Università degli Studi di Ferrara

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Matematica
Indirizzo: Matematica Pura

Sulla legge di gruppo sopra le curve ellittiche e sulle varietà abeliane

Relatore:
Chiar.mo Prof.
Philippe Ellia

Laureando:
Alex Massarenti

Anno Accademico 2006-2007

A mio nonno, mia nonna e mio zio,
che mi hanno insegnato tanto
con la loro morte.
E ancora di più
con la loro vita.

Indice

Introduzione **7**

1 Risultati generali **9**
1.1 Gruppi, Anelli e Campi 9
1.2 L'anello dei polinomi 12
1.3 Campi, P.I.D. e U.F.D. 14
1.4 Anelli Noetheriani 17
1.5 Il Teorema fondamentale dell'Algebra 19
1.6 Spazi e Varietà topologiche 20

2 Geometria Algebrica in $\mathbb{A}^n$ e in $\mathbb{P}^n$ **25**
2.1 Insiemi algebrici affini 25
2.2 Corrispondenza tra ideali e insiemi algebrici 26
2.3 Teorema degli zeri di Hilbert 28
2.4 Lo spazio proiettivo $\mathbb{P}^n$ 32
2.5 Insiemi algebrici proiettivi 34

3 Topologia di Zariski e varietà algebriche **38**
3.1 Costruzione della topologia di Zariski 38
3.2 Decomposizione in componenti irriducibili 40
3.3 Topologia di Zariski in $\mathbb{P}^n$ 41
3.4 Il Concetto di dimensione 44

4 Morfismi **45**
4.1 Funzioni razionali 45
4.2 Applicazioni razionali 48
4.3 Applicazioni razionali dominanti 49

5 Curve algebriche di $\mathbb{P}^2$ **50**
5.1 Molteplicità d'intersezione con una retta in un punto 50
5.2 Spazio tangente di Zariski 51
5.3 Singolarità delle curve piane 53
5.4 Cubiche di $\mathbb{P}^2$ 55

6 Teorema di Bezout e sistemi di curve piane **60**
6.1 Risultante di due polinomi 60
6.2 Sistemi di curve piane 63
6.3 La funzione di Hilbert di un insieme di punti 66

7 Legge di gruppo sopra le cubiche lisce di $\mathbb{P}^2$ 69
7.1 Legge di gruppo 69
7.2 Formule d'addizione su una cubica liscia 72
7.3 Punti razionali delle cubiche lisce 74

8 Varietà Abeliane 76
8.1 Punti lisci e punti singolari sulle varietà algebriche 76
8.2 Gruppi algebrici e varietà abeliane 80
8.3 Funzione $\wp$ di Weierstrass e legge di gruppo sulle curve ellittiche 82
8.4 Curve ellittiche e tori complessi 83

Bibliografia 87

Elenco delle figure

1.1 Proiezione stereografica della Sfera 24

2.1 Conica proiettiva e cono affine associato 36
2.2 Cono sopra una curva di $\mathbb{P}^2$ 37

3.1 Intersezione tra una quadrica e una cubica di $\mathbb{A}^3$ 42
3.2 Cubica Gobba come intersezione di superfici in $\mathbb{A}^3$ 43
3.3 Cubica Gobba in $\mathbb{A}^3$ 43

4.1 Morfismo tra varietà algebriche 48

5.1 Spazio Tangente a una quadrica liscia di $\mathbb{A}^3$ 52
5.2 Esempio di curva in $\mathbb{A}^2$ - I 54
5.3 Esempio di curva in $\mathbb{A}^2$ - II 55
5.4 Esempio di curva in $\mathbb{A}^2$ - III 55
5.5 Cubica, conica osculatrice e retta tangente 57
5.6 Cubica e curva Hessiana associata 58
5.7 Traccia reale di una cubica liscia I 59
5.8 Traccia reale di una cubica liscia II 59

7.1 Caso I - Intersezione su tre punti distinti 69
7.2 Caso II - Intersezione su due punti 70
7.3 Caso III - Intersezione su un punto di molteplicità tre 70
7.4 Somma di due punti su una cubica 71
7.5 Associatività della somma su una cubica 71
7.6 Curva di Fermat 75

8.1 Legge di composizione sulla cubica attraverso la funzione $\wp$ . . . 83
8.2 Traccia reale della cubica $y^2=x^3-x$ 84
8.3 Le due copie della sfera di Riemann opportunamente tagliate . . 85
8.4 Toro complesso 85
8.5 Costruzione del toro complesso 86

Introduzione

«*Il pensiero è un lampo tra due lunghe notti, ma quel lampo è tutto.*»

Jules Henri Poincaré (1854-1912).

L'oggetto principale di questa tesi è la legge di gruppo sulle curve ellittiche, tali curve sono sostanzialmente cubiche lisce di $\mathbb{P}^2$. La struttura di gruppo sulle cubiche verrà prima eplicitata dal punto di vista della geometria algebrica poi da quello dell'analisi complessa. Rigurderemo poi le curve ellittiche come particolari varietà abeliane.

Nel primo capitolo verrano definiti alcuni oggetti fondamentali dell'algebra, della topologia e della geometria differenziale, e verranno dimostrate alcune delle loro principali proprietà, necessarie per comprendere la correlazione tra queste tre discipline e la geometria algebrica.

Nel secondo capitolo definiremo gli oggetti della geoemetria algebrica con particolare riferimento alle varietà. Vedremo inoltre che sotto opportune ipotesi una varietà algebrica può essere vista come definita da un ideale dell'annello dei polinomi a coefficienti in un campo K. Grazie al teorema degli zeri di Hilbert potremmo restringere le nostre considerazioni a particolari ideali, detti ideali radicali, in modo da avere una corrispondenza biunivoca tra ideali e varietà.

Nel terzo capitolo costruiremo la topologia di Zariski. Lo spazio affine e lo spazio proiettivo saranno allora spazi topologici i cui chiusi saranno proprio i sottoinsiemi algebrici. Vedremo che con tale topologia $\mathbb{A}^n$ e $\mathbb{P}^n$ diventeranno spazi topologici compatti e che le applicazioni polinomiali risulteranno essere continue. Infine daremo una connotazione del concetto di dimensione di una varietà legata al concetto algebrico di dimensione di Krull di un anello.

Nel quarto capitolo verranno definiti i morfismi a partire dalle applicazioni regolari e dalle applicazioni razionali. Daremo poi la definizione di applicazione e morfismo dominante, grazie a queste ultime mappe potremmo sempre considerare la composizione di morfismi.

Nel quinto capitolo tratteremo delle curve algebriche di $\mathbb{P}^2$ in generale. Introdurremo i concetti di molteplicità d'intersezione con una retta, di retta tangente e di punto di flesso. Faremo particolare riferimento alle cubiche e dimostreremo che, a meno di proiettività, l'equazione di una cubica liscia di $\mathbb{P}^2$ può sempre essere scritta in due forme canoniche dette di Legendre e di Weierstrass, con opportune restrizioni sulla caratteristica del campo K.

Nel sesto capitolo introdurremo il concetto di risultante di due polinomi e daremo l'enunciato del teorema di Bezout per le curve algebriche di $\mathbb{P}^2$. Considereremo poi i sistemi di curve piane. In particolare dimostreremo il criterio di separazione, definiremo la funzione di Hilbert di un insieme di punti e daremo una dimostrazione del paradosso di Cramer. Quest'ultimo risultato sarà per noi fondamentale al fine di dimostrare l'associatività della legge di composizione sulle curve ellittiche.

Nel settimo capitolo definiremo una legge di composizione interna sulle cubiche lisce di $\mathbb{P}^2$. Vedremo che una cubica con tale legge diventerà un gruppo abeliano e un gruppo algebrico. Troveremo poi delle formule esplicite per l'addizione di punti sulla cubica. Infine definiremo il concetto di punto razionale su una curva piana proiettiva e enunceremo alcuni importanti teoremi quali il teorema di Mordell e il teorema di Wiles (ultimo teorema di Fermat).

Nell'ottavo e ultimo capitolo definiremo lo spazio tangente a una varietà in un suo punto. Daremo poi la definizione di gruppo algebrico e di varietà abeliana, vedremo allora che le curve ellittiche sono un esempio particolare di tali varietà. Dimostreremo poi che ogni varietà abeliana è liscia, che è commutativa e che se due varietà abeliane sono isomorfe come varietà lo sono anche come gruppi astratti. Infine riguarderemo brevemente alla legge di gruppo sulle curve ellittiche attraverso l'analisi complessa, in particolare attraverso la teoria delle funzioni ellittiche. Infatti grazie ad alcune proprietà di una delle più semplici funzioni ellittiche non costanti, la $\wp$ di Weierstrass, ricaveremo per altra via la struttura di gruppo sulle curve ellittiche. Infine vedremo, attravero la teoria delle superfici di Riemann, che è possibile associare ad un toro complesso una cubica liscia grazie ad un'immersione del toro in $\mathbb{P}^2$ che ha per immagine una curva ellittica.

A.M. - 14 Luglio 2007

Capitolo 1

Risultati generali

«Le scoperte matematiche, piccole o grandi che siano, non nascono mai da una generazione spontanea. Presuppongono sempre un terreno seminato con una conoscenza preliminare e ben dissodato dalla fatica, sia conscia che inconscia.»

Jules Henri Poincaré (1854-1912).

In questo primo capitolo intruduciamo i concetti di anello, ideale e anello noetheriano. In particolare dimostriamo alcuni risultati sull'anello dei polinomi a coefficienti in un campo K necessari in seguito. Concludiamo il capitolo con alcune considerazioni di topologia e di geometria differenziale.

1.1 Gruppi, Anelli e Campi

Definiamo alcune importanti strutture algebriche e le loro sottostrutture e dimostriamo le principali proposizioni loro riguardanti.

Definizione 1. *Un gruppo è una coppia (G,+) dove G è un insieme non vuoto e + una legge di composizione interna a G tale che:*

- *+ è associativa ovvero* $(x + y) + z = x + (y + z)$ *per ogni* $x, y, z \in G$,
- *Esiste un'elemento neutro 0 ovvero* $x + 0 = 0 + x = x$ *per ogni* $x \in G$,
- *Ogni elemento di G ha un inverso rispetto a + ovvero per ogni* $g \in G$ *esiste* $h \in G$ *tale che* $g + h = h + g = 0$.

Se + è commutativa ovvero se $x + y = y + x$ *per ogni* $x, y \in G$ *il gruppo G si dice abeliano.*

Definizione 2. *Un anello è un insieme non vuoto A dotato di due leggi di conposizione interne + (addizzione) e* $\times$ *(moltiplicazione) tali che:*

- *(A,+) è un gruppo abeliano,*
- *(A,*$\times$*) è un monoide avvero* $\times$ *è associativa ed esiste un elemento neutro 1*$\in$ *A rispetto a* $\times$*, 1*$\neq$*0,*
- $\times$ *è distributiva rispetto a +, ovvero (x+y)*$\times z = x \times z + y \times z$.

Un anello A si dice commutativo se anche la moltiplicazione $\times$ è commutativa.

Introduciamo ora una struttura algebrica fondamentale per dare la definizione di varietà algebrica.

Definizione 3. *Sia A un anello commutativo un ideale I dell'anello A è un sottoinsieme non vuoto I di A tale che:*

- *I è sottogruppo di (A,+) ovvero I è un gruppo rispetto a +,*
- *Per ogni $a \in A$ e $x \in I$ si ha $ax=xa \in I$.*

Definizione 4. *Un ideale I di un anello A si dice:*

- *Primo se I è un ideale proprio di A e se dati $x,y \notin I$ si ha $xy \notin I$.*
- *Massimale se I è un ideale proprio di A e se dato un ideale J di A tale che $I \subseteq J$ allora $I=J$ o $J=A$ ovvero I non è propriamente contenuto in nessun ideale proprio di A.*

Proposizione 1. *Sia I un ideale di un anello A, $I=A \Leftrightarrow 1 \in I$*

Dimostrazione: Se I=A ovviamente $1 \in I$. Supponiamo ora $1 \in I$ allora per ogni $a \in A$ possiamo scrivere a=1a ma $1a=a \in I$ essendo I un ideale, allora $A \subseteq I$, poiche $I \subseteq A$ concludiamo che I=A. □

Definizione 5. *Un anello non banale A si dice un dominio se $x,y \in A$, $x \neq 0$ e $y \neq 0$ implica $xy \neq 0$.*

Definizione 6. *Un anello nel quale ogni elemento ha un inverso anche rispetto alla moltiplicazione si dice un corpo. Un corpo commutativo rispetto alla moltiplicazione si dice una campo.*

Definizione 7. *Uno spazio vettoriale V sul campo K (K-Spazio vettoriale) è un insieme non vuoto V tale che:*

1. *per ogni coppia di vettori $v,w \in V$ sia definito un terzo elemento $v+w \in V$, detto somma di v e w,*
2. *per ogni $v \in V$ e per ogni $k \in K$ sia definito un elemento $kv \in V$, detto prodotto del vettore v per lo scalare k,*

in modo che siano soddisfatte le seguenti proprietà:

- *(Associatività) Per ogni $u,v,w \in V$ si ha $(u+v)+w=u+(v+w)$.*
- *(Esistenza dello zero) Esiste un elemento $0 \in V$, detto vettore nullo, tale che $0+v=v+0=v$ per ogni $v \in V$.*
- *(Esistenza dell'opposto) Per ogni $v \in V$ l'elemento $(-1)v=-v$ soddisfa l'identità $v+(-v)=-v+v=0$.*
- *(Proprietà commutativa) Per ogni $u,v \in V$ si ha $u+v=v+u$.*
- *(Proprietà distributiva rispetto alla somma di vettori) Per ogni $u,v \in V$ e per ogni $k \in K$ si ha $k(u+v)=ku+kv$.*

- *(Proprietà distributiva rispetto alla somma di scalari) Per ogni v∈V e per ogni h,k∈K si ha (h+k)v=hv+kv.*
- *Per ogni v∈V e per ogni h,k∈K si ha (hk)v=h(kv).*
- *Per ogni v∈V si ha 1v=v1=v.*

Si dice anche che le due operazioni definiscono su V una struttura di K-spazio vettoriale.

Vogliamo ora mettere in relazione i concetti di ideale primo e massimale con quelli di dominio e di campo. Per fare questo dobbiamo introdurre l'anello quoziente.

Sia A un anello commutativo e I un ideale proprio di A. Definiamo su A la seguente relazione d'equivalenza:

$$\text{Per ogni } x,y\in A,\ x\Re y \Leftrightarrow x-y\in I$$

L'insieme quoziente $A/\Re$ è un anello detto anello quoziente di A modulo l'ideale I e viene indicato con A/I.
Vediamo ora che per particolari ideali A/I assume la struttura di dominio o di campo, i particolare vale la seguente

Proposizione 2. *Sia I un ideale di un anello commutativo A*

1. *I è ideale primo di A ⇔ A/I è un dominio.*
2. *I è ideale massimale di A ⇔ A/I è un campo.*

Dimostrazione: Sia I ideale primo di A, poichè I è propriamente contenuto in A si ha che A/I non è l'anello banale. Siano x+I e y+I due elementi di A/I entrambi diversi da 0+I, x e y non appartengono ad I ed essendo I primo xy non appartiene a I ovvero xy+I=(x+I)(y+I)≠(0+I), concludiamo che A/I è un dominio. Viceversa, sia A/I un dominio. Poichè A/I è non banale si ha che I propriamente contenuto in A. Siano x,y elementi di A tali che xy appartiene a I, allora xy+I=0+I, essendo A/I un dominio dobbiamo avere x+I=0+I o y+I=0+I ovvero x∈I o y∈I, quindi I è un ideale primo.
Sia ora I un ideale massimale di A. Ancora A/I è non banale perchè I è propriamente contenuto in A. Sia x+I un elemento di A/I diverso da 0+I, allora x∉I, x∈A. Consideriamo l'ideale I+Ax, I è propriamente contenuto in I+Ax infatti se y∈I possiamo sempre scrivere y=y+0x∈I+Ax e x=0+1x che appartiene a I+Ax. Poichè I è un ideale massimale di A si ha che I+Ax=A. Allora esistono un y in I e uno z in A tali che 1=y+zx, in A/I abbiamo (x+I)(z+I)=1+I quindi x+I è invertibile e A/I è un campo. Viceversa sia A/I un campo. Sia J un ideale di A tale che I è propriamente contenuto in J. Esiste allora x∈J tale che x∉I. Ora x∉I implica x+I≠0+I, essendo A/I un campo si ha che x+I è invertibile in A/I ovvero esiste y∈A tale che (x+I)(y+I)=1+I. Quindi xy+I=1+I e 1-xy∈I⊆J. Se scriviamo 1=(1-xy)+xy∈J vediamo che 1∈J e allora J=A. □

Definizione 8. *Sia A un anello. Consideriamo l'insieme* $\mathbb{C}=\{n\in\mathbb{N}\ n\neq 0$ *t.c.* $1_A n=0_A\}$*, distinguiamo due casi:*

- *l'insieme* $\mathbb{C}$ *è vuoto, ovvero* $1_A n\neq 0_A$ *per ogni* $n\neq 0$*. In tal caso diciamo che la caratteristica di A è zero e scriviamo char(A)=0.*
- *l'insieme* $\mathbb{C}$ *non è vuoto, poichè* $\mathbb{C}\subseteq\mathbb{N}$*, che sappiamo essere ben ordinato, esiste* $n=min\{m\in\mathbb{N},\ m\neq 0$ *t.c.* $m1_A=0_A\}$*. Diciamo allora che la caratteristica di A è n e scriviamo char(A)=n.*

Definizione 9. *Sia A un anello commutativo. Un A-modulo è un gruppo abeliano G e un'applicazione* $F:A\times G\to G$ *che manda* $(a,g)\mapsto F(a,g)$ *(denotiamo con ag l'immagine di F(a,g)) tale che per ogni* $a_1,a_2\in A$ *e per ogni* $g_1,g_2\in G$ *si ha:*

- $a_1(g_1+g_2)=a_1g_1+a_1g_2=(g_1+g_2)a_1$.
- $(a_1+a_2)g_1=a_1g_1+a_2g_1=g_1(a_1+a_2)$.
- $a_1(a_2g_1)=(a_1a_2)g_1=(a_2g_1)a_1$.

Se A è un anello con divisione ovvero un corpo allora un A-modulo unitario si dice uno spazio vettoriale.

Ad esempio ogni gruppo abeliano G è uno $\mathbb{Z}$-modulo. Inoltre $A[X_1,...,X_n]$ è un A-modulo.

Definizione 10. *Sia K un anello commutativo. Una K-algebra è un anello A tale che:*

- *(A,+) è un K-modulo unitario.*
- *k(ab)=(ka)b=a(kb) per ogni* $k\in K$ *e* $a,b\in A$*.*

Ad esempio un anello R è in particolare un gruppo abeliano e quindi uno $\mathbb{Z}$-modulo. Ora per ogni $n\in\mathbb{Z}$ e per ogni $r,s\in R$ si ha $n(rs)=(nr)s=r(ns)$. Vediamo allora che ogni anello è una $\mathbb{Z}$-algebra. Inoltre se K è un anello commutativo allora $K[X_1,...,X_n]$ è una K-algebra.

1.2 L'anello dei polinomi

Sia A un anello, una sequenza di elementi di A è una mappa $f:\mathbb{N}\to A$ denotata con $(f_0,f_1,...,f_n,...)$, dove per ogni $n\in\mathbb{N}$ $f_n=f(n)$. Denotiamo con A^N l'insieme di tutte le sequenze di elementi di A. Vogliamo ora introdurre su A^N una struttura d'anello, per fare questo useremo la somma puntuale e il **prodotto di convoluzione**, definito come segue:

$$\text{siano } f=(f_n),\ g=(g_n)\in A^N \text{ allora } (f*g)_n=\sum_{i=0}^{n} f_i g_{n-i}=\sum_{i+j=n} f_i g_j$$

Teorema 1. *Con la somma puntuale e il prodotto di convoluzione* $(A^N,+,*)$ *è un anello, inoltre se A è un anello commutativo anche* $(A^N,+,*)$ *lo è.*

Dimostrazione: Con la somma puntuale A^N è un gruppo abeliano. Mostriamo che il prodotto di convoluzione è associativo. Siano f,g,h$\in A^N$. Per ogni n$\in\mathbb{N}$ abbiamo:

$((f*g)*h)_n=\sum_{i+j=n}(f*g)_i h_j=\sum_{i+j=n}(\sum_{k+l=i})h_j=\sum_{i+j=n}(\sum_{k+l=i}h_j)$
$=\sum_{k+l+j=n}f_k g_l h_j=\sum_{k+i=n}(\sum_{l+j=i}f_k(g_l h_j))=\sum_{k+i=n}f_k(\sum_{l+j=i}g_l h_j)=$
$=\sum_{k+i=n}f_k(g*h)_i=(f*(g*h))_n$.

Sia ora $1=(1_A,0_A,...,0_A,...)$. Questo elemento è il neutro di $(A^N,*)$. Infatti per ogni n$\in\mathbb{N}$ abbiamo:

$(f*1)_n=\sum_{i=1}^{n}f_i 1_{n-i}=f_n 1_0=f_n 1_A=f_n=1_A f_n=1_0 f_n=\sum_{i=1}^{n}1_i f_{n-i}=(1*f)_n$ per ogni f$\in A^N$.

Vediamo che $*$ è distributiva rispetto a $+$. Siano f,g,h$\in A^N$, per ogni n$\in\mathbb{N}$ abbiamo:

$(f*(g+h))_n=\sum_{i=0}^{n}f_i(g+h)_{n-i}=\sum_{i=0}^{n}f_i(g_{n-i}+h_{n-i})=$
$=\sum_{i=0}^{n}f_i g_{n-i}+f_i h_{n-i})=\sum_{i=0}^{n}f_i g_{n-i}+\sum_{i=0}^{n}f_i h_{n-i})=(f*g)_n+(f*h)_n=$
$=((f*g)+(f*h)_n=((f*g)+(f*h))_n$.

Abbiamo così mostrato che f$*$(g+h)=(f$*$g)+(f$*$h). Analogamente si vede che (f+g)$*$h=(f$*$h)+(g$*$h).

Supponiamo ora che A sia commutativo, allora:

$(f*g)_n=\sum_{i+j=n}f_i g_j=\sum_{i+j=n}g_j f_i=(g*f)_n$

quindi anche $(A^N,+,*)$ è commutativo. □

Consideriamo adesso l'elemento $X=(0_A,1_A,0_A,...,0_A,...,0_A,...)$ in A^N. Tale elemento si dice **un'indeterminata**.

Lemma 1. *Per ogni i$\in\mathbb{N}$ la i-esima potenza X^i di X in $(A^N,+,*)$ soddisfa:*

$$X^i=(0_A,0_A,...,1_A,0_A,...) \text{ dove } 1_A \text{ occupa la i-esima posizione.}$$

Per ogni a$\in$A si ha:

$$a*X^i=(0_A,...,a,0_A,...)=X^i*a, \text{ dove a occupa la i-esima posizione.}$$

Dimostrazione: Procediamo per induzione su n. Se n=0 abbiamo $X^0=1=(1_A,0_A,...,0_A,...)$. Supponiamo che per un dato i$\in\mathbb{N}$ sia $X^i=(0_A,0_A,...,1_A,0_A,...)$ dove 1_A occupa la i-esima posizione. Per ogni k$\in\mathbb{N}$, k$>$0 abbiamo:

$$(X^{i+1})_k=(X*X^i)_k=\sum_{j=0}^{k}X_j(X^i)_{k-j}=X_1(X^i)_{k-1}=(X^i)_{k-1} \text{ e } (X^{i+1})_0=0.$$

Per ipotesi di induzione sappiamo che $(X^i)_j\neq 0$ se i$\neq$j a $(X^i)_i=1$. Da cui $(X^{i+1})_k=0$ per ogni k$\neq$i+1 e $(X^{i+1})_{i+1}=(X^i)_i=1_A$.
Sia ora a$\in$A. Allora $(a*X^i)_k=\sum_{j=0}^{k}a_j(X^i)_{k-j}$. Vediamo che $(a*X^i)_k=a(X^i)_k$, così si ha $(a*X^i)_k=0_A$ se k$\neq$i e $(a*X^i)_i=a$.
In modo analogo $(X^i*a)_k=\sum_{j=0}^{k}(X^i)_j a_{k-j}$. Da cui $(X^i*a)_k=(X^i)_k a$ e come prima $(X^i*a)_k=0$ se k$\neq$i e $(X^i*a)_i=a$. □

Sia ora f∈A^N. Grazie al lemma precedente possiamo scrivere
f=(f_0,f_1,...,f_n,...)=(f_0,0,...,0,...)+(0,f_1,0,...,0,...)+...+(0,...,f_n,0,...)+...=f_0+f_1X+...+$f_n X^n$+...
L'anello (A^N,+,∗) si dice **anello delle serie formali nell'indeterminata X a coefficienti nell'anello A**. Tale anello viene denotato con A[[X]]. Gli elementi di A[[X]] vengono detti serie formali e denotati con f=$\sum_{n=0}^{\infty} f_n X^n$. Da A[[X]] costruiremo ora l'anello dei polinomi a coefficienti in A che verrà denotato con A[X]. Introduciamo:

A[X]={f∈A[[X]] t.c. esiste n∈ℕ tale che f_h=0 per ogni h>n}.

Vediamo che A[X] è il sottoinsieme di A[[X]] costituito dalle serie formali che sono nulle da un certo indice in poi. Gli elementi di A[X] si dicono polinomi a coefficienti in A nell'ideterminata X. Sia f∈A[X], f≠0 allota {i∈ℕ tali che f_i≠0} è un isieme finito e non vuoto, ha senso allora considerare il numero n=max{i∈ℕ tali che f_i≠0} che viene detto grado del polinomio f e denotato con deg(f). Il coefficiente f_n si dice coefficiente direttivo del polinomio f e viene denotato con c(f). Infine se c(f)=1 il polinomio si dice monico.

Osservazione 1. *A[X] è un sottoanello di A[[X]] contenente A.*

Proposizione 3. *Sia A un anello. Allora:*

1. *char(A)=char(A[X])=char(A[[X]]);*
2. *se A è un dominio gli elementi invertibili di A[X] sono tutte e sole le costanti invertibili di A.*

Dimostrazione: 1) Segue dal fatto che A è un sottoanello di A[X] e A[X] è un sottoanello di A[[X]].
2) Sia A un dominio, supponiamo che f∈A[X] sia invertibile, allora esiste f^{-1} tale che ff^{-1}=1. Perciò deg(ff^{-1})=deg(f)+deg(f^{-1})=deg(1)=0 e questo implica che deg(f)=0 ovvero f è una costante invertibile di A. □

Sia A un anello. L'anello dei polinomi A[X_1,...,X_n] in n indeterminate a coefficienti in A può essere definito ricorsivamente ponendo:

- A[X_1] = l'anello dei polinomi nella sola indeterminata X_1 a coefficienti in A;
- A[X_1,...,X_n]=A[X_1,...,X_{n-1}][X_n] se n>1.

