. Infatti $V(X, 0) = -X^2$, $F(X, 0) = X^2$, poniamo pertanto $H = F - (-V) = Y^2$. Dal teorema si ha che $I(P, V \cap F) = I(P, H \cap V)$ ed inoltre P è punto semplice per $H = Y^2$. Dal teorema 3.7 ci si può riportare al calcolo precedente, invece dal teorema 3.8 dobbiamo calcolare:

$$U = dim_K(K[X, Y]/(H, V))$$

Si vede facilmente che $\overline{Y} = \overline{(X^2)}$ ed inoltre $\overline{Y^2} = \overline{0}$, quindi lo spazio vettoriale ha come base $\overline{1}, \overline{X}, \overline{X^2}, \overline{X^3}$ che ha dimensione quattro.

3.7 Alcuni esempi in K^n

Esempio 3.7.1. Si consideri la varietà $V = \mathcal{V}(I) \subset K^3$, con
$I = (X(X^2 - Z^2)(Z - 1), X(Y - 1)) \subset K[X, Y, Z]$. La varietà V corrisponde al seguente insieme:

$$V = \{(x, y, z) \in K^3 \mid x(x^2 - z^2)(z - 1) = x(y - 1) = 0\}.$$

che dopo semplici passaggi, possiamo scrivere:

$$V = \{x = 0\} \cup \{x - z = y - 1 = 0\} \cup \{x + z = y - 1 = 0\} \cup \{z - 1 = y - 1 = 0\}.$$

Cerco gli ideali che definiscono tali luoghi. $V_1 = \{x = 0\}$ è definito da $I_1 = (x)$, abbiamo che I_1 è primo perchè $K[X, Y, Z]/(X) \cong K[Y, Z]$ e, applicando il teorema degli zeri di Hilbert si ha $\mathcal{I}(\mathcal{V}(I_1)) = I_1$. La dimensione di tale varietà è due. Degli altri tre ne verifichiamo soltanto uno perchè si svolgono in maniera analoga. Prendiamo $V_4 = \mathcal{V}(X + Z, Y - 1)$, vediamo se $I_4 = (X + Z, Y - 1)$ è primo. Si ha che $K[X, Y, Z]/(X + Z, Y - 1) \cong K[X]$, pertanto è primo visto che $K[X]$ è dominio. Come prima, per il teorema degli zeri di Hilbert $\mathcal{I}(\mathcal{V}(I_4)) = I_4$. In questo caso la dimensione è uno. In conclusione si ottiene come scomposizione:

$$V = V_1 \cup V_2 \cup V_3 \cup V_4.$$

con V_1 di dimensione due, V_i con $i = 2, 3, 4$ di dimensione uno. La dimenione di V è due.

Esempio 3.7.2. Consideriamo la curva $C = \{(t, t^2, t^3) \in K^3\}$. Si verifica facilmente che $C = \mathcal{V}(J)$, con $J = (Y - X^2), Z - XY)$. L'anello delle coordinate affini $K[X, Y, Z]/(Y - X^2), Z - XY) \cong K[X]$ è un dominio di integrità, quindi si può applicare il teorema degli zeri di Hilbert, e si ottiene che $\mathcal{I}(\mathcal{V}(I)) = I$. Si vede, sfruttando l'isomorfismo che la dimensione è uno.

Verifichiamo ora che $(0, 0, 0)$ è punto non singolare:

$$K[X, Y, Z] \to K[X, Y, Z]/(Y - X^2, Z - X^3) \to S^{-1}A$$

con $S = K[C] - (X, Y, Z)$. Bisogna che la dimensione dell' ideale massimale sia uno, quindi da $(\frac{\overline{X}}{1}, \frac{\overline{Y}}{1}, \frac{\overline{Z}}{1})$ dobbiamo togliere due generatori (se possibile). Questo si risolve osservando l'ideale di partenza, che ci permette di dire che $\overline{Y} = \overline{X^2}$ e $\overline{Z} = \overline{X^3}$. Ci porta a concludere che l'ideale massimale è generato da $\overline{X}$. Quanto voluto.

Esempio 3.7.3. Sia $V = \mathcal{V}(XY(X - 1), XY(Z - 1))$ una varietà che corrisponde a:

$$\{(x, y, z) \mid xy(x - 1) = xy(z - 1) = 0\}.$$

dopo vari semplici passaggi possiamo scriverlo:

$$\{x = 0\} \cup \{y = 0\} \cup \{x - 1 = z - 1\}.$$

Si risolve in modo analogo a 3.7.1.

Capitolo 4

Varietà Proiettive

4.1 Introduzione allo spazio proiettivo

Vogliamo ora estendere lo spazio affine in modo da ottenere uno spazio nel quale lo studio delle curve algebriche risulti semplificato. Questo ci permetterà di comprendere meglio le varietà affini e, grazie ai punti all'infinito (varietà proiettive) si otterranno dei nuovi teoremi, come il teorema di Bézout.

Definizione 4.1.1. Si definisce spazio poiettivo di dimensione n l'insieme:

$$\mathcal{P}^n(K) = K^{n+1} - \{(0, ..., 0)\}/\text{-}$$

dove - è la relazione di equivalenza così definita:

$$((x_1, ..., x_{n+1}), (y_1, ..., y_{n+1})) \in \text{-} \;\; se (y_1, ..., y_{n+1}) = \lambda(x_1, ..., x_{n+1})$$

per qualche $\lambda \in K$.

Osservazione 4.1. Tale definizione visualizza lo spazio proiettivo come l'insieme delle rette di K^{n+1} passanti per l'origine. Dato un punto $(x, y, z) \in K^{n+1}$ esiste un unica retta passante per quel punto. In sostanza un punto di K^{n+1} è un rappresentante della classe di equivalenza. I punti dello spazio proiettivo sono anche dei sottospazi vettoriali di K^{n+1}. Infatti uno spazio vettoriale di quella partizione verifica gli assiomi di retta e, pertanto ha tutto il diritto di chiamarsi tale.

Gli elementi $\in P^n(K)$ saranno chiamati punti. Se P è determinato da $(x_1, ..., x_{n+1})$ noi diremo che $(x_1, ..., x_{n+1})$ è l'ennupla delle coordinate omogenee. Siano $\mathcal{U}_i = \{(x_1, ..., x_{n+1}) \mid x_i \neq 0\}$.Ogni $P \in \mathcal{U}_i$ possiede un unica coordinata omogenea del tipo $(x_1, ..., x_{i-1}, 1, x_{i+1}, ..., x_{n+1})$. Tale coordinata viene detta anche coordinata non omogenea (si noti il legame con i polinomi omogenei e non). Se definiamo:

$$\varphi_i : K^n \to \mathcal{U}_i$$

come

$$\varphi_i(((x_1, ..., x_n))) = (x_1, ..., x_{i-1}, 1, x_{i+1}, ..., x_{n+1})$$

allora φ_i è una corrispondenza biunivoca. Si noti inoltre che:

$$\mathcal{P}^n(K) = \bigcup_{i=1}^{n+1} \mathcal{U}_i$$

Per quanto detto, lo spazio proiettivo può essere scomposto in molti modi diversi, per convenienza si usa la scomposizione che chiameremo canonica che è la seguente:

$$H_\infty = \mathcal{P}^n(K) - \mathcal{U}_{n+1} = \{(x_1, ..., x_{n+1}) \mid x_{n+1} = 0\}$$

tale insieme, viene spesso chiamato iperpiano all'infinito. Si vede così che lo spazio proiettivo non è nient' altro che l'unione di uno spazio affine e dei punti all'infinito. Ovviamente si poteva scegliere anche un' altra coordinata.

Osservazione 4.2. Quando rappresentiamo i punti dello spazio proiettivo con le coordinate omogenee dobbiamo stare attenti al fatto che sono dei rappresentanti, se definiamo un insieme in questo modo:

$$V = \{(x_1, ..., x_{n+1}) \mid \mathcal{P}((x_1, ..., x_{n+1}))\}$$

dove $\mathcal{P}((x_1, ..., x_{n+1}))$ è una propietà che un punto può avere o meno, tale propietà preferibilmente non deve dipendere dalla scelta dei rappresentanti. Esempio l'insieme $\{(x, y, z) \mid y^2 = x^2 + z^2\}$ è ben posta perchè se (x, y, z) verifica la propietà, tale propietà è verificata anche da tutti gli altri rappresentanti. Invece l'insieme $\{(x, y, z) \mid y^2 = x^2 + z\}$ dipende dai rappresentanti. L'unico modo di intendere il secondo insieme è quello di pensare, che ci stiamo riferendo a tutti i rappresentanti. Se un elemento ha alcuni che verificano la propietà e altri rappresentanti no allora non sta nel insieme. Partendo da un polinomio non-omogeneo, l'omogeneizzazione permette di definire un' insieme in modo indipendente dai rappresentanti, proprio quanto voluto.

4.1.1 Varietà proiettive

In questa sottosezione costruiremo l'idea delle varietà proiettive. Noteremo fin da subito i forti legami esistenti con quelle affini.

Definizione 4.1.2. Un punto $P = (x_1, ..., x_{n+1})$ si dice zero di un polinomio $F \in K[X_1, ..., X_{n+1}]$ se $F(x_1, ..., x_{n+1}) = 0$ per qualsiasi scelta delle coordinate omogenee $(x_1, ..., x_{n+1})$.

Definizione 4.1.3. Come nel caso affine , definiamo varietà proiettiva il luogo degli zeri di un ideale I di $K[X_1, ..., X_{n+1}]$. Si riduce agli zeri di un numero finito di polinomi vista la notherianità dell'anello dei polinomi.

Riprendendo quanto fatto nel caso affine usiamo anche le stesse notazioni per $\mathcal{V}(I)$ e $\mathcal{I}(V)$ solo che ora, aggiungiamo i pedici sia per il caso proiettivo che per quello affine per poterli distinguere. Di importanza fondamentale questa definizione e la successiva proposizione:

Definizione 4.1.4. Un' ideale I di $K[X_1, ..., X_{n+1}]$ è omogeneo se per ogni polinomio $\in I$ tutti i polinomi omogenei della sua scomposizione appartengono all'ideale.

Lavorare su ideali omogenei permette di dimenticarsi del fatto che, in realtà si usano dei rappresentanti.

Proposizione 4.1. *Un ideale $I \subset K[X_1, ..., X_{n+1}]$ è omogeneo se e solo se è generato da un numero finito di polinomi omogenei.*

Il concetto di irruducibilità è analogo a quanto visto nel caso affine.

Definizione 4.1.5. Una varietà proiettiva si dice irriducibile se non è l'unione di due più piccole (strettamente) varietà.

Si dimostra in modo simile alle varietà affini che:

Proposizione 4.2. *Se V è irriducibile $\Rightarrow$ $\mathcal{I}(V)$ è primo.*

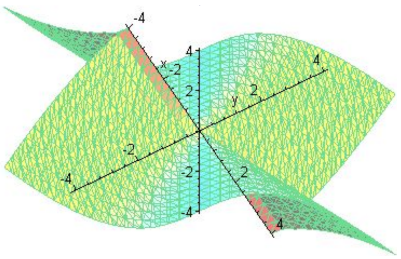
Osservazione 4.3. Un punto $P = (x_1, ..., x_{n+1})$ del piano proiettivo lo possiamo rappresentare così $(\frac{x_1}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_{n+1}}{x_i})$ qualunque scelta di i. Si chiamano anche coordinate demogeneizzate.

Un esempio di varietà proiettiva demogeneizzando poi il polinomio che la definisce per tutte le coordinate possibili.