Nel seguito noi considereremo l'anello dei polinomi in n indeterminate a coefficienti in un campo algebricamente chiuso. Osseriviamo che l'anello dei polinomi a coefficienti in un campo K ha una struttura di K-spazio vettoriale di dimensione infinita, infatti una sua base è:

{1, X, X^2, X^3,....., X^n,.....}

1.3 Campi, P.I.D. e U.F.D.

Definizione 11. *Un campo K si dice algebricamente chiuso se ogni polinomio p(X)∈K[X] non costante ha almeno una radice in K, ovvero se esiste x_0 in K tale che p(x_0)=0.*

Osservazione 2. *Se K è algebricamente chiuso e p∈K[X] ha grado n allora p ha esattamente n radici in K contate con molteplicità.*

Definizione 12. *Sia A un anello e sia T un sottoinsieme di A allora $\bigcap I_j$, dove gli I_j sono gli ideali di A contenenti T, è il più piccolo ideale di A contenente T, si dice ideale di A generato da T e si indica con (T). Se T è finito (T) si dice finitamente generato.*

Definizione 13. *Sia A un anello, I è un ideale principale di A se esiste x∈A tale che I=(x). Se D è un dominio, D si dice un dominio a ideali principali (P.I.D.) se ogni ideale di D è principale.*

Definizione 14. *Sia D un dominio, D si dice un dominio euclideo se esiste una mappa $\varphi: D^* \longrightarrow N$ tale che per ogni a∈D e per ogni b∈D* esistono q,r∈D tali che a=bq+r con r=0 o r≠0 e $\varphi(r) < \varphi(b)$.*

Teorema 2. *Ogni dominio euclideo D è un P.I.D.*

Dimostrazione: Sia I un ideale di D. Se I è l'ideale banale allora I=(0) e siamo a posto. In caso contrario esiste x∈I, x≠0. L'insieme $\Omega=\{\varphi(x)$ tale che $x\in I^*\}$ non è vuoto ed è un sottoinsieme di $\mathbb{N}$ che sappiamo essere ben ordinato, perciò esiste $n=\min(\Omega)$. In particolare $n\in\Omega$ quindi esiste un x_0 in I* tale che $\varphi(x_0)=n$. Vogliamo mostrare che $I=(x_0)$. Sia x un elemento di I. Se x=0 allora $x=x_0*0$. Se x≠0 poichè $x_0\neq 0$ per l'algoritmo euclideo di divisione con resto esistono unici q,r in D tali che $x=qx_0+r$ con r=0 o $\varphi(r)\leq\varphi(x_0)$. Vediamo che $r=x-qx_0$ è in I, se fosse r≠0 avrei trovato in Ω un elemento r tale che $\varphi(r)\leq\varphi(x_0)$, assurdo. Allora r=0 e $x=qx_0$ appartiene all'ideale (x_0). Concludiamo che $I=(x_0)$ e D è un dominio a ideali principali. □

Teorema 3. *Se K è un campo K[X] è un dominio euclideo e in particolare K[X] è un P.I.D.*

Dimostrazione: Consideriamo l'applicazione $\varphi: K[X]^* \longrightarrow \mathbb{N}$ che associa al polinomio p il suo grado deg(p). Siano ora f e g polinomi in K[X], g non identicamente nullo. Allora il coefficiente direttivo di g è non nullo ed essendo K un campo è invertibile. Possiamo dunque applicare l'algoritmo di divisione tra polinomi e concludere che esistono due polinomi q e r in K[X] tali che f=gq+r con r=0 o deg(r)<deg(g). Quindi D è un dominio euclideo e per il teorema precedente è un P.I.D. □

Definizione 15. *Sia D un dominio e sia d∈D*

1. *d si dice elemento primo di D se d è non nullo, non invertibile e se d|ab implica d|a o d|b.*
2. *d si dice elemento irriducibile di D se d è non nullo, non invertibile e se d=ab implica a inveritbile o b invertibile.*

Teorema 4. *Sia D un dominio valgono i seguenti fatti:*

1. *p è primo in D⇔p è non nullo e (p) è ideale primo di D.*
2. *Ogni p primo in D è irriducibile in D.*

Dimostrazione: Sia p primo in D. Poichè p è non nullo e non invertibile si ha che (p) non è banale ed è un ideale proprio di D. Siano ora x,y$\notin$(p) allora p non divide x e p non divide y, p non può dividere xy essendo primo quindi xy$\notin$(p) e (p) è ideale primo di D. Viceversa sia (p) ideale primo e non banale. L'elemento p è non nullo inoltre non è invertibile perchè (p) è ideale proprio di D. Siano ora x,y$\in$D tali che p divide xy. Allora xy$\in$(p), essendo questo un ideale primo sia ha che x$\in$(p) o y$\in$(p). Nel primo caso p divide x, nel secondo p divide y. Vediamo ora che ogni primo è irriducibile. Sia p un primo. Per definizione p è non nullo e non invertibile. Siano x,y$\in$D tali che p=xy allora p divide xy e poichè è primo deve essere p divide x o p divide y. Nel primo caso possiamo scrivere pa=x, allora x=pa=xya da cui ya=1 (D è un dominio) perciò y è invertibile. Nel secondo caso si ha pb=y da cui y=pb=xyb e xb=1 (D è un dominio) e x è invertibile. Concludiamo che p è irriducibile. □

Teorema 5. *Sia D un P.I.D. e sia x$\in$D i seguenti fatti sono equivalenti:*

1. *x è irriducibile in D.*
2. *(x) è ideale massimale di D.*
3. *(x) è ideale primo di D.*
4. *x è primo in D.*

Dimostrazione: 1)$\Rightarrow$2) Sia x irriducibile in D. Essendo x non invertibile si ha che (x) è ideale proprio di D. Sia ora I un ideale proprio di D contenente (x). Vogliamo mostare che I=(x) ovvero che I$\subseteq$(x). Ora D è un P.I.D. quindo esiste un elemento y di D tale che I=(y), dunque (x)$\subseteq$(y) e allora possiamo scrivere x=ay e vediamo che y divide x. Ma y non è invertibile perchè I=(y) è ideale proprio di D, inoltre x è irriducibile quindi esiste un elemento invertibile b tale che by=x, e quindi y=b^{-1}x. Vediamo così che (x)=(y)=I.
2)$\Rightarrow$3)Sia (x) massimale. Sappiamo allora che D/(x) è un campo quindi in particolare è un dominio e allora (x) è primo.
3)$\Rightarrow$4) Vero per il teorema precedente
4)$\Rightarrow$1) Sia p$\in$D un elemento primo, allora p$\neq$0 e p non è invertibile in D. Siano a,b$\in$D tali che p=ab, allora p|ab, essendo p primo si ha che p|a oppure p|b, ovvero a=pa' o b=pb'. Si ha allora a=aba' o b=abb' da cui a(1-ba')=0 o (1-ab')b=0. Essendo D un dominio si ha 1-ba'=0 o 1-ab'=0 ovvero a è invertibile oppure b è invertibile. □

Definizione 16. *Un dominio D si dice un dominio a fattorizzazione unica (U.F.D.) se è possibile esprimere ogni elemento non nullo e non invertibile di D come prodotto di elementi primi in D in un unico modo.*

Introduciamo ora la nozione di ideale radicale.

Definizione 17. *Sia A un anello commutativo e I un suo ideale. Il radicale di I, denotato con r(I), è $\bigcap$P, dove l'interzesione è fatta su tutti gli ideali primi P di A che contengono I. Se l'insieme degli ideali primi di A che contengono I è vuoto, allora si definisce r(I)=A. Un ideale J di A si dice radicale se r(J)=J.*

Ad esempio in un dominio di integrità l'ideale (0) è primo, dunque r({0})={0}. Nell'anello $\mathbb{Z}$, r(12)=(2)∩(3)=(6) e r(4)=(2)=r(32).

Proposizione 4. *Sia A un anello commutativo e I un suo ideale, allora*

1. *r(I) è un ideale.*
2. *r(I)={a∈A tali che a^n∈I per qualche n>0}, in particolare I⊆r(I).*
3. *Un ideale primo è sempre radicale.*
4. *r(I) è sempre radicale.*

Dimostrazione: 1) Notiamo che 0∈r(I) dunque r(I) non è vuoto. Siano x,y∈r(I), allora certamente x e y appartengono ad uno stesso ideale primo P contenente I, dunque x-y∈P e ax=xa∈P per ogni a∈A e x∈P. Quindi x-y∈r(I) e ax∈r(I) per ogni a∈A e x∈r(I) ovvero r(I) è un ideale di A.
2) Se r(I)=A, allora {a∈A tali che a^n∈I}⊂r(I). Possiamo supporre allora r(I) propriamente contenuto in A. Se a^n∈I e P è un ideale primo di A contenente I allora a^n∈P ed essendo P primo si ha a∈P e P è contenuto in r(I). Dunque {a∈A tali che a^n∈I}⊂r(I). Viceversa se a∈A e a^n∉I per ogni n>0, allora S={a^n+x con n∈$\mathbb{N}^*$, x∈I} è un insieme moltiplicativo tale che S∩I è vuoto. Allora esiste un ideale primo P disgiunto da S che contiene I. Per costruzione a∉P e perciò a∉r(I). Dunque r(I)⊆{a∈A tali che a^n∈I}.
3) Supponiamo per assurdo che I sia propriamente contenuto in r(I) allora possiamo trovare un x∈r(I) tale che x∉I. Sia n il più piccolo intero positivo tale che x^n∈I, allora x^{n-1}∉I ed essendo I primo x^{n-1}x=x^n∉I, assurdo.
4) Consideriamo r(r(I)) e mostriamo r(r(I))⊆r(I). Sia x∈r(r(I)) allora esiste un k intero positivo tale che x^k∈r(I) e ancora esiste un h intero positivo tale che $(x^k)^h$∈I ovvero x^{kh}∈I. Abbiamo così trovato un intero positivo kh tale che x^{kh}∈I dunque x∈r(I). □

1.4 Anelli Noetheriani

Introduciamo ora una particolare classe di anelli detti anelli Noetheriani. Gli anelli Noetheriani sono fondamentali in geometria algebrica perchè ogni loro ideale è finitamente generato, diventa così possibile descrivere una varietà algebrica attraverso un numero finito di equazioni polinomiali. Gli anelli Noetheriani possono essere definiti in modi diversi che però risultano tra loro equivalenti. Mostriamo per prima cosa l'equivalenza delle due definizioni seguenti.

Definizione 18. *Un anello A si dice Noetheriano se*

1. *Ogni successione crescente $I_0⊆I_1⊆I_2$.....$⊆I_n⊆$.... di ideali di A è stazionaria ovvero se esiste un I_k tale che $I_j=I_k$ per ogni j≥k.*
2. *Ogni ideale di A è finitamente generato.*

1)⇒2) Sia I un ideale di A non banale e sia x_1 un elemento non nullo di I. Poniamo $I_1=(x_1)$, se I_1=I siamo a posto, in caso contario sia x_2 ∈I-I_1. Poniamo $I_2=(x_1, x_2)$. Se I_2=I a posto altrimenti procediamo e otteniamo una succesione I_1, I_2,...., I_n,... crescente di ideali. Questa succesione è per ipotesi stazionaria

e I è un suo elemento quindi deve essere I=I_k dove I_k=(x_1, x_2,...., x_k) per un certo intero k. Vediamo così che un generico ideale di A è finitamente generato. 2)⇒1) Supponiamo ora che ogni ideale di A sia finitamente generato. Sia I_1, I_2,...., I_n,... una successione crescente di ideali di A. Consideriamo l'ideale I=$\bigcup_n I_n$. L'ideale I è finitamente generato e possiamo scrivere I=(x_1,...,x_n). Ora gli x_1,...,x_n sono distribuiti su al più n distinti ideali della catena. Possiamo supporre che x_1∈I_1,...,x_n∈I_n e per come è cotruita la catena si ha x_1,...,x_n∈I_n, dunque I_k=I per ogni k≥n e la catena è stazionaria.

Proposizione 5. *Ogni P.I.D. è un anello Noetheriano.*

Dimostrazione: In un P.I.D. ogni ideale è principale ovvero generato da un solo elemento, in particolare ogni ideale è finitamente generato e quindi ogni P.I.D. è un anello Noetheriano. □

Diamo ora un risultato fondamentale in geometria algebrica, il Teorema della base di Hilbert. Questo teorema asserisce che se A è un anello Noetheriano anche A[X_1,X_2,....,X_n] lo è.

Teorema 6 (Della base di Hilbert)**.** *Sia A un anello Noetheriano allora A[X_1, X_2,....,X_n] è un anello Noetheriano.*

Dimostrazione: Cominciamo col provare che se A è noetheriano anche A[X] lo è. Sia J un ideale di A[X] vogliamo mostrare che J è finitamente generato. Per ogni n∈ℕ sia I_n l'insieme degli a∈A tali che a=0 oppure a è il coefficiente direttivo di un polinomio f∈J di grado n. Verifichiamo che gli I_n sono ideali di A. Per definizione 0∈I_n dunque gli I_n sono non vuoti. Siano poi p,q∈I_n se p=0 oppure q=0 allora p-q=p∈I_n analogmente se p=q si ha p-q=0∈I_n. Possiamo perciò suppore p,q entrambi non nulli. Allora esistono due polinomi P(X)=pX^n+...+P_0 e Q(X)=qX^n+...+Q_0 quindi P(X)-Q(X)=(P-Q)(X)=(p-q)X^n+...+P_0-Q_0, e p-q è il coefficiente direttivo di un polinomio di grado n ovvero p-q∈I_n. Siano poi p∈I_n e a∈A. Allora esiste un polinomio P(X)=pX^n+...+P_0 quindi aP(X)=(ap)X^n+...+aP_0 e perciò anche ap∈I_n. Quindi gli I_n sono ideali di A. Ora se p∈I_n è il coefficiente direttivo di un polinomio f∈J di grado n si ha che p è anche il coefficiente direttivo del polinomio xf∈J di grado n+1. Vediamo così che I_0⊆I_1⊆...⊆I_n⊆..., essendo A noetheriano sappiamo che la catena è stazionaria ovvero che esiste un t∈ℕ tale che I_t=I_n per ogni t≥n. Inoltre ogni ideale I_n è finitamente generato e possiamo scrivere I_n=(a_{i1},...,a_{in}). Per ogni a_{nj} con n≤t è 1≤j≤i_n, sia f_{nj} un polinomio in J di grado n con coefficiente direttivo a_{nj}. Notiamo che f_{0j}=r_{0j}∈A⊂A[X]. Denotiamo con X l'insieme finito {f_{nj} tali che n≤t è 1≤j≤i_n}. Vogliamo mostrare che J è generato da X. Chiaramente (X)⊆J. Ora i polinomi di grado 0 in J sono proprio gli elementi di I_0 e perciò sono contenuti in (X). Procediamo per induzione, supponiamo che (X) contenga tutti i polinomi di J di grado minore di k e sia G un polinomio di J di grado k con coefficiente direttivo g≠0.
Se k≤t allora g∈I_k e possiamo scrivere g=s_1r_{k1}+...+$s_{ik}r_{kik}$, per opportuni s_j∈A. Allora il polinomio $\sum_{j=1}^{ik} s_j f_{kj}$∈(X) ha coefficiente direttivo g e grado k. Quindi G-$\sum_{j=1}^{ik} s_j f_{kj}$ ha grado al più k-1. Per ipotesi di induzione G-$\sum_{j=1}^{ik} s_j f_{kj}$∈(X) e quindi anche G∈(X).
Se k≥t, allora g∈I_k=I_t e G=$\sum_{j=1}^{it} s_j a_{tj}$. Inoltre $\sum_{j=1}^{it} s_j X^{k-t} f_{tj}$∈(X) ha coefficiente direttivo g e grado k. Allora G-$\sum_{j=1}^{it} s_j X^{k-t} f_{tj}$ ha grado al più k-1 e sta

in (X) per ipotesi induttiva. Quindi anche G∈(X). Concludiamo che J=(X) è finitamente generato.
Mostriamo ora che A noetheriano implica A[X_1, X_2,....,X_n] noetheriano per induzione su n. Se n=1 siamo nel caso precedente. Supponiamo l'asserto vero per n-1, allora B=A[X_1, X_2,....,X_{n-1}] è un anello noetheriano per ipotesi di induzione. Ora possiamo riguaradare A[X_1, X_2,....,X_n]=B[X_n] che è noetheriano ancora per la prima parte della dimostrazione. □

Proposizione 6. *Sia A un anello Noetheriano. Allora ogni famiglia non vuota F di ideali di A ha un elemento massimale per l'inclusione.*

Dimostrazione: Sia P(F) l'insieme delle parti di F. Per l'assioma della scelta possiamo costruire l'applicazione f: P(F)⟶F definita da f(S)=I_S dove I_S è un ideale di A scelto tra gli ideali del sottoinsieme S di F. Sia I_0=f(F) e S_1={J in F tali che I_0 è propiamente contenuto in J}. Se S_1 è vuoto siamo a posto perchè I_0 è massimale per l'inclusione in F. Se S_1 non è vuoto sia I_1=f(S_1). Definiamo S_2={J in F tali che I_1 è propriamente contenuto in J}. Se S_2 è vuoto allora I_1 è massimale per l'inclusione. Dobbiamo dimostare allora che esiste un n tale che S_n è vuoto. Supponiamo per assurdo che S_n sia non vuoto per ogni n. Per come è stato costruito si ha che I_p∈S_p={J in F tali che I_{p-1} è propriamente contenuto in J}, quindi I_{p-1}⊂I_p. Ora I=$\bigcup I_n$ è un ideale di A. Essendo A Noetheriano I è finitamente generato: I=(f_1,....,f_m), con f_i ∈I_{ni}. Sia M=max(n_i) con n_i=1,...,m. Allora f_i∈I_M per ogni i=1,....,r, questo implica I=I_M, assurdo.

□

1.5 Il Teorema fondamentale dell'Algebra

Abbiamo dato in precedenza la definizione di campo algebricamente chiuso. Buona parte delle considerazioni di geometria algebrica che faremo in seguito valgono proprio sotto questa ipotesi su K, in particolare il teorema di Bezout. Il teorema fondamentale dell'algebra asserisce che il campo dei numeri complessi $\mathbb{C}$ è algebricamente chiuso. Questo fatto diventerà per noi molto importante perchè potremmo ambientare la nostra geometria su spazi affini o proiettivi su $\mathbb{C}$. Tra tutte le dimostrazioni del teorema fondamentale dell'algebra quella a mio parere più bella e più semplice viene dall'Analisi Complessa.

Consideriamo il piano complesso, una regione di $\mathbb{C}$ è un sottoinsieme aperto e connesso di $\mathbb{C}$ dotato della topologia usuale su $\mathbb{R}^2$.

Definizione 19. *Sia R una regiore di $\mathbb{C}$ e sia f:R⟶$\mathbb{C}$ una funzione definita su R. Diremo che f è olomorfa in R se è differenziabile in senso complesso in R ovvero se per ogni z_0∈R esiste finito*

$$\lim_{z\to z0} \frac{f(z)-f(z0)}{z-z0} = D(f)(z_0).$$

Una funzione olomorfa su tutto $\mathbb{C}$ si dice intera.

Un risultato fondamentale in Analisi Complessa è il teorema di sviluppabilità delle funzioni olomorfe [1] il quale afferma che ogni funzione olomorfa in R è sviluppabile in serie di Taylor in ogni punto di R, ovvero se $z_0 \in R$ in un disco $D(z_0,r)$ è possibile scrivere

$$f(z)=\sum_{n=0}^{\infty} f^{(n)}(z_0)/n!\ (z-z_0)^n$$

e che inoltre i coefficienti di tale sviluppo in serie sono dati da

$$a_n=1/2\pi \int f(z)/(z-z_0)^{n+1}\ dz$$

dove l'integrale è fatto sulla frontiera δD di un disco D contenuto nel disco di convergenza della serie di f.

Grazie a questo fatto introduciamo ora le stime di Cauchy per i coefficienti di Taylor di una funzione olomorfa al fine di dimostare il teorema di Liouville. Il teorema fondamentale dell'algebra sarà allora un immediato corollario di quest' ultimo risultato. Si ha

$$a_n=1/2\pi\ \int f(z)/(z-z_0)^{n+1}\ dz \leq |f|/r^n = M(r)/r^n$$

Dove M(r) è il massimo di |f| sulla frontiera del disco D di raggio r.

Teorema 7 (Di Liouville)**.** *Ogni funzione intera e limitata su* $\mathbb{C}$ *è costante.*

Dimostrazione: Abbiamo che f è intera e quindi sviluppabile in serie di potenze in tutto $\mathbb{C}$, applichiamo le stime di Cauchy ai suoi coefficienti di Taylor. Poichè f è limitata esiste un reale M tale che $|f| \leq M$ su $\mathbb{C}$.

$$a_n \leq M(r)/r^n \leq M/r^n \longrightarrow 0 \text{ per } r \mapsto \infty \text{ per ogni } n>0.$$

Allora l'unico coefficiente non nullo è a_0 e quindi $f(z)=a_0$ su $\mathbb{C}$ è costante. □

Lemma 2 (Teorema fondamentale dell'Algebra)**.** *Ogni polinomio non costante a coefficienti in* $\mathbb{C}$ *ha una radice in* $\mathbb{C}$*, ovvero* $\mathbb{C}$ *è algebricamente chiuso.*

Dimostrazione: Supponiamo per assurdo che $p \in \mathbb{C}[z]$ non costante non abbia radici in $\mathbb{C}$. Allora $f(z)=1/p(z)$ è una funzione intera e limitata infatti poichè $p(z) \to \infty$ per $z \to \infty$ si ha che $1/p(z) \to 0$ per $z \to \infty$. Quindi per il teorema di Liouville è costante, ma allora anche p(z) è costante e questo è assurdo. Concludiamo che p ha una radice in $\mathbb{C}$. □

1.6 Spazi e Varietà topologiche

In questa sezione facciamo alcune premesse riguardo gli spazi topologici. Vedremo che $\mathbb{A}^n$ e $\mathbb{P}^n$ diventeranno infatti spazi topolocigi una volta introdotta la topologia di Zariski. Nel seguito parleremo spesso di varietà algebriche, ogni curva algebrica e in particolare ogni cubica di $\mathbb{P}^2$ è una varietà algebrica di dimensione uno. Vogliamo ora introdurre il concetto più generale di varietà topologica e di varietà differenziabile. Molti concetti di geometria algebrica ad esempio quello di spazio tangente possono infatti essere reinterpretati attraverso

[1] Si veda Walter Rudin - Analisi reale e complessa

la geometria differenziale. Le varietà algebriche come luoghi geometrici definiti dagli zeri di polinomi sono infatti particolari varietà differenziabili. Osserviamo che è possibile introdurre formalmente la derivata di un polinomio cioè senza ricorerre al concetto analitico di limite. Esiste però una differenza sostanziale tra la geometria algebrica e la geometria differenziale. In geometria differenziale, grazie al teorema delle funzioni implicite, possiamo invertire localmente un diffeomorfismo nell'intorno di ogni suo punto di definizione. L'inversa locale così trovata è ancora un'applicazione differenziabile. In geometria algebrica consideriamo funzioni polinomiali P(X) definite su varietà algebriche. Notiamo però che in generale l'inversa di una funzione polinomiale è una funzione razionale. Perciò si passa a considerare le funzioni razionali del ripo R(X)=P(X)/Q(X). Tuttavia anche se un punto x non è uno zero di Q non è detto che R sia invertibile in un intorno di x e che la sua inversa sia ancora una funzione razionale. Per questo si introducono le applicazioni birazionali, tali applicazioni sono proprie della geometria algebrica.

Definizione 20. *Uno spazio topologico è una coppia (X,T) dove X è un insieme e T una topologia su X, ovvero T è una famiglia di insiemi A_i detti aperti di X tali che:*

- *L'insieme vuoto e X appartengono a T.*
- *Ogni unione arbitraria di aperti appartiene a T.*
- *Ogni intersezione finita di aperti appartiene a T.*

Definizione 21. *Un sottoinsieme C di uno spazio topologico X si dice un chiuso se è il complementare di un aperto di X.*

Definizione 22. *Uno spazio topologico X si dice di Hausdorff se comunque presi x_1, $x_2 \in X$ distinti esistono due aperti A_1 e A_2 contenenti rispettivamente x_1, x_2 tali che $A_1 \cap A_2$ è il vuoto.*

Definizione 23. *Uno spazio topologico X si dice compatto se da ogni ricoprimento aperto di X è possibile estrarre un sottoricoprimento finito.*

Vedremo che $\mathbb{A}^n$ con la topologia di Zariski non è di Hausdorff ma è compatto.

Proposizione 7. *Ogni sottoinsieme chiuso di uno spazio topologico compatto X è compatto.*

Dimostrazione: Sia C un chiuso dello spazio topologico compatto X. Allora C^C è aperto e $C \cup C^C = X$. Sia (A_i) un ricoprimento aperto di C, allora $(A_i) \cup C^C$ è un ricoprimento aperto di X. Essendo X compatto possiamo estarre un sottoricoprimento finito $(A_i)_{i=1,\dots,n}$ che potrebbe anche includere C^C. Ma certamente $(A_i)_{i=1,\dots,n}$-C^C è un sottoricoprimento finito di C estratto da (A_i). Dunque il chiuso C è compatto. □

Definizione 24. *Sia X uno spazio topologico un sottoinsieme V di X si dice denso in X se per ogni aperto A di X si ha che $V \cap A$ non è vuoto.*

Definizione 25. *Uno spazio topologico X si dice irriducibile se per ogni coppia di aperti non vuoti U,V, si ha che $U \cap V$ non è vuoto. In caso contrario X si dice riducibile. Il vuoto è per convenzione riducibile.*

Proposizione 8. *Sia X un spazio topologico. I seguenti fatti sono equivalenti.*

1. *X è irriducibile.*
2. *Se C e F sono due chiusi di X tali che C∪F=X allora X=C o X=F.*
3. *Ogni aperto non vuoto di X è denso in X.*

Dimostrazione: 1)⇒2) Sia C∪F=X allora $C^c \cap F^c$ è vuoto. Ma C^c e F^c sono due aperti che hanno intersezione vuota in X irriducibile, assurdo. Allora uno dei due deve essere il vuoto. Equivalentemente o X=C o X=F.
2)⇒3) Sia U un aperto non vuoto di X. Sia poi V un aperto non vuoto di X diverso da U. Supponiamo per assurdo che U∩V sia vuoto. Allora $U^c \cup V^c$=X. Abbiamo scritto X come unione di chiusi, per ipotesi uno tra gli aperti U e V deve essere vuoto, assurdo.
3)⇒1) Se ogni aperto non vuoto U di X è denso in X per definizione di insieme denso si ha che comunque preso un secondo aperto V di X si ha che U∩V non è vuoto. Quindi X è irriducibile. □

Proposizione 9. *Uno spazio topologico X è di Hausdorff se e solo se la diagonale D={(x,x) tali che x∈X} è chiusa in X×X dotato della topologia prodotto.*

Dimostrazione: Supponiamo che X sia di Hausdorff. Consideriamo X×X-D, sia (x,y)∈A allora x≠y con x,y∈X. Ora X è di Hausdorff quindi esistono due intorni U_x e U_y rispettivamente di x e y tali che $U_x \cap U_y$ è vuoto. Consideriamo ora V=$U_x \times U_y$. Vediamo che se esistesse una coppia (t,t)∈V avremmo che t∈$U_x \cap U_y$ e questo è assurdo. Allora V∩D è vuoto e V è contenuto in X×X-D che risulta essere aperto. Dunque D è chiuso in X×X. Viceversa sia D chiuso in X×X. Siano x,y∈X, x≠y. Ora la coppia (x,y)∈X×X-D che è aperto, quindi esiste un intorno I di (x,y) in X×X tutto contenuto in X×X -D. Scriviamo I come prodotto di aperti di X, I=U×V, con U intorno di x e V intorno di y, dove U=P_1(I) e V=P_2(I) sono le immagini di I attraverso le due proiezioni canoniche che sono in particolare omeomorfismi. Se fosse U∩V non vuoto avremmo un t∈U∩V ovvero una coppia (t,t)∈I, assurdo. Allora U∩V è vuoto e X è di Hausdorff. □

Definizione 26. *Una varietà topologica V di dimensione n (n è un numero naturale) è uno spazio topologico di Hausdorff nel quale ogni punto ha un intorno aperto omeomorfo ad un disco D^n di $\mathbb{R}^n$. Ogni aperto di V omeomorfo ad un disco D^n si dice una carta locale.*

Introduciamo ora il concetto di varietà differenziabile. Sia U⊆$\mathbb{R}^n$ un aperto e F:U→$\mathbb{R}^m$ un'applicazione che ad ogni x∈U associa F(x)=(F_1(x),...,F_m(x)). Diremo che F è di classe C^k in U se le sue componenti F_1,...,F_m sono di classe C^k in U ovvero ammettono derivate continue in U fino all'ordine k. Un'applicazione di classe C^k in un aperto U è ancora di classe C^k anche su ogni aperto V⊆U. Se U⊆$\mathbb{R}^n$ e V⊆$\mathbb{R}^m$ sono due aperti, F:U→$\mathbb{R}^m$ e G:V→$\mathbb{R}^p$ sono applicazioni di classe C^k tali che F(U)⊆V, allora l'applicazione composta G∘F:U→$\mathbb{R}^p$ è ancora un'applicazione di classe C^k.

Definizione 27. *Se U,V sono due aperti di $\mathbb{R}^n$, una biezione F:U→V si dice un diffeomorfismo di classe C^k se sia F sia la sua inversa F^{-1}:V→U sono*

applicazioni di classe C^k. Se esiste un diffeomorfismo di classe C^k $F:U\to V$ anche $F^{-1}:U\to V$ è un diffeomorfismo di classe C^k e in tal caso U e V si dicono diffeomorfi di classe C^k.

Abbiamo fino ad ora considerato sottoinsiemi aperti. Estendiamo le definizioni di applicazione e diffeomorfismo di classe C^k a un qualsiasi sottoinsieme $X\subseteq\mathbb{R}^n$. Sia $X\subseteq\mathbb{R}^n$ un sottoinsieme e $F:X\to\mathbb{R}^m$ un'applicazione. Si dice che F è di classe C^k in X se per ogni $x\in X$ esiste un intorno aperto U_x di x ed un'applicazione $\overline{F}:U_x\to\mathbb{R}^m$ di classe C^k tale che $\overline{F}(x)=F(x)$ per ogni $x\in X\cap U_x$.