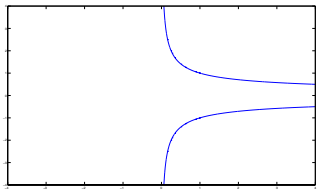
Esempio 4.1. Si consideri come esempio la cubica proiettiva definita dal polinomio omogeneo $P(X, Y, Z) = YZ^2 - X^3$. La varietà proiettiva demoneigizzando il polinomio individua tre varietà affini del piano:

1. $\mathcal{V}_a((YZ^2 - 1))$.
2. $\mathcal{V}_a((Z^2 - X^3))$.
3. $\mathcal{V}_a((Y - X^3))$.

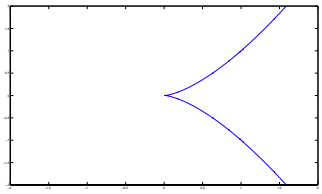
i vari disegni in figura



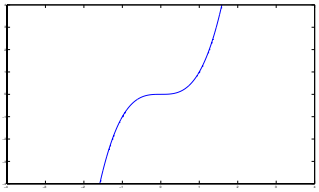
(a) `cubica`



(b) `prima`



(c) `seconda`



(d) `terza`

Figura 4.1: Le tre varietà affini.

4.2 Varietà affini e proiettive

In questo paragrafo cercheremo di legare i due tipi di varietà.

Se V è una varietà proiettiva di $\mathcal{P}^n(K)$ noi definiamo:

$$\mathcal{C}(V) \doteq \{(x_1, ..., x_{n+1}) \in K^{n+1} \mid (x_1, ..., x_{n+1}) \in V \; o \; (x_1, ..., x_{n+1}) = 0\}$$

chiamato cono sopra V(è una varietà affine). Se $V \neq \emptyset$, allora $\mathcal{I}_a(\mathcal{C}(V)) = \mathcal{I}_p(V)$; e se I è un ideale omogeneo di $K[X_1, ..., X_{n+1}]$ e $\mathcal{V}_p(I) \neq \emptyset$,allora $\mathcal{C}(\mathcal{V}_p(I)) = \mathcal{V}_a(I)$. Come già anticipato questo semplifica molte domande nello spazio proiettivo in quello affine. Come nel capitolo precedente K in linea di massima algebricamente chiuso.

Teorema 4.1. *Sia I un ideale omogeneo di $K[X_1, ..., X_{n+1}]$. Allora*

1. *$\mathcal{V}_p(I) = \emptyset$ se e solo se esiste un intero $N \mid I$ contiene tutti i polinomi omogenei di grado $> N$.*
2. *se $\mathcal{V}_p(I) \neq \emptyset$, allora $\mathcal{I}_p(\mathcal{V}_p(I)) = \sqrt{I}$.*

Dimostrazione. Cfr. [2]. □

Anche tutti i corollari del teorema sono corretti, bisogna però fare alcune eccezioni, ad esempio per l'ideale $(X_1, ..., X_{n+1})$, perchè l'unico zero è l'ennupla nulla, pertanto non ha zeri nello spazio proiettivo e quindi non si applica il teorema. In particolare esiste una corrispondenza suriettiva e iniettiva tra le ipersuperfici di $\mathcal{P}^n(K)$ e i polinomi omogenei non costanti. Le ipersuperfici irriducibili sono in corrispondenza con i polinomi omogenei irriducibili.

Sia V varietà proiettiva irriducibile. $\mathcal{I}_p(V)$ è un ideale primo, pertanto l'anello $\Gamma[V] = K[X_1, ..., X_{n+1}]/\mathcal{I}_p(V)$ è un dominio di integrità. È chiamato anello delle coordinate omogenee.

Più in generale senza pretendere che la varietaà proiettiva sia irriudicbile (nemmeno K algebricamente chiuso). Un elemento $f \in \Gamma[V]$ si dice elemento omogeneo di grado d se esiste un polinomio omogeneo del medesimo grado F tale che $\overline{F} = f$. Proprio per colpa dei rappresentanti bisogna sistemare una complicazione che nel caso affine non si poteva presentare.

Sia $\Gamma_h(V)$ il campo delle frazioni di $\Gamma[V]$. Contrariamente a quanto accadeva nel caso affine i suoi elementi non possono essere pensati come funzioni su V perchè dipendono dai rappresentanti però se f, g sono entrambi elementi omogenei dello stesso grado d allora $\frac{f}{g}$ non dipende dai rappresentanti e pertanto è una funzione su V ben posta (al denominatore non deve mai esserci lo zero). Definiamo $\Gamma(V)$ in queso modo:

$$\{z \in \Gamma_h(V) \mid z = \frac{f}{g} \; per \; qualche \; f, g \; con \; stesso \; grado\}$$

Sia $P \in V$, $z \in \Gamma(V)$. Noi diciamo che z è definito su P se z può essere scritto come $z = \frac{f}{g}$, f, g omogenei di grado d, e $g(P) \neq 0$.Noi definiamo in modo analogo a quanto fatto per le varietà affini:

$$\mathcal{O}_P(V) = \{z \in \Gamma(V) \mid z \; definito \; su \; P\}$$

è un anello locale e il suo ideale massimale è:

$$M_P = \{z \mid z = \frac{f}{g}, g(P) \neq 0, f(P) = 0\}$$

4.2.1 Legame tra K^n e $\mathcal{P}^n(K)$

Riprendiamo e definiamo con maggior rigore quanto visto nel primo esempio di questo capitolo. Cioè poniamo l'attenzione tra lo spazio affine e proiettivo della medesima dimensione.

All'inizio del capitolo abbiamo visto che possiamo considerare K^n sottoinsieme di $\mathcal{P}^n(K)$ proprio grazie alla funzione $\varphi_{n+1} : K^n \to \mathcal{U}_{n+1}$.

Sia V una varietà affine , $I = \mathcal{I}_a V$. Sia I^* l'ideale di $K[X_1, ..., X_{n+1}]$ generato da $\{F^* \mid F \in I\}$. I^* è un ideale omogeneo; noi definiamo V^* come $\mathcal{V}_p(I^*)$. Viceversa , sia V varietà proiettiva e $I = \mathcal{I}_p(V)$. Sia I_* l' ideale in $K[X_1, ..., X_n]$ generato da $\{F_* \mid F \in I\}$. Noi definiamo V_* come $\mathcal{V}_a(I_*)$. Si ha la seguente proposizione di importanza fondamentale.

Proposizione 4.3. *Valgono:*

1. *Se $V \subset K^n$, $\varphi_{n+1}(V) = V^* \cap \mathcal{U}_{n+1}$ e $(V^*)_* = V$.*
2. *Se $V \subset W \subset K^n$, allora $V^* \subset W^* \subset \mathcal{P}^n$. Se $V \subset W \subset \mathcal{P}^n$, allora $V^* \subset W^* \subset K^n$.*
3. *Se V è irriducibile in K^n, allora V^* è irriducibile.*
4. *Se $V = \bigcup_{i=1} V_i$ è la sua scomposizione irriducibile,allora $V^* = \bigcup_{i=1} V_i^*$ è la scomposizione di V^*.*
5. *Se $V \subset K^n$, allora V^* è la più piccola varietà di $\mathcal{P}^n$ che contiene V.*
6. *Se $V \subset\neq K^n$, allora nessuna sua componenete si trova in o contiene H_∞.*
7. *Se $V \subset \mathcal{P}^n$,e nessuna componente di V si trova in o contiene H_∞, allora $V_* \subset\neq K^n$ e $(V_*)^* = V$.*

V^* viene anche chiamata chiusura proiettiva di V. Si può notare che esiste una corrispondenza biunivoca (tranne per le varietà che si trovano in H_∞).

Sia V una varietà affine irriducibile, V^* la sua chiusura proiettiva. Se $f \in \Gamma_h[V^*]$ è un elemento omogeneo di grado d noi possiamo definire $f^* \in \Gamma[V]$ nel seguente modo: si sceglie un polinomio F che è il rappresentante del laterale f si calcola F^* e si definisce f^* il suo laterale(è indipendente dalla scelta del laterale).Noi possiamo definire un isomorfismo naturale:

$$\alpha : \Gamma(V^*) \to \Gamma(V)$$

Se $P \in V$, possiamo considerare $P \in V^*$(grazie a φ_{n+1}) e α induce un isomorfismo tra i due anelli locali $\mathcal{O}_P(V)$, $\mathcal{O}_P(V^*)$.

Osservazione 4.4. Partendo da una varietà affine F, omogeneizzando rispetto ad una variabile troviamo una varietà proiettiva F^*; demogeneizzando rispetto alla stessa variabile otteniamo la varietà affine F. Non è invece detto il contrario ad esempio scegliamo $F_P = \mathcal{V}((Z))$ demogeneizzando rispetto alla variabile Z otteniamo la varietà affine $\mathcal{V}((1)) = \emptyset$. Se ora omogeneizziamo, otteniamo sempre l'insieme vuoto (come varietà proiettiva). Quanto detto sopra non significa che presa una varietà proiettiva la demogenizzazione porta ad una varietà affine con il campo delle funzioni isomorfo a quello proiettivo.

4.3 Varietà proiettive nel piano $P(K^2)$

In questo paragrafo cerchiamo di sfruttare le definizioni del capitolo 3, e il legame trovato nei paragrafi precedenti per caratterizzare le varietà proiettive del piano $\mathcal{P}^2$. Si può immediatamente notare che una curva proiettiva è rappresentata da un polinomio omogeneo non costante e ogni polinomio da lui ottenuto moltiplicato per uno scalare definisce la medesima curva, quindi possiamo affermare, che esiste una corrispondenza tra le curve proiettive e la classi di equivalenza dei polinomi omogenei. Dove due polinomi P, Q appartengono alla stessa classe di equivalenza se esiste uno scalare $\lambda \mid P = \lambda Q$. Ora alcune importanti definizioni:

Definizione 4.3.1. Sia $\mathcal{V}_p((F))$ una varietà proiettiva (assumiamo senza perdita di generalità F omogeneo) e sia $P \in \mathcal{P}^2$, scegliamo un $\mathcal{U}_i \mid P \in \mathcal{U}_i$ e domogeneizziamo F rispetto all' $i - esima$ componente. Definiamo la molteplicità

$$m_P(F) = m_P(F_*)$$

la molteplicità è indipendente dalla scelta di i.

Definizione 4.3.2. Siano F, G curve piane proiettive, $P \in \mathcal{P}^2$. Noi definiamo molteplicità di intersezione in questo modo:

$$I(P, F \cap G) = dim_k(\mathcal{O}_P(\mathcal{P}^2)/(F_*, G_*))$$

dove in realtà abbiamo usato un l'isomorfismo definito sopra che ci permette di scrivere $\mathcal{O}_P(\mathcal{P}^2)$ al posto di $\mathcal{O}_P(K^2)$.

Osservazione 4.5. La definizione di punto semplice è rimandata al caso affini ma, si può dimostrare che se F (sempre omogeneo) è una curva proiettiva un punto P è punto multiplo se e solo se $F(P) = F_X(P) = F_Y(P) = F_Z(P) = 0$. Nel caso in cui P per F sia un punto semplice la tangente in P è data da $F_X(P)(X) + F_Y(P)(Y) + F_Z(P)(Z)$.

Si considerano spesso gli insiemi formati da tutte le curve di uno stesso grado d. Sia $M_1, ..., M_N$ un ordine definito dei monomi X, Y, Z di grado d, dove $N = \frac{1}{2}(d+1)(d+2)$. Data una curva F, essendo F omogeneo di grado d , si può scrivere $F = a_1M_1 + ... + a_NM_N$. Considerando però che anche ogni polinomio moltiplicato per uno scalare determina la medesima curva. Si capisce subito che un polinomio individua una classe di equivalenza, cioè proprio un punto proiettivo $\in \mathcal{P}^{\frac{1}{2}(d)(d+3)}$. Pertanto esiste una corrispondenza biunivoca.

Osservazione 4.6. Nel caso affine è possibile dimostrare cfr. [2] che una retta L è tangente ad una curva del piano F in un punto P se e solo se $I(P, F \cap L) > m_P(F)$. Sfruttiamo tale fatto per estenderlo al caso proiettivo. Noi diremo che una retta $L \in \mathcal{P}^2$ è tangente ad una curva F nel punto P se vale quanto già detto nel caso affine in simboli:

$$I(P, F \cap L) > m_P(F).$$

Esempio 4.2. Ogni retta proiettiva $aX + bY + cZ$ corrisponde al punto $(a, b, c) \in \mathcal{P}^2$. In sostanza le rette dello spazio proiettivo formano lo spazio proiettivo.

4.3.1 Teorema di Bézout

Teorema (Bézout) 4.2. *Siano F, G due curve piane proiettive senza componenti in comune di grado m,n rispettivamente. Allora*

$$\sum_P I(P, F \cap G) = mn$$

Dimostrazione. Cfr. [2]. □

Si possono dimostrare i seguenti corollari sfruttando la propietà (5) della molteplicità di intersezione:

Corollario 4.1. *Se F e G non hanno componenti in comune, allora*

$$\sum_P m_P(F) m_P(G) \leq mn$$

dove m, n i gradi rispettivamente di F, G.

Corollario 4.2. *Se F e G si intersecano in un numero pari a mn di punti, allora tutti tali punti sono semplici.*

Corollario 4.3. *Se due curve di grado m ed n hanno più di mn punti in comune, allora hanno almeno una componente in comune.*

Un semplice esempio considerando delle coniche per capire il significato geometrico del teorema di Bézout.

Esempio 4.3. Il teorema di Bézout afferma che il numero di punti di intersezione contati con le dovute molteplicità, nel caso delle coniche è quattro. Queste sono le varie situazioni che possono accadere:

1. quattro punti distinti, tutti punti semplici (vedi corollario due).
2. tre punti distinti,uno doppio due semplici.
3. due punti distinti, due doppi.
4. due punti distnti, uno triplo uno semplice.
5. un punto distinto, punto quadruplo.

4.3.2 Teorema di Max Noether

Un zero-ciclo su P^2 è una somma formale $\sum_{P \in P^2} n_P P$, dove n_P è un numero intero. Il grado di una zero-ciclo $\sum n_P P$ è definito come la somma dei coefficienti. Siano F, G due curve piane proiettive di grado n, mrispettivamente. Noi definiamo il ciclo di intersezione $F.G$ come:

$$\sum_{P \in P^2} I(P, F \cap G) P.$$

Sia $P \in \mathcal{P}^2$, F, G curve, senza componenti in comune passanti per P e H un' ulteriore curva. Si dice che le condizioni di Noether sono soddisfatte in P se $H_* \in (F_*, G_*) \subset \mathcal{O}_P(\mathcal{P}^2)$.

Teorema(Max Noether) 4.3. *Siano F, G, H curve piane proiettive con F e G senza componenti in comune (passanti nei punti $\in F \cap G$). Allora esiste un' equazione $H = AF + BG$ se e solo se le condizioni di Noether sono verificate $\forall$ $P \in F \cap G$.*

Dimostrazione. Cfr. [2]. □

Abbiamo bisogno, per poter utilizzare il teorema, di un criterio per la condizione di Noether.

Proposizione 4.4. *Siano F, G, H curve piane proiettive, $P \in F \cap G$. La condizione di Noether è soddisfatta se e solo se una qualsiasi di queste è vera:*

1. *P è un punto semplice di F, e $I(P, H \cap F) \geq I(P, G \cap F)$.*
2. *F e G hanno tangenti distinte in P,e $m_P(H) \geq m_P(F) + m_P(G) - 1$.*

Dimostrazione. Cfr. [2]. □

Alcune conseguenze del teorema di Bézout e del teorema fondamentale di Max Noether.

Proposizione 4.5. *Siano C e C' due cubiche, $C'.C = \sum_{i=1}^{9} P_i$; supponiamo Q una conica e $Q.C = \sum_{i=1}^{6} P_i$. Assumiamo $P_1, ..., P_6$ punti semplici di C. Allora P_7, P_8, e P_9 giacciono sulla stessa retta.*

Dimostrazione. Sia $F = C$,$G = Q$,$H = C'$ da 4.3.1 sappiamo sono semplici e la 4.4 ci garantisce che è soddisfatta la condizione di $Noether$, dunque $H = AF + BG$ con $A = costante$, invece B forma di grado uno pertanto $H = BG$, H e G si intersecano per forza in $P_1, ..., P_6$ quindi P_7, P_8, P_9 sono zeri di B, che è una retta. □

Teorema 4.4. *Se un esagono proiettivo è inscritto in una conica allora i punti d' intersezione dei lati opposti dell'esagono sono allineati.*

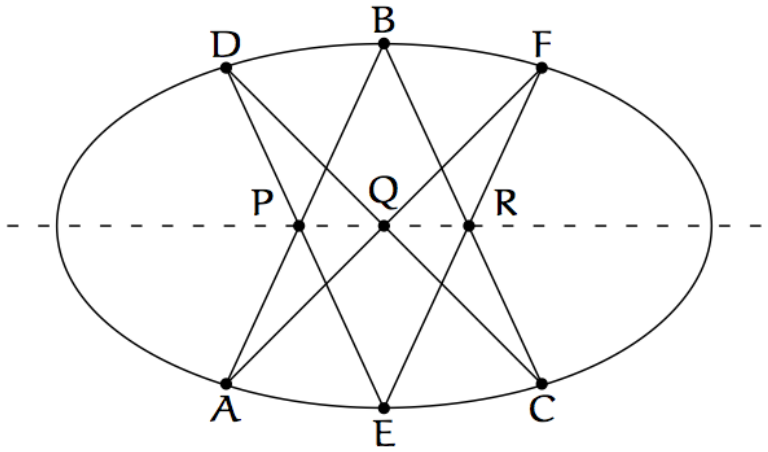
Dimostrazione. Nel caso di una conica irriducibile, scegliamo le due coniche C,C' nel seguente modo:

$$C = \overline{AB} \cup \overline{EF} \cup \overline{CD},\ C' = \overline{DE} \cup \overline{BC} \cup \overline{FA}.$$

che si intersecano in nove punti:

$$C \cap C' = \{A, B, C, D, E, F, P, Q, R\}.$$

da 4.5 abbiamo che una retta passa per P, Q, R quindi i punti dell' esagono sono allineati. □



(a) `Pascal`.

4.4 Spazio proiettivo multiplo

Nel caso affine si può facilmente considerare il prodotto cartesiano tra due spazi affini $K^n \times K^m$ come lo spazio affine K^{n+m}. Nel caso proiettivo la questione non è altrettanto facile, bisogna fare alcune considerazioni e generalizzare un pò la teoria.

Definizone 4.4.1. Un polinomio $K[X_1, ..., X_n, Y_1, ..., Y_n]$ si dice biomogeneo di grado (p, q) se F è un polinomio omogeneo se considerato come polinomio in $X_1, ..., X_n$ $(Y_1, ..., Y_m)$ con coefficienti in $K[X_1, ..., X_n](K[Y_1, ..., Y_m])$.

Come nel caso dei polinomi omogenei ogni polinomio si può scrivere in modo unico come somma di polinomi biomogenei.Si definisce varietà proiettiva nel caso multiplo un sottoinsieme di $P^n \times P^m$ che è zero di un ideale di $K[X_1, ..., X_{n+1}, Y_1, ..., Y_m]$ cioè se
$I = (F_1(X_1, ..., X_{n+1}, Y_1, ..., Y_{m+1}), ..., F_r(X_1, ..., X_{n+1}, Y_1, ..., Y_{m+1}))$ $\mathcal{V}(I)$ è l'insieme così definito:

$$\{(x_1, ..., x_{n+1}, y_1, ..., y_{m+1} \mid F(x_1, ..., x_{n+1}, y_1, ..., y_{m+1}) = 0 \; qualunque \; F \; di \; I\}$$

Possiamo definire tutto quanto fatto nel caso proiettivo ad esempio l'anello delle coordinate di una varietà V di $\mathcal{P}_n \times \mathcal{P}_m$:

$$\Gamma[V] = K[X_1, ..., X_{n+1}, Y_1, ..., Y_{m+1}]/\mathcal{I}(V)$$

ecc ecc. Come si vede è più generale di prima e, coincide ovviamente con la precedente quando non c'è il prodotto cartesiano. Si può fare il prodotto cartesiano anche in questo modo $\mathcal{P}^n \times \cdots \times \mathcal{P}^m \times K^s$.

Capitolo 5

Singolarità

Questo capitolo sfrutterà la classificazione birazionale delle curve per far scoppiare le singolarità di una curva affine o proiettiva del piano. L'idea di base è quella di trovare una curva del piano birazionalmente equivalente a quella di partenza che però non presenta più le singolarità. Iniziamo con il caso affine che è più semplice.

5.1 Scoppiare singolarità in K^2

In questa sezione ci occuperemo di far scoppiare le singolarità nel piano affine, facendo vari esempi elementari.

Sia $P = (0,0)$. Sia $U = \{(x,y) \in K^2 \mid x \neq 0\}$. Definiamo il seguente morfismo $f : U \to K, f(x,y) = \frac{y}{x}$. Sia G il grafico di f cioè $G = \{(x,y,z) \in K^3 \mid y = xz, x \neq 0\}$ e $B = \{(x,y,z) \in K^3 \mid y = xz\}$. Sia $\pi : B \to K^2$ la restrizione a B della proiezione di K^3 su K^2. Si noti che $\pi^{-1}(U) = \{(0,0,x) \mid z \in K\} = L$ è una retta passante per l'origine.

Sia $\varphi : K^2 \to B$ definita nel seguente modo $\varphi(x,y) = (x,xz,z)$. φ è un isomorfismo. Sia $\psi = \pi \circ \varphi$. Abbiamo definito tutti gli strumenti per ottenere una curva birazionalmente equivalente a quella di partenza.

Sia C una curva irriducibile di K^2. Sia $C_0 = C \cap U$ un aperto di C, sia $C_0' = \psi_{-1}(C_0)$, e sia C' la chiusura di C_0' in K^2. Si ha che $f : C' \to C$ la restrizione di ψ in C' è un morfismo birazionale da C' a C (ricordo che f è un rappresentante della mappa razionale). Si ha pertanto che C' e C sono birazionalmente equivalenti, ed inoltre abbiamo:

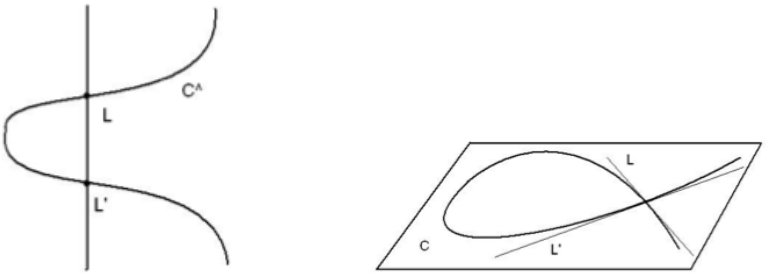
Proposizione 5.1. *Sia $C = \mathcal{V}((F))$ una curva individuata da F (come sopra), F lo possiamo scrivere in modo unico come somma di polinomi omogenei $F = F_s + F_{s+1} + ... + F_n$ in $K[X,Y]$. Allora $C' = \mathcal{V}((F'))$, dove $F' = F_s(1,Z) + XF_{s+1}(1,Z) + ... + X^{n-s}F_n(1,Z)$.*

Proposizione 5.2. *Sia $C = \mathcal{V}((F))$ una curva individuata da F (come sopra), $f^{-1}(P) = \{P_1, ..., P_r\}$ dove $P_i = (0,a_i)$, e $m_{P_i}(C') \leq I(P_i, C' \cap E)$ con $E = \{(x,z) \in K^2 \mid x = 0\} = s_i$. Se P è punto singolare ordinario di C, allora ogni P_i è punto semplice su C'.*

Il procedimento esposto sopra funziona anche nel caso riducibile, i teoremi si possono estendere scegliendo un polinomio F senza componenti multiple.