Definizione 28. *Siano $X\subseteq\mathbb{R}^n$ e $Y\subseteq\mathbb{R}^m$, un'applicazione $F:X\to Y$ è un diffeomorfismo di classe C^k se è biettiva e se anche F^{-1} è di classe C^k. Se una tale F esiste si dice che X e Y sono diffeomorfi di classe C^k.*

La composizione e la restrizione di funzioni di classe C^k a sottoinsiemi qualsiasi sono ancora funzioni di classe C^k.

Definizione 29. *Sia X uno spazio topologico. Una coppia (U,φ_U) dove U è un aperto di X e $\varphi_U:U\to\mathbb{R}^n$ un omeomorfismo di U su un aperto di $\mathbb{R}^n$ si dice una n-carta locale. Due n-carte locali (U,φ_U) e (V,φ_V) in X si dicono C^k-compatibili se $U\cap V$ è il vuoto oppure se $U\cap V$ è non vuoto e l'applicazione $\varphi_V\circ{\varphi^{-1}}_U:\varphi_U(U\cap V)\to\varphi_V(U\cap V)$ è un diffeomorfismo di classe C^k.*

Ad esempio le carte locali $(\mathbb{R},x)$ e $(\mathbb{R},x^3)$ non sono C^1-compatibili, infatti la funzione $\sqrt[3]{x}$ è un omeomorfismo di $\mathbb{R}$ in sè ma non è di classe C^1 in $x_0=0$.

Definizione 30. *Un n-atlante differenziabile di classe C^k nello spazio topologico V è una famiglia di n-carte locali $(U_i,\ \varphi_i)$ dove gli U_i costituiscono un ricoprimento di V e le carte $(U_i,\ \varphi_i)$ sono a due a due C^k-compatibili. Si dice allora che l'atlante $(U_i,\ \varphi_i)$ definisce su uno spazio topologico di Hausdorff e a base numerabile V una struttura di varietà differenziabile di classe C^k. L'intero n si dice la dimensione della varietà V.*

Definizione 31. *Sia X una varietà differenziabile. Un sottoinsieme $Y\subseteq X$ si dice una sottovarietà differenziabile di dimensione m di X se per ogni $y\in Y$ esiste un intorno U_y di y in X e un'applicazione differenziabile $F_x:U_y\to\mathbb{R}^m$ che induce una biezione F_y di $U_y\cap Y$ su un aperto V di $\mathbb{R}^m$ tale che la biezione inversa $V\to U_y\cap Y$ sia differenziabile come applicazione di V in X. Se dim(X)=n, l'intero n-m si dice codimensione di Y in X.*

Sia ora X una varietà differenziabile e $p\in X$. Denotiamo con $\Omega(X,p)$ l'insieme delle funzioni a valori reali definite su qualche intorno di p in X. Ora se $F,G\in\Omega(X,p)$ allora anche F+G e FG appartengono a $\Omega(X,p)$. Un vettore tangente a X in p è un'applicazione $v:\Omega(X,p)\to\mathbb{R}$ tale che $v(aF+bG)=aV(F)+bV(G)$ e $v(FG)=v(F)G(p)+F(p)v(G)$ per ogni $F,G\in\Omega(X,p)$ e $a,b\in\mathbb{R}$. L'insieme di tutti i vettori tangenti a X in p si denota con $T_p(X)$ e si chiama spazio tangente a X in p. Una volta introdotta la nozione di spazio tangente possiamo dare la definizione di immersione e summersione entrambe come vedremo di natura locale.

Definizione 32. *Un morfismo di varietà differenziabili $F:X\to Y$ è un'immersione nel punto $x\in X$ se il differenziale di F in x, $DF_x:T_x(X)\to T_{F(x)}(Y)$ è iniettivo. Si dice che F è un'immersione se F è un'immersione in ogni $x\in X$.*

Definizione 33. *Un morfismo di varietà differenziabili $F:X\to Y$ è una summersione nel punto $x\in X$ se il differenziale di F in x, $DF_x:T_x(X)\to T_{F(x)}(Y)$ è suriettivo. Si dice che F è una summersione se F è una summersione in ogni $x\in X$. Il punto x si dice regolare per F se F è una summersione in x. In caso contrario x si dice punto critico per F. Un punto $y\in Y$ si dice un valore regolare per F se ogni $x\in F^{-1}(y)$ è un punto regolare, altrimenti y è detto valore critico per F.*

Ad esempio l'applicazione $F:\mathbb{R}\to\mathbb{R}^2$ definita da $F(t)=(\cos(t),\sin(2t))$ è un'immersione. Infatti $DF_x=(-\sin(x),2\cos(2x))$ differenziale di F in x è iniettivo per ogni $x\in\mathbb{R}$.
Diamo un esempio di varietà topologica e differenziabile. Consideriamo la sfera S^2 in $\mathbb{R}^3$, S^2 con la topologia usuale indotta da $\mathbb{R}$ è di Hausdorff. Consideriamo il punto $N=(0,0,1)$ su S^2 e un altro punto p diverso da N sempre su S^2. La retta per p e N è unica e incontrerà un piano $\mathbb{R}^2$ non passante per N in un solo punto. Viceversa preso un punto q su $\mathbb{R}^2$ la retta per q e N intersecherà S^2 in un unico punto. Dunque l'applicazione $f:S^2\text{-}(0,0,1)\longrightarrow\mathbb{R}^2$ definisce un omeomorfismo tra S^2-(0,0,1) (aperto perchè complementare di un punto in uno spazio di Hausdorff) e $\mathbb{R}^2$. Proiettando analogamente dal punto S=(0,0,-1) si ottiene un altro omeomorfismo. Si ricopre così tutto S^2 che risultà essere una varietà topologica di dimensione due. Vediamo ora che la sfera è anche una varietà differenziabile. Diamo un espressione analitica delle due proiezioni stereografiche.

$N:S^2\text{-}(0,0,1)\longrightarrow\mathbb{R}^2$ definita da $N(x,y,z)=(x/(1-z),y/(1-z))$.
$S:S^2\text{-}(0,0,-1)\longrightarrow\mathbb{R}^2$ definita da $S(x,y,z)=(x/(1+z),y/(1+z))$.

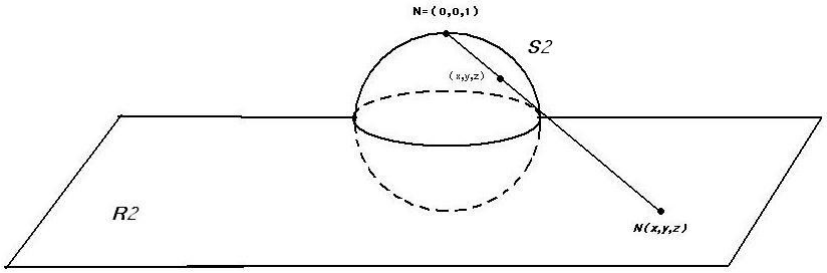

Figura 1.1: Proiezione stereografica della Sfera

Le proiezioni definiscono due carte locali sugli aperti S^2-(0,0,1) e S^2-(0,0,-1) che formano un atlante differenziabile. Inoltre le due applicazioni sono di classe C^∞, dunque la sfera è anche una varietà differenziabile di dimensione due. La sfera $S^2=\{(x,y,z)\in\mathbb{R}^3$ tali che $x^3+y^2+z^2=1\}$ è una varietà algebrica. E' definita infatti da un'equazione polinomiale. Poichè basta un'unica equazione per definirla la sfera è una superfice nello spazio affine $\mathbb{R}^3$, in particolare è una quadrica. In generale una varietà algebrica di $\mathbb{A}^n$ o $\mathbb{P}^n$ definita da un'unica equazione polinomiale di dice un'ipersuperficie. Daremo più avanti la definizione rigorosa di varietà algebrica.

Capitolo 2

Geometria Algebrica in $\mathbb{A}^n$ e in $\mathbb{P}^n$

«I matematici non studiano oggetti, ma relazioni tra gli oggetti. In questo modo sono liberi di rimpiazzare alcuni oggetti con altri, fintantoché le relazioni rimangano immutate. Per loro il contenuto è irrilevante: sono solamente interessati alla forma.»

Jules Henri Poincaré (1854-1912)

In questo capitolo daremo alcuni risultati fondamentali in geometria algebrica. Denoteremo con $\mathbb{A}^n$ lo spazio affine di dimensione n sul campo K. Useremo sempre il riferimento standard e quindi potremmo identificare $\mathbb{A}^n$ con K^n. Indicheremo con $K[X_1, X_2,...,X_n]$ l'anello dei polinomi a coefficienti in K di n variabili.

2.1 Insiemi algebrici affini

Definizione 34. *Sia T un sottoinsieme di $K[X_1, X_2,...,X_n]$ il luogo degli zeri di T (o la varietà definita da T) è $\boldsymbol{V}(T)=\{a\in K^n$ tali che $P(a)=0$, per ogni $P\in T\}$.*

Definizione 35. *Un sottoinsieme $Z\subseteq K^n$ si dice un sottoinsieme algebrico affine se è il luogo degli zeri di un sottoinsieme di $K[X_1, X_2,..., X_n]$, ovvero se esiste $T\subseteq K[X_1, X_2,...,X_n]$ tale che $Z=\boldsymbol{V}(T)$.*

In generale un insieme algebrico affine è definito da un sistema infinito di equazioni polinomiali. Sappiamo che nel caso di sottospazi lineari questo sistema può sempre essere ridotto ad un sistema finito. Sarebbe bello fare questo per un qualsiasi sottoinsieme algebrico. Il teorema della base di Hilbert dice che $K[X_1, X_2,...,X_n]$ è Noetheriano quindi tutti i suoi ideali sono finitamente generati. Per sfruttare questo fatto dobbiamo mostrare che un sottoinsieme algebrico $Z=\mathbf{V}(T)$ può essere sempre riguardato come definito da un ideale $Z=\mathbf{V}(I)$. In particolare mostreremo che tale I è proprio l'ideale generato da T.

Proposizione 10. *Sia T un sottoinsieme di $K[X_1, X_2,...,X_n]$ e sia $I=(T)=\{\sum_{finita} P_i Q_i$ tali che $P_i\in T$ e $Q_i\in K[X_1,X_2,...,X_n]\}$. Allora $\boldsymbol{V}(T)=\boldsymbol{V}(I)$.*

Dimostrazione: Sia a∈$\mathbf{V}$(T). Allora per tutti i polinomi P∈T vale P(a)=0. Ogni polinomio in I=(T) è della forma f=$\sum_{finita} P_i Q_i$, quindi f(a)=$\sum_{finita} P_i(a)Q_i(a)$=0, dunque a∈$\mathbf{V}$(I). Viceversa supponiamo che a∈$\mathbf{V}$(I). Allora f(a)=0 per ogni polinomio f∈I. Riguardiamo ora l'ideale I come I=(T)=$\bigcap J_i$ dove i J_i sono gli ideali di K[X_1, X_2,..., X_n] contenenti T. Vediamo che T⊆I. Se P∈T allora P∈I e perciò P(a)=0 per ogni P∈T. Duque a∈V(T). □

Osservazione 3. *Osserviamo che la rappresentazione Z=$\mathbf{V}$(I) non è unica. L'insieme algebrico Z può essere definito da ideali diversi. Ad esempio se I_n=(X^n), si ha $\mathbf{V}(I_n)$=(0) per ogni n>0 ma $I_n \neq I_m$ se n≠m.*

Sappiamo dal teorema della base di Hilbert che K[X_1, X_2,..., X_n] è Noetheriano, quindi ogni suo ideale è finitamente generato. La proposizione precedente mostra che possiamo riguardare ogni insieme algebrico Z=V(T)=$\mathbf{V}$(I) dove I è l'ideale generato da T, I è un ideale di K[X_1, X_2,..., X_n] dunque è finitamente generato. Possiamo scrivere I=(P_1, P_2,....,P_k) e riguardare Z come luogo degli zeri di un sistema finito di equazioni polinomiali.

$$Z=\mathbf{V}(I)=\{P_1=0,\ P_2=0,....,P_k=0\}$$

2.2 Corrispondenza tra ideali e insiemi algebrici

Abbiamo visto che un insieme algebrico Z può essere definito da ideali diversi. Vogliamo ora capire sotto quali condizioni è possibile stabilire una corrispondenza biunivoca tra ideali e insiemi algebrici. Introduciamo l'operatore $\mathbb{I}$ che può essere visto come una sorta di operatore duale a $\mathbf{V}$.

Definizione 36. *Sia Z un insieme algebrico. L'ideale di defizione di Z è l'ideale di tutti i polinomi che si annullano su Z,*

$$\mathbb{I}(Z)=\{P\in K[X_1,\ X_2,...,\ X_n] \text{ tali che } P(x)=0 \text{ per ogni } x\in Z\}$$

Per come è definito, $\mathbb{I}$(Z) è il più grande ideale che definisce Z.

Proposizione 11. *Siano I,J ideali di K[X_1, X_2,..., X_n] e siano Z,Y sottoinsiemi algebrici di K^n.*

1. *I⊆J⇒$\mathbf{V}$(J)⊆$\mathbf{V}$(I)*
2. *Z⊆Y⇒$\mathbb{I}$(Y)⊆$\mathbb{I}$(Z)*
3. *$\mathbb{I}$(Z∪Y)=$\mathbb{I}$(Z)∩$\mathbb{I}$(Y)*
4. *I⊆$\mathbb{I}$($\mathbf{V}$(I))*
5. *$\mathbf{V}$($\mathbb{I}$(Y))=Y*
6. *Se K è infinito $\mathbb{I}$(K^n)=(0)*

Dimostrazione:1) Sia a∈$\mathbf{V}$(J), allora P(a)=0 per ogni P∈J. Ora I⊆J perciò P(a)=0 per ogni P∈I ovvero a∈$\mathbf{V}$(I).
2) Sia P∈$\mathbb{I}$(Y), allora P(a)=0 per ogni a∈Y. Ma poichè Z⊆Y si ha P(a)=0 per ogni a∈Z ovvero $\mathbb{I}$(Y)⊆$\mathbb{I}$(Z).

3) Sia $P\in\mathbb{I}(Z\cup Y)$, $P(a)=0$ per ogni $a\in Z\cup Y$, $P(a)=0$ per ogni $a\in Z$ implica che $P\in\mathbb{I}(Z)$ e $P(a)=0$ per ogni $a\in Y$ implica che $P\in\mathbb{I}(Y)$. Allora $P\in\mathbb{I}(Z)\cap\mathbb{I}(Y)$. Viceversa sia $P\in\mathbb{I}(Z)\cap\mathbb{I}(Y)$, $P\in\mathbb{I}(Z)$ implica $P(a)=0$ per ogni $a\in Z$ e $P\in\mathbb{I}(Y)$ implica $P(a)=0$ per ogni $a\in Y$. Dunque $P(a)=0$ per ogni $a\in Z\cup Y$ ovvero $P\in\mathbb{I}(Z\cup Y)$.
4) Sia $P\in I$ allora $P(a)=0$ per ogni $a\in\mathbf{V}(I)$ ovvero $P\in\mathbb{I}(\mathbf{V}(I))$.
5) Poichè Y è un sottoinsieme algebrico si deve avere $Y=\mathbf{V}(I)$ per qualche ideale I, $I\subseteq\mathbb{I}(Y)$ perchè $\mathbb{I}(Y)$ è il più grande ideale che definisce Y. Da 1) si ha che $\mathbf{V}(\mathbb{I}(Y))\subseteq V(I)=Y$. Sia ora $a\in Y$ allora $P(a)=0$ per ogni $p\in\mathbb{I}(Y)$ ovvero $a\in V(\mathbb{I}(Y))$.
6) E' sufficiente mostare che ogni polinomio non costante non può annullarsi su tutto K^n. Procediamo per iduzione su n. Se n=1 sappiamo che un polinomio P(X) non costante in una variabile ha su K al più deg(P) radici distinte. Sia P un polinomio in n variabili, riscriviamo P secondo le potenze di X_n.

$$P(X_1,..,X_n)=p_k(X_1,..,X_{n-1}){X_n}^k+...+p_1(X_1,..,X_{n-1})X_n+p_0(X_1,..,X_{n-1})$$

Per ipotesi di induzione esiste una (n-1)-upla $(x_1,..,x_{n-1})$ tale che $p_k(x_1,...,x_{n-1})\neq 0$. Allora il polinomio:

$$P(x_1,...,X_n)=p_k(x_1,...,x_{n-1}){X_n}^k+.....+p_1(x_1,...,x_{n-1})X_n+p_0(x_1,...,x_{n-1})$$

ha grado k ed ha al più k radici distinte su K che è infinito. Perciò esiste $x_n\in K$ tale che $P(x_1,...,x_n)\neq 0$. □

Osservazione 4. *Osserviamo che se K è finito 6) in generale non è vera, ad esempio $P(X)=X(X+1)$ non è costante ma è identicamente nullo su $\mathbb{Z}_2$. Riguardo a 4) osserviamo che in generale $I\neq\mathbb{I}(\mathbf{V}(I))$, ad esempio se $I=(X^2)$ si ha $\mathbf{V}(I)=(0)$ ma $\mathbb{I}(\mathbf{V}(I))=(X)$. Un altro esempio: sia $J=(X^2+1)$ in $\mathbb{R}[X]$. Allora $\mathbf{V}(J)$ è il vuoto e $\mathbb{I}(\mathbf{V}(I))$ è tutto $\mathbb{R}[X]$. Osserviamo che l'ideale J è massimale infatti X^2+1 è irriducibile in $\mathbb{R}[X]$ essendo di grado 2 è non avendo radici in $\mathbb{R}$ ($\mathbb{R}[X]/J=\mathbb{C}$).*

Consideriamo ora le applicazioni:

$$F:\{\text{sottoinsiemi algebrici di } K^n\}\longrightarrow\{\text{ideali di } K[X_1, X_2,.., X_n]\}: Z\to\mathbb{I}(Z)$$
$$G:\{\text{ideali di } K[X_1, X_2,.., X_n]\}\longrightarrow\{\text{sottoinsiemi algebrici di } K^n\}: I\to\mathbf{V}(I)$$

Dalla proposione precedente abbiamo che F e G non sono biettive e che $G\circ F=Id$ ma $F\circ G\neq Id$. Vogliamo rendere F biettiva e vogliamo che sia $F^{-1}=G$. Per fare ciò dobbiamo restringere il dominio di G, in particolare possiamo considerare ideali radicali grazie al seguente

Lemma 3. *Sia Z un sottoinsieme algebrico di K^n, allora $\mathbb{I}(Z)$ è un ideale radicale.*

Dimostrazione: Poniamo $\mathbb{I}(Z)=\mathbb{I}$, $\mathbb{I}\subseteq r(\mathbb{I})$ perchè ogni ideale è contenuto nel suo radicale. Sia $P\in r(\mathbb{I})$, allora esiste un intero k tale che $P^k\in\mathbb{I}$. Ora $\mathbb{I}$ è l'ideale di definizione di Z perciò $P^k(a)=0$ per ogni $a\in Z$. Ma $P^k(a)=(P(a))^k=0$ implica $P(a)=0$ per ogni $a\in Z$ ovvero $P\in\mathbb{I}$. Concludiamo che $\mathbb{I}$ è radicale. □

Vogliamo a questo punto restringere le nostre considerazioni a ideali radicali. Il primo problema sollevato nell'osservazione precedente viene così eliminato, tuttavia non abbiamo risolto la questione relativa all'ideale J. Questo perchè $\mathbb{R}$ non è algebricamente chiuso. Consideriamo ora K algebricamente chiuso. Sotto queste ipotesi vale il teorema degli zeri di Hilbert.

2.3 Teorema degli zeri di Hilbert

Diamo in questa sezione una dimostrazione del Teorema degli zeri di Hilbert e di alcune sue conseguenze. Questo teorema ci consentirà di mettere in relazione le varietà algebriche e gli ideali radicali di $K[X_1, X_2,..., X_n]$. Questo fatto è estremamente importante perchè se in geometria algebrica ci si restringe a ideali radicali si ha una buona dualità tra le varietà definite da questi ideali e gli ideali di definizione delle varietà. Cominciamo con alcune premesse sulle estensioni di anelli.

Definizione 37. *Sia S un anello commutativo e R un sottoanello di S contenente 1_S. Allora S si dice un anello estensione di R.*

Definizione 38. *Sia S un anello estensione di un anello R e sia s∈S. Se esiste un polinomio monico f∈R[X] tale che f(s)=0, ovvero s è radice di f, allora s viene detto integrale su R. Se ogni elemento di S è integrale su R, S viene detto un'estensione integrale di R.*

Si dimostra che se S è un anello estensione di R e $s_1,...,s_t \in S$ sono integrali su R, allora $R[s_1,...,s_t]$ è un R-modulo finitamente generato e un'estensione integrale di R. Vale inoltre che se T è un'estensione integrale di un anello S e S è un'estensione integrale di un anello R, allora T è un'etensione integrale di R[1].

Teorema 8 (Lemma di normalizzazione di Noether)**.** *Sia R un dominio di integrità che risulta essere anche un'estensione finitamente generata di un campo K e sia r il grado di trascendenza di K sul campo dei quozienti F di R. Allora esiste un sottoinsieme algebricamente indipendente $\{t_1,...,t_r\}$ di R tale che R è integrale su $K[t_1,...,t_r]$.*

Dimostrazione: Sia $R=K[u_1,...,u_n]$, allora $F=K(u_1,...,u_n)$. Se $\{u_1,...,u_n\}$ è algebricamente indipendente su K allora $\{u_1,...,u_n\}$ è una base di F su K quindi r=n e il teorema è vero. Se invece $\{u_1,...,u_n\}$ è algebricamente dipendente su K, allora r<n e possiamo scrivere $\sum_{(i1,...,in)inI} K_{i1,...,in} u_1^{i1} u_2^{i2}...u_n^{in}=0$, dove I è un insieme finito di n-uple di interi non negativi e $k_{i1...in}$ è un elemento non nullo di K per ogni $(i_1,...,i_n)\in I$. Sia c un intero positivo maggiore di ogni elemento i_h per ogni n-upla $(i_1,...,i_n)\in I$. Se $(i_1,...,i_n)$, $(j_1,...,j_n)\in I$ sono tali che

$$i_1+ci_2+...+c^{n-1}i_n=j_1+cj_2+...+c^{n-1}j_n,$$

allora $i_1-j_1=cj_2+...+c^{n-1}j_n-ci_2-...-c^{n-1}i_n=c(j_2+...+c^{n-2}j_n-i_2-...-c^{n-2}i_n)$ e quindi c divide i_1-j_1, ma i_1, j_1 sono interi non negativi e c è maggiore di entrambi quindi $c>|i_1-j_1|$ perciò deve essere $i_1=j_1$. Di conseguenza $j_2+...+c^{n-2}j_n=i_2+...+c^{n-2}i_n$ e come prima $i_2=j_2$. Procedendo con questa argomentazione si ha che $(i_1,...,i_n)=(j_1,...,j_n)$. Quindi l'insieme

$$\{i_1+ci_2+...+c^{n-1}i_n \text{ t.c. } (i_1,...,i_n)\in I\}$$

consiste di Card(I) interi non negativi, in particolare esiste un unico elemento massimo $j_1+cj_2+...+c^{n-1}j_n$ per qualche $(j_1,...,j_n)\in I$. Siano ora

$$v_2=u_2-u_1^c,\ v_3=u_3-u_1^{c2},...,v_n=u_n-u_1^{n-1}.$$

Possiamo ora riscrivere la relazione di dipendenza algebrica come

[1]Per la dimostrazione dei fatti enunciati si veda Hungerford - Algebra.

$$k_{j1\dots jn}u_1^{j1+cj2+\dots+c(n-1)jn}+f(u_1,v_2,\dots,v_n)=0,$$

dove il grado si $f\in K[x_1,\dots,x_n]$ in x_1 è strettamente minore di $j_1+cj_2+\dots+c^{n-1}j_n$. Allora u_1 è una radice del polinomio monico

$$X^{j1+cj2+\dots+c(n-1)jn}+k_{j1\dots jn}^{-1}f(X,v_2,\dots,v_n)\in K[v_2,\dots,v_n][X].$$

Di conseguenza u_1 è integrale su $K[v_2,\dots,v_n]$, perciò $K[u_1,v_2,\dots,v_n]=K[v_2,\dots,v_n][u_1]$ è integrale su $K[v_2,\dots,v_n]$. Analogamente si ha che ogni u_1 per $2\leq i\leq n$ è integrale su $K[u_1,v_2,\dots,v_n]$. Quindi $R=K[u_1,\dots,u_n]$ è integrale su $K[v_2,\dots,v_n]$. Ora se $\{v_2,\dots,v_n\}$ sono algebricamente indipendenti r=n-1 e abbiamo concluso. Se non lo sono consideriamo $K[v_2,\dots,v_n]$ al posto di R e mostriamo che esistono $w_3,\dots,w_n\in R$ tali che $K[v_2,\dots,v_n]$ è integrale su $K[w_3,\dots,w_n]$ e quindi R è integrale su $K[w_3,\dots,w_n]$. Se ora $\{w_3,\dots,w_n\}$ è algebricamente indipendente r=n-2 e abbiamo concluso altrimenti procediamo in modo analogo argomentando per induzione. Troviamo così un sottoinsime algebricamente indipendente $\{\xi_{n-r+a},\dots,\xi_n\}$ costituito da r elementi di R tale che R è integrale su $K[\xi_{n-r+a},\dots,\xi_n]$. □

Sia ora K un campo e F un'estensione algebricamente chiusa di K. Preso un ideale I di $K[X_1,\dots,X_n]$ sappiamo che I è finitamente generato ovvero $I=(P_1,\dots,P_k)$. La varietà definita da I, $\mathbf{V}(I)$ è costituita dai punti di F^n che sono zeri comuni ai polinomi generatori. Se n=1 allora K[X] è un P.I.D. quindi ogni suo ideale I=(P) è generato da un solo elemento. Essendo F algebricamente chiuso è chiaro che se P non è costante risulterà che $\mathbf{V}(I)$ non è vuoto. La cosa sorprendente è che questo vale anche per un ideale I di $K[X_1,\dots,X_n]$.

Proposizione 12. *Se F è un'estensione algebricamente chiusa del campo K e I un ideale di $K[X_1,\dots,X_n]$, allora la varietà affine $\mathbf{V}(I)$ definita da I in F^n non è vuota.*

Dimostrazione: Sappiamo che un generico ideale I è contenuto in un ideale proprio e primo P, ora $I\subset P$ implica $\mathbf{V}(P)\subset\mathbf{V}(I)$. Di conseguenza è sufficiente provare che $\mathbf{V}(P)$ non è vuoto per ogni ideale proprio e primo P di $K[X_1,\dots,X_n]$. Abbiamo che $P\cap K=(0)$, infatti se esistesse un a non nullo in $P\cap K$, allora $1_K=a^{-1}a\in P$ e questo contraddice il fatto che P è un ideale proprio. Consideriamo ora il dominio $R=K[X_1,\dots,X_n]/P$ e sia $\Pi:K[X_1,\dots,X_n]\to R$ la proiezione canonica. Se denotiamo $\Pi(X_i)=u_i$ allora $R=\Pi(K)[u_1,\dots,u_n]$. Inoltre poichè $P\cap K=(0)$ si ha che Π mappa K isomorficamente dentro $\Pi(K)$, in particolare $\Pi(K)$ è un campo. Per il lemma di normalizzazione esiste un sottoinsieme $\{t_1,\dots,t_r\}$ di R tale che $\{t_1,\dots,t_r\}$ è algebricamente indipendente su $\Pi(K)$ e R è integrale su $S=\Pi(K)[t_1,\dots,t_r]$. Se M è l'ideale di S generato da $t_1,\dots,t_r$, allora la mappa $\Pi(K)\to S/M$ che manda $\Pi(a)\to\Pi(a)+M$ è un isomorfismo. Allora S/M è un campo e perciò M è un ideale massimale di S. Allora esiste un ideale massimale N di R tale che $N\cap S=M$. Sia $f:R\to R/N$ l'isomorfismo canonico, $f(R)=R/N$ è un campo. Il secondo teorema di isomorfismo grazie alle mappe prima introdotte induce l'isomorfismo

$$K\cong\Pi(K)\cong S/M=S/(N\cap S)\cong(S+N)/N=f(S),$$
$$\text{che manda } a\mapsto\Pi(a)\mapsto\Pi(a)+M\mapsto\Pi(a)+N=f(\Pi(a)).$$

Sia $\overline{f(R)}$ una chiusura algebrica si f(R). Poichè R è integrale su S, f(R) è un'estensione algebrica del campo f(S), perciò $\overline{f(R)}$ è anche una chiusura algebrica di

f(S). Ora F contiene una chiusura algebrica $\overline{K}$ del campo K, possiamo estendere l'isomorfismo tra K e f(S) a un isomorfismo tra $\overline{K}$ e $\overline{f(R)}$. La restrizione a f(R) dell'inversa di questo isomorfismo induce un morfismo g:f(R)$\to\overline{K}\subset$F. Sia ora Λ la composizione $K[X_1,...,X_n]\xrightarrow{\Pi}R\xrightarrow{f}f(R)\xrightarrow{g}F$. Ora $\Lambda(k)=1_K$ per ogni k$\in$K e $\Lambda_{|P}=0$. Allora per ogni p$\in$P$\subset$K[X_1,...,X_n] si ha $p(\Lambda(X_1,...,\Lambda(X_n))=\Lambda(p(X_1,...,X_n)=0$, quindi $(\Lambda(X_1),...,\Lambda(X_n))$ è uno zero di P in F^n ovvero $\mathbf{V}$(P) non è vuota. □

Teorema 9 (Degli zeri di Hilbert)**.** *Sia F un estensione algebricamente chiusa di un campo K e sia I un ideale proprio di K[X_1,...,X_n]. Sia V(I)={(a_1,...,a_n)$\in F^n$ tali che P(a_1,...,a_n)=0 per ogni P$\in$I}. Allora*

r(I)=$\mathbb{I}(\mathbf{V}(I))$={P$\in$K[$X_1$,...,$X_n$] t.c. P($a_1$,...,$a_n$)=0 per ogni ($a_1$,...,$a_n$)$\in\mathbf{V}(I)$}.