Qui quattro esempi che mettono in pratica il procedimento illustrato anche nel caso di curva riducibile.

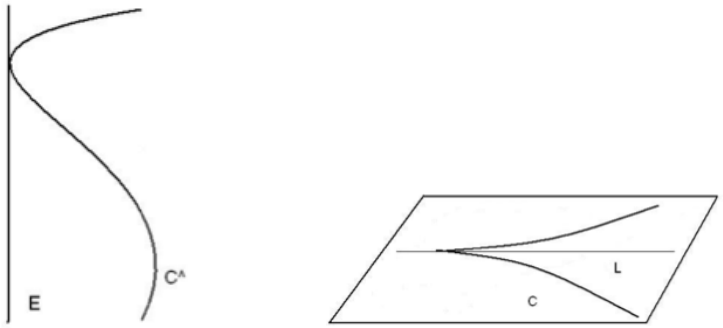
Esempio 5.1.1. Riprendiamo la curva $C = \mathcal{V}((F))$ con $F = Y^2 - X^2(X+1)$, come già anticipato presenta una singolarità nel punto $P = (0,0)$. Dobbiamo innanzitutto calcolare la sua controimmagine (escludendo i punti con $x = 0$) rispetto alla funzione π. Il calcolo porta ad un sottoinsieme della varietà generata dall' ideale $I = (Y - XZ, Y^2 - X^2(X+1))$ (bisogna togliere i punti in cui $x = 0$). Scomponendo la varietà in questo modo $\mathcal{V}(I) = \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$ con $I_1 = (Y - XZ, Z^2 - X - 1)$ e $I_2 = (Y - XZ, X^2)$, si capisce subito che I_2 va escluso e la chiusura dell'insieme corrisponde con $\mathcal{V}(I_1)$. Si è così ottenuta una nuova varietà (curva di K^3) che non presenta più singolarità in $P = (0,0)$. Possiamo infine riportarci ad una curva di K^2 senza la singolarità calcolando $\varphi^{-1}(\mathcal{V}(I_1)) = \mathcal{V}((Z^2 - X - 1))$ che corrisponde ad una parabola.



(b) (c)

Figura 5.1: Il punto P viene associato a $(0,0,1)$ e a $(0,0,-1)$.

Esempio 5.1.2. In questo esempio risolviamo la singolarità sempre in $P = (0,0)$ della curva $C = \mathcal{V}(Y^2 - X^3)$. La controimmagine $\pi^{-1}(C \cap U)$ è un sottoinsieme di $\mathcal{V}((Y - XZ, Y^2 - X^3)) = \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$ con $I_1 = (Y - XZ, Z^2 - X)$ e $I_2 = (Y - XZ, X^2)$ che come nel caso precedente va eliminato e, si ha che la chiusura coincide con $\mathcal{V}(I_1)$ (curva di K^3). Calcolando $\varphi^{-1}(\mathcal{V}(I_1)) = \mathcal{V}((Z^2 - X))$ otteniamo una curva di K^2 senza singolarità.



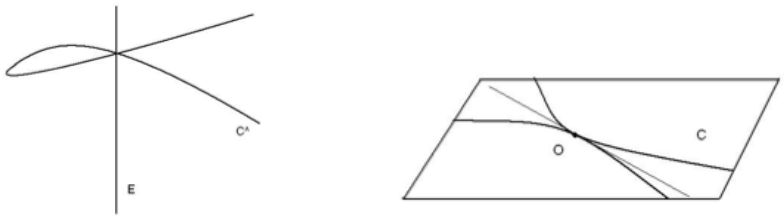
(a) (b)

Figura 5.2:

Osservazione 5.1. Prima di fare il terzo esempio è importate notare che quanto fatto all'inizio del capitolo si può ripetere ponendo $y \neq 0$ al posto di x. In sostanza possiamo definire $U = \{(x,y) \in K^2 \mid y \neq 0\}$, $f : U \to K, f(x,y) = \frac{x}{y}$, $B = \{(x,y,z) \in K^3 \mid x = yz\}$ ecc ecc.

Esempio 5.1.3. Con il terzo esempio, vediamo un caso in cui il punto singolare $P = (0,0)$ non è ordinario, quindi non vengono rispettate le ipotesi di 5.2. Consideriamo dunque la curva $C = \mathcal{V}(X^2 - X^4 - Y^4)$ che ha un unica tangente in $P = (0,0)$ di molteplicità 2. Eseguiamo quanto già

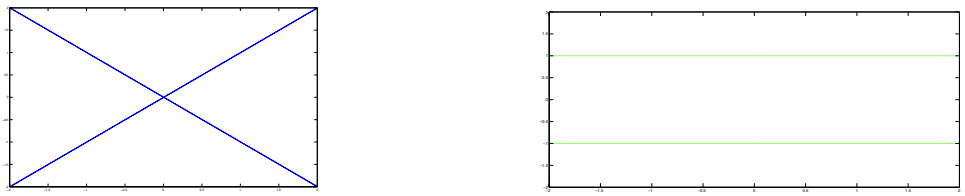
fatto negli esempi precedenti; la controimmagine è contenuta in $\mathcal{V}((X - YZ, X^2 - X^4 - Y^4))$ e, la sua chiusura corrisponde a $\mathcal{V}((X - YZ, Y^2 - Z^2 - Y^2Z^4))$. La sottovarietà $P' = (0,0,0) = \mathcal{V}(X,Y,Z)$ non è semplice perchè la l'ideale massimale dell'anello locale è generato da $\overline{Y}, \overline{Z}$ e il numero di generatori minimo è pari a $2 \neq 1 = dim\mathcal{V}((X - YZ, Y^2 - Z^2 - Y^2Z^4)) - dim\mathcal{V}(X,Y,Z)$. Quindi lo scoppiamento non ha risolto la singolarità.



(a) (b)

Figura 5.3:

Esempio 5.1.4. Trattiamo ora una singolarità di una curva riducibile. Sia $P = (0,0)$ e $C = \mathcal{V}((Y^2 - X^2))$. La chiusura della controimmagine è $\mathcal{V}((Y - XZ, Z^2 - 1))$ due rette passanti per il punto $(0,0,1)$ e $(0,0,-1)$ rispettivamente. Tali due rette possono essere proiettate su un piano ed otteniamo $\mathcal{V}((Z^2 - 1))$ che è la varietà del piano birazionalmente equivalente a quella di partenza priva di singolarità.



(a) (b)

Figura 5.4:

5.2 Scoppiare singolarità in $\mathcal{P}^2$

In questo paragrafo cercheremo di capire come scoppiare i punti di P^2 relativi ad una varietà proiettiva. Come prima, diamo innanzitutto alcune definizioni.

Sia $U = \mathcal{P}^2 - \{P_1, ..., P_t\}$ con $P_i = (a_{i1}, a_{i2}, a_{i3}) \in \mathcal{P}^2$. Definiamo $f_i : U \to \mathcal{P}^1$ un morfismo.Sia $f = (f_1, ..., f_t)$ e sia G il grafico di f. Siano X_1, X_2, X_3 le coordinate omogenee per $\mathcal{P}^2$; Y_{i1}, Y_{i2} le coordinate omogenee della i-esima copia di $\mathcal{P}^1$. Sia $B = \mathcal{V}((Y_{i2}(X_2 - a_{i2}X_3 - Y_{i1}(X_1 - a_{i1}X_3)) \subset \mathcal{P}^2 \times \mathcal{P}^1 \times \cdots \times \mathcal{P}^1$ che è la chiusura di G. Sia $\pi : B \to \mathcal{P}^2$ la restrizione della proiezione a B.

Sia C una curva irriducibile di $\mathcal{P}^2$. Sia $C_0 = C \cap U$, $C_0' = \pi^{-1}(C_0)$, e sia C' la chisura di C_0' in B. π ristretto a C' è un morfismo birazionale tra C' a C. Si ha la seguente proposizione:

Proposizione 5.3. *Sia C una curva piana irriducibile con tutti i punti multipli ordinari (tutti con tangenti distinte). Allora esiste una curva C' non singolare e un morfismo birazionale f da C' a C.*

Dimostrazione. Si dimostra sfruttando quanto detto nel paragrafo precedente e utilizzando il procedimento appena illustrato cfr. [2]. □

Osservazione 5.2. Tutto quanto come nel caso affine è vero nel caso in cui F è priva di componenti multiple, quindi per tutte le curve. Non serve la irriducibilità.

Non sempre le singolarità si risolvono così facilmente, riprendendo l'esempio 5.1.3 si nota che nel caso di punti non ordinari, sebbene la singolarità sia migliorata rispetto a quella di partenza, non si è risolta. Si potrebbe pensare di modificare il procedimento per poter considerare curve di spazi di dimensione maggiore, anche se è possibile, non è la via più facile. La soluzione che mostreremo, permette di elaborare preventivamente la curva, trovandone un'altra che possiede solamente punti ordinari.

Siano $P = (0, 0, 1)$, $P' = (0, 1, 0)$, $P'' = (1, 0, 0) \in \mathcal{P}^2$. Chiamiamo questi tre punti i punti fondamentali. Le tre rette $L = \mathcal{V}((Z))$, $L' = \mathcal{V}((Y))$, $\mathcal{V}((X))$ sono chiamate le rette eccezionali. Definiamo il morfismo $Q : \mathcal{P}^2 - \{P, P', P''\} \to \mathcal{P}^2, Q(x, y, z) = (yz, xz, xy)$, che chiameremo trasformazione quadratica standard. Sia C una curva piana irriducibile ($\in \mathcal{P}^2$) che non sia una retta eccezionale. Allora $C \cap U$ è aperto in C, e chiuso in U. Sia C' la chisura di $Q^{-1}(C \cap U)$ in $\mathcal{P}^2$.Q è un morfismo birazionale tra $C' - \{P, P', P''\}$ e C.

Osservazione 5.3. La curva C' è birazionale a C.

Dimostrazione. Abbiamo che $Q : Q^{-1}(C \cap U) \to C \cap U$ è un isomorfismo, pertanto abbiamo trovato il morfismo birazionale. □

Noi diremo che C è in buona posizione se nessuna retta eccezionale è tangente a C nei punti fondamentali cfr. 4.6.

Esempio 5.2.1. Mostriamo che la curva $F = 8X^3Y + 8X^3Z + 4X^2YZ - 10XY^3 - 10XY^2Z + 3Y^3Z$ è in buona posizione. Per farlo bisogna semplicemente verificare quanto sopra. Considerando l'osservazione 4.6 basta che $I(P, F \cap L) > m_P(F)$ per qualunque punto fondamentale e per qualunque retta eccezionale. Facciamo solo qualche confronto:

Consideriamo $P = (0, 0, 1) \in U_3$ e la retta eccezionale $L' = \mathcal{V}((Y))$, $P \in F, L$, demogeneizziamo entrambe le varietà rispetto ad U_3 e otteniamo $F_* = 8X^3Y + 8X^3 + 4X^2Y - 10XY^3 - 10XY^2 + 3Y^3$ $L_* = Y$. La molteplicità di P rispetto a F è 3; invece per il calcolo della molteplicità di intersezione dobbiamo calcolare:

$$dim_K \mathcal{O}_P(K^2)/(F_*, Y)$$

abbiamo che $\overline{Y} = 0$ pertanto da $\overline{F_*} = \overline{8X^3}$ si deduce $\overline{X^3} = 0$ (essendo dominio) cioè $\overline{X} = 0$. Allora $\mathcal{O}_P(K^2)/(F_*, Y) \cong K$ quindi la dimensione è uno. Il resto in modo analogo.

Proposizione 5.4. *Se m_P=r, allora Z^r è la più grande potenza di Z che divide $F^Q = F(YZ, XZ, XY)$, con F un polinomio che individua C.*

Indicheremo con n il grado di F.

Proposizione 5.5. *Se C è in buona posizione, allora lo è pure C'*

Due curve F, G si intersecano trasversalmente in un punto P se P è semplice per entrambe ed inoltre la tangente di F è diversa dalla tangente di G in P. Noi diremo che C è in posizione eccellente se è in buona posizione e se L interseca trasversalmente C in n punti distinti non fondamentali e L', L'' intersecano C in $n - r$ punti distinti non fondamentali.

Proposizione 5.6. *Sia F una curva piana proiettiva irriducibile, P un punto di F. Allora esiste un cambiamento di coordinate T per cui F^T è in posizione eccellente, e $T((0,0,1)) = P$.*

$Q \circ T$ la chiameremo trasformazione quadtratica e, F^T è chiamata trasformazione quadratica. Se F^T è in posizione eccellente e $T((0,01)) = P$, noi diremo che la trasformazione quadratica è centrata in P. Se $F = F_1, F_2, ..., F_m = G$ e ogni F_i è la trasformazione quadratica di F_{i-1}, noi diremo che F si è trasformata in G per mezzo di una finita sequenza di trasformazioni quadratiche.

Teorema 5.1. *Ogni curva irriducibile può essere trasformata in una curva con solo singolarità ordinarie utilizzando una sequenza di trasformazioni quadratiche.*

Abbiamo trovato proprio quello che serviva, cioè una curva piana birazionale a quella di partenza a cui possiamo applicare 5.3. Si ha pertanto il seguente importante teorema.

Teorema 5.2. *Sia C una curva proiettiva (anche non del piano). Allora esiste una curva proiettiva X non singolare e un morfismo birazionale f da X a C.*

Dimostrazione. Si può dimostrare utilizzando C.1, 5.1, 5.3. □

Il teorema afferma anche che se esiste un altra applicazione $f' : X' \to C$ questa è tale per cui $X \cong X'$.

Osservazione 5.4. Per risolvere le singolarità nel caso più generale, bisogna innanzitutto portarsi ad una curva piana con sole singolarità ordinarie e poi applicare il procedimento di inizio capitolo. In alcuni casi, ad esempio se una curva piana C proiettiva ha una sola singolarità ordinaria P con $P \in U_i$ per qualche i, ed inoltre esiste una curva piana affine che omogeneizzata rispetto a i da C. Noi possiamo grazie a 4.2.1 (sono birazionali) risolvere la singolarità nel caso affine.

Esempio 5.2.1. Come curva proiettiva scegliamo la omogeneizzazione di $F = Y^2 - X^2(X+1)$ che è $F^* = Y^2Z - X^3 - X^2Z$ che ha come punto singolare $(0,0,1)$. La soluzione trovata nel esempio uno è birazionalmente eqivalente anche a F^* proprio perchè il campo delle funzioni razionali di F e F^* è lo stesso, cioè F e F^* sono birazionalmente equivalenti.

5.2.1 Modelli non singolari di curve.

Sia C una curva proiettiva C, $f : X \to C$ come nel teorema. X lo chiameremo il modello non singolare di X. I punti di X saranno chiamati posti (luoghi) di C o di $K = k(C)$ con k il campo dove sono definiti i polinomi. Per ogni curva piana proiettiva, possiamo considerare la sua G_* demogeneizzata in $\mathcal{O}_P(\mathcal{P}^2) \cong \mathcal{O}_P(k^2)$, sia $f : X \to C$ con $f(Q) = P$ definiamo $ord_Q(G) = ord_Q(g)$, g immagine di G_* in $\mathcal{O}_P(C)$.

Qui alcuni importanti risultati utili al successivo capitolo:

Proposizione 5.7. *Sia C una curva proiettiva piana irriducibile, $P \in C$,$f : X \to C$. Sia G una curva piana. Allora*

$$I(P, C \cap G) = \sum_{Q \in f^{-1}(P)} ord_Q(G).$$

Proposizione 5.8. *Sia P un punto singolare ordinario di C di molteplicità r. Sia $f^{-1}(P) = \{P_1, ..., P_r\}$. Se $z \in k(C)$, e $ord_{P_i}(z) \geq r - 1$, allora $z \in \mathcal{O}_P(C)$.*

Proposizione 5.9. *Sia F una curva irriducibile piana, P un punto ordinario di molteplicità r di F. Siano $P_1, ..., P_r$ i posti centrati in P. Siano G, H curve piane. Allora le condizioni di Noether 4.4 sono soddisfatte su P se*

$$ord_{P_i}(H) \geq ord_{P_i}(G) + r - 1 \, per \, i = 1, ..., r.$$

Capitolo 6

Teorema di Riemann-Roch

6.1 Spazio vettoriale $L(D)$

In questo capitolo C curva irriducibile proiettiva e, $f : X \to C$ il morfismo birazionale del modello non singolare X di C.

Definizione 6.1.1. Un divisore su X è una somma formale $D = \sum_{P \in X} n_P P$, $n_P \in Z$, con n_P tutti nulli tranne per un numero finito.

Si definisce il grado di un divisore D come la somma dei coefficienti. Un divisore si dice efficace se i suoi coefficienti sono tutti positivi. L'insieme dei divisori di X forma un gruppo abeliano.

Osservazione 6.1. Il grado forma un ordine sui divisori che indicheremo con $\succ$ in caso di grado maggiore e $\prec$ in quello minore.

Definizione 6.1.2. Sia G una curva proiettiva che non contiene C come componente, definiamo il divisore di G, $div(G) = \sum_{P \in X} ord_P(G)P$.

Definizione 6.1.3. Per ogni elemento $z \neq 0 \in K = k(C) = k(X)$, definiamo il divisore di z, $div(z) = \sum_{P \in X} ord_P(z)P$. Definiamo $z_0 = \sum_{ord_P(z)>0} ord_P(z)P$ il divisore degli zeri di z.

Proposizione 6.1. *$\forall\ z \in K$, $div(z)$ ha grado zero.*

Dimostrazione. $z = \frac{f}{h}$ con f, h dello stesso grado m. Prendiamo due polinomi $F, H \in k[X, Y, Z]$ che sono i rappresentanti di f ed h rispettivamente. Abbiamo che $div(z) = div(F) - div(H)$ e dal teorema di Bézout il grado di $div(F), div(H)$ è mn. □

Corollario 6.1. *Siano $z, z' \in K$, entrambi non nulli, allora $div(z) = div(z')$ se e solo se $z = \lambda z'$ per qualche $\lambda \in K$.*

Diciamo che due divisori sono equivalenti se $D' = D + div(z)$ per qualche $z \in K$ ($D' \equiv D$). Quanto visto in 5.9 si può tradurre usando i divisori. Assumiamo ora C solo con punti multipli ordinari. Per ogni $Q \in X$, sia $r_Q = m_{f_Q}(C)$, definiamo il divisore efficace $E = \sum_{Q \in X}(r_Q - 1)Q$. Ogni curva G dove $div(G)$ ha grado maggiore del grado di E si dice aggiunta.

Teorema 6.1. *Siano C, E come sopra. Supponiamo D e D' divisori efficaci di X, e $D' \equiv D$. Supponiamo G una aggiunta di grado m tale che $div(G) = D + E + A$ per qualche divisore efficace A. Allora esiste una aggiunta G' di grado m per cui $div(G') = D' + E + A$.*

Dimostrazione. Cfr. [2]. □

Definiamo ora lo spazio vettoriale $L(D)$.

Definizione 6.1.4. Definiamo:

$$L(D) = \{f \in K \mid ord_P(f) \geq -n_P \; \forall \, P \in X\}.$$

Indicheremo la dimensione di $L(D)$ su k con $l(D)$.

Proposizione 6.2. *Si hanno i seguenti fatti:*

1. *se $D \prec D'$, allora $L(D) \subset L(D')$, e $dim_k(L(D')/L(D)) \leq deg(D' - D)$.*
2. *$L(D)$ è uno spazio vettoriale di dimensione finita $\forall$ D.*
3. *Se $deg(D) \geq 0$, allora $l(D) \leq deg(D) + 1$.*
4. *se $D \equiv D'$, allora $l(D) = l(D')$.*

Dimostrazione. Cfr. [2]. □

Proposizione 6.3. *Sia $x \in K$, $x \notin k$, sia $(x)_0$ il divisore degli zeri di x, e sia $dim_{k(x)}K = [K : k(x)]$. Allora*

1. *$(x)_0$ è un divisore efficace di grado n.*
2. *Esiste una costante τ per cui $l(r(x)_0) \geq rn - \tau \; \forall \; r$.*

Osservazione 6.2. Si può dimostrare che K è algebrico (ogni elemento di K è algebrico su k(x)) su $k(x)$ per qualunque x. Dal fatto che K è un estensione finita di k, lo è pure di $k(x)$ e, il fatto che sia algebrico ci assicura che la dimensione di K su $k(x)$ è finita.

6.1.1 Teorema di Riemann.

Teorema 6.2. *Esiste una costante g per cui $l(D) \geq deg(D) + 1 - g$ per ogni divisore D. Il più piccolo g è chiamato genere di X*

Dimostrazione. Per ogni D, sia $S(D) = deg(D) + 1 - l(D)$. Noi vogliamo trovare un numero intero g tale che $S(D) \leq g \; \forall \; D$.

1. $S(0) = 0$, quindi se esiste $g \geq 0$.

2. Se $D \equiv D'$,allora $S(D) = S(D')$ (al lettore).

3. se $D \prec D'$, allora $S(D) \leq S(D')$ (al lettore).

Sia $x \in K$, $x \notin k$, sia $Z = (x)_0$, e sia τ il più piccolo intero della proposizione 6.3. Dato che $S(rZ) \leq \tau + 1$, e dato $rZ \prec (r+1)Z$, si deduce che:

4. $S(rZ) = \tau + 1 \; \forall \; r > 0$ sufficientemente grande.

5. Per ogni divisore D esiste un divisore $D' \equiv D$, e un intero $r \geq 0$ per cui $D' \prec rZ$.

Per provare il punto 5, sia $Z = \sum n_P P$, $D = m_P P$. Noi vogliamo $D' = D - div(f)$, quindi vogliamo $m_P - ord_P(f) \geq r n_P \ \forall \ P$. Sia $y = x^{-1}$, e sia $T = \{P \in X \mid m_P > 0\}$ e $ord_P(y) > 0$. Sia $f = \prod_{P \in T}(y - y(P))^{m_P}$, allora $m_P - ord_P(f) \leq 0$ ogni volta che $ord_P(y) = 0$. Se $ord_P(y) < 0$, allora $n_P > 0$, così basta prendere un intero r abbastanza grande che verificherà questo. □

Corollario 6.1.1.1. *Se $l(D_0) = deg(D_0) + 1 - g$, e $D \equiv D' \succ D'_0$, allora $l(D) = deg(D) + 1 - g$ (con g genere).*

Corollario 6.1.1.2. *Se $x \in K$, $x \notin k$, allora $g = deg(r(x)_0) - l(r(x)_0) + 1 \ \forall \ r$ abbastanza grande.*

Corollario 6.1.1.3. *Esiste un intero N per cui per ogni divisore D di grado $> N$, $l(D) = deg(D) + 1 - g$.*

I primi due sono immediati, per il terzo cfr. [2]. Si ha inoltre la seguente importante proposizione:

Proposizione 6.4. *Sia C una curva con solo singolarità ordinarie. Sia n il grado di C, $r_P = m_P(C)$. Allora il genere g di C è dato dalla seguente formula:*

$$g = \frac{(n-1)(n-2)}{2} - \sum_{P \in C} \frac{r_P(r_P - 1)}{2}.$$

Dimostrazione. Cfr. [2]. □

6.2 Differenziali,Divisori canonici.

Vogliamo definire i concetti di derivata e differenziale, in modo tale che abbiano le medesime propietà, e comportamenti che hanno in analisi.