Ovvero P(a_1,...,a_n)=0 per ogni zero (a_1,...,a_n) di I in F^n se e solo se $P^k\in I$ per qualche k$\geq$1.

Dimostrazione: Se P$\in$r(I) allora $P^k\in$I per qualche k$\geq$1. Se (a_1,...,a_n) è uno zero di I in F^n allora $P^k(a_1,...,a_n)=(P(a_1,...,a_n))^k=0$ e quindi essendo F un campo si ha P(a_1,...,a_n)=0. Allora r(I)$\subset\mathbb{I}(\mathbf{V}(I))$.
Viceversa sia P$\in\mathbb{I}(\mathbf{V}(I))$. Possiamo supporre P non identicamente nullo perchè 0$\in$r(I). Riguardiamo K[X_1,...,X_n] come sottoanello di K[X_1,...,X_n,Y] anello dei polinomi in n+1 variabili su K. Sia L un ideale non banale di K[X_1,...,X_n,Y] generato da I e da YP-1_F. Abbiamo allora che se (a_1,...,a_n,b) è uno zero di L in F^{n+1} e (a_1,...,a_n) è uno zero di I in F^n. Osserviamo ora che (YP-1_F)(a_1,...,a_n,b)=bP(a_1,...,a_n)-1_F=-1_F per ogni (a_1,...,a_n) zero di I in F^n. Allora L non ha zeri in F^{n+1} ovvero $\mathbf{V}$(L) è vuota. Per la proposizione precedente deve essere L=K[X_1,...,X_n,Y] da cui $1_F\in$L. Allora possiamo scrivere

$$1_F=\sum_{i=1}^{t-1}g_if_i+g_t(YP\text{-}1_F),$$

dove $f_i\in$I e $g_i\in$K[X_1,...,X_n,Y]. Definiamo un morfismo di valutazione K[X_1,...,X_n,Y]$\to$K(X_1,...,X_n) che manda $X_i\mapsto X_i$ e $Y\mapsto P^{-1}=1_K/P(X_1,...,X_n)$. Allora nel campo K($X_1$,...,$X_n$) possiamo scrivere

$$1_F=\sum_{i=1}^{t-1}g_i(X_1,...,X_n,P^{-1})f_i(X_1,...,X_n).$$

Sia ora m un intero positivo maggiore del grado di g_i rispetto a Y per ogni i. Allora per ogni i, $P^m(X_1,...,X_n)g_i(X_1,...,X_n,P^{-1})$ appartiene a K[X_1,...,X_n]. Osserviamo ora che

$$P^m=P^m1_F=\sum_{i=1}^{t-1}P^m(X_1,...,X_n)g_i(X_1,...,X_n,P^{-1})f_i(X_1,...,X_n)\in I.$$

Quindi P$\in$r(I) e $\mathbb{I}(\mathbf{V}(I))\subset$r(I). Concludiamo che $\mathbb{I}(\mathbf{V}(I))$=r(I). □

Proposizione 13. *Alla luce del teorema degli zeri le applicazioni:*

F:{sottoinsiemi algebrici di K^n}$\longrightarrow${ideali radicali di K[X_1,..,X_n]}: Z$\to\mathbb{I}$(Z)
G:{ideali radicali di K[X_1,..,X_n]}$\longrightarrow${sottoinsiemi algebrici di K^n}: I$\to\mathbf{V}$(I)

sono biettive e F^{-1}=G:

Dimostrazione: L'applicazione F è ben definita perchè sappiamo che se Z è algebrico allora $\mathbb{I}(Z)$ è radicale. Sappiamo che G∘F=Id. Si ha poi che (G∘F)(I)=$\mathbb{I}(\mathbf{V}(I))$. Dal teorema degli zeri $\mathbb{I}(\mathbf{V}(I))$=r(I)=I perchè I è un ideale radicale. Vediamo così che $\mathbb{I}(\mathbf{V}(I))$=I, ovvero F∘G=Id. □

Vediamo ora alcune importanti conseguenze del teorema degli zeri.

Proposizione 14. *Sia K un campo algebricamente chiuso. Il sistema di equazioni polinomiali* $P_1(x_1,..,x_n)=0,\ldots..,\ P_m(x_1,..,x_n)=0$, *non ammette soluzioni in* K^n $\Leftrightarrow$ *esistono dei polinomi* $Q_1,\ldots,\ Q_m$ *tali che* $1=\sum P_iQ_i$.

Dimostrazione: Sia I=(P_1,..., P_n). Il sistema non ha soluzione se e solo se $\mathbf{V}(I)$ è il vuoto. Dal teorema degli zeri $\mathbb{I}(\mathbf{V}(I))$=r(I). Quindi il sistema non ha soluzioni se e solo se r(I)=K[X_1,..,X_n], cioè se e solo se 1∈r(I), se e solo se esiste un intero k tale che 1^k=1∈I. □

Proposizione 15 (Teorema degli zeri debole)**.** *Sia K un campo algebricamente chiuso. Un ideale M di* $K[X_1,..,\ X_n]$ *è massimale se e solo se* $M=(X\text{-}a_1,..,\ X\text{-}a_n)$ *per opportuni* $a_1,..,\ a_n$ *in K.*

La proposizione dice che se K è algebricamente chiuso l'applicazione a=(a_1,.., a_n)→M=(X-a_1,.., X-a_n) è una biezione tra K^n e l'insieme degli ideali massimali di K[X_1,.., X_n].

Dimostrazione: Consideriamo l'applicazione E_a:K[X_1,.., X_n]→K definita da E_a(P)=P(a), E_a è la funzione di valutazione in a, pertanto è un morfismo suerittivo d'anelli tra K[X_1,.., X_n] e K. Consideriamo il suo nucleo: Ker(E_a)={P∈K[X_1,.., X_n] tali che P(a)=0}=(X-a_1,.., X-a_n). Allora K[X_1,.., X_n]/(X-a_1,.., X-a_n) è isomorfo a K, quindi è un campo. Concludiamo che (X-a_1,.., X-a_n) è un ideale massimale. Viceversa sia M un ideale massimale di K[X_1,.., X_n] e sia Z=$\mathbf{V}$(M). Dal teorema degli zeri $\mathbb{I}$(Z)=r(M). Ora M è massimale e in particolare è primo. Sia x∈r(M) allora x=m^k per opportuni m∈M e k intero. Ora M primo e m∈M implica m^k∈M, quindi r(M)=M. Perciò $\mathbb{I}$(Z)=r(M)=M. Quindi $\mathbb{I}$(Z)≠K[X_1,..,X_n] e Z è non vuoto. Sia a∈Z allora M=$\mathbb{I}$(Z)⊆$\mathbb{I}$(a)=(X-a_1,.., X-a_n). Per la massimalità di M concludiamo che M=(X-a_1,.., X-a_n). □

Facciamo alcune osservazioni di carattere generale. Sia K un campo. Ogni polinomio P∈K[X_1,...,X_n] definisce una funzione polinomiale da K^n in K che manda (a_1,...,a_n)↦P(a_1,...,a_n). Se V=$\mathbf{V}$(I) è una varietà affine contenuta in K^n la restrizione di tale funzione a V si dice una funzione regolare su V. Le funzioni regolari da V in F formano un anello A(V) isomorfo a K[X_1,...,X_n]/$\mathbb{I}(\mathbf{V}(I))$. Tale anello viene detto l'anello delle coordinate di V. Inoltre A(V) è una K-algebra finitamente generata essendo K[X_1,...,X_n] e $\mathbb{I}(\mathbf{V}(I))$ finitamente generati a loro volta, infatti se f,g sono funzioni regolari su V e λ∈K si ha che f+g, fg e λf sono ancora funzioni regolari su V. Si dimostra anche che ogni K-algebra finitamente generata priva di elementi nilpotenti non nulli è l'anello delle coordinate di una qualche varietà affine. In conclusione esiste una corrispondenza biunivoca tra le varietà affini e una certa classe di anelli commutativi.

2.4 Lo spazio proiettivo $\mathbb{P}^n$

Vogliamo ora introdurre brevemente lo spazio proiettivo di dimensione n costruito a partire da uno spazio vettoriale di dimensione n+1. Sia V un K-Spazio vettoriale di dimensione n+1. Introduciamo su V*=V-(0) la relazione d'equivalenza $\Re$ definita da:

$$\text{Dati v,w vettori di V, } v\Re w \Leftrightarrow v=kw \text{ per qualche } k\in K^*$$

$\mathbb{P}(V)=V^*/\Re$ è lo spazio proiettivo di dimensione n associato allo spazio vettoriale V.
Possiamo riguardare $\mathbb{P}^n$ come all'insieme delle rette vettoriali di V. Ogni retta vettoriale in V corrisponde ad un punto in $\mathbb{P}^n$, un punto di $\mathbb{P}^n$ è una n+1-upla $[x_0,..,x_n]$ univocamente determinata a meno di uno fattore moltiplicativo $k\in K^*$ (coordinate omogenee).
Un sottospazio lineare di $\mathbb{P}^n$ è il proiettivizzato di un sottospazio vettoriale di V. Se $W=<w_0,..,w_r>$ è un sottospazio di dimensione r+1, $\mathbb{P}(W)=(w_0,..,w_r)$ è il sottospazio lineare di dimensione r associato a W, inteso come sottospazio passante per i punti $w_0,..,w_r$ di $\mathbb{P}^n$. Anche nel proiettivo vale la relazione di Grassman se si assume che la dimensione del vuoto sia -1. Consideriamo la relazione vettoriale $\dim(<W,L>)=\dim(W)+\dim(L)-\dim(W\cap L)$. Siano ora $P=\mathbb{P}(W)$ e $Q=\mathbb{P}(L)$ allora $\dim((P,Q))-1=(\dim(P)-1)+(\dim(Q)-1)-(\dim(P\cap Q)-1)=\dim(P)-1+\dim(Q)-1-\dim(P\cap Q)+1=\dim(P)+\dim(Q)-\dim(P\cap Q)-1$, dunque:

$$\mathbf{\dim((P,Q))=\dim(P)+\dim(Q)-\dim(P\cap Q)}$$
$$\mathbf{\dim(P\cap Q)=\dim(P)+\dim(Q)-\dim((P,Q))}$$

Vediamo che in $\mathbb{P}^n$ un iperpiano e una retta si incontrano sempre e in particolare in $\mathbb{P}^2$ non esistono rette parallele.

Il duale del K-Spazio vettoriale V è lo spazio vettoriale delle forme lineari su V, se V ha dimensione n anche il suo duale ha dimensione n. Fissata una base su V basta considerarne la base duale. Il duale di $\mathbb{P}^n$ è il proiettivizzato del duale di V.
Definiamo ora le proiettività. Sia $f:V\to V$ un endomorfismo biettivo di V, consideriamo l'applicazione:

$$F:\mathbb{P}^n \longrightarrow \mathbb{P}^n \text{ che manda } [v]\to[f(v)]$$

F si dice proiettività associata all'isomorfismo f.
Notiamo che F è ben definita perchè f è lineare e inoltre essendo f biettiva e in particolare iniettiva si ha $\text{Ker}(f)=\{0\}$.

Vogliamo poter passare dall'affine al proiettivo e viceversa, per fare questo introduciamo il concetto di **carta affine**.

Riguardiamo lo spazio proiettivo con le coordinate omogenee standard (abbiamo fissato in K^{n+1} la base canonica). Un punto di $\mathbb{P}^n$ è identificato da una (n+1)-upla di coordinate omogenee non identicamente nulla. A meno di riordinare possiamo suppurre $X_0\neq 0$ e pertanto dividere per X_0. Otteniamo così una n-upla del tipo $(1,Y_1,..,Y_n)$ e possiamo identificare in modo naturale $\mathbb{P}^n-\{X_0=0\}$ con $\mathbb{A}^n$. Perciò $\mathbb{P}^n=\mathbb{A}^n\cup\{X_0=0\}$. Il ragionamento vale per ogni $U_i=\{[X_0,..,X_n]$

tale che $X_i \neq 0\}$. Ognuno degli U_i si dice una carta affine. Infine associamo ad ogni carta affine un'applicazione:

$$\Pi_i : U_i \to \mathbb{A}^n \text{ che manda } [X_0,..,X_n] \to (Y_0,.., \underbrace{1}_{i-esimo}, .., Y_n)$$

Nel seguito diventerà per noi particolarmente importante il passaggio da $\mathbb{P}^2$ a $\mathbb{A}^2$ per studiare le curve algebriche piane proiettive ovvero i luoghi geometrici definiti dalle soluzioni di equazioni polinomiali del tipo $F(X,Y,Z)=0$.
Sia C la curva algebrica di $\mathbb{P}^2$ di equazione $F(X,Y,Z)=0$, $\mathbb{P}^2$ è ricoperto dalle tre carte affini U_X, U_Y e U_Z e ogni carta è in biezione con $\mathbb{A}^2$. Ad esempio abbiamo:

$$f_X : U_X \to \mathbb{A}^2 \text{ che manda } (x:y:z) \to (y/x, z/x)$$
$$f_{X-1} : \mathbb{A}^2 \to U_X \text{ che manda } (u,v) \to (1:u:v)$$

Per studiare $\mathbf{V}(F)$ possiamo considerare le intersezioni $\mathbf{V}(F) \cap U_X$, $\mathbf{V}(F) \cap U_Y$ e $\mathbf{V}(F) \cap U_Z$ in $\mathbb{A}^2$.
Determiniamo $C_X = f_X(V(F) \cap U_X)$ in $\mathbb{A}^2$. Un punto (x,y,z) di $\mathbb{P}^2$ appartiene a $V(F) \cap U_X$ se:

1. $x \neq 0$;
2. $F(x,y,z)=0$.

Ora $F(X,Y,Z) = \sum a_{ijk} X^i Y^j Z^k$ con i+j+k=d (F è omogeneo di grado d). Poichè $x \neq 0$ possiamo scrivere $F(x,y,z) = \sum a_{ijk} x^i y^j z^k = \sum a_{ijk} x^i x^{j+k} (z/x)^k (y/x)^j =$
$= x^d \sum a_{ijk} (z/x)^k (y/x)^j = x^d F(1, y/x, z/x)$. Essendo $x \neq 0$ si ha $F(x,y,z)=0 \Leftrightarrow F(1,y/x,z/x)=0$.
Vale allora il seguente:

Lemma 4. *La curva algebrica C_X di $\mathbb{A}^2$ é $C_X = \{(u,v) \in \mathbb{A}^2$ tali che $F_X(u,v)=0\}$, dove F_X è il deomogeneizzato di F rispetto alla variabile X.*

Definizione 39. *La curva C_X si dice parte affine di C ralativa alla carta affine U_X.*

Sia ora C una curva affine di $\mathbb{A}^2$ definita da $f(u,v)=0$. Immergiamo $\mathbb{A}^2$ in $\mathbb{P}^2$ attraverso la mappa ${f_X}^{-1}$. Consideriamo poi la chiusura in $\mathbb{P}^2$ di ${f_X}^{-1}(C)$ che indichiamo con Y (Chiusura nella topologia di Zariski che introduremo nel capitolo 3). Otteniamo così un sottoinsieme algebrico Z di $\mathbb{P}^2$. Un punto (x,y,z) appartiene a ${f_X}^{-1}(C)$ se e solo se:

1. $x \neq 0$;
2. $f(y/x, z/x)=0$.

Sia F_X l'omogeneizzato di f rispetto a X. Ora $x^n f(y/x,z/x) = F(x,y,z)$. Quindi $(x,y,z) \in {f_X}^{-1}(C)$ se e solo se $F(x,y,z)=0$. Allora Y è il supporto della curva algebrica definita da $F(X,Y,Z)=0$.

Definizione 40. *La curva C^* di $\mathbb{P}^2$ di equazione $F=0$ si dice la chiusura proiettiva della curva C di $\mathbb{A}^2$.*

Osservazione 5. *Se il supporto della curva proiettiva C coincide con la retta all'infinito rispetto alla quale si deomogeneizza si ritrova un polinomio costante che non ha zeri in $\mathbb{A}^2$. Inoltre il grado di f deomogeneizzato di F può essere diverso dal grado di F. Infatti se $X^r|F$ e X^{r+1} non divide F allora deg(f)+r=deg(F). Per esempio se $F(X,Y,Z)=X^2(Y+Z)$ si ha f(u,v)=u+v. Nel passaggio dal proiettivo all'affine perdiamo:*

- *Le eventuali intersezioni di C con la retta all'infinito X=0.*
- *Un'eventuale componente irriducibile (contata con la sua molteplicità) avente per supporto la retta all'infinito X=0.*

2.5 Insiemi algebrici proiettivi

Siano C e H due curve affini di grado rispettivamente n e m. Vorremmo poter dire che C e H si intersecano in nm punti ma in generale questo non è vero.

1. Se K non è algebricamente chiuso potrebbe essere che C è il vuoto. Ad esempio $\mathbf{V}(X^2+Y^2=1)$ in $\mathbb{R}^2$. Assumiamo perciò K algebricamente chiuso.
2. Se le due curve hanno una componente comune la loro intersezione è un insieme infinito. Ad esempio se C=$\mathbf{V}$(XY) e H=$\mathbf{V}$(Y(X-1)) l'intersezione è tutta la retta Y=0.
3. Pur prendendo K algebricamente chiuso e C, H senza componenti in comune l'enunciato è ancora falso. Ad esempio due rette parallele in $\mathbb{C}^2$ non si incontrano. Introduciamo allora il piano proiettivo $\mathbb{P}^2(\mathbb{C})$, nel proiettivo non esistono rette parallele.

Sotto queste condizioni potremmo dimostare la versione debole del teorema di Bezout il quale afferma che una retta e una curva algebrica di grado n in $\mathbb{P}^2$(K) con K algebricamente chiuso si intersecano in n punti contati con molteplicità.

Definizione 41. *Un polinomio $P\in K[X_1,..,X_n]$ si dice omogeneo di grado d se tutti i monomi che lo compongono hanno grado d. In tal caso $P(\lambda X)=\lambda^d P(X)$. Chiaramente ogni polinomio P si può scrivere nella forma $P=P_d+P_{d-1}+...+P_0$ dove P_i è omogeneo di grado i, ragguppando i monomi di uguale grado.*

Definizione 42. *Il punto z di $\mathbb{P}^n$ è uno zero del polinomio omogeneo $P\in K[X_1,.., X_n]$ se $P(z_0,.., z_n)=0$, dove $(z_0: .. :z_n)$ è un rappresentante qualsiasi di z.*

Definizione 43. *Un ideale I di $K[X_1,.., X_n]$ si dice omogeneo se può essere generato da polinomi omogenei.*

Proposizione 16. *Un ideale I di $K[X_1,.., X_n]$ è omogeneo se e solo se per ogni polinomio P si ha $P\in I \Leftrightarrow P_i\in I$, per ogni i, dove $P=\sum_{i=0}^{d}P_i$ è la decomposizione di P in polinomi omogenei.*

Dimostrazione: Suppiamo I omogeneo e sia $P=\sum_{i=0}^{d}P_i$ con P_i omogeneo di grado i. Se ogni $P_i\in$I ovviamente si ha che P∈I. Viceversa supponiamo P∈I. Possiamo scrivere $P=\sum h_j g_j$ dove i g_j sono polinomi omogenei che generano I. Decomponiamo ogni h_j come somma di polinomi omogenei: $h_j=\sum_k f_k$ con f_k omogeneo di grado k. Abbiamo $P=\sum P_i=\sum_{j,k} g_j f_k$ allora ogni $P_i=g_j f_k$ per

opportuni j e k, ovvero $P_i \in I$. Sia ora $I=(P_1,..,P_r)$. Per ipotesi possiamo scrivere $P_j=\sum_k P_{j,k}$ con $P_{j,k}$ omogeneo di grado k. Allora I è generato da polinomi omogenei. □

Definizione 44. *Sia $I=(P_1,..,P_r)$ un ideale omogeneo. Il luogo degli zeri di I è $\boldsymbol{V}(I)=\{z\in\mathbb{P}^n$ tali che $P_i(z)=0$ per ogni $i\}$. Un sottoinsieme X di $\mathbb{P}^n$ è un insieme algebrico proiettivo se esiste un ideale omogeneo I tale che $X=\boldsymbol{V}(I)$. Infine sia X un insieme algebrico di $\mathbb{P}^2$ l'ideale di definizione di X, $\mathbb{I}(X)$, è l'ideale generato da tutti i polinomi omogenei che si annullano su X.*

Lemma 5. *Siano I e J ideali omogenei di $K[X_1,..,X_n]$ allora I+J, IJ, $I\cap J$ e r(I) sono omogenei.*

Dimostrazione: Scriviamo $I=(f_1,..,f_h)$ e $J=(g_1,...,g_k)$ come generati da polinomi omogenei. Sia P un polinomio in I+J allora P=Q+V con Q in I e V in J. Perciò P può essere scritto come combinazione degli f_i e dei g_j, quindi possiamo riguardare $I+J=(f_1,..,f_h,g_1,...,g_k)$, dunque I+J è omogeneo.
Sia P in IJ, allora P=Q.V sempre con Q in I e V in J. Scriviamo $Q=Q_1f_1+...+Q_hf_h$ e $V=V_1g_1+...+V_kg_k$. Ora $P=Q.V=Q_1f_1V_1g_1+...+Q_1f_1V_kg_k+...+Q_hf_hV_kg_k$, allora possiamo riguardare IJ come l'ideale generato da tutti i possibili prodotti di un generatore di I con un generatore di J. Ora se F è un polinomio omogeneo di grado d e G un polinomio omogeneo di grado q, FG è omogeneo di grado d+q. Infatti $FG(ax)=F(ax)G(ax)=a^dF(x)a^qG(x)=a^{d+q}FG(x)$. Allora IJ è generato da polinomi omogenei e quindi è un ideale omogeneo.
Sia $P\in I\cap J$. Ora $P=\sum P_i\subseteq I$ e $P=\sum P_i\subseteq J$, con P_i omogeneo di grado i, ma I e J sono omogenei quindi $P_i\in I$ e $P_i\in J$ per ogni i, dunque $P_i\in I\cap J$ per ogni i e allora $I\cap J$ è omogeneo.
Sia $P\in r(I)$ allora esiste un naturale n tale che $P^n\in I$. Scriviamo $P=\sum P_i$ con P_i omogeneo di grado i. Ora $P^n=P_0^n+P_1^n+...+P_d^n+...+P_1P_d^{n-1}+...+P_{d-1}^{n-1}P_d$, notiamo che in questo modo P^n è visto come somma di polinomi omogenei, infatti se P_i è omogeneo P_i^k è ancora omogeneo e il prodotto di polinomi omogenei e un polinomio omogeneo. Essendo per ipotesi I un ideale omogeneo deve essere $P_i^n\in I$ per ogni i ovvero $P_i\in r(I)$ per ogni i. Vediamo allora che anche r(I) è omogeneo. □

Anche nel caso proiettivo vogliamo stabilire una corrispondenza tra ideali è insiemi algebrici. Introduciamo a tal fine il seguente oggetto geometrico.

Definizione 45. *Sia X un sottoinsieme algebrico di $\mathbb{P}^n$. Il cono affine associato ad X, C(X) é definito da $C(X)=\{(x_0,..,x_n)$ in $\mathbb{A}^{n+1}$ tali che $(x_0,..,x_n)=(0,..,0)$ o $(x_0,..,x_n)\in X\}$.*

Osservazione 6. *Sia $\Pi:K^{n+1}\text{-}(0)\to\mathbb{P}^n$ la proiezione canonica. Possiamo riguardare $C(X)=\Pi^{-1}(X)$ (chiusura di $\Pi^{-1}(X)$ in K^{n+1}). Se $p\in C(X)$ allora ogni punto della retta per p e l'origine sta su X e quindi tutta la retta è contenuta in C(X). Vediamo che C(X) è proprio un cono affine con vertice nell'origine.*
Consideriamo ad esempio in $\mathbb{P}^2$ il sottoinsieme algebrico $X=\boldsymbol{V}(X_0^2+X_1^2-X_2^2=0)$. Il corrispondente cono affine in $\mathbb{A}^3$ è $C(X)=\{(X,Y,Z)$ tali che $X^2+Y^2-Z^2=0\}$.

Proposizione 17. *Sia X un sottoinsieme algebrico non vuoto di $\mathbb{P}^n$. Allora il cono affine di X è un sottoinsieme algebrico di $\mathbb{A}^{n+1}$ e $\mathbb{I}_a(C(X))=\mathbb{I}(X)$.*

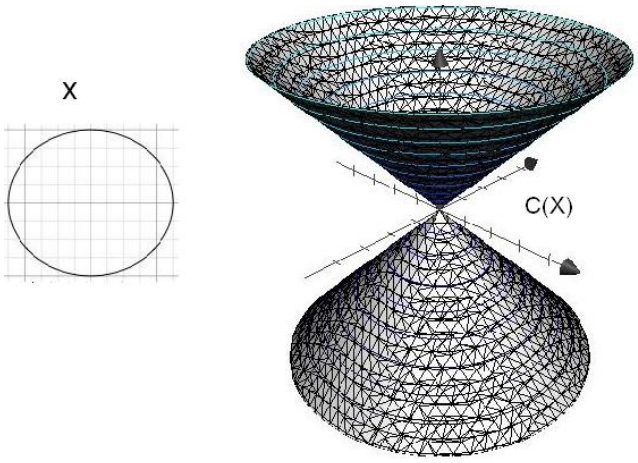

Figura 2.1: Conica proiettiva e cono affine associato

Dimostrazione: Sia P$\in\mathbb{I}_a$(C(X)). Allora P si annulla su ogni retta vettoriale di C(X) ovvero si annulla su ogni z$\in$X. Perciò P$\in\mathbb{I}$(X). Viceversa sia Q$\in\mathbb{I}$(X), scriviamo Q=$\sum$Q$_i$ come somma di polinomi omogenei. Essendo $\mathbb{I}$(X) omogeneo si ha che Q$_i\in\mathbb{I}$(X) per ogni i. Inoltre X non vuoto implica che $\mathbb{I}$(X) non contiene costanti ovvero deg(Q$_i$)>1. Poichè ogni polinomio omogeneo ha grado almeno uno si ha Q(0,..,0)=0 e quindi Q$\in\mathbb{I}_a$(C(X)). □

Proposizione 18 (Teorema degli zeri omogeneo)**.** *Sia I un ideale omogeneo di K[X$_0$,.., X$_n$]. Valgono i seguenti fatti:*

1. ***V**(I) è vuoto se e solo se (X$_0$,.., X$_n$)$^N\subseteq$I per qualche N>0.*
2. *se **V**(I) non è vuoto allora $\mathbb{I}$(**V**(I))=r(I).*

Dimostrazione: 1) Abbiamo **V**(I) è vuoto se e solo se $\mathbf{V}_a$(I)=(0,..,0). Dal teorema degli zeri $\mathbb{I}_a(\mathbf{V}_a(\mathrm{I}))$=r(I). Poichè $\mathbf{V}_a$(I)=(0,..,0) si ha (X$_0$,.., X$_n$)$\subseteq$r(I). Quindi per ogni i esiste n tale che $X_i{}^n\in$I. Sia M=max(n), allora per ogni i, $X_i{}^k\in$I se k$\geq$M. Pertanto per N sufficientemente grande (X$_0$,.., X$_n$)$^N\subseteq$I.
2) Dalla proposizione precedente $\mathbb{I}_a$(C(X))=$\mathbb{I}$(**V**(I)), con X=**V**(I). Ora C(X)=$\mathbf{V}_a$(I), $\mathbb{I}_a(\mathbf{V}_a(\mathrm{I}))=\mathbb{I}(\mathbf{V}(\mathrm{I}))$. Dal teorema degli zeri $\mathbb{I}_a(\mathbf{V}_a(\mathrm{I}))$=r(I), quindi $\mathbb{I}(\mathbf{V}(\mathrm{I}))$=r(I).