Sia R un anello contenente k (k il campo utilizzato per $k[X_1, ..., X_n]$), e sia M un $R - modulo$. La funzione derivata da R a M su k è una mappa lineare $D : R \to M$ per cui $D(xy) = xD(y) + yD(x) \ \forall \ x, y \in R$.

Proposizione 6.5. *Se R è un dominio con il campo delle frazioni K, e M è uno spazio vettoriale su K, allora la funzione derivata si estende unicamente a una derivata da K ad M.*

Definiamo i differenziali su R in questo modo: per ogni $x \in R$ sia $[x]$ un simbolo. Sia F l' $R - modulo$ sopra $\{[x] \mid x \in R\}$. Sia N un sottomodulo di F, generato dai seguenti insiemi:

1. $\{[x + y] - [x] - [y] \mid x, y \in R\}$.
2. $\{[\lambda x] - \lambda[x] \mid x \in R, \lambda \in k\}$.
3. $\{[xy] - x[y] - y[x] \mid x, y \in R\}$.

Sia $\Omega_k(R) = F/N$ il modulo quoziente. Sia dx il laterale di $[x]$ in F/N, e sia $d : R \to \Omega_k(R)$ che ad x associa dx. $\omega_P(R)$ è un $R - modulo$ chiamato modulo dei differenziali di R, e d è una funzione derivata. Sono vere le seguenti proposizioni lasciate senza dimostrazione, si veda la bibliografia per tali dimostrazioni.

Proposizione 6.6. *Per ogni $R - modulo$ M, e qualunque funzione derivata $D : R \to M$, esiste un unico omomorfismo di $R - moduli$ $\varphi : \Omega_k(R) \to M$ per cui $D(x) = \varphi(dx) \ \forall \ x \in R$.*

Proposizione 6.7. *Sia K un campo di funzioni razionali (di una curva C) su k, allora $\Omega_k(K)$ è uno spazio vettoriale di dimensione uno su K.*

Se $x \in K$, $x \notin k$, allora dx è una base di $\Omega_k(K)$ su K(ad esempio questa proposizione non vale se la caratteristica di k è diversa da zero).

Proposizione 6.8. *Sia K come sopra e $\mathcal{O}$ un anello DVR il cui campo delle frazioni coincide con K e che contiene k, e sia t un parametro uniformizzante di $\mathcal{O}$. Se $f \in \mathcal{O}$, allora $\frac{df}{dt} \in \mathcal{O}$ (ricordiamo che l'appartenenza è sempre a meno di isomorfismi).*

Introduciamo a questo punto il concetto di divisore canonico che utilizzeremo nel teorema di Roch-Riemann. Sia C una curva proiettiva, e X il suo modello non singolare (è unico a meno di isomorfismi) e K il loro campo delle funzioni razionali. Sia $\Omega = \Omega_k(K)$ lo spazio dei differenziali di K su k. Sia $\omega \in \Omega$, $\omega \neq 0$, e sia $P \in X$. Noi definiamo l'ordine di ω, in simboli $ord_P(\omega)$ nel seguente modo: Scegliamo un parametro uniformizzante t di $\mathcal{O}_P(X)$, scriviamo $\omega = f(dt)$, $f \in K$, e sia $ord_P(w) = ord_P(f)$ (non dipenda dalla scelta del parametro uniformizzante scelto).

Osservazione 6.3. *Noi possiamo scrivere $w = fdt$ grazie a 6.7.*

Se $0 \neq \omega$ $\omega \in \Omega$, definiamo il divisore di ω $div(\omega) = \sum_{P \in X} ord_P(\omega)P$. Ogni divisore W per cui esiste un $\omega \in \Omega$ il cui divisore coincide si chiama divisore canonico. I divisori canonici formano una classe di equivalenza in $\equiv$. In particolare tutti i divisori canonici hanno lo stesso grado.

6.2.1 Teorema di Riemann-Roch

Teorema 6.3. *Sia W un divisore canonico di X, allora per ogni divisore D,*

$$l(D) = deg(D) + 1 - g + l(W - D).$$

Dimostrazione. Cfr. [2]. □

Proposizione 6.2.1.1. *Se $l(D) > 0$, e $l(W - D - P) \neq l(W - D)$, allora $l(D + P) = l(D)$.*

Dimostrazione. Cfr. [2]. □

La dimostrazione del teorema di Riemann-Roch deriva sostanzialmente da 6.2.1.1. Qui i principali corollari.

Corollario 6.1. *l(W)=g se W è un divisore canonico.*

Corollario 6.2. *Se $deg(D) \geq 2g - 1$, allora $l(D) = deg(D) + 1 - g$.*

Corollario 6.3. *Se $deg(D) \geq 2g$, allora $l(D - P) = l(D) - 1 \ \forall \ P \in X$.*

Corollario 6.4. *Se $l(D) > 0$, e $l(W - D) > 0$, allora $l(D) \leq \frac{1}{2}deg(d) + 1$ (chiamato anche teorema di Clifford).*

Capitolo 7

Applicazioni

7.1 Codici di Goppa.

L'insieme dei codici conosciuti ora con il nome di Algebraic Geometric Codes (Codici algebrici geometrici, AG-codice) sono stati introdotti inizialmente da Valerii Denisovich Goppa. L'intuizione di Goppa è stata quella di capire che era possibile costruire dei codici, partendo da una curva algebrica proiettiva priva di singolarità.

7.1.1 Codice funzione.

Dobbiamo prima definire cosa sono i punti razionali di una curva.

Definizione 7.1.1.1. Sia $C = \mathcal{V}((F))$ una curva, sia K un estensione di k. Noi definiamo un punto $K - razionale$ di C come un punto che è zero di F in K. $C(K)$ indicherà l'insieme di tutti i punti $K - razionali$. Gli elementi di $C(k)$ sono chiamati punti razionali (i punti di C sono razionali).

Osservazione 7.1. Si noti che un punto x è razionale se e solo se $k(x)$ ha dimensione uno su k.

Definizione 7.1.1.2. Sia C una curva proiettiva non singolare, siano P_i con $i = 1, ..., n$ n punti razionali distinti su C, sia

$$B = P_1 + P_2 + \cdots + P_n$$

e sia D un divisore con supporto disgiunto dal supporto di B (per supporto intendiamo i punti con coefficiente diverso da zero).

Il codice funzione di B e D, chiamato $C_L(B, D)$, è l'immagine della seguente funzione chiamata mappa di valutazione:

$$mp : L(D) \to K^n; f \mapsto (f(P_1), ..., f(P_n))$$

o anche:

$$C_L(B, D) = \{(f(P_1)), ..., f(P_n) \mid f \in L(D)\}$$

È facile vedere che è un codice lineare.

Proposizione 7.1. *Il codice funzione $C_L(B, D)$ è un codice lineare di lunghezza $n = deg(B)$, rango $m = l(D) - l(D - B)$ e distanza minima $d \geq n - deg(D)$.*

Dimostrazione. Cfr. [5]. □

7.1.2 Codice residuo.

Definizione 7.1.2.1. Sia B e D come sopra. Il codice residuo è il codice duale del codice funzione $C_L(B, D)$. Noi abbiamo

$$C_\Omega(B, D) = \{(f_1, ..., f_n) \in K^n \mid \sum_{i=1}^{n} f_i \varphi(P_i) = 0 \, \forall \, \varphi \in L(D)\}.$$

Proposizione 7.2. *Un codice residuo $C_\Omega(B, D)$ è lineare di lunghezza $n = deg(B)$, rango $m = n - l(D) + l(D - B)$ e distanza minima di Hamming $d \geq d(D) - (2g - 2)$ dove g è il genere di C.*

Dimostrazione. Cfr. [5]. □

Corollario 7.1.1. *Supponiamo $deg(D) > 2g - 2$. Il codice residuo $C_\Omega(B, D)$ ha rango $m = n - deg(D) + g - 1 + l(D - V)$.*

Dimostrazione. Dal teorema di Riemann Roch cioè da 6.2 si sostituisce in 7.2. □

7.2 Esempi di AG-codici.

Noi vogliamo determinare la matrice di parità per alcuni codici residui. Si può dimostrare che la matrice generatrice di un codice e la matrice di parità del suo codice duale coincidono.

Esempio 7.1. Consideriamo la curva proiettiva piana $F = YZ - X^2$ su K_7. Questa curva è non singolare con genere pari a 0 e i suoi punti razionali sono $P_i = (i, i^2, 1)$ per $i = 0, ..., 6$ e Q=(0,1,0) (punto all'infinito). Sia $x = \overline{X/Z}$ e consideriamo $L(mQ)$, spazio vettoriale generato da x^i con $i = 0, 1, ..., m$.

$$B = P_0 + \cdots P_6$$

allora la matrice di parità di $C_\Omega(B, mQ)$ è

$$\begin{pmatrix} 1 & 1 & 1 & . & . & . & 1 \\ x(P_0) & x(P_1) & x(P_2) & . & . & . & x(P_6) \\ x^2(P_0) & x^2(P_1) & x^2(P_2) & . & . & . & x^2(P_6) \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ x^m(P_0) & x^m(P_1) & x^m(P_2) & . & . & . & x^m(P_6) \end{pmatrix}$$

numericamente:

$$\begin{pmatrix} 1 & 1 & 1 & . & . & . & 1 \\ 0 & 1 & 2 & . & . & . & 6 \\ 0 & 1 & 4 & . & . & . & 6^2 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 0 & 1 & 2^m & . & . & . & 6^m \end{pmatrix}$$

Esempio 7.2. Consideriamo la curva $F = X^3 + Y^2Z + YZ^2$. È non singolare con genere pari a 1; ha nove punti razionali con uno $Q = (0, 1, 0)$ considerando $K_4 = K_2(w)/(w^2 + w + 1)$. Sia $C_\Omega(aQ)$ con B la somma di tutti i punti razionali eccetto Q. Il codice ha distanza di Hammnig a. Supponiamo $a = 5$, $L(5Q) = \langle 1, x, y, X^2, xy\rangle$. I punti sono:

$$P_1 = (0, 0, 1)\ P_2 = (0, 1, 1)\ P_3 = (1, w, 1)\ P_4 = (1, w^2, 1),$$

$$P_5 = (w, w, 1)\ P_6 = (w, w^2, 1)\ P_7 = (w^2, w, 1)\ P_8 = (w^2, w^2, 1).$$

Il codice $C_\Omega(5Q)$ ha la matrice di parità.

$$\begin{pmatrix} 1 & 1 & . & . & . & 1 \\ x(P_1) & x(P_2) & . & . & . & x(P_8) \\ y(P_1) & y(P_2) & . & . & . & y(P_8) \\ x^2(P_1) & x^2(P_2) & . & . & . & x^2(P_8) \\ xy(P_1) & xy(P_2) & . & . & . & xy(P_8) \end{pmatrix}$$

numericamente:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & w & w & w^2 & w^2 \\ 0 & 1 & w & w^2 & w & w^2 & w & w^2 \\ 0 & 0 & 1 & 1 & w^2 & w^2 & w & w \\ 0 & 0 & w & w^2 & w^2 & 1 & 1 & w \end{pmatrix}$$

Infine mostriamo il seguente teorema:

Teorema 7.1. Sia C una curva proiettiva definita su K_q, sia N il numero di punti razionali di C, allora

$$|N - (q + 1)| \leq g|2\sqrt{(q)}|.$$

dove g è il genere di C.

Appendice A

Estensione di campi

Siano k e K due campi con $k \subset K$. Noi diremo che K è un estensione di k. Se $x_1, ..., x_n$ sono elementi di K, possiamo considerare questo nuovo insieme

$$k[x_1, ..., x_n] = \{x \in K \mid x = f(x_1, ..., x_n) \textit{ per qualche } f \in k[X_1, ..., X_n]\}$$

Questo campo è un dominio di integrità, pertanto è possibile definire anche il suo campo delle frazioni, che indicheremo con $k(x_1, ..., x_n)$. Un estensione K di k si dice finitamente generata su k, se $K = k(x_1, ..., x_n)$. Noi diremo che K è un' estensione semplice di k se può essere ottenuto da k con l'aggiunta di un solo elemento.

Sia K un'estensione di un campo k, e sia x un elemento di K che è algebrico sopra k. Sia $f(X)$ un polinomio di $k[X]$ di grado minimo $\mid f(x) = 0$.

Teorema A.1. *Il polinomio $f(X)$ è irriducibile su $k[X]$. Se $g(X)$ è un qualsiasi altro polinomio che ha x come radice, allora $f(X) \mid g(X)$.*

Di importanza fondamentale la seguente proposizione:

Proposizione A.1. *Sia K un campo e $P(X)$ un polinomio di $K[X]$ di grado $n \geq 2$, allora esiste un anello A contenente K, a meno di isomorfismi, contenete una radice di $P(X)$.*

Dimostrazione. Poniamo $A \doteq K[X]/(P(X))$. Ovviamente esiste un omomorfismo φ iniettivo tra K e A, pertanto possiamo identificare gli elementi di K con l'immagine dell'omomorfismo $Im\varphi = A' \subset A$. Pertanto $\overline{P(X)} = P(\overline{X}) = \overline{0} = 0$. □

Corollario A.1. *Se $P(X)$ è irriducibile, allora esiste un campo C contenente K e una radice $P(X)$.*

Corollario A.2. *Se $P(X)$ è irriducibile di grado n, allora esiste un campo Δ contenente K e n radici di $P(X)$.*

Deinizione A.1. Un campo K si dice algebricamente chiuso se contiene ogni elemento algebrico su di esso (il contiene è sempre inteso a meno di isomorfismo).

Proposizione A.2. *K è algebricamente chuso $\Leftrightarrow$ qualunque polinomio $P(X) \in K[X]$ si fattorizza in fattori lineari a coefficienti in K.*

A.1 Basi di trascendenza.

Quanto faremo in questa sezione è sostanziale per la dimensione di una varietà.

Definizione A.1.1. Siano K e K' due campi con $K' \subset K$. $x_1, ..., x_n$ di K si dicono algebricamente indipendenti su K', se per ogni polinomio $F(X_1, ..., X_n) \in K'[X_1, ..., X_n]$ si ha:

$$F(x_1, ..., x_n) = 0 \Rightarrow F(X_1, ..., X_n) = \textit{ polinomio nullo.}$$

in caso contrario si dicono algebricamente dipendenti.

Definizione A.1.2. Siano K, K' de campi. Siano $x_1, ..., x_s$ s elementi algebricamente indipendenti, essi si dicono base di trascendenza di K su K' se ogni elemento di K è algebrico sul campo delle frazioni dell'anello dei polinomi di $K[x_1, ..., x_n]$. Questo ha senso perchè se $x_n, ..., x_2, x_1$ algebricamente indipendenti allora x_1 trascendente su K x_2 trascendente su $K[x_1]$ e così via (l'ordine non conta).

Teorema A.2. *Se x è algebrico su $K \Rightarrow K[x] = K(x)$. Inoltre x è algebrico su $K \Leftrightarrow K[x]$ è spazio vettoriale di dimensione finita su K.*

Si ha inoltre un'altro importante teorema che non dimostreremo:

Teorema A.3. *Se $K' \subset K$ e $x_1, ..., x_s$ è una base di trascendenza di K su $K' \Rightarrow$ ogni altra base di K su K', ha s elementi.*

Appendice B

Caratteristica di un campo

Definiremo cos' è la caratteristica di un qualsiasi campo. Noi per la geometria, ci siamo sempre posti in un campo di caratteristica 0 perchè vale certamente il principio di identità dei polinomi, il quale afferma che due polinomi sono uguali $\Leftrightarrow$ sono identicamente uguali.

Sia K un campo, consideriamo l'insieme:

$$E \doteq \{x \in K \mid x = ne \, per \, qualche : \; n \, naturale\}$$

con $ne = e + ... + e$ n volte (con e intendo l'identità rispetto al prodotto).

Tale insieme E è un sottoanelllo dominio di K, pertanto si può considerare il suo campo delle frazioni, che ovviamente è contenuto in K e da qualsiasi sottocampo di K.

Definizione B.1. Un campo K che non ha sottocampi propri viene detto campo primo.

Per quanto detto allora si ha che E è primo. Noi possiamo considerare il seguente omomorfismo:

$$\varphi : Z \to E, \varphi(n) = ne \, \forall \, n \in Z$$

Ci sono due possibilità:

1. φ è isomorfismo
2. φ è suriettivo $\varphi(n) = 0_E$ per qualche n.

Se è isomorfismo allora si dice che K è di caratteristica zero, altrimenti si definisce caratteristica di K il più piccolo intero diverso da zero che sta nel nucleo dell'omomorfismo. Per alcune considerazioni riguardo la validità dei teoremi svolti in un campo di caratteristica > 0 cfr. [2].

Appendice C

Topologia, morfismi

In questa appendice diamo i concetti elementari sulla topologia (noi ci focalizzeremo sulla topologia di Zariski) e sui morfismi.

Definizione C.1. Una topologia su un insieme X è una collezione di sottoinsiemi di X, chiamati gli aperti di X, che verificano:

1. X e l'insieme vuoto sono aperti.
2. l'unione di qualsiasi famiglia (anche infinita) di aperti di X è un aperto.
3. L'intersezione di un numero finito di aperti di X è un aperto.

La coppia (X, topologia di X) si chiama spazio topologico. Un insieme $C \subset X$ è chiuso se il suo complementare è aperto. Su un sottoinsieme C è possibile inoltre definire una topologia indotta da X che è così definita:

Definizione C.2. Sia C un sottoinsieme di un' insieme X su cui è definita una topologia. Definisco gli aperti di C come i sottoinsiemi W di C per cui esiste un aperto U in X che contiene $W \mid W = U \cup C$.

Definisco la chiusura di un sottoinsieme Y di X come l'intersezione di tutti i chiusi contenenti Y in sostanza il più piccolo insieme chiuso che contiene Y. Y è denso in X se X è la chiusura di Y. Definiamo inoltre il concetto di funzione continua:

Definizione C.3. Una funzione tra due spazi topologici X', X $f : X \to X'$ si dice continua se:

$$\forall \, insieme\ aperto\ U\ di\ X\ si\ ha\ f^{-1}(U).$$

Date tali definizioni si può introdurre la topologia di Zariski che ovviamente verifica gli assiomi della topologia.

Definizione C.4. Sia $X = \mathcal{P}^n \times \cdots \times \mathcal{P}^m \times K^s$. La topologia di Zariski è definita nel seguente modo: un insieme U di X si dice aperto se il suo complementare in X è una varietà algebrica (in senso generale definito alla fine del capitolo 4).

Sia V una varietà irriducibile di X ogni sottoinsieme aperto di V lo chiameremo varietà. Su tale insieme è possibile definire l'insieme delle funzioni razionali $\Gamma(X) = \Gamma(V)$, si può dimostrare che non dipende dalla scelta di V per un X fissato.

Se Y è un sottoinsieme chiuso di X (topologia indotta), Y è anche una varietà nel senso che esiste una varietà che ha Y come aperto, tale varietà è la chiusura di Y in V indicata con $\overline{Y}$. Y è anche chiamata sottovarietà chiusa di X (si usa smpre la topologia indotta).

Sia X una varietà, U un sottoinsieme aperto di X. Definiamo $\Gamma[U, \mathcal{O}_X]$ di U rispetto a X in questo modo:

$$\Gamma[U, \mathcal{O}_X] = \bigcup_{P \in U} \mathcal{O}_X(P)$$

Introduciamo il concetto di morfismo

Definizione C.5. Un morfismo da X a Y con X, Y varietà (nel nuovo senso) è un'applicazione $\varphi : X \to Y$ che verifica:

1. φ è continua.
2. $\forall$ aperto U di Y se $f \in \Gamma[U, \mathcal{O}_Y] \Rightarrow f \circ \varphi \in \Gamma[\varphi^{-1}(U), \mathcal{O}_X]$

se inoltre è biunivoco si dice isomorfismo. Se $X = K^n$ e $Y = K^m$ un morfismo è una funzione polinomiale.

Sfruttando la topologia siamo pronti ha dare una definizione più generale di varietà algebrica. Diciamo che un sottoinsieme V di $X = \mathcal{P}^n \times \cdots \times \mathcal{P}^m \times K^s$ viene definito varietà algebrica affine (proiettiva) se esiste un isomorfismo tra V e una varietà affine nel senso definito nel capitolo 3 (capitolo 4). Se vogliamo marcare che non si tratta di un isomorfismo, ma l'insieme è una varietà in senso classico allora diremo che è una varietà appartenete a K^n o $\mathcal{P}^n$.

Osservazione C.1. Vista la definizione data possiamo estendere il concetto di dimensione di una varietà definendola in tale modo. Sia X una varietà, $\Gamma(X)$ è un estensione di K finitamente generata; definiamo la dimensione di X il grado di trascendenza su K in simboli:

$$dim(X) \doteq gr.tr_K \Gamma(X)$$

Ci sono importanti teoremi e proposizioni ma noi ne elencheremo solo alcuni senza dare la dimostrazione.

Proposizione C.1. *Ogni sottovarietà chiusa di $\mathcal{P}^n \times \cdots \times \mathcal{P}^m$ è una varietà proiettiva. Ogni varietà è isomorfa ad una varietà aperta di uno spazio proiettivo.*

Proposizione C.2. *Sia V una varietà affine, e sia $f \in \Gamma(V)$, $f \neq 0$. Sia $V_f = \{P \in V \mid f(P) \neq 0\}$, una sottovarietà aperta di V. Allora*

1. *$\Gamma[V_f] = \{\frac{a}{f^n} \in \Gamma[V], n \in Z\}$.*
2. *V_f è una varietà affine.*

C.1 Birazionali

Vogliamo definire una classificazione delle varietà algebriche.

Siano X e Y varietà. Due morfismi $f_i : U_i \to Y$ da sottovarietà aperte di X a Y si dicono equivalenti se la loro restrizione a $U_1 \cap U_2$ è la stessa (forma una relazione di equivalenza). Una classe di equivalenza viene chiamata mappa razionale da X a Y.