□

Osservazione 7. *Consideriamo **M**=(X$_0$,.., X$_n$) ideale massimale dei polinomi senza termine costante, **M** è omogeneo e **V**(**M**) è il vuoto. Infatti ogni punto di $\mathbb{P}^n$ ha almeno una coordinata non nulla.*

Proposizione 19. *Consideriamo le applicazioni:*

*F:{stt alg di P^n}$\rightarrow${id omogenei rad di K[X$_1$,..,X$_n$] escluso **M**}: X$\rightarrow\mathbb{I}$(X)*
*G:{id omogenei rad di K[X$_1$,..,X$_n$] escluso **M**}$\rightarrow${stt alg di P^n}: I$\rightarrow$**V**(I)*

F è biettiva e F^{-1}=G. Inoltre F e F^{-1} invertono le inclusioni.

Dimostrazione: Abbiamo $(G\circ F)(X)=\mathbf{V}(\mathbb{I}(X))=X$. Si ha $(F\circ G)(I)=\mathbb{I}(\mathbf{V}(I))=r(I)=I$ per la proposizione precedente e perchè I è radicale.
Siano ora X e Y sottoinsiemi algebrici tali che $X\subseteq Y$, consideriamo F(X) e F(Y). Sia $P\in F(Y)$ allora $P(y)=0$ per ogni $y\in Y$ in particolare $P(y)=0$ per ogni $y\in X$ ovvero $P\in F(X)$. Siano poi I e J ideali omogenei radicali tali che $I\subseteq J$, consideriamo $F^{-1}(I)$ e $F^{-1}(J)$. Sia $x\in F^{-1}(J)$ allora per ogni $P\in J$ si ha $P(x)=0$, in particolare $P(x)=0$ per ogni $P\in I$ ovvero $x\in F^{-1}(I)$. □

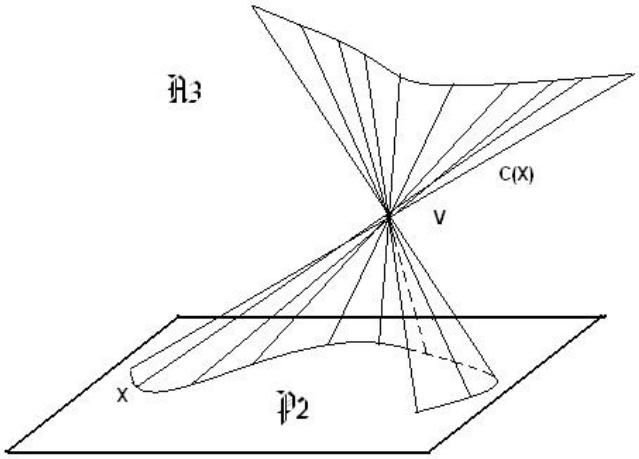

Figura 2.2: Cono sopra una curva di $\mathbb{P}^2$

Capitolo 3

Topologia di Zariski e varietà algebriche

«...per selezione naturale la nostra mente si è adattata alle condizioni del mondo esterno. Ha adottato la geometria più vantaggiosa per la specie, o in altre parola la più conveniente. La geometria non è vera, è vantaggiosa.»

Jules Henri Poincaré (1854-1912)

Vogliamo introdurre su $\mathbb{A}^n$ una topologia. In particolare vogliamo che le funzioni polinomiali $P:K^n \to K$ siano morfismi e quindi applicazioni continue. Se supponiamo che $\{0\} \subseteq K$ sia un chiuso richiediamo che $P^{-1}(0)=\mathbf{V}(P)$ sia un chiuso della topologia. Dal teorema della base di Hilbert questo equivale a richiedere che ogni sottoinsieme algebrico $Z=\mathbf{V}(I)$ in K^n sia un chiuso.

3.1 Costruzione della topologia di Zariski

Proposizione 20. *1. K^n e il vuoto sono sottoinsiemi algebrici di K^n.*

2. Un'intersezione qualsiasi di sottoinsiemi algebrici di K^n è un sottoinsieme algebrico di K^n.

3. Un'unione finita di sottoinsiemi algebrici di K^n è un sottoinsieme algebrico di K^n.

Dimostrazione: 1) K^n è il luogo degli zeri del polinomio nullo e il vuoto è $\mathbf{V}(1)$.
2) Siano $Z_i \subseteq K^n$ e $Z_i=\mathbf{V}(I_i)$. Allora $\bigcap_i Z_i=\mathbf{V}(J)$, dove J è l'ideale generato da $\bigcup_i I_i$.
3) Sia $Z=\mathbf{V}(I)$ e $Y=\mathbf{V}(J)$. Mostriamo che $\mathbf{V}(I)\cup\mathbf{V}(J)=\mathbf{V}(IJ)$. Sia $a\in\mathbf{V}(I)\cup\mathbf{V}(J)$ allora $P(a)=0$ per ogni $P\in I$ o $Q(a)=0$ per ogni $Q\in J$, se $F\in IJ$ allora $F=PQ$ con $P\in I$ e $Q\in J$. Si ha allora $F(a)=P(a)Q(a)=0$ per ogni $F\in IJ$ ovvero $a\in\mathbf{V}(IJ)$. Prendiamo ora $a\notin\mathbf{V}(I)\cup\mathbf{V}(J)$ allora $a\notin\mathbf{V}(I)$ e $a\notin\mathbf{V}(J)$. Quindi esiste $P\in I$ tale che $P(a)\neq 0$ ed esiste $Q\in J$ tale che $Q(a)\neq 0$. Se prendiamo $F=PQ$ abbiamo che $F\in IJ$ e $F(a)=P(a)Q(a)\neq 0$ dunque $F\notin\mathbf{V}(IJ)$. □

Definizione 46. *Dalla proposione precedente abbiamo che i sottoinsiemi algebrici sono i chiusi di una topologia su K^n. Tale topologia si dice topologia di Zariski. Se $Z \subseteq K^n$ è un insieme algebrico la topologia di Zariski su Z è la topologia indotta dalla topologia di Zariski su K^n.*

Osservazione 8. *1. Consideriamo $\mathbb{A}^1$. Ora K[X] è un P.I.D. quindi ogni suo ideale è generato da un unico elemento I=(P). Vediamo che gli insiemi algebrici di $\mathbb{A}^1$ sono tutto $\mathbb{A}^1$, il vuoto o gli insiemi finiti di punti (P ha al più deg(P) radici distinte). Siano A e B due aperti non vuoti, supponiamo che $A \cap B$ sia vuoto. Allora $A^C \cup B^C = \mathbb{A}^1$. Ma A^C e B^C sono entrambi unioni finite di punti mentre $\mathbb{A}^1$ è infinito dunque o $A^C = \mathbb{A}^1$ o $B^C = \mathbb{A}^1$ ma questo è assurdo perchè A e B sono non vuoti. Dunque $\mathbb{A}^1$ con la topologia di Zariski non è di Hausdorff.*

2. Inoltre $K^2 = K \times K$ ma la topologia di Zariski su K^2 non è la topologia prodotto delle topologie di Zariski su K. Supponiamo che la topologia su K^2 sia la topologia prodotto. La diagonale $D \subset K^2$ è il luogo degli zeri del polinomio P(X,Y)=X-Y e quindi è chiusa per la topologia di Zariski, questo implica (Capitolo 1 - Proposizione 9) che K è di Hausdorff e questo contraddice l'osservazione precedente.

3. Abbiamo visto che un chiuso proprio di K è un insieme finito. Il luogo degli zeri di un polinomio non costante in K^2 al contrario è sempre un insieme infinito. Più in generale vale la seguente:

Proposizione 21. *Sia $P \in K[X_1,..,X_n]$ un polinomio non costante (K algebricamente chiuso). Se $n \geq 2$ allora $\mathbf{V}(P)$ è un insieme infinito.*

Dimostrazione: Possiamo sempre decomporre P in componenti irriducibili. Ogni polinomio irriducibile nella fattorizzazione di P definisce una varietà contenuta nella varietà definita da P. Possiamo senza restrizioni mostrare l'asserto per un qualsiasi polinomio Q irriducibile. Supponiamo per assurdo che $\mathbf{V}(Q)$ non sia infinito. Allora $\mathbf{V}(Q)$ è un insieme finito di punti ed essendo irriducibile è un singolo punto. Per la corrispondenza biunivoca tra punti e ideali massimali $\mathbb{I}(\mathbf{V}(Q))=(Q)$ è un ideale massimale. Ovvero $(Q)=(X_1\text{-}a_1,...,X_n\text{-}a_n)$. Se $n \geq 2$ $X_1\text{-}a_1$ e $X_2\text{-}a_2$ non hanno fattori in comune e questo è assurdo. □

Definizione 47. *Un aperto standard di K^n con la topologia di Zariski è il complementare di un $\mathbf{V}(P)$ dove $P \in K[X_0,.., X_n]$, si denota con D(P) e si dice aperto standard definito da P.*

Gli aperti standard sono i complementari delle ipersuperfici di K^n. Ogni aperto di K^n si può scrivere come unione finita di aperti standard ovvero gli aperti standard sono una base per la topologia di Zariski. Questo deriva dal fatto che per il teorema della base ogni insieme algebrico si può scrivere come unione finita di ipersuperfici.

Proposizione 22. *Lo spazio affine $\mathbb{A}^n$ è compatto per la topologia di Zariski e anche ogni sottoinsieme algebrico Z di $\mathbb{A}^n$ è compatto.*

Dimostrazione: Poichè gli aperti standard sono una base della topologia consideriamo un ricoprimento di aperti standard $\bigcup_i D(P_i)=K^n$. Allora $\bigcap_i \mathbf{V}(P_i)$

è il vuoto, ovvero $\mathbf{V}(J)$ è il vuoto dove J è l'ideale generato dai P_i. Per il teorema della base J è finitamente generato e possiamo scrivere $J=(P_1,...,P_k)$. Allora $\mathbb{A}^n=D(P_1)\cup..\cup D(P_k)$. Dunque $\mathbb{A}^n$ è compatto. Ogni sottoinsieme algebrico Z è un chiuso in $\mathbb{A}^n$ compatto e dunque (Proposizione 7 - Capitolo 1) anche Z è compatto. □

Vogliamo ora tradurre la nozione topologica di irruducibilità (Capitolo I) in termini algebrici.

Proposizione 23. *Sia Z un sottoinsieme algebrico di $\mathbb{A}^n$. Si ha che Z è irriducibile $\Leftrightarrow$ $\mathbb{I}(Z)$ è un ideale primo.*

Dimostrazione:$\Rightarrow$) Supponiamo che $\mathbb{I}(Z)$ non sia primo. Allora esistono $P,Q\notin\mathbb{I}(Z)$ tali che $PQ\in\mathbb{I}(Z)$. Allora $Z\subseteq\mathbf{V}(PQ)=\mathbf{V}(P)\cup\mathbf{V}(Q)$. Scriviamo $Z=C\cup W$ dove $C=Z\cap\mathbf{V}(P)$ e $W=Z\cap\mathbf{V}(Q)$. Poiche $P,Q\notin\mathbb{I}(Z)$, C e W sono chiusi propri di Z. Perciò Z è riducibile.
$\Leftarrow$) Supponiamo Z riducibile. Allora $Z=Z_1\cup Z_2$ dove i Z_i sono chiusi propri di Z. Poichè $Z_i\subset Z$ si ha $\mathbb{I}(Z)\subset\mathbb{I}(Z_i)$ strettamente. Esistono allora $P_i\in\mathbb{I}(Z_i)$-$\mathbb{I}(Z)$. Inoltre $P_1P_2\in\mathbb{I}(Z_1)\cap\mathbb{I}(Z_2)=\mathbb{I}(Z_1)\cup\mathbb{I}(Z_2)=\mathbb{I}(Z)$, quindi $\mathbb{I}(Z)$ non è primo. □

Osservazione 9. *$\mathbb{A}^n$ è irruducibile. Infatti $\mathbb{A}^n=\mathbf{V}((0))$ che è un ideale primo.*

3.2 Decomposizione in componenti irriducibili

Mostriamo che ogni sottoinsieme algebrico Y può essere decomposto in maniera unica nell'unione di un numero finito di sottoinsiemi algebrici irriducubili.

Definizione 48. *Un sottoinsieme algebrico Y di $\mathbb{A}^n$ ammette una decomposizione in componenti irriducibili se si può scrivere $Y=\bigcup_{i=1}^{k} Y_i$, dove ogni Y_i è un sottoinsieme algebrico irriducibile e Y_i non è contenuto in Y_j se $i\neq j$.*

Proposizione 24. *Sia T un insieme non vuoto di sottoinsiemi algebrici di $\mathbb{A}^n$ allora T ha un elemento minimale per l'inclusione.*

Dimostrazione: L'anello dei polinomi a coefficienti in K è Noetheriano. Sappiamo che ogni insieme non vuoto di ideali di $K[X_0,.., X_n]$ ammette un elemento massimale per l'inclusione (Proposizione 6 - Capitolo 1) è che la corrispondenza biunivoca tra ideali radicali e sottoinsiemi algebrici inverte le inclusioni. Dunque esiste in T un elemento minimale per l'inclusione. □

Proposizione 25. *Ogni sottoinsieme algebrico non vuoto di $\mathbb{A}^n$ ammette un'unica decomposizione in componenti irriducibili.*

Dimostrazione: Sia Y un sottoinsieme algebrico non vuoto di $\mathbb{A}^n$. Sia T l'insieme dei sottoinsiemi algebrici non vuoti di $\mathbb{A}^n$ che non ammettono una decomposizione in componenti irriducibili. Supponiamo che T sia non vuoto, allora per la proposizione precedente T ammette un elemento minimale X. Per come è definito T si ha che X è riducibile e possiamo scrivere $X=U\cup W$ dove U e W sono insiemi algebrici strettamente contenuti in X. Per minimalità di X si ha che U e W ammettono una decomposizione in componenti irriducibili,

U=$\bigcup$U$_i$ e W=$\bigcup$W$_i$. Ma allora X=($\bigcup$U$_i$)$\cup$($\bigcup$W$_i$) è una decomposizione di X in componenti irriducibili, assurdo. Allora ogni insieme algebrico Y ammette una decomposizione in componenti irriducibili. Mostriamo ora l'unicità della decomposizione. Supponiamo di poter scrivere Y=$\bigcup$Y$_i$=$\bigcup$Z$_j$, i=1,..,r e j=1,..,t. Abbiamo Y$_1$=$\bigcup$(Z$_j\cap$Y$_1$). Ma Y$_1$ è irriducibile perciò Y$_1\subseteq$Z$_k$ per qualche k. A meno di riordinare possiamo supporre k=1. Analogamente si ha che Z$_1\subseteq$Y$_s$, da cui Y$_1\subseteq$Y$_s$ quindi s=1 e Y$_1$=Z$_1$. Sia ora Y' la chiusura di Y-Y$_1$. Y' è un sottoinsieme algebrico. Possiamo scrivere Y' come unione di componenti irriducibile usando le decomposizione di Y alle quali abbiamo tolto Y$_1$ e Z$_1$. Procedendo analogamente su Y' otteniamo la tesi. □

Definizione 49. *Una varietà algebrica affine Z di $\mathbb{A}^n$ è un sottoinsieme algebico irriducibile. Una varietà quasi-affine è un aperto non vuoto di una varietà affine.*

Proposizione 26. *Sia $P\in K[X_0,..,X_n]$ un polinomio non costante e sia $P=P_1^{r1}...P_t^{rt}$ la sua decomposizione in componenti irriducibili. La decomposizione in componenti irriducibili di $T=\mathbf{V}(P)$ è data da $T=\mathbf{V}(P_1)\cup...\cup\mathbf{V}(P_t)$. Inoltre $\mathbb{I}(T)=(Q)$ dove Q è il polinomio $Q=P_1...P_t$.*

Dimostrazione: Chiaramente T=$\mathbf{V}$(P$_1$)$\cup$...$\cup\mathbf{V}$(P$_t$). Ogni $\mathbf{V}$(P$_i$) è irriducibile ed essendo P$_i$ irriducibile l'ideale (P$_i$) è primo. Inoltre $\mathbf{V}$(P$_i$) non è contenuto in nessuno dei $\mathbf{V}$(P$_j$) se i$\neq$j perchè P$_j$ è irriducibile. Per l'unicità questa è la decomposizione in componenti irriducibili di T. Inoltre $\mathbb{I}(\bigcup\mathbf{V}(P_i))=\bigcap\mathbb{I}(\mathbf{V}(P_i))$. Poichè (P$_i$) è un ideale primo si ha che $\mathbb{I}$(V(P$_i$))=(P$_i$). Concludiamo che $\bigcap\mathbb{I}(\mathbf{V}(P_i))$=(P$_1$...P$_t$) infatti essendo i P$_i$ primi ogni polinomio divisibile per ogni P$_i$ è divisibile per il prodotto P$_1$...P$_t$. □

Osservazione 10. *Dalla proposizione precedente si ha che esiste una corrispondenza biunivoca tra ipersuperfici irriducibili di $\mathbb{A}^n$ e i polinomi irriducibili di $K[X_0,..,X_n]$ se si identifica P con λP per $\lambda\in K^*$.*

3.3 Topologia di Zariski in $\mathbb{P}^n$

Vogliamo dare a $\mathbb{P}^n$ la struttura di spazio topologico attraverso la topologia di Zariski.

Lemma 6. *Ogni unione finita e ogni intersezione arbitraria di sottoinsiemi algebrici proiettivi è un insieme algebrico proiettivo. Il vuoto e $\mathbb{P}^n$ sono insiemi algebrici proiettivi.*

Dimostrazione: Siano X=$\mathbf{V}$(I) e Y=$\mathbf{V}$(J) due sottoinsiemi algebrici proiettivi. Allora X$\cup$Y=$\mathbf{V}$(IJ) dove IJ è un ideale omogeneo. Sia X$_i$=$\mathbf{V}$(I$_i$) una famiglia di sottoinsiemi algebrici. Allora $\bigcap$X$_i$=$\mathbf{V}$(H), dove H è l'ideale omogeneo generato da $\bigcup$I$_i$. Infine $\mathbb{P}^n$=$\mathbf{V}$((0)) e il vuoto è definito da $\mathbf{V}$(1). □

Definizione 50. *Dal lemma precedente segue che i sottoinsiemi algebrici proiettivi sono i chiusi di una topologia su $\mathbb{P}^n$, la topologia di Zariski su $\mathbb{P}^n$.*

Definizione 51. *Una varietà proiettiva è un sottoinsieme algebrico di $\mathbb{P}^n$ irriducibile (per la topologia indotta dalla topologia di Zariski). Una varietà quasi proiettiva è un aperto di una varietà proiettiva.*

Lemma 7. *Sia I un ideale omogeneo di K[X_0,.., X_n]. L'ideale I è primo se e solo se: per ogni P,Q omogenei, PQ∈I⇒P∈I o Q∈I.*

Dimostrazione: Supponiamo I omogeneo e tale che per ogni P,Q, PQ∈I implica P∈I o Q∈I, mostriamo che I è primo. Siano G,H∈I e consideriamo le loro decomposizioni in polinomi omogenei G=G_m+...+G_0, H=H_t+...+H_0, dove deg(G_i)=deg(H_i)=i. Ora GH=$\sum F_i$ dove F_i=$\sum G_{i-k}H_k$. Essendo I omogeneo F_i∈I per ogni i. In particolare G_mH_t∈I quindi G_m∈I o H_t∈I. Se entrambi stanno in I consideriamo G-G_m e H-H_t anzichè G e H. Supponiamo allora che G_m∈I e H_t∉I. Mostraimo ora per induzione che G_i∈I per ogni i. Supponiamo di aver dimostrato che G_m,...,G_r stanno in I. Si ha F_{r-1+t}=$G_{r-1}H_t$+(G_rH_{t-1}+$G_{r+1}H_{t-2}$+...) =$G_{r-1}H_t$+Q con Q∈I. Dunque $G_{r-1}H_t$=F_{r-1+t}-Q∈I. Perciò G_{r-1}∈I e quindi G∈I. □

Lemma 8. *Un sottoinsieme algebrico X in $\mathbb{P}^n$ è irriducibile se e solo se $\mathbb{I}(X)$ è un ideale primo.*

Dimostrazione: Grazie al lemma precedente la dimostrazione è uguale a quella del caso affine. □

Come nel caso affine, si dimostra:

Proposizione 27. *Ogni sottoinsieme algebrico non vuoto X di $\mathbb{P}^n$ ammette una ed un'unica decomposizione in componenti irriducibili: $X=\bigcup_{i=1}^{r} X_i$ con X_i irriducibili e $X_i \neq X_j$ se $i \neq j$.*

Riportiamo ora due esempi:
Consideriamo il sottoinsieme algebrico V di $\mathbb{A}^3$ definito dai polinomi X^2-YZ e XZ-X. Mostiamo che V è unione di tre componenti irriducibili e troviamo i loro ideali primi. Ora X^2-YZ è una quadrica irriducibile mentre XZ-X è riducibile

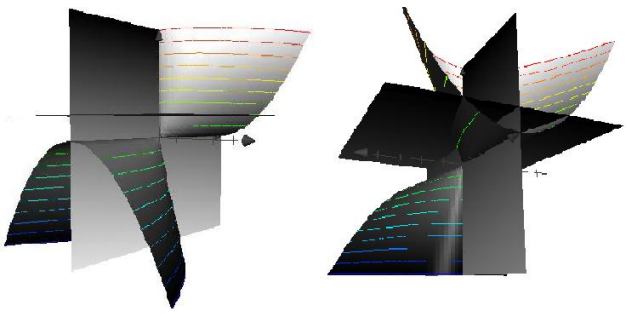

Figura 3.1: Intersezione tra una quadrica e una cubica di $\mathbb{A}^3$

ed è unione dei piani X=0 e Z-1=0. Le tre componenti irriducibili cercate sono allora le varietà di $\mathbb{A}^3$ definite dagli ideali primi I_1=(X,Y), I_2=(X,Z) e I_3=(Z-1,X^2-Y). Le prime due sono rette la terza una parabola.

In particolare la quadrica X^2-YZ è un'ipersuperfice in $\mathbb{A}^3$, quindi un chiuso della topologia di Zariski, il suo complementare è un aperto standard. La varietà definita da I_1=(X,Y) è una retta, un chiuso sulla varietà è un'unione finita di suoi punti infatti possiamo riguardare la retta come un $\mathbb{A}^1$. Quindi se alla retta togliamo un numero finito di punti abbiamo un aperto della varietà avvero un esempio di varietà quasi-affine di $\mathbb{A}^3$.

Un altro esempio è dato dall'insieme algebrico Z=$\{(t,t^2,t^3)$, con t∈K$\}$. Posto

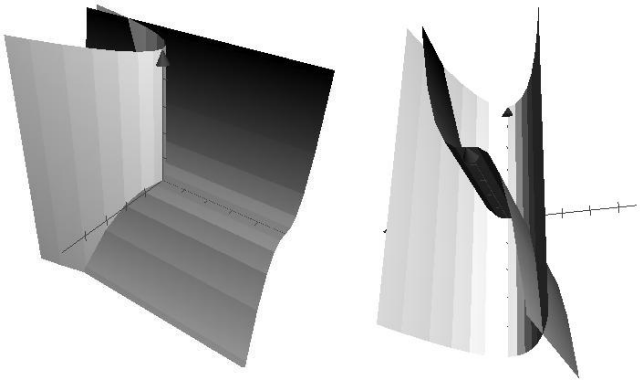

Figura 3.2: Cubica Gobba come intersezione di superfici in $\mathbb{A}^3$

X=t,Y=t^2 e Z=t^3 si ha che Y=X^2 e Z=X^3. Allora possiamo vedere Z con il sottoinsieme algebrico definito da X^2-Y e X^3-Z. Quindi Z=V(I) dove I=(X^2-Y,X^3-Z), il sottoinsieme algebrico Z è una varietà di $\mathbb{A}^3$ detta cubica gobba.

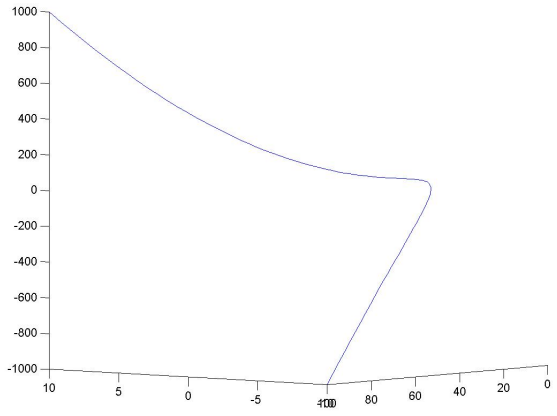

Figura 3.3: Cubica Gobba in $\mathbb{A}^3$

3.4 Il Concetto di dimensione

Definizione 52. *Sia X uno spazio topologico. La dimensione di X é: dim(X)=Sup{n∈ℕ tali che esiste una catena $Z_0 \subset Z_1 \subset ... \subset Z_n$ di sottoinsiemi distinti di X chiusi e irriducibili}. La dimensione di un insieme algebrico $Y \subset \mathbb{A}^n$ è la sua dimensione come spazio topologico munito della topologia indotta dalla topologia di Zariski.*

Vogliamo ora tradurre la nozione topologica di dimensione in linguaggio algebrico.

Definizione 53. *Sia A un anello e P un ideale primo di A. L'altezza di P è: ht(P)=Sup{n∈ℕ tali che esiste una catena $P_0 \subset P_1 \subset ... \subset P_n = P$ di ideali primi distinti di A}. La dimensione di Krull dell'anello A è: dim(A)=Sup{ht(P) tali che P è un ideale primo di A}.*

Lemma 9. *Sia A un anello, I un ideale di A e $\Pi: A \to A/I$ la proiezione canonica. Allora la mappa che manda l'ideale J di A in $\Pi(J)$ definisce una biezione tra gli ideali di R che contengono I e gli ideali di A/I. Inoltre posto J'=$\Pi(J)$, si ha che J' è radicale o massimale se e solo se J lo è.*

Dimostrazione: Se I è contenuto in J abbiamo un'applicazione suriettiva da R/I in R/J il cui nucleo è J/I. Per i teoremi di isomorfismo l'ideale Π(J) di R/I si identifica con J/I e (R/I)/Π(J)≅R/J. Da ciò risulta che Π(J) è primo o massimale se e solo se J lo è. Supponiamo ora che J sia radicale. Sia $\Pi(f)^n \in J' = \Pi(J)$. Abbiamo $\Pi(f)^n = \Pi(f^n) = \Pi(u)$ con u∈J. Quindi $\Pi(f^n - u) = 0$ ovvero $\Pi(f^n - u) \in I \subset J$, da cui $f^n \in J$. Essendo J radicale si ha che f∈J quindi Π(f)∈J' e J' è radicale. Viceversa supponiamo J' radicale. Sia $u^n \in J$, allora $\Pi(u^n) = \Pi(u)^n \in J'$. Essendo J' radicale si ha che Π(u)∈J' e perciò u∈J. □

Corollario 1. *Sia $Y \subset \mathbb{A}^n$ un sottoinsieme algebrico. Sia Λ={Z⊂ Y tali che Z è un sottoinsieme algebrico} e Ω={J'⊂A(Y) tali che J' è un ideale radicale}. Sia $\Pi: K[X_1,...,X_n] \to A(Y)$ la proiezione canonica.*

- *L'applicazione $\varphi: \Lambda \to \Omega$: $Z \to \Pi(\mathbb{I}(Z))$ è biettiva.*
- *L'applicazione $\varphi^{-1}: \Omega \to \Lambda$ è definita da $\varphi^{-1}(J') = \boldsymbol{V}(\Pi^{-1}(J'))$. Inoltre Z è irriducibile o un singolo punto a seconda che J' sia primo o massimale.*

Abbiamo così una corrispondenza biunivoca tra i sottoinsiemi algebrici di di Y e gli ideali radicali di A(Y). Le sottovarietà di Y corrispondono agli ideali primi di A(Y) ovvero agli ideali di $K[X_1,...,X_n]$ contenenti $\mathbb{I}(Y)$.

Proposizione 28. *Sia Y una varietà affine allora dim(Y)=dim(A(Y)).*

Dimostrazione: Sappiamo che dim(Y)=Sup{n∈ℕ tali che esiste una catena $Z_0 \subset Z_1 \subset ... \subset Z_n$ di sottoinsiemi distinti di Y chiusi e irriducibili}. Se Q è un ideale primo di A(Y) allora ht(Q)=Sup{n∈ℕ tali che esiste una catena $P_0 \subset P_1 \subset ... \subset P_n = Q$ di ideali primi distinti di A}. Ora dim(A(Y))=Sup{ht(Q) tale che Q è un ideale primo di A}=Sup{N∈ℕ tali che $I_0 \subset I_1 \subset ... \subset I_N$ è una successione di ideali primi di A(Y)}=Sup{N∈ℕ tali che $Z_0 \subset Z_1 \subset ... \subset Z_N$ è una successione di sottovarietà algebriche di Y}=dim(Y). □

Capitolo 4

Morfismi

«Uno scienziato degno di tal nome, e specialmente un matematico, sperimenta nel suo lavoro la stessa sensazione di un artista; il suo piacere è della stessa intensità e natura.»
Jules Henri Poincaré (1854-1912)

Abbiamo fino ad ora introdotto gli oggetti della geometria algebrica vogliamo ora fare lo stesso per i morfismi. In questo capitolo daremo una prima definizione globale di funzione regolare poi introdurremo una definizione locale. Potremmo così definire i morfismi tra varietà algebriche e infine dare la definizione di morfismo dominante e di applicazione birazionale.

Definizione 54. *Sia $Z \subset \mathbb{A}^n$ un sottoinsieme algebrico. Una funzione $f:Z \to K$ si dice polinomiale se esiste un polinomio $P \in K[X_1,\dots,X_n]$ tale che $f(x)=P(x)$ per ogni $x \in Z$. Si denota con $\mathbb{O}(Z)$ l'insieme delle funzioni regolari su Z. Si ha che $\mathbb{O}(Z)$ è un anello e una K-algebra.*

Osservazione 11. *Siano P,Q due polinomi, P e Q definiscono la stessa funzione regolare su Z se e solo se $P(x)=f(x)=Q(x)$ per ogni $x \in Z$. Ora $P(x)=Q(x)$ per ogni $x \in Z$ se e solo se $(P-Q)(x)=0$ per ogni $x \in Z$ ovvero se e solo se $P-Q \in \mathbb{I}(Z)$. Qundi abbiamo un isomorfismo di anelli tra $K[X_1,\dots,X_n]/\mathbb{I}(Z)$ e $\mathbb{O}(Z)$. In altri termini $\mathbb{A}(Z) \cong \mathbb{O}(Z)$.*

Definizione 55. *Siano $X \subset \mathbb{A}^n$ e $Y \subset \mathbb{A}^m$ due sottoinsiemi algebrici. Un'applicazione $f:X \to Y$ è un morfismo se $f=(f_1,\dots,f_m)$ dove le $f_i:X \to K$ sono funzioni regolari. Un morfismo $f:X \to Y$ si dice un isomorfismo se esiste un morfismo $g:Y \to X$ tale che $f \circ g = Id_Y$ e $g \circ f = Id_X$.*

Osservazione 12. *Un morfismo è sempre un'applicazione continua e ogni funzione regolare è un morfismo. Se la composione di due morfismi è definita allora è ancora un morfismo.*

4.1 Funzioni razionali

Consideriamo ora varietà affini, ovvero insiemi algebrici irriducibili. Sia $Z \subset \mathbb{A}^n$ una varietà affine, $\mathbb{I}(Z)$ è un ideale primo. L'anello delle coordinate $A(Z)$ è un dominio di integrità, ha senso quindi considerarne il campo dei quozienti che denotiamo con $K(Z)$. Allora:

$$K(Z)=(P/Q \text{ tali che } P,Q\in K[X_1,...,X_n],\ Q\notin \mathbb{I}(Z))$$

Osserviamo che due elementi P/Q e R/T di K(Z) coincidono se e solo se PT=RQ su Z, ovvero se e solo se PT-RQ$\in\mathbb{I}$(Z).

Proposizione 29 (Prolungamento delle identità algebriche)**.** *Sia $Z\subset K^n$ un sottoinsieme algebrico e siano P,Q due polinomi in $K[X_1,...,X_n]$. Se P(x)=Q(x) per ogni $x\in K^n$-Z allora P=Q.*

Dimostrazione: Mostriamo che se un polinomio P si annulla su K^n-Z allora è identicamente nullo. Poniamo U=K^n-Z. Allora U$\subset\mathbf{V}$(P) quindi $\overline{U}\subset\overline{\mathbf{V}(P)}=\mathbf{V}$(P), essendo $\mathbf{V}$(P) un chiuso. Ora K^n è irriducibile e abbiamo un aperto non vuoto U$\subset K^n$ irriducibile, sappiamo allora che U è denso in K^n ovvero $\overline{U}=K^n$. Deve esserè perciò $\mathbf{V}$(P)=K^n ovvero P è identicamente nullo. □

Definizione 56. *Una funzione f si dice razionale se può essere scritta come f=P/Q dove P e Q sono due polinomi. Una funzione razionale R si dice definita o regolare nel punto $x\in Z$ se può essere scritta nella forma R=P/Q con Q(x)≠0.*

L'insieme dei punti regolari di una funzione razionale f è un aperto non vuoto. Presa una rappresentazione di f=P/Q, Q$\notin\mathbb{I}$(Z), si ha che esiste x$\in$Z tale che Q(x)≠0, perciò l'insieme dei punti regolari non è vuoto. Siano ora f=P_i/Q_i tutte le possibili rappresentazioni di f. Allora f è definita sull'aperto U=$\bigcup_i$Z-$\mathbf{V}(Q_i)$.
Osserviamo che se due funzioni razionali coincidono su un aperto allora sono uguali. Siano f=P/Q e g=R/T, supponiamo che f(x)=g(x) per ogni x appartenente ad un aperto U, allora (f-g)(x)=r(x)=0 per ogni x$\in$U. Mostriamo ora che una funzione razionale che si annulla su un aperto è identicamente nulla. Sia f=P/Q tale che f(x)=0 per ogni x nell'aperto U. Sia V=Z-$\mathbf{V}$(Q), V è aperto e W=U$\cap$V è un aperto non vuoto di Z essendo Z irriducibile. Allora P(x)=0 su W e per il principio di prolungamento delle identità algebriche P=0 su Z ovvero f(x)=0 per ogni x$\in$Z.

Proposizione 30. *Una funzione razionale f$\in$K(Z) definita in ogni punto della varietà affine Z è una funzione polinomiale.*

Dimostrazione: Per ogni x$\in$Z esiste Q_x, con $Q_x(x)\neq 0$ tale che f=P_x/Q_x. Sia I l'ideale generato dai Q_x, essendo K[X_1,...,X_n] noetheriano I è finitamente generato e possiamo supporre I=(Q_{x1},...,Q_{xt}). Per come è definito I si ha che $\mathbf{V}$(I)$\cap$Z è vuoto. Ora $\mathbf{V}$(I)$\cap\mathbf{V}(\mathbb{I}(Z))=\mathbf{V}(I+\mathbb{I}(Z))$ è vuoto. Questo significa che I+$\mathbb{I}$(Z) è l'ideale di tutti i polinomi costanti non nulli, in particolare 1$\in$I+$\mathbb{I}$(Z). Possiamo perciò scrivere $1=\sum_{i=1}^m H_i Q_{xi}(\mathrm{mod}(\mathbb{I}(Z)))$. Moltiplicando per f si ha $f=\sum_{i=1}^m H_i fQ_{xi}(\mathrm{mod}(\mathbb{I}(Z)))=\sum_{i=1}^m H_i(P_{xi}/Q_{xi})Q_{xi}(\mathrm{mod}(\mathbb{I}(Z)))$. Vediamo allora che $f=\sum_{i=1}^m H_i P_{xi}(\mathrm{mod}(\mathbb{I}(Z)))$ è una funzione polinomiale ovvero una funzione regolare su Z. □

Le definizioni di funzione regolare e di morfismo date in precedenza sono globali. Notiamo che se f:X$\to$K è una funzione regolare con f(x)≠0 allora 1/f non è un morfismo in un intorno di x perchè 1/f è una funzione razionale e non polinomiale. Vogliamo cercare una definizione locale di morfismo, basata sul concetto di funzione razionale che elimini questo problema.

Definizione 57. *Sia $Y \subset \mathbb{A}^n$ una varietà affine o quasi affine. Un'applicazione $f: Y \to K$ si dice regolare in $y \in Y$ se esiste un intorno aperto U_y di y e dei polinomi P_y, Q_y con $Q_y(x) \neq 0$ per ogni $x \in U_y$, tali che $f = P_y/Q_y$ su U_y. L'applicazione f si dice regolare se è regolare in ogni punto di Y. Si denota con $\mathbb{O}(Y)$ l'anello delle funzioni regolari su Y.*

Lemma 10. *Sia X uno spazio topologico. Un sottoinsieme $Z \subset X$ è chiuso in X se e solo se esiste un ricoprimento aperto di X, $X = \bigcup_i U_i$, tale che $Z \cap U_i$ sia chiuso in U_i per ogni i.*

Dimostrazione: Sia Z chiuso in X. Consideriamo il ricoprimento di X costituito da X stesso e dal vuoto. Ora $Z \cap X = Z$ è chiuso e Z intersecato il vuoto è il vuoto che è ancora chiuso. Vicerversa supponiamo che esista un ricoprimento con le proprietà richieste, mostriamo che X-Z è aperto. Notiamo che $(X\text{-}Z) \cap U_i = U_i\text{-}(Z \cap U_i)$ è aperto in U_i e quindi in X. Se $x \in X\text{-}Z$ esiste j tale che $x \in U_j$ e $(X\text{-}Z) \cap U_j$ è un intorno aperto in X di x contenuto in X-Z, allora X-Z è aperto. □

Proposizione 31. *Sia $Y \subset \mathbb{A}^n$ una varietà quasi affine.*

1. *Se $f \in \mathbb{O}(Y)$ allora f è continua per la topologia di Zariski.*
2. *Siano $f, g \in \mathbb{O}(Y)$, se f e g coincidono su un aperto non vuoto di Y allora coincidono su tutto Y.*
3. *$\mathbb{O}(Y)$ è un dominio di integrità.*

Dimostrazione: 1) Per mostrare che f è continua basta far vedere che la preimmagine di un chiuso è un chiuso. Ora f è a valori in $K = \mathbb{A}^1$, sappiamo che i chiusi non banali di $\mathbb{A}^1$ sono unioni finite di punti, riduciamo così il problema a dimostrare che la preimmagine di un punto $a \in \mathbb{A}^1$ è un chiuso di Y. Per definizione di funzione regolare per ogni $y \in Y$ esiste un aperto U_y tale che $f = P/Q$ su U_y. Gli U_y costituiscono un ricoprimento aperto di Y, per il lemma precedente è sufficente mostrare che $f^{-1}(a) \cap U_y$ è chiuso per ogni $y \in Y$. Ora $f^{-1}(a) \cap U_y = \{x \in U_y \text{ tali che } f(x) = P(x)/Q(x) = a\} = \{x \in U_y \text{ tali che } aQ(x)\text{-}P(x) = 0\} = \mathbf{V}(aQ\text{-}P) \cap U_y$. Allora $f^{-1}(a)$ è chiuso in U_y.
2) Sia $Z = \{x \in Y \text{ tali che } f(x) = g(x)\}$. Notiamo che $Z = (f\text{-}g)^{-1}(0)$ e quindi è un chiuso di Y. Se U è un aperto non vuoto contenuto in Z allora $\overline{U} \subset Z$, ma $\overline{U} = Y$ essendo Y uno spazio topologico irriducibile. Concludiamo che $Z = Y$.
3) Sia $f \in \mathbb{O}(Y)$, $D(f) = \{x \in Y \text{ tali che } f(x) \neq 0\}$ è un aperto non vuoto di Y perchè è il complementare di $f^{-1}(0)$ che è chiuso per 1). Siano ora $f, g \in \mathbb{O}(Y)$ non identiacamente nulle, allora D(f) e D(g) sono due aperti non vuoti di Y. Inoltre D(f) e D(g) hanno intersezione non vuota perchè Y è irriducibile e i suoi aperti sono densi. Quindi esiste $x \in D(f) \cap D(g)$ tale che $(fg)(x) \neq 0$, ovvero fg non è identicamente nulla. □

Lemma 11. *Se Y è una varietà affine ogni funzione regolare è polinomiale.*

Dimostrazione: Sia f una funzione regolare su Y, allora per ogni $y \in Y$ esiste U_y aperto tale che $f = P/Q$ su U_y e $Q(x) \neq 0$ per ogni $x \in U_y$. Ora f è una funzione razionale definita in ogni punto di U_y sappiamo allora (Proposizione 30) che f è

polinomiale, ovvero esiste un polinomio F(x) tale che f(x)=F(x) per ogni x∈U_y. Le applicazioni f e F sono in particolare elementi di $\mathbb{O}(Y)$ che coincidono su un aperto e per la proposizione precedente coincidono su tutto Y. □

Diamo ora la definizione definitiva di morfismo tra varietà quasi affini.

Definizione 58. *Siano X e Y due varietà quasi affini e φ:X→Y un'applicazione, φ è un morfismo se:*

- *φ è continua.*
- *Per ogni aperto U⊂Y e per ogni funzione regolare f:U→K si ha che f∘φ:V=φ^{-1}(U):→K è una funzione regolare.*

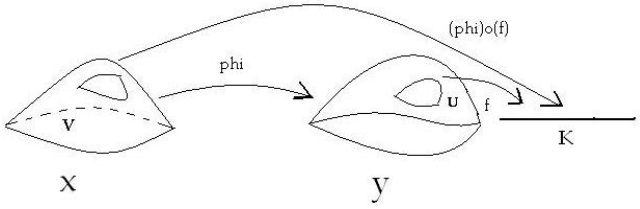

Figura 4.1: Morfismo tra varietà algebriche

Ogni funzione regolare è un morfismo. Inoltre la composizione di morfismi è un morfismo. Infatti se F,G:X→Y sono due morfismi F∘G è continua e F∘G∘f=F∘(G∘f) è regolare. Infine diamo la definizione di morfismo per un insieme algebrico qualsiasi.

Definizione 59. *Sia Y un sottoinsieme algebrico di $\mathbb{A}^n$, F:Y→$\mathbb{A}^m$ è un morfismo se e solo se F_{Yi} (F ristretto a Y_i) è un morfismo per ogni Y_i componente irriducibile di Y.*

4.2 Applicazioni razionali

Definizione 60. *Sia Z una varietà affine. Un' applicazione razionale f:Z→$\mathbb{A}^m$ è del tipo f=(f_1,...,f_m), dove le f_i:Z→K sono funzioni razionali. L'applicazione f si dice definita o regolare in x∈Z se tutte li f_i lo sono. Pertanto il dominio di definizione di f è U=$\bigcap U_i$, con U_i dominio di definizione di f_i. L'immagine di f è f(Z)={f(x) tali che x∈Z e f è definita in x}. Un'applicazione razionale dalla varietà affine Z all'insieme algebrico Y⊂$\mathbb{A}^m$ è un'applicazione razionale f:Z→$\mathbb{A}^m$ tale che f(Z)⊂Y.*

Lemma 12. *Sia Z una varietà affine, f=(f_1,...,f_m):Z→$\mathbb{A}^m$ un'applicazione razionale e Y⊂$\mathbb{A}^m$ un insieme algebrico. Allora f(Z)⊂Y se e solo se per ogni P∈$\mathbb{I}$(Y) si ha P(f_1,...,f_m)=0 in K(Z).*

Dimostrazione: Sia P∈$\mathbb{I}$(Y) allora P(x)=0 per ogni x∈Y, dove P:$\mathbb{A}^n$→K. Se f(Z)⊂Y allora per ogni P∈$\mathbb{I}$(Y) P∘f:Z→K è una funzione razionale su Z che si annulla su un aperto non vuoto quindi P∘f=0 in K(Z). Viceversa supponiamo che P∘f=0 in K(Z) per ogni P∈$\mathbb{I}$(Y). Se x∈Z e se f è definita in x allora P(f(x))=0 per ogni P∈$\mathbb{I}$(Y), quindi f(x)∈Y. □

Osserviamo che se f:X→Y e g:Y→Z sono due applicazioni razionali tra varietà affini, in generale non è possibile considerare g∘f:X→Z, infatti potrebbe accadere che $f^{-1}(V)$ è vuoto, dove V è il dominio di g. Per ovviare a questo introduciamo il concetto di applicazione dominante.

4.3 Applicazioni razionali dominanti

Definizione 61. *Sia Z una varietà affine. Un'applicazione f:Z→Y, dove Y è un insieme algebrico, è dominante se f(Z) è denso in Y.*

Osservazione 13. *Ogni applicazione razionale è un morfismo nel suo dominio di definizione e in particolare è continua. Perciò f(Z) e irriducibile da cui* $Y=\overline{f(Z)}$ *ovvero anche Y è una varietà affine. Inoltre dalle applicazioni razionali dominanti si può introdurre la nozione di morfismo dominante. Un morfismo è dominante se è quasi-suriettivo, nel senso che la sua immagine è densa nel codominio. Notiamo esplicitamente che esistono morfismi dominanti non suriettivi, consideriamo ad esempio* $Z=\boldsymbol{V}(xy-1)\subset\mathbb{A}^2$ *e dia p:Z→K l'applicazione che manda (x,y)→x (proiezione sull'asse x), notiamo che p è dominante ma non suriettivo infatti p(Z)=K-(0).*
Infine se f:X→Y e g:Y→Z sono applicazioni razionali dominanti allota f(Z) è denso in Y e se V⊂Y è il dominio di definizione di g, f(Z)∩V non è vuoto e perciò anche $f^{-1}(V)$ *non lo è, quindi possiamo sempre considerare g∘f.*

Introduciamo ora un concetto proprio della geometria algebrica, quello di applicazione birazionale.

Definizione 62. *Un'applicazione birazionale β:X→Y tra le varietà affini X e Y, è un' applicazione razionale che ammette un' applicazione razionale inversa, ovvero tale che esiste un applicazione razionale dominante α:Y→X tale che* $\beta\circ\alpha=Id_Y$ *e* $\alpha\circ\beta=Id_X$*. In tal caso si dice che X e Y sono birazionalmente equivalenti.*

Proposizione 32. *Siano X e Y varietà affini. I seguenti fatti sono equivalenti:*

1. *X e Y sono birazionalmente equivalenti.*
2. *Esitono due aperti non vuoti U⊂X e V⊂Y tali che U e V siano isomorfi.*

Dimostrazione: 1)⇒2) Siano f e g applicazioni birazionali definite rispettivamente su U' e V'. Allora g∘f è definita su $f^{-1}(V')$ e f∘g è definita su $g^{-1}(U')$. Consideriamo gli aperti $U=f^{-1}(g^{-1}(U'))$ e $V=g^{-1}(f^{-1}(V'))$, U e V sono isomorfi.
2)⇒1) Se abbiamo un'applicazione razionale tale che f(U)=V con U aperto di X e V aperto di Y allora essendo U e V densi in X e Y si ha f(X)=Y. □

Concludiamo il capitolo con la definizione di varietà razionale.

Definizione 63. *Una varietà affine X si dice razionale se è birazionalmente equivalente a uno spazio affine* $\mathbb{A}^n$*.*

Capitolo 5

Curve algebriche di $\mathbb{P}^2$

«Tutti sanno cos'è una curva fino a quando non si studia abbastanza matematica da confondersi tra le innummerevoli possibili eccezioni.»

Felix Klein (1849-1925).

In questo capitolo verranno esposti alcuni importanti risultati riguardo le curve algebriche di $\mathbb{P}^2$ con particolare attenzione alle cubiche. Inoltre mostreremo che esistono due forme canoniche per l'equazione di una cubica liscia dette di Legendre e di Weierstrass.

Definizione 64. *Una curva algebrica piana proiettiva C, è un elemento di $\mathbb{P}(O_d)$ proiettivizzato dello spazio vettoriale dei polinomio omogenei di grado $d\geq 1$. Se F(X,Y,Z) è un rappresentante di C si dice che F(X,Y,Z)=0 è un'equazione di C. Il grado di C è il grado del polinomio F(X,Y,Z). Il sottoinsieme algebrico $\boldsymbol{V}(F)\subseteq\mathbb{P}^2$ si dice il supporto di C.*

Definizione 65. *Una curva algebrica piana proiettiva C di equazione F=0 si dice irriducibile se il polinomio F è irriducibile. Quindi una curva irriducibile è una varietà di dimensione uno di $\mathbb{P}^2$.*

Sia C una curva riducibile e $F=F_1^{a1}...F_t^{at}$ una decomposizione in fattori irriducibili del polinomio F che definisce C. Allora $\mathbf{V}(F)=\mathbf{V}(F_1)\cup...\cup\mathbf{V}(F_t)$ è la decomposizione in componenti irriducibili di $\mathbf{V}(F)$.

Definizione 66. *Con le notazioni precedenti, se esiste i tale che $a_i\geq 2$ la curva C_i di equazione $F_i=0$ si dice una componente multipla di molteplicità a_i di C. Se $a_i=1$ per ogni i si dice che C è ridotta.*

5.1 Molteplicità d'intersezione con una retta in un punto

Sia C la curva di $\mathbb{P}^2$ definita da F(X,Y,Z)=0 e sia p un punto di C. Consideriamo una retta R passante per p. Vogliamo definire la molteplicità dell'intersezione tra C e R nel punto p che denoteremo con i(C,R,p). Se q è un punto di R diverso da p possiamo scrivere $R=\{\alpha p+\beta q$ tali che $(\alpha:\beta)\in\mathbb{P}^1\}$. Consideriamo il polinomio $F(\alpha p+\beta q)$. Questo polinomio è omogeneo di grado d=deg(F) nelle

variabili α e β, ammette quindi d radici contate con molteplicità (R non è contenuta in C). Perciò lo possiamo decomporre nel prodotto di forme lineari: $F(\alpha p+\beta q)=L_1^{m1}...L_r^{mr}$, con $m_1+...+m_r=d$ e $L_i(\alpha p+\beta q)=a_i\alpha+b_i\beta$. Allora $C\cap R$ è data dal luogo degli zeri in $\mathbb{P}^1$ del polinomio $F(\alpha p+\beta q)$, ovvero dai punti $(-b_i,a_i)$. Tra questi punti c'è anche (1:0) perchè $p\in C\cap R$, perciò possiamo assumere $(-b_1,a_1)=(1:0)$. Definiamo allora $i(C,R,p)=m_1$.
La definizione non dipende dalla scelta del punto q su R. Infatti sia x un punto di R diverso da p e da q allora possiamo sempre scrivere x=ap+bq. La retta R $\alpha p+\beta x$ può essere riguardata come $\alpha p+\beta x=\alpha p+\beta(ap+bq)=(\alpha+a\beta)p+\beta bq=\lambda p+\mu q$. Dunque $F(\alpha p+\beta x)=F(\lambda p+\mu q)$ e ritroviamo gli stessi punti di $\mathbb{P}^1$ con le stesse molteplicità.

Proposizione 33 (Versione debole del Teorema di Bezout)**.** *Sia X una curva in $\mathbb{P}^2$ di grado d e sia R una retta di $\mathbb{P}^2$ non contenuta in X. Allora X e R si intersecano in d punti contati con molteplicità. Ovvero $\sum_p i(X,R,p)=d$.*

Dimostrazione: Con le notazioni precedenti essendo K algebricamente chiuso il polinomio $F(\alpha p+\beta q)$ ha esattamente d radici in $\mathbb{P}^1$ contate con molteplicità.

□

Osservazione 14. *Possiamo reinterpretare geometricamente il grado di una curva come il numero di punti contati con molteplicità nei quali una retta interseca la curva.*

5.2 Spazio tangente di Zariski

Sia $p\in C\subseteq\mathbb{P}^2$ e sia R una retta per p.

Definizione 67. *La retta R è tangente a C in p se $i(C,R,p)\geq 2$. Lo spazio tangente di Zariski immerso in $\mathbb{P}^2$ a C nel punto p è $T_pC=\{q\in\mathbb{P}^2$ tali che la retta R per p e q è tangente a C$\}$=Unione delle rette tangenti in p a C.*

Consideriamo ora il caso generale di un sottoinsieme algebrico X di $\mathbb{P}^n$ poi torneremo a $\mathbb{P}^2$. Associare lo spazio tangente di Zariski a X in p è un problema locale quindi possiamo tramite una carte affine metterci in uno spazio affine $\mathbb{A}^n$ che contenga p determinare lo spazio tangente e tornare a $\mathbb{P}^n$.

Definizione 68. *Sia Y un sottoinsieme algebrico di $\mathbb{A}^n$ e sia $a\in Y$. Lo spazio tangente di Zariski a Y in a è T_aY=Unione delle rette tangenti a Y in a (Daremo la definizione rigorosa di retta tangente ad una varietà algebrica nel capitolo 8).*

A meno di una traslazione possiamo supporre che il punto a sia l'origine. Vogliamo decrivere T_OY.
Sia $Q\in K[X_0,..,X_n]$ scriviamo Q come somma di polinomi omogenei $Q=Q_r+...+a_0$ dove Q_i è omogeneo di grado i. La parte lineare è : $Q_1=\sum_{i=1}^n(\partial Q(O)/\partial x_i)X_i$. Se $Q\in\mathbb{I}(Y)$ si ha $a_0=0$.
Sia ora $R=\{tq$ tali che $t\in K\}$ una retta passante per l'origine e per il punto $q\neq O$. Se $Q\in\mathbb{I}(Y)$ si ha $Q(tq)=Q_r(tq)+...+Q_1(tq)$. Poichè Q_i è omogeneo di grado i, $Q_i(tq)=t^iQ(q)$. Possiamo perciò scrivere $Q(tq)=tQ_1(q)+t^2(F(tq))$, per $t=0$ troviamo proprio il punto O. Vediamo che $t=0$ è radice di $Q(tq)=0$ di molteplicità

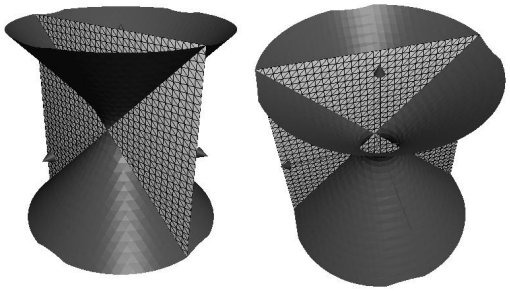

Figura 5.1: Spazio Tangente a una quadrica liscia di $\mathbb{A}^3$

almeno due se e solo se $Q_1(q)=\sum_{i=1}^{n}(\partial Q(O)/\partial x_i)X_i=0$.
Sia ora $\mathbb{I}(Y)=(P_1,...,P_m)$. Consideriamo l'applicazione: $\varphi:\mathbb{A}^n:\rightarrow K^m$ che manda $a\rightarrow(P_1(a),...,P_m(a))$. La matrice Jacobiana di φ è:

$$J(\varphi)(a) = \begin{pmatrix} \partial P_1(a)/\partial x_1 & \dots & \partial P_1(a)/\partial x_n \\ \vdots & & \vdots \\ \partial P_m(a)/\partial x_1 & \dots & \partial P_m(a)/\partial x_n \end{pmatrix}$$

Allora possiamo riguardare $T_O Y$ come al sottospazio vettoriale $\mathrm{Ker}(J(\varphi)(O))$ di $\mathbb{A}^n$.
Consideriamo il caso generale ovvero $a\neq O$. Possiamo ricondurci al caso precedente tramite l'affinità che manda $a\rightarrow X-a$. Abbiamo così $Q(X-a)=Q(a)+Q_1(X-a)+...+Q_r(X-a)$ (Sviluppo di Taylor). Per $X=(1-t)a+tq$, si ha $Q(t(q-a))=tQ_1(q-a)+t^2G(q-a)$, infatti $Q(a)=0$ se $Q\in\mathbb{I}(Y)$. Quindi $t=0$ è radice di molteplicità almeno due se e solo se $Q_1(q-a)=\sum_{i=1}^{n}(\partial Q(a)/\partial x_i)q_i-a_i=0$.
Allora $T_a Y$ è l'insieme delle soluzioni del sistema lineare nelle incognite q_i: $\sum_{i=1}^{n}(\partial P_j(a)/\partial x_i)q_i-a_i=0$ con $1\leq j\leq m$. L'insime delle soluzioni è un sottospazio affine di $\mathbb{A}^n$. Ovviamente a è soluzione del sistema, perciò $T_a Y$ è il sottospazio affine a+V, dove V è il sottospazio vettoriale $V=\mathrm{Ker}(J(\varphi)(a))$. Per quanto detto vale la seguente:

Proposizione 34. *Sia Y un sottoinsieme algebrico di $\mathbb{A}^n$, $a\in Y$, e $\mathbb{I}(Y)=(P_1,...,P_m)$. Lo spazio tangente immerso di Zariski è il sottospazio affine di $\mathbb{A}^n$ dato da $T_a Y=a+Ker(J(P_1,...,P_m)(a))$. Inoltre $dim(T_a Y)=n-r$, dove $r=rango(J(P_1,...,P_m)(a))$. Lo spazio vettoriale $V=Ker(J(P_1,...,P_m)(a))$ di dice spazio vettoriale tangente di Zariski in a a Y e si denota con TY_a.*

Torniamo ora al caso particolare delle curve algebriche di $\mathbb{P}^2$.

Proposizione 35. *1. Se C è un curva algebrica affine di $\mathbb{A}^2$ allora $T_p C$ è il sottospazio affine passante per p di direzione*

$$V=\{(x,y) \text{ tali che } (\partial f(p)/\partial x,\partial f(p)/\partial y)\ \begin{pmatrix} x \\ y \end{pmatrix}=0\}$$

Abbiamo a questo punto due possibilità:
a) *$(\partial f(p)/\partial x,\partial f(p)/\partial y)\neq(0,0)$ e $T_p C$ è la retta di equazione $(x-x_p)\partial f(p)/\partial x+(y-y_p)\partial f(p)/\partial y=0$. In tal caso p si dice un punto liscio della curva C.*
b) *$(\partial f(p)/\partial x,\partial f(p)/\partial y)=(0,0)$ e allora $T_p C=\mathbb{A}^2$. In questo caso p si dice un punto singolare di C.*

2. *Sia C una curva riducibile di equazione f=gh. Siano A e B le curve di equazioni g=0 e h=0. Se p∈A∩B allora p è un punto singolare per C.*

3. *Sia C una curva non ridotta di equazione f^k=0 allora ogni punto di C è singolare.*

Dimostrazione: 1)Sappiamo che V=Ker(Jφ(p)), se C=$\mathbf{V}$(f) con f=f(x,y) si ha V={∂f(p)/∂x,∂f(p)/∂y) $\begin{pmatrix} x \\ y \end{pmatrix}$=0}.
2) Sappiamo che g(p)=h(p)=0, ora $f_x=g_xh+gh_x$ $f_y=g_yh+gh_x$. Perciò (f_x(p),f_y(p))=(0,0) ovvero p è un punto singolare per C.
3)Sia p un punto di C allora f^k(p)=0 poichè K è un campo si ha f(p)=0. Ora $(f^k(x,y))_x=kf^{k-1}(x,y)f_x$ e $(f^k(x,y))_y=kf^{k-1}(x,y)f_y$. Perciò $((f^k(x,y))_x$(p), $(f^k(x,y))_y$(p))=0 e p è singolare. □

Sia C⊆$\mathbb{P}^2$ una curva algebrica e sia p∈C. Per determinare lo spazio tangente di Zariski a C in p possiamo considerare una carta affine contenente p, calcolare lo spazio tangente nell'affine e poi omogeneizzare l'equazione trovata. Ad esempio se C è la curva di equazione X^2-Y^2+Z^2=0 e p=(1:1:0) consideriamo la carta affine U_x e troviamo la curva affine di equazione f(x,y)=1-y^2+z^2=0 e il punto (1,0). La curva affine ha tangente y-1=0. Omogeneizzando troviamo la retta di $\mathbb{P}^2$ Y-X=0.

5.3 Singolarità delle curve piane

Definizione 69. *Sia C una curva piana affine o proiettiva e sia p un punto del piano. La molteplicità di p per C è $m_p(C)=min\{i(C,L,p)\}$, dove L è una retta per p.*

Osservazione 15. *Se p∉C si pone $m_p(C)=0$. Se p∈C allora $m_p(C)=1$ se e solo se p è un punto liscio per C. Si ha $0\leq m_p(C)\leq deg(C)$.*

Vogliamo ora poter calcolare la molteplicità di una curva in un punto.
Sia C una curva di $\mathbb{A}^2$ di equazione f(x,y)=0 con f(0,0)=0. Calcoliamo m_O(C) dove O=(0,0). Decomponiamo f come somma di polinomi omogenei:
$f(x,y)=f_n(x,y)+f_{n-1}(x,y)+...+f_1(x,y)$, dove $f_i(x,y)$ è omogeneo di grado i. Vale il seguente:

Lemma 13. *Si ha $m_O(C)=m\Leftrightarrow f_1=...=f_{m-1}=0$ e $f_m\neq 0$.*

Dimostrazione: Sia Q un punto del piano diverso dall'origine e sia L la retta per O e Q. Allora L={(tq,tq') con t∈K}. Abbiamo $f(tq,tq')=t^nf_n(q,q')+....+t^if_i(q,q')+...+tf_1(q,q')$. Per come abbiamo definito la molteplicità si ha che m_O(C)=m se:

1. t=0 è radice di molteplicità maggiore o uguale ad m di f(tQ)=0;

2. esiste almeno un Q tale che t=0 è radice di molteplicità m di f(tQ)=0.

La prima condizione è equivalente a $f_1(Q)=...=f_{m-1}(Q)=0$ per ogni Q, essendo K infinito perchè algebricamente chiuso questo implica $f_1=...=f_{m-1}=0$. La seconda condizione equivale a dire che esiste un Q_0 tale che $f_m(Q_0)\neq 0$ ovvero $f_m\neq 0$. □

Osservazione 16. *Se p è un punto diverso dall'origine possiamo sempre ricondurci al caso precedente con un'affinità.*

Definizione 70. *Sia C una curva piana e p∈C. Una retta L per p si dice una tangente principale a C in p se i(C,L,p)>$m_p(C)$. Se p è un punto liscio esiste un'unica tangente principale (la retta tangente). L'insieme delle tangenti principali a C in p si dice cono tangente a C in p.*

Lemma 14. *Esistono al più $m_p(C)$ tangenti principali a C in p.*

Dimostrazione: A meno di considerare una carta affine e un'affinità possiamo assumere la curva C affine e p=O. Sia m=m_O(C) e f(x,y)=f_n(x,y)+...+f_m(x,y) l'equazione di C. Abbiamo che i(C,L,O)>m⇔f_m(Q)=0, dove L è la retta per O e Q. Se ora Q' è un altro punto di L si ha Q'=kQ con k∈K e f_m(Q')=$k^m f_m$(Q). Quindi le rette L, per O e tali che i(C,L,O)>m corrispondono agli zeri in $\mathbb{P}^1$ di f_m, $\mathbf{V}(f_m)\subseteq\mathbb{P}^1$. Essendo f_m un polinomio omogeneo di grado m nelle due variabili x e y avrà in $\mathbb{P}^1$ m radici contante con molteplicità, possiamo perciò fattorizzarlo come prodotto di termini lineari: $f_m=l_1^{m1}...l_r^{mr}$ con $m_1+...+m_r$=m, e dove l_i(x,y)=a_ix+b_iy. Le tangenti principali sono proprio le rette di equazione: l_i(x,y)=0 e sono al più m distinte. □

Osservazione 17. *Grazie al lemma precedente possiamo studiare localmente la molteplicità della curva affine C di equazione $f(x,y)=f_n(x,y)+...+f_1(x,y)$ con f_i omogeneo di grado i nell'origine. Infatti se $f_1\neq 0$ l'origine è un punto liscio e la tangente principale è la retta di equazione $f_1(x,y)=0$. Se $f_1=0$ allora O è un punto singolare; se f_m è la componente omogenea non nulla di grado più basso allora $m_O C=m$ e le tangenti principali sono le rette di equazione $l_i(x,y)=0$ dove $f_m(x,y)=l_1^{m1}...l_r^{mr}$ con $m_1+...+m_r=m$.*

Facciamo alcuni esempi:

1. Consideriamo la curva di equazione y^2-x^2-x^3=0. L'origine è un punto singolare in particolare è un punto doppio infatti manca il termine lineare e c'è il termine quadratico. Abbiamo f_2(x,y)=y^2-x^2=(y-x)(y+x). Le tangenti principali sono le rette y=x e y=-x.

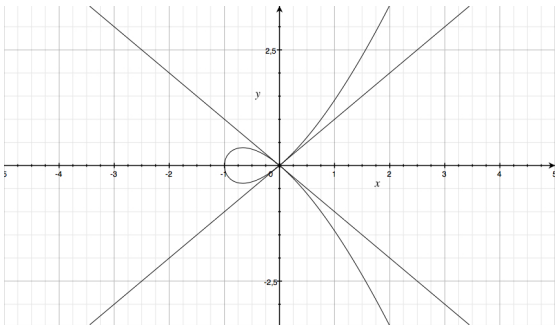

Figura 5.2: Esempio di curva in $\mathbb{A}^2$ - I

2. La curva di equazione y^2-x^3=0 ha un punto doppio nell'origine. Le tangenti principali sono date da y^2=0. Abbiamo perciò un'unica tangente principale, la retta y=0. Infine si ha i(C,L,O)=3.

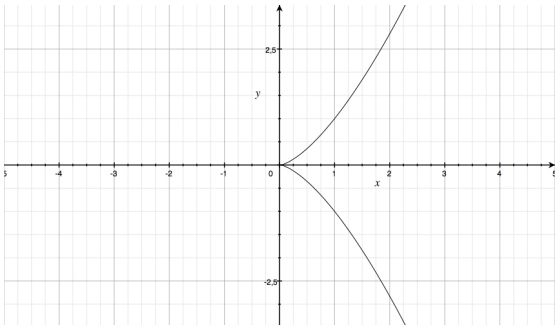

Figura 5.3: Esempio di curva in $\mathbb{A}^2$ - II

3. La curva di equazione x^2-x^4-y^4=0 ha nell'origine un punto doppio. La tangente principale è unica ed è la retta y=0 e i(C,T,O)=4.

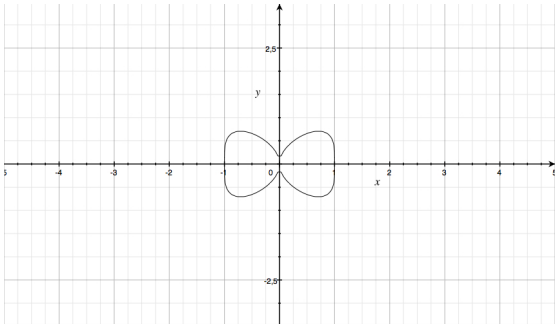

Figura 5.4: Esempio di curva in $\mathbb{A}^2$ - III

5.4 Cubiche di $\mathbb{P}^2$

Definizione 71. *Una cubica in $\mathbb{P}^2$ è una curva algebrica C definita da un polinomio omogeneo P di grado tre. Ovvero C=**V**(P) dove P è omogeneo e deg(P)=3.*

Lemma 15. *Sia C una cubica irriducibile di $\mathbb{P}^2$, C ha al più un punto singolare.*

Dimostrazione: Siano p e q due punti singolari per C con p≠q. Allora la retta R per p e q interseca C in almeno quattro punti contati con moltplicità. Questo è assurdo perchè contraddice la versione debole del teorema di Bezout.

□

Definizione 72. *Un punto liscio p di una curva piana C si dice un flesso se $i(C,T_p,p)\geq 3$, dove T_p è la tangente in p a C.*

Osservazione 18. *Se C è una cubica e p un suo punto di flesso si ha $i(C,T_p,p)=3$.*

Il nostro prossimo obiettivo è classificare le cubiche piane lisce, per fare questo troviamo prima una forma canonica per una generica cubica di $\mathbb{P}^2$.

Teorema 10. *Sia K un campo algebricamente chiuso, con ch(K)≠2. Sia C una cubica di $\mathbb{P}^2$. Supponiamo che C ammetta un flesso. Allora C è proiettivamente equivalente ad una cubica di equazione $Y^2Z-F(X,Z)=0$, dove F è un polinomio omogeneo di grado tre.*

Dimostrazione: Per ipotesi C ammette un flesso p, possiamo con una proiettività mandare p in (0:1:0) e T_pC nella retta Z=0. L'equazione di C è del tipo $a_0X^3+a_1X^2Y+a_2X^2Z+a_3XY^2+a_4XYZ+a_5XZ^2+a_6Y^3+a_7Y^2Z+a_8YZ^2+a_9Z^3=0$, raccogliendo le potenze di X si ha $a_0X^3+X^2(a_1Y+a_2Z)+X(a_3Y^2+a_4YZ+a_5Z^2)$ $+a_6Y^3+a_7Y^2Z+a_8YZ^2+a_9Z^3=0$. Nella carta affine U_y l'equazione di C è data da $f(x,z)=a_0x^3+x^2(a_1+a_2z)+x(a_3+a_4z+a_5z^2)+a_6Y+a_7z+a_8z^2+a_9z^3=a_6+(a_7z+a_3x)$ $+(a_1x^2+a_4xz+a_8z^2)+(a_0x^3+a_2x^2z+a_5xz^2+a_9z^3)$. Poichè p∈C si ha che f(0,0)=0 quindi $a_6=0$. Inoltre essendo $T_p(C)=\{Z=0\}$, la tangente nell'origine di $\mathbb{A}^2$ ha equazione z=0, quindi $a_3=0$ e $a_7\neq0$ essendo p non singolare per C. Infine essendo p un flesso deve essere $i(C,T_p(C),p)\geq3$, quindi $a_1=0$. L'equazione diventa così $f(x,z)=a_7z+a_4xz+a_8z^2+A(x,z)$. Ora poichè $a_7\neq0$ possiamo dividere per a_7, otteniamo così $f(x,z)=z+axz+bz^2+B(x,z)$. Omogeneizzando rispetto a Y otteniamo: $Y^2Z+aXYZ+bYZ^2+B(X,Z)=Z(Y^2+aXY+bYZ)+B(X,Z)$. Poichè ch(K)≠2 possiamo ridurre la forma quadratica $Y^2+aXY+bYZ$ con il metodo di Gauss:
$Y^2+aXY+bYZ=Y(Y+aX+bZ)=(Y+(a/2)X+(b/2)Z)^2-((a/2)X+(b/2)Z)^2$ e posto Y'=Y+(a/2)X+(b/2)Z si ha:

$$F(X,Y',Z)=ZY'^2-Z((a/2)X+(b/2)Z)^2+B(X,Z)$$

ovvero: $F(X,Y',Z)=Y'^2Z+A(X,Z)$ con A(X,Z) omogeneo di grado tre. □

Per procedere abbiamo bisogno di definire la **conica osculatrice ad una curva piana in un punto liscio**.
Supponiamo ch(K)=0. Sia C una curva di grado d>1, di equazione F(X,Y,Z)=0, sia p∈C un punto liscio e sia T la tangente a C in p. Il punto p è un flesso se e solo se i(C,T,P)>2. Sia q∈T, q≠p, si ha: $F(p+aq)=F(p)+DF(P)(aq)+(1/2)D^2F(p)(aq)^2+...$ Poichè p∈C e q∈T l'espressione si riduce a:
$F(p+aq)=a^2\sum_{i,j}F_{i,j}(p)q_iq_j+a^3+....$ Dove $F_{i,j}$ indica la derivata parziale seconda di F rispetto a X_i e X_j. Vale quindi il seguente:

Lemma 16. *Con le natazioni precedenti p è un punto di flesso se e solo se $i(C,T,p)>2$, cioè se e solo se $\sum_{i,j}F_{i,j}(p)q_iq_j=0$ per ogni $q\in T$.*

Definizione 73. *La conica Γ_p di equazione $\sum_{i,j}F_{i,j}(p)q_iq_j=0$ si dice conica osculatrice a C in p.*

Osservazione 19. *Possiamo riformulare il lemma precedente nel seguente modo. Il punto p∈C è un flesso se e solo se la tangente T è una componente della conica osculatrice Γ_p.*

Lemma 17 (Relazione di Eulero)**.** *Sia $F(X_0,...,X_n)$ un polinomio omogeneo di grado d. Allora $dF(X_0,...,X_n)=\sum_{i=1}^n X_i\partial F/\partial X_i$.*

Dimostrazione: Essendo F omogeneo di grado d si ha $F(hX_0,...,hX_n)=h^dF(X_0,...,X_n)$. Derivando rispetto ad h si ottiene $\sum_{i=0}^n X_i(\partial F/\partial X_i)(hX_0,...,hX_n)=dh^{d-1}F(X_0,...,X_n)$. Per h=1 si ottiene la tesi. □

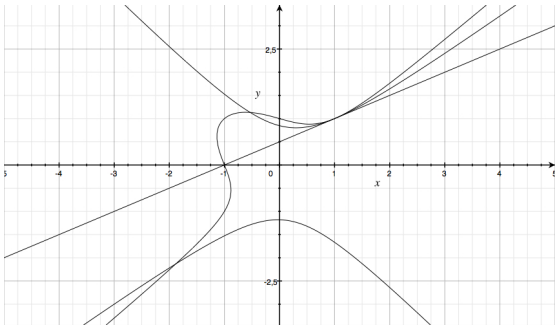

Figura 5.5: Cubica, conica osculatrice e retta tangente

Proposizione 36. *Con le notazioni precedenti:*

1. *$p \in \Gamma_p$ è un punto liscio di Γ_p;*
2. *la tangente a Γ_p in p è T;*
3. *p è un flesso di C se e solo se Γ_p è degenere.*

Dimostrazione: 1) Si ha $\sum_{ij} F_{ij}(p)p_j r_i = (\sum_j F_{0j}(p)p_j)r_0 + (\sum_j F_{1j}(p)p_j)r_1 + (\sum_j F_{2j}(p)p_j)r_2$. Dalla relazione di Eulero $\sum_{ij} F_{ij}(p)p_j r_i = (d\text{-}1)(F_0(p)r_0 + F_1(p)r_1 + F_2(p)r_2)$. In particolare $\sum_{ij} F_{ij}(p)p_j r_i = 0$ se e solo se $(r_0:r_1:r_2) \in T$. Dall'ultima relazione si ha che $p \in \Gamma_p$. Ora p è un punto singolare della conica Γ_p se e solo se la retta vettoriale $<p>$ di K^3 è nell'ortogonale della forma bilineare simmetrica associata alla matrice $M=(F_{ij}(p))$, ovvero se e solo se $\sum_{ij} F_{ij}(p)p_j r_i = 0$ per ogni $(r_0:r_1:r_2)$. Ma dalla relazione mostrata prima si ha che questo è verificato se e solo se $(r_0:r_1:r_2) \in T$.
2) Consideriamo la conica di equazione $\sum_{ij} a_{ij}X_iX_j = a_{11}X_1^2 + 2a_{12}X_1X_2 + a_{22}X_2^2 = 0$ e sia p un suo punto liscio. La retta tangente in p alla conica ha direzione $(a_{11}p_1 + a_{12}p_2, a_{12}p_1 + a_{22}p_2)$, la sua equazione è allora $(a_{11}p_1 + a_{12}p_2)X_1 + (a_{12}p_1 + a_{22}p_2)X_2 = \sum_{ij} a_{ij}p_iX_j = 0$.
3) Se p è un punto di flesso di C allora sappiamo che T è una componente di Γ_p e quindi Γ_p è degenere. Viceversa se Γ_p è degenere da 1) segue che Γ_p è unione di due rette $R \cup D$ distinte e che $p \in R - (R \cap D)$ essendo p un punto liscio di Γ_p. Da 2) segue che $T = R$ è quindi p è un flesso di C. □

Introduciamo ora la **curva Hessiana** associata ad una una curva di $\mathbb{P}^2$.
Sia H(F) la matrice simmetrica, tre per tre, dei coefficienti delle derivate parziali seconde di F: $H(F) = (F_{i,j}(x))$. Il determinante di H(F) è un polinomio omogeneo di grado 3(d-2).

Definizione 74. *La curva $H(F) \subseteq \mathbb{P}^2$ di equazione $\det(H(F)) = 0$, si dice la curva Hessiana associata a C.*

Proposizione 37. *Sia $C \subseteq \mathbb{P}^2$ una curva. I flessi di C sono esattemente i punti lisci di C che appartengono a $C \cap H(C)$.*

Dimostrazione: Sia $p \in C$ un punto non singolare, p è un flesso se e solo se Γ_p è degenere, ma Γ_p è degenere se e solo se $|F_{i,j}(p)| = 0$ cioè $p \in H(C)$. □

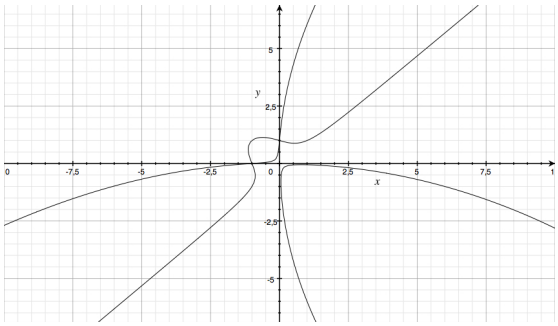

Figura 5.6: Cubica e curva Hessiana associata

Lemma 18. *Ogni curva $C \subseteq \mathbb{P}^2$ di grado $d \geq 3$ ammette almeno un flesso.*

Dimostrazione: Se C ed H(C) hanno una componente in comune questa è C. Se C e H(C) non hanno componenti comuni per il teorema di Bezout si intersecano in 3d(d-2) punti contati con molteplicità. □

Teorema 11. *Sia K un campo algebricamente chiuso, con ch(K)≠2,3. Sia C una cubica non singolare di $\mathbb{P}^2$.*

1. *C è proiettivamente equivalente ad una curva di equazione $Y^2Z=X(X-Z)(Z-aZ)$, con $a \neq 0,1$* (forma di Legendre).
2. *C è proiettivamente equivalente ad una curva di equazione $Y^2Z=X^3+aXZ^2+bZ^3$, con $4a^3+27b^2 \neq 0$* (forma di Weierstrass).

Dimostrazione: La cubica C ammette almeno un flesso essendo non singolare. Dal teorema precedente C è proiettivamente equivalente a una curva di equazione $Y^2Z-F(X,Z)=0$, con F(X,Z) polinomio omogeneo di grado tre. Nella carta affine U_Z, C ha equazione $y^2-F(x,1)=y^2-(ax^3+bx^2+cx+d)=0$. Deve essere $a \neq 0$, se infatti fosse a=0 ovremmo che Z divide $Y^2Z-F(X,Z)=0$ e C sarebbe riducibile e quindi singolare. Il polinomio f(x)=F(x,1) ha tutte le sue radici in K e queste sono distinte. Infatti se ξ è radice multipla di f allora $(x-\xi)^2$ divide f(x), duque $f(x)=q(x)(x-\xi)^2$ e il punto di $\mathbb{A}^2$ di coordinate $(\xi,0)$ è un punto singolare per C ma questo è escluso per ipotesi. Possiamo allora scrivere $f(x)=a(x-r_1)(x-r_2)(x-r_3)$ con $r_i \neq r_j$ se $i \neq j$. Poniamo $x=(r_2-r_1)x'+r_1$ e $y=(a(r_2-r_3)^3))^{1/2}y'$. Mediante questo cambiameto di variabili ottaniamo l'equazione $y'^2=x'(x'-1)(x'-\lambda)$ con $\lambda=(r_3-r_1)/(r_2-r_1)$. Omogeneizzando rispetto a Z si ottiene $Y'^2Z'=X'(X'-Z')(X'-\lambda Z')$. Inoltre $\lambda \neq 0$ perchè $r_3 \neq r_1$ e $\lambda \neq 1$ perchè $r_3 \neq r_2$. Abbiamo così ottenuto la forma di Legendre.
Come prima consideriamo l'equazione $y^2=(ax^3+bx^2+cx+d)$, sappiamo che $a \neq 0$. Dividendo per a otteniamo $y'^2=(y/\sqrt{a})^2=(ax^3+bx^2+cx+d)$. Vogliamo ora completare il cubo al fine di far sparire il termine in x^2. Avendo supposto $ch(K) \neq 3$ possiamo porre $x=(x'-b)/3$, otteniamo così $y'^2=(x'-b)^3/27+b(x'-b)^2/9+c(x'-b)/3+d$ ovvero $27y'^2=x'^3-b^3-3x'^2b+3x'b^2+3bx'^2+3b^3-6x'b^2+9cx'-9cb+27d=x'^3-3x'^2b+3x'b^2-b^3+3b(x'^2+b^2-2bx')+9c(x'-b)+27d=x'^3-b^3+3x'b^2+3b^3-6x'b^2+9cx'-9cb+27d$. Otteniamo un'espressione del tipo $y'^2=x'^3/27+x'A'/3+B$. Posto $\xi=x'/3$ si ha $y'^2=\xi^3+A\xi+B$ e omogeneizzando rispetto a Z otteniamo $Y^2Z=X^3+AXZ^2+BZ^3$

ovvero la forma di Weierstrass. Come nel caso precedente il polinomio g(x)=x^3+Ax+B ha tre radici distinte altrimenti C sarebbe singolare. Questo è equivalente a richiedere che il discriminante di g ovvero il risultente tra g e g' sia non nullo, D(g)=R(g,g')≠0. Ma D(g)=-4A^3-27B^2 e allora -4A^3-27B^2≠0. □

Introduciamo ora, al fine di dare la definizione di curva ellittica, un'invariante delle curve algebriche irriducibili e lisce di $\mathbb{P}^2$ detto genere

$$g=\frac{(n-1)(n-2)}{2}$$

dove n è il grado della curva. Per concludere il capitolo diamo una definizione molto importante e strettamente legata al concetto di cubica liscia.

Definizione 75. *Sia K un campo. Una* ***curva ellittica*** *definita su K è una curva algebrica di $\mathbb{P}^2$ irriducibile e liscia di genere g=1.*

La traccia reale di una cubica liscia si presenta a meno di proiettività in una delle due forme riportate nelle figure seguenti.

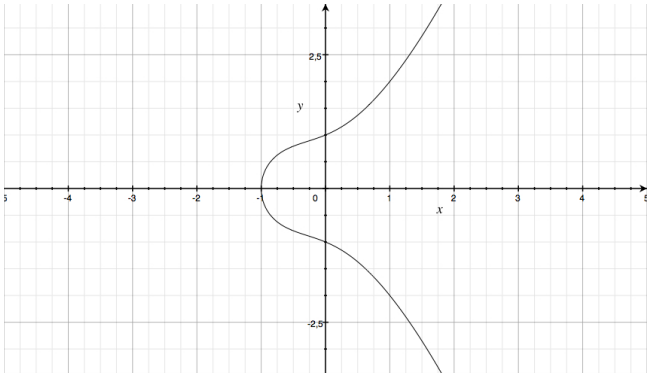

Figura 5.7: Traccia reale di una cubica liscia I

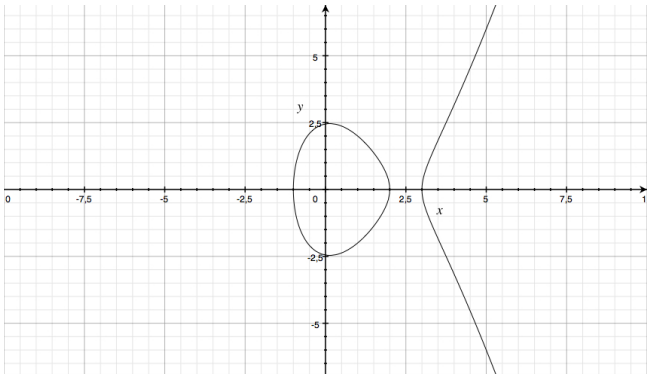

Figura 5.8: Traccia reale di una cubica liscia II

Capitolo 6

Teorema di Bezout e sistemi di curve piane

«La geometria è l'arte di ragionare bene sopra figure disegnate male.»

Jules Henri Poincaré (1854-1912).

In questo capitolo introdurremo il risultante di due polinomi. Enunceremo poi il teorema di Bezout. Infine dimostreremo alcuni risultati riguardo i sistemi di curve piane, con particolare attenzione al paradosso di Cramer che sarà fondamentale per dimostrare l'associatività della legge di composizione sulle curve ellittiche.

6.1 Risultante di due polinomi

Sia A un U.F.D. e siano f,g∈A[X] due polinomi. Vogliamo stabilire se f e g hanno componenti irriducibili comuni senza fattorizzarli.

Lemma 19. *I polinomi f e g, di grado m e n rispettivamente, hanno un fattore irriducibile comune se e solo se esistono due polinomi F e G con deg(F)<m e deg(G)<n tali che fG=gF.*

Dimostrazione: Supponiamo che h sia il fattore irriducibile comune ad f e g. Possiamo scrivere f=hF con deg(F)<m e g=hG con deg(G)<n. Allora fG=hFG=hGF=gF. Viceversa supponiamo che fG=gF con deg(F)<m e deg(G)<n. Allora f divide gF, ora deg(F)<deg(f) implica che esiste in f un fattore irriducibile h tale che h divide g. Vediamo che h è proprio il fattore irriducibile cercato. □

Lemma 20. *Due polinomi F e G hanno un fattore comune se e solo se esiste un polinomio H, di grado minore o uguale a deg(F)+deg(G)-1, divisibile per F e per G.*

Dimostrazione: Supponiamo che sia H=FF'=GG' e che per assurdo F e G non abbiano radici comuni. Allora tutte le radici di F in K sono radici di G',

ma questo è assurdo perchè deg(G')=deg(F)-1. Viceversa se F=RF' e G=RG' allora H=RF'G' è un polinomio di grado minore o uguale a deg(F)+deg(G)-1 divisibile per F e per G. □

Sia ora V_F={P∈K[X] tali che F divide P e deg(P)≤deg(F)+deg(G)-1} il K-spazio vettoriale dei polinomi di grado minore o uguale a deg(F)+deg(G)-1 divisibili per F. In altre parole V_F è l'insieme dei multipli di F di grado minore o uguale a deg(F)+deg(G)-1. Una base di V_F è {F,XF,...,$X^{deg(g)-1}$F}. Analogamente una base di V_G è {G,XG,...,$X^{deg(F)-1}$G}. Dire che F e G hanno un multiplo di grado minore o uguale a deg(F)+deg(G)-1 equaivale a dire che V_F e V_G non sono in somma diretta ovvero che i vettori F,XF,...,$X^{deg(g)-1}$F, G,XG,...,$X^{deg(F)-1}$G sono linearmente dipendenti.
Scriviamo ora F(X)=f_0+f_1X+...+$f_f X^f$ e G(X)=g_0+g_1X+...+$g_g X^g$, dove abbiamo posto deg(F)=f e deg(G)=g. Ora (1,X,X^2,...,X^{f+g-1}) è una base dello spazio vettoriale dei polinomi di K[X] di grado minore o uguale a f+g-1, V_F e V_G sono suoi sottospazi, ha senso perciò riscirvere i vettori F,XF,...,$X^{deg(g)-1}$F, G,XG,...,$X^{deg(F)-1}$G nella base {1,X,X^2,...,X^{f+g-1}}. Abbiamo:
F=(f_0,...,f_f,0,...0);
XF=(0,f_0,.....,f_f,0,..0);
⋮
X^{g-1}F=(0,0,...0,f_0,....,f_f);
G=(g_0,...,g_g,0,...0);
XG=(0,g_0,.....,g_g,0,..0);
⋮
X^{f-1}G=(0,0,...0,g_0,....,g_g);
Dire che questi vettori sono dipendenti e equivalnete a imporre che il determinanate della matrice (deg(F)+def(G))×(deg(F)+deg(G)) che ha per righe i vettori stessi sia nullo. La matrice in questione è la seguente:

$$\mathbb{M}=\begin{pmatrix} f_0 & \dots & f_f & 0 & 0 & \dots & 0 \\ 0 & f_0 & \dots & f_f & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & f_0 & \dots & \dots & f_f \\ g_0 & \dots & g_g & 0 & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_g & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & g_0 & \dots & \dots & g_g \end{pmatrix}$$

Definizione 76. *Il determinanate della matrice* $\mathbb{M}$ *si dice risultante dei polinomi F e G e si indica con R(F,G)=det(*$\mathbb{M}$*).*

Vediamo che due polinomi F e G hanno un fattore in comune ovvero una radice comune se e solo se R(F,G)=0. Possiamo ora stabilire quando un polinomio P ha radici multiple.
Sia P(X)=a_0+a_1X+...+$a_p X^p$ un polinomio di grado p. La sua derivata formale è il polinomio di grado p-1: P'(X)=a_1+...+p$a_p X^{p-1}$. Sappiamo che X_0 è radice doppia di P se è radice di P'. Dunque P ha almeno una radice multipla se e solo se R(P,P')=0.

Definizione 77. *Il risultante tra P e P', R(P,P'), si dice discriminante del polinomio P e si denota con D(P). Per quanto visto P ha almeno una radice multipla se e solo se D(P)=0.*

Riportiamo due esempi:

- Consideriamo il polinomio P(X)=aX^2+bX+c, si ha P'(X)=2aX+b. La matrice $\mathbb{M}$ relativa a P e P' è:

$$\mathbb{M}=\begin{pmatrix} c & b & a \\ b & 2a & 0 \\ 0 & b & 2a \end{pmatrix}$$

  Si ha det($\mathbb{M}$)=-a(b^2-4ac), ora a$\neq$0, e quindi D(P)=b^2-4ac.

- Sarà per noi necessario nello studio delle cubiche conoscere il discriminante di un polinomio di grado tre P(X)=X^3+aX^2+bX+c. Si ha P'(X)=3X^2+2aX+b. In questo caso la matrice da considerare è:

$$\mathbb{M}=\begin{pmatrix} c & b & a & 1 & 0 \\ 0 & c & b & a & 1 \\ b & 2a & 3 & 0 & 0 \\ 0 & b & 2a & 3 & 0 \\ 0 & 0 & b & 2a & 3 \end{pmatrix}$$

  Si ha det($\mathbb{M}$)=D(P)=-4a^{3}c+a^{2}b^2+18abc-4b^3-27c^2.

Lemma 21. *Siano F e G due polinomi omogenei di grado m ed n allora R(F,G) è un polinomio omogeneo di grado mn.*

Dimostrazione: Vogliamo mostrare che R(tF,tG)=t^{mn}R(F,G). Possiamo scrivere F e G come polinomi in K[X,Z][Y] nel seguente modo: F=f$_0$Y^m+f$_1$Y^{m-1}+...+f$_m$ e G=g$_0$Y^n+g$_1$Y^{n-1}+...+g$_n$, dove f$_i$,g$_i$∈K[X,Z] hanno grado i, in modo che F e G risultino essere proprio omogenei di grado m e n. Sappiamo che:

$$\mathrm{R(F,G)=det}(\mathbb{M})=\begin{pmatrix} f_0 & \dots & f_m & 0 & 0 & \dots & 0 \\ 0 & f_0 & \dots & f_m & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & f_0 & \dots & \dots & f_m \\ g_0 & \dots & g_n & 0 & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_n & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & g_0 & \dots & \dots & g_n \end{pmatrix}$$

Cosideriamo ora la matrice del risultante tra F(tX,tY,tZ) e G(tX,tY,tZ):

$$\mathrm{R(F}_t\mathrm{,G}_t\mathrm{)=det}(\mathbb{M}_t)=\begin{pmatrix} f_0 & \dots & t^m\mathrm{f}_m & 0 & 0 & \dots & 0 \\ 0 & f_0 & \dots & t^m\mathrm{f}_m & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & f_0 & \dots & \dots & t^m\mathrm{f}_m \\ g_0 & \dots & t^n\mathrm{g}_n & 0 & 0 & \dots & 0 \\ 0 & g_0 & \dots & t^n\mathrm{g}_n & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & g_0 & \dots & \dots & t^n\mathrm{g}_n \end{pmatrix}$$

Se ora moltplichiamo la i-esiama riga di ciascun blocco di questa matrice per t^i

otteniamo una nuova matrice che avrà determinante pari a q·det($(M)^t$). Dove q=(1+2+...+m)+(1+2+...+n)=(m(m+1)/2)+(n(n+1))/2.

$$\mathrm{t}^q\mathrm{R}(\mathrm{F}_t,\mathrm{G}_t)=\det\begin{pmatrix} tf_0 & \dots & t^{m+1}\mathrm{f}_m & 0 & 0 & \dots & 0 \\ 0 & t^2\mathrm{f}_0 & \dots & t^{m+2}\mathrm{f}_m & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & t^n\mathrm{f}_0 & \dots & \dots & t^{m+n}\mathrm{f}_m \\ tg_0 & \dots & t^{n+1}\mathrm{g}_n & 0 & 0 & \dots & 0 \\ 0 & t^2\mathrm{g}_0 & \dots & t^{n+2}\mathrm{g}_n & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & t^m\mathrm{g}_0 & \dots & \dots & t^{n+m}\mathrm{g}_n \end{pmatrix}$$

Riguardiamo ora la matrice per colonne. Notiamo che sulle colonne compaiono le potenze crescenti di t da 1 a m+n. Applichiamo la stessa proprietà del determinante per colonne. Abbiamo che $\mathrm{t}^p\mathrm{R}(\mathrm{F},\mathrm{G})=\mathrm{t}^q\mathrm{R}(\mathrm{F}_t,\mathrm{G}_t)$, dove p=1+2+...+(m+n)=(m+n)(m+n+1)/2. Otteniamo così che $\mathrm{R}(\mathrm{F}_t,\mathrm{G}_t)=\mathrm{t}^{p-q}\mathrm{R}(\mathrm{F},\mathrm{G})$. Vediamo che p-q=(m+n)(m+n+1)/2-m^2/2-m/2-n^2/2-n/2=m^2/2+mn+n^2/2+m/2+n/2-m^2/2-m/2-n^2/2-n/2=mn. Dunque:

$$\mathrm{R}(\mathrm{F}_t,\mathrm{G}_t)=\mathrm{t}^{mn}\mathrm{R}(\mathrm{F},\mathrm{G}),\text{ dove }\mathrm{F}_t=\mathrm{F}(\mathrm{tX},\mathrm{tY},\mathrm{tZ})\text{ e }\mathrm{G}_t=\mathrm{G}(\mathrm{tX},\mathrm{tY},\mathrm{tZ}).$$

□

Enunciamo ora il teorema di Bezout per le curve algebriche piane senza darne la dimostrazione[1].

Teorema 12 (Di Bezout)**.** *Siano C e C' due curve di $\mathbb{P}^2$(K), con K algebricamente chiuso, di gradi m ed n, prive di componenti comuni. Allora C e C' si intersecano esattamente in nm punti contati con molteplicità*

6.2 Sistemi di curve piane

Sia S_n=K[X,Y,Z] l'insieme dei polinomi di grado n in X,Y,Z. Sappiamo che S_n è un K-spazio vettoriale di dimensione (n+2)(n+1)/2. Allora $\mathbb{P}(\mathrm{S}_n)$ insieme delle curve piane di grado n è uno spazio proiettivo di dimensione N_n=(n+2)(n+1)/2-1.

Definizione 78. *Un sistema lineare di curve piane di grado n è un sottospazio lineare di $\mathbb{P}(S_n)$. La dimensione proiettiva del sistema lineare è la dimensione del sottospazio lineare di $\mathbb{P}(S_n)$. Un punto p∈$\mathbb{P}^2$ si dice un punto base del sistema lineare se ogni curva del sistema passa per p. Il luogo base del sistema è l'insieme dei punti base ed è un sottoinsieme algebrico. Se il luogo base contiene una curva questa si dice una curva fissa per il sistema.*

Osserviamo che possiamo prendere come base di S_n $\{\mathrm{X}^i\mathrm{Y}^j\mathrm{Z}^k\}$ con i+j+k=n. Ad ogni curva C di equazione $\mathrm{F}(\mathrm{X},\mathrm{Y},\mathrm{Z})=\sum \mathrm{a}_{ijk}\mathrm{X}^i\mathrm{Y}^j\mathrm{Z}^k$ possiamo associare delle coordinate omogenee costruite sui coefficienti di una sua equazione (...,a_{ijk}...). In altre parole ad ogni curva di $\mathbb{P}(\mathrm{S}_n)$ possiamo associare un punto di $\mathbb{P}^{Nn}$.
Sia ora p∈$\mathbb{P}^2$. Si ha p∈C⇔$\sum \mathrm{a}_{ijk}\mathrm{p}_0{}^i\mathrm{p}_1\mathrm{Y}^j\mathrm{p}_2\mathrm{Z}^k$=0. Essendo p fissato l'ultima

[1] Per la dimostrazione del teorema di Bezout si veda ad esempio Makoto Namba - Geometry of projective algebraic curves.

equazione può essere interpretata come l'equazione nelle variabili a_{ijk} di un iperpiano in $\mathbb{P}^{Nn}$. Vediamo così che le curve di grado n passanti per un punto p fissato formano un sistema lineare.
Più in generale se $p_1,...,p_d$ sono d punti di $\mathbb{P}^2$, con $p_i=(a_i:b_i:c_i)$, l'insieme delle curve di grado n che passano per tutti i p_i è dato dall'insieme delle soluzioni del sistema lineare omogeneo:

$$\begin{cases} \sum a_{ijk} {a_1}^i {b_1}^j {c_1}^k &= 0 \\ \vdots & \vdots \ \vdots \\ \sum a_{ijk} {a_d}^i {b_d}^j {c_d}^k &= 0 \end{cases}$$

Ora le curve di grado n che passano per p_i costituisco un iperpiano $H(p_i)$. Le curve di grado n passanti per i punti $p_1,...,p_d$ costituisco il sottospazio lineare $L(p_1,...,p_d)=H(p_1)\cap...\cap H(p_d)$. Inoltre $\dim(L)\geq N^n\text{-}d$.
Ancora più in generale supponiamo che sia assegnato il punto p con molteplicità almeno r. Questo significa che p è uno zero delle derivare parziali fino all'odine r-1, abbiamo $r(r+1)/2$ di tali derivate. Concludiamo allora con la seguente:

Proposizione 38. *Le curve di grado n che passono per i punti p_i con molteplicità almeno r_i, $0\leq i\leq d$, costituiscono un sistema lineare $L({p_1}^{r1},...,{p_d}^{rd})$ di dimensione maggiore o uguale a $N_n\text{-}\sum_{i=1}^{d} r_i(r_i+1)/2$. In particolare se $N_n\text{-}\sum_{i=1}^{d} r_i(r_i+1)/2\geq 0$ esiste almeno una curva di grado n che passa per i punti p_i con molteplicità almeno r_i, $0\leq i\leq d$.*

Osservazione 20. *Consideriamo le cubiche.*

1. *Ad esempio se n=3 abbiamo $N_n=9$. Se assegnamo nove punti, abbiamo che $\dim(L(p_1,...,p_9))\geq 0$, ovvero per nove punti passa sempre una cubica.*
2. *I punti $p_1,...,p_d$ sono punti base del sistema.*

Definizione 79. *Denotiamo con $S(p_1,...,p_d)$ il sistema costruito sui punti base $p_1,...,p_d$. Si dice che i punti $p_1,...,p_d$ impongono condizioni indipendenti se $\dim(S(p_1,...,p_d))=\max\{N_n\text{-}d,\text{-}1\}$, con la convenzione che la dimensione del vuoto è -1.*

Ad esempio se n=1 (consideriamo le rette), tre punti non danno sempre condizioni indipendenti. Infatti se i tre punti sono allineati $\dim(S(p,q,t))=1$ e $\max(N_n\text{-}d,\text{-}1)=\max(2\text{-}3,\text{-}1)=\text{-}1$. Se invece n=2 allora $\max(N_n\text{-}d,\text{-}1)=\max(5\text{-}3,\text{-}1)=2$ e $\dim(S(p,q,t))=2$. Quindi tre punti danno sempre condizioni indipendenti alle curve di grado due.

Lemma 22 (Criterio di separazione)**.** *Siano n e d degli interi, $n\geq 1$ e $d\leq N_n+1=$ $=(n+1)(n+2)/2$. Un insieme di punti $p_1,...,p_d$ impone condizioni indipendenti alle curve di grado n se e solo se: per ogni i, esiste una curva C_i, di grado n, che passa per p_j se $j\neq i$, e che non passa per p_i.*

Dimostrazione: Sia $S=\bigcap S_n(p_i)$. Vogliamo mostrare che $\dim(S)=\max(N_n\text{-}d,\text{-}1)$ se e solo se per ogni i, esiste una curva C_i che passa per p_j se e solo se $j\neq i$. Ovvero che $\dim(S)=\max(N_n\text{-}d,\text{-}1)$ se e solo se per ogni i, esiste un punto C_i di $\mathbb{P}^{Nn}$ che appartiene a $S_n(p_j)$ se e solo se $j\neq i$. Adesso che abbiamo fatto il punto della situazione procediamo. Supponiamo $\dim(S)=\max(N_n\text{-}d,\text{-}1)$ e consideriamo $S'=\bigcap S_n p(_j)$, fatta per $j\neq i$. Ora S' è un sottospazio lineare non vuoto di $\mathbb{P}^{Nn}$,

perchè di dimensione maggiore o uguale a N_n-(d-1). Inoltre S' non è contenuto in $S_n(p_i)$, infatti se così fosse S' sarebbe contenuto in S ma questo è assudo perchè dim(S')>dim(S) essendo per ipotesi dim(S)=max(N_n-d,-1)<N_n-(d-1). Concludiamo che esiste un punto $C_i \in$S', che non appartiene a $S_n(p_i)$. Viceversa sia C_i un punto di $\mathbb{P}^{Nn}$ che appartiene a $S_n(p_j)$ se e solo se j≠i. A meno di riordinare possiamo supporre i=1. Allora dim($S_n(p_1) \cap S_n(p_2)$)=N_n-1+N_n-1-N_n=N_n-2. Analogamente dim($S_n(p_1) \cap S_n(p_2) \cap S_n(p_3)$)=$N_n$-2+$N_n$-1-$N_n$=$N_n$-3. Procediamo per induzione e supponiamo che dim($S_n(p_1) \cap ... \cap S_n(p_{d-1})$)=$N_n$-(d-1). Allora dim($S_n(p_1) \cap ... \cap S_n(p_d)$)=dim($S_n(p_1) \cap ... \cap S_n(p_{d-1})$)+dim($S_n(p_d)$)-dim($\bigcup_{i=1}^{d} S_n(p_i)$)=$N_n$-(d-1)+$N_n$-1-$N_n$=$N_n$-d. Abbiamo così mostrato che i punti impongono condizioni indipendenti. □

Corollario 2. *Sia X={p_1,...,p_d} (d≤N_n+1) un insieme di punti in $\mathbb{P}^2$ che impongono condizioni indipendenti alle curve di grado n. Se X'⊆X allora anche X' impone condizioni indipendenti alle curve di grado n.*

Dimostrazione: Ora X impone condizioni indipendeti perciò per ogni i possiamo trovare una curva di grado n passante per p_j se e solo se j≠i. Ora gli elementi di X' sono alcuni dei p_i per i quali vale il criterio di separazione, perciò anche X' impone condizioni indipendenti alle curve di grado n. □

Il nostro prossimo obiettivo è mostrare che è sempre possibile trovare d punti che impongono condizioni indipendenti alle curve di grado n.

Lemma 23. *Per ogni n≥1 esiste un insieme di N_n+1 punti che non è contenuto in nessuna curva di grado n ovvero impone condizioni indipendenti alle curve di grado n.*

Dimostrazione: Osserviamo che N_n+1=(n+2)(n+1)/2=(n+1)+n+...+2+1. Costruiamo un insieme X di N_n+1 punti p_i e costituito da n+1 sottoinsiemi come segue: il primo sottoinsieme X_1={p_1,...,p_{n+1}} consta di n+1 punti che prendiamo allineati su una retta R_1. Il secondo sottoinsieme X_2={p_{n+2},...,p_{2n+1}} consta di n punti allineati su una retta $R_2 \neq R_1$. L'n-esimo sottoinsieme X_n consta di due punti allineati su una retta $R_n \neq R_i$ per ogni i<n. L'ultimo sottoinsieme X_{n+1} consta di un solo punto che non appartiene a nessuna delle rette R_1,...,R_n. Supponiamo ora per assurdo che esista una curva C di grado n contenente X. Allora $X_1 \subseteq C \cap R_1$, quindi C e R_1 si intersecano in n+1 punti e per la versione debole del teorema di Bezout R_1 è una componente di C. Possiamo scrivere C=R_1∪C', dove C' è una curva di grado n-1. La curva C' interseca R_2 in n punti e come prima R_2 deve essere una componente di C'. Possiamo scrivere C'=R_2∪C", dove C" ha grado n-1. Andando avanti così si ha che C contiene R_1,...,R_n. Poichè C ha proprio grado n deve essere C=R_1∪...∪R_n. Allora C non contiene X_{n+1} e quindi non contiene X, assurdo. □

Proposizione 39. *Per ogni n≥1 e per ogni d≥1 esiste un insieme di d punti che impone condizioni indipendenti alle curve di grado n.*

Dimostrazione: Se d=N_n+1 la proposizione segue dal lemma precedente. Se d<N_n+1 segue dal lemma precedente e dal corollario secondo il quale se X impone condizioni indipendenti ogni X' sottoinsieme di X impone condizioni indipendenti. Se d>N_n+1 prendiamo un insieme X di N_n+1 punti che impongono

condizioni indipendenti (che sappiamo esistere per il lemma) e lo completiamo con d-(N_n+1) punti qualsiasi. □

6.3 La funzione di Hilbert di un insieme di punti

Sia X un insieme di d punti p_i in $\mathbb{P}^2$, consideriamo una carta affine costruita togliendo a $\mathbb{P}^2$ una retta che non interseca X, possiamo allora riguardare X come sottoinsieme di $\mathbb{A}^2$. A meno di un cambiamento di base possiamo supporre che la retta all'infinito sia X_0=0. Sia ora f(x,y)∈K[x,y], possiamo valutare f sui punti p_i=(x_i,y_i) di X. Otteniamo così il vettore (f(p_1),...,f(p_d))∈K^d. La curva di equazione f(x,y)=0 contiene X se e solo se f(p_i)=0 per ogni i. Sia ora F(X_0,X_1,X_2) un polinomio omogeneo di grado n e sia f(x,y)=F(1,x,y) il suo deomogeneizzato rispetto a X_0. Per quanto detto la curva di equazione F(X_0,X_1,X_2)=0 contiene X se e solo se f(p_i)=0 per ogni i. Abbiamo così l'applicazione:

r_X(n):{P∈K[X_0,X_1,X_2] omogenei di grado n}→K^d: F→(f(p_1),...,f(P_d)).

Lemma 24. *L'applicazione r_X(n) è lineare. Inoltre Ker(r_X(n))=$\boldsymbol{I}(X)_n$ e Im(r_X(n))≅$A(X)_n$.*

Dimostrazione: Siano F,G due polinomi omogenei di grado n e siano a,b∈K.
r_X(n)(aF+bG)=((aF+bG)(p_1),...,(aF+bG)(p_d))=a(f(p_1),...,f(p_d))+
+b(g(p_1),...,g(p_d))=ar_X(n)(F)+br_X(n)(G).
Inoltre r_X(n)(F)=0 se e solo se F∈$\mathbf{I}(X)_n$. Infine per definizione $A(X)_n$=$S_n/\mathbf{I}(X)_n$ e per un teorema di isomorfismo tra anelli segue la tesi. □

Definizione 80. *L'applicazione h_X:ℕ→ℕ:n→dim(Im(r_X(n))) si dice funzione di Hilbert dell'insieme di punti X.*

Proposizione 40. *Sia X⊆$\mathbb{P}^2$ un insieme di punti X={p_1,...,p_d}.*

1. *X impone condizioni indipendenti alle curve di grado n se e solo se r_X(n) è di rango massimo.*
2. *L'applicazione r_X(n) è suriettiva⇔per ogni i esiste una curva di grado n C_i, che passa per p_j se j≠i e che non passa per p_i.*
3. *Se r_X(n) è suriettiva allora r_X(m) è suriettiva per ogni m≥n.*
4. *r_X(d-1) è suriettiva, con d=Card(X).*

Dimostrazione:

1. Per come è definita h_X(n) è la codimensione del sistema costruito sui punti base p_1,...,p_d ovvero il numero di condizioni imposte dai punti. Tale numero è massimo se e solo se h_X(n)=dim(Im(r_X(n)) è massima ovvero se e solo se r_X(n) ha rango massimo.
2. La mappa r_X(n) è suriettiva ovvero ha rango massimo se e solo se X impone condizioni indipendenti se e solo se vale il criterio di separazione. Diamo però un'altra dimostrazione di questo fatto. Se r_X(n) è suriettiva

i vettori della base canonica (0,0,..,1,0,..0) (1 all'i-esimo posto) appartengono all'immagine di $r_X(n)$ per ogni i. Quindi per ogni i esiste un polinomio F_i tale che $r_X(n)(F_i)$=(0,0,..,1,..,0), (1 all'i-esimo posto). Allora la curva C_i di equazione F_i=0 passa per p_j se e solo se j≠i. Supponiamo ora che per ogni i esista una curva C_i che passa per p_j se e solo se j≠i. Allora i vettori del tipo (0,0..,v_i,..0) con v_i≠0, appartengono a $\mathrm{Im}(r_X(n))$. Tali vettori al variare di i formano una base di K^d che è anche una base di $\mathrm{Im}(r_X(n))$, quindi $r_X(n)$ è suriettiva.

3. Se il criterio di separazione vale per le curve di grado n a maggior ragione vale per le curve di grado m≥n.

4. Il criterio di separazione vale sempre per le curve di grado d-1. Infatti scelto un punto p_j tra i d punti dati possiamo sempre considerare una retta R_j che interseca X solo in p_j. Definiamo allora la curva $C_i=\bigcup R_j$, fatta su j≠i. Allora C_i passa per p_j se e solo se j≠i.

□

Dimostriamo ora due risultati sulle cubiche che ci saranno utili in seguito.

Lemma 25. *Sia X={p_1,...,p_8} un insieme di otto punti del piano proiettivo di cui mai quattro allineati e mai sette su una stessa conica. Allora X impone condizioni indipendenti alle cubiche.*

Dimostrazione: Iniziamo col caso generale, X non contiene nè tre punti allineati nè sei punti su una conica. Verifichiamo il criterio di separazione, per ogni i dobbiamo trovare una cubica passante per tutti i punti di X meno p_i. A meno di riordinare possiamo supporre i=1. Sia R la retta individuata da p_2 e p_3, allora R∩X={p_2,p_3} perchè X non contiene tre punti allineati. I cinque punti p_4, p_5, p_6, p_7, p_8, sono contenuti in una conica C e C∩X={p_4, p_5, p_6, p_7, p_8} perchè X non contiene sei punti su una stessa conica. Ora C_1=C∪X è una cubica che passa per tutti i punti di X meno p_1.
Supponiamo ora che X contenga tre punti allineati p_1, p_2, p_3 su una stessa retta R. Sia p_9 un ulteriore punto su R e poniamo X'=X∪{p_9}. Ogni cubica contenente X' interseca R in quattro punti, allora per la versione debole del teorema di Bezout una tale cubica contiene R. Perciò ogni cubica contenete X' è della forma R∪K, dove K è una conica contenente p_4,...,p_8. I cinque punti p_4,...,p_8 danno condizioni indipendenti alle coniche perchè non ve ne sono quattro allineati. Perciò X' impone condizioni indipendenti alle cubiche e quindi questo vale anche per X⊆X'.
Supponiamo infine che X contenga sei punti p_1,...,p_6 su una conica K. Sia poi p_9 un ulteriore punto su K. Sia C una cubica contenente X'=X∪{p_9}, allora C interseca K in sette punti. Per il teorema di Bezout K e C si devono intersecare in 2.3=6 punti contati con molteplicità. Allora K è una componente di C e possiamo scrivere C=K∪R dove R è la retta per p_7 e p_8. Quindi X' e di conseguenza anche X⊆X' impongono condizioni indipendenti alle cubiche. □

Proposizione 41 (Paradosso di Cramer)**.** *Sia X'=$\{p_1,...,p_9\}$ un insieme di nove punti intersezione completa di due cubiche. Se C è una cubica passante per $p_1,...,p_8$ allora C passa anche per p_9.*

Dimostrazione: Sia X=$\{p_1,...,p_8\}$, mostriamo che X soddisfa alle ipotesi del teorema precedente. Sappiamo che X'=D∩D', dove D e D' sono le due cubiche dell'enunciato. Supponiamo che X contenga quattro punti allineati, allora anche X' li contiene. Abbiamo così quattro punti allineati nell'intersezione di due cubiche, per la versione debole del teorema di Bezout tutta la retta R sulla quale giacciono i quattro punti è contenuta nelle cubiche, quindi D e D' hanno intersezione non finita lungo R e questo è assurdo perchè per ipotesi X' è la loro intersezione completa. Supponiamo ora che X (e di conseguenza X') contenga sette punti su una conica K, per il teorema di Bezout D e K, D' e