Una mappa razionale da X a Y è detta dominante se $f(U)$ è denso in Y, con f qualunque rappresentante della mappa. Definiamo cos'è una mappa birazionale

Definizone C.1.1. Una mappa razionale G da X a Y è detta birazionale se $\exists\ U, V$ aperti e un'isomorfismo $g : U \to V$ che rappresenta G (ricordiamo che G è una classe di equivalenza).

Siamo pronti per dire quando due varietà sono birazionali.

Definizione C.1.2. Due varietà X, Y si dicono birazionali se esiste una mappa birazionale da X a Y.

La classificazione appena data è di importanza fondamentale; noi la useremo negli ultimi capitoli ed inoltre si hanno tali proposizioni.

Teorema C.1. *Due varietà sono birazionalmente equivalenti se e solo se il loro campo delle funzioni è isomorfo.*

Corollario C.1. *Ogni curva (varietà nel senso generale di dimensione uno) è equivalente a una curva del piano.*

Appendice D

Introduzione ai codici

Prima di introdurre i codici, descriviamo a parole, lo scopo di quest' ultimi. Il fine della codifica di canale è quella di aggiungere dei simboli all'interno del messaggio per renderlo più robusto nei confronti degli errori. Ad esempio, supponiamo che si voglia trasferire da un punto ad un altro una sequenza binaria, un modo intuitivo per renderlo più sicuro è quello di aggiungere un bit di parità (uno se dispari, zero se pari). Nella teoria dei codici si studiano le tecniche per poter risolvere e anche rivelare il più possibile numero di errori allungando la lunghezza del messaggio; in controtendenza con la codifica di sorgente che serve ad altri scopi. In questa appendice daremo le definizioni base e, svilupperemo come esempio base i codici di Hamming.

D.1 Block Codes

Definizione D.1.1. Sia K un campo (la caratteristica di K è diversa da zero) . Un block code C, di lunghezza n su K è un sottoinsieme K^n. Un elemento di C si chiama parola di codice. Un block code C si dice sistematico se ogni parola di informazione (l'alfabeto iniziale) è prefisso di una parola di codice.

Un parametro di importanza fondamentale di un codice è la distanza di Hamming. Si vedrà che essa misura la quantità di errori che è possibile correggere o rivelare.

Definizione D.1.2. Sia $p \in K^n$. Il peso di p in simboli $w(p)$ è definito come il numero di componenti di p diversi da zero. La distanza di Hamming tra due elementi x, y di K^n $d(x, y) = w(x - y)$. La distanza di Hamming del codice è così definita:

$$d(C) \doteq min\{d(x, y) \mid x, y \in C\}.$$

Definizione D.1.3. Sia C un block code, si definisce peso di Hamming minimo:

$$w_{min} = min\{d(x, 0) \mid x \in C\}.$$

Osservazione D.1. K^n con $d : K^n \to N$ distanza di hamming formano uno spazio metrico.

La mancanza di struttura dei block codes comporta una grossa difficoltà nel capire se una parola appartiene o no al codice. Questo motiva la scelta di introdurre i codici lineari.

D.2 Codici lineari.

Definizione D.2.1. Sia K un campo. Un codice lineare C di lunghezza n è una terna (U, F, W) dove U è un sottospazio vettoriale di K^n, $F : K^{dimU} \to K^n$ è un omomorfismo tra spazi vettoriali per cui $ImF = U$, e $W : K^n \to K^{n-dimU}$ con $KerW = U$. Il rango di C lo definiamo uguale a $dimU$.

Proposizione D.1. *In un codice lineare C la peso minimo e distanza minima di Hammnig coincidono.*

Dimostrazione. La dimostrazione segue dal fatto che in un codice lineare somma e differenza di parole sono ancora parole di codice. □

Osservazione D.2. I campi finiti, quindi con caratteristica diversa da zero hanno la seguente classificazione:

1. Ogni campo finito ha pn elementi, per qualche numero primo p e qualche numero naturale n^31.
2. Per ogni numero primo p e naturale n^31, esiste un solo campo finito con p^n elementi, a meno di isomorfismo.

chiameremo ordine del campo K il numero $q = p^n$. Dimostriamo che la caratteristica del campo è un numero primo.

Dimostrazione. Sia K un campo finito, ha caratteristica p diversa da 0. Usando solo l'elemento unità troviamo un sottocampo isomorfo a $Z/(p)$, ma essendo tale insieme campo abbiamo che (p) ideale massimale quindi p primo. D'ora in poi consideriamo solo campi finiti con un certo ordine. □

Definizione D.2.2. L'operatore lineare F è chiamato matrice generatrice.

Osservazione D.3. F e W sono unicamente individuate da U.

Nella teoria dei codici, come già anticipato si usano campi finiti con $q = pn$ elementi. Così un codice lineare di rango m possiede q^m vettori distinti. Se ogni vettore rappresenta un simbolo, allora C può essere pensato come un alfabeto di dimensione q^m.

Notazione D.1. Sia $K = K_q$. Noi chiameremo un codice lineare di lunghezza n, rango k e distanza minima di Hamming d un codice $q - ary[n, k, d]$.

Per poter definire il codice duale dobbiamo introdurre il concetto di prodotto interno o scalare.

Definizione D.2.3. Sia C un codice $q - ary[n, k, d]$. Definiamo il prodotto interno:

$$\langle x, y \rangle \doteq \sum_{i=1}^{n} x_i y_i$$

noi diremo che due parole sono ortogonali se il loro prodotto scalare è nullo.

Definizione D.2.4. Noi definiamo il duale di C l'insieme:

$$C^{\perp} \doteq \{x \in K^n \mid \langle x, c \rangle = 0 \, \forall \, c \in C\}.$$

Proposizione D.2. *Si hanno:*

1. *Lo spazio $C^{\perp}$ è il complemento ortogonale di C.*
2. *È facile vedere che $C^{\perp}$ è sottospazio di K^n, ed inoltre è un codice lineare.*

3. La dimensione di $C^{\perp}$ è $n-k$, con k dimensione di C.

4. Si ha $(C^{\perp})^{\perp} = C$.

Proposizione D.3. *Per un $q-ary[n,k,d]$, la distanza minima di Hamming verifica:*

$$d_{min} \leq n-k+1.$$

Dimostrazione. Cfr. [1]. □

Definizione D.2.5. Sia $C^{\perp}$ con una base $c'_1, ..., c'_{n-k}$ con c'_i un vettore riga $\forall\ i = 1, ..., n-k$, la matrice

$$W = \begin{pmatrix} c'_1 \\ c'_2 \\ . \\ . \\ . \\ c'_{n-k} \end{pmatrix}$$

è chiamata matrice di parità. Si noti che qualunque base va bene.

La matrice di parità ha un importante caratteristica.

Proposizione D.4. *Sia W come sopra, allora $Wc^T = 0 \Leftrightarrow c \in C$.*

Dimostrazione. Se $c \in C$, allora $\langle c, c'_i \rangle = 0\ \forall i$. Si ha inoltre:

$$Wc^T = \begin{pmatrix} \langle c'_1, c \rangle \\ \langle c'_2, c \rangle \\ . \\ . \\ . \\ \langle c'_{n-k}, c \rangle \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ . \\ . \\ . \\ 0 \end{pmatrix}$$

Viceversa, supponiamo $Wc^T = 0$, i.e $\langle c'_i, c \rangle = 0\ \forall\ i = 1, ..., n-k$. Dato che il prodotto interno è lineare, ogni combinazione lineare dei c'_i è ortogonale a c, i.e ogni elemento di $C^{\perp}$ è ortogonale a c, dalla definizione segue $c \in (C^{\perp})^{\perp} = C$. □

Proposizione D.5. *Una matrice $W \in K^{(n-k)n}$ è una matrice di parità per un codice lineare C con matrice generatrice $F \in K^{nk} \Leftrightarrow$*

$$WF = 0\, e\, rango(W) = n-k.$$

Dimostrazione. Cfr. [1]. □

Esempio D.1. Come primo esempio di codice, mostriamo il codice di Hammning [7,4,3] in cui $K \cong Z/(2)$:
$C = \{(0000000), (1000110), (0100101), (0010011), (0001111), (1100011), (1010101), (0110110), (1110000), (1001001), (0101010), (1101100, (0011100), (1011010), (0111001), (1111111)\}$. Tale codice ha la seguente matrice generatrice:

$$F = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Ed ha come matrice di parità:

$$W = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

D.3 Codifica di sindrome.

La matrice di parità di un codice lineare permette di implementare in modo efficiente un algoritmo, per l'uso della decodifica della distanza di Hamming minima, chiamata anche decodifica di sindrome.

Definizione D.3.1. Sia c (vettore riga) $\in K^n$, definisco:

$$\xi = Wc^T.$$

la sindrome di c.

Proposizione D.6. *Due parole c_1 e c_2 hanno la stessa sindrome se e solo se la loro differenza λ è una parola di codice.*

Dimostrazione. c_1 e c_2 hanno la stessa sindrome ξ. Allora, noi abbiamo

$$W\lambda = Wc_1 - Wc_2 = \xi - \xi = 0,$$

così λ è una parola di codice da D.4.Viceversa se λ è una parola di codice, noi abbiamo

$$Wc_1 = W(c_2 + \lambda) = Wc_2 + W\lambda = Wc_2 + 0 = Wc_2.$$

□

Osservazione D.4. Si può facilmente notare che due elementi hanno la stessa sindrome $\Leftrightarrow$ appartengono alla medesima classe laterale, in sostanza possiamo considerare il gruppo quoziente K^n/C in corrispondenza biunivoca con i valori delle sindromi.

Supponiamo che sia inviata la parola c e che sia ricevuta c', c' individua una sindrome e pertanto una classe laterale. Scegliamo all'interno di questa classe un rappresentante che ha il peso minimo all'interno della classe chiamandolo $c_{min}(Wc')$.

Proposizione D.7. *La parola di codice:*

$$c_m = c' - c_{min}(Wc').$$

è una parola di codice avente distanza minima di Hamming rispetto all' elemento ricevuto c'.

Dimostrazione. Innanzitutto mostriamo che c_m è una parola di codice. Questo si dimostra sfruttando la linearità della matrice di parità e vedendo che si ottiene 0:

$$Wc_m = Wc' - Wc_{min}(Wc') = \xi - \xi = 0.$$

□

quanto voluto. Per il resto della dimostrazione vedi [1].

Questo ci permette di realizzare un metodo per la decodifica che si usa spesso in telecomunicazioni, che è per l'appunto il criterio a minima distanza di Hamming. Facciamo per concludere un facile esempio.

Esempio D.2. Consideriamo il codice binario (sistematico) di Hamming $[4, 2, 2]$:

$$C = \{(0000), (1010), (0101), (1111)\}.$$

ha come matrice generatrice:

$$F = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

come matrice di parità:

$$W = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Classi	Rappresentante	Sindrome
$C_0 = \{(0000), (1010), (0101), (1111)\}$	(0000)	00
$C_1 = \{(0001), (1011), (0100), (1110)\}$	(0001)	01
$C_1 = \{(0010), (1000), (0111), (1101)\}$	(0010)	10
$C_1 = \{(0011), (1001), (0110), (1100)\}$	(0011)	11

Questo codice corregge al massimo un errore.

Indice analitico

Bibliografia

[1] N. Benvenuto. *Communication Systems.* Wiley, Wheinheim, 2007.

[2] W. Fulton. *Algebraic Curves.* W.A. BENJAMIN,INC, New York,Amsterdam, 1969.

[3] O. Zariski P. Samuel. *Commutative Algebra volume 1.* Springer, New York,Paris,Berlin, 1975.

[4] E. Stagnaro. *Algebra Commutativa.* Univer, Verona, 2003.

[5] J. Zhuo. *Algebraic Geometric Coding Theory.* University of Sydney, Sydney, 2006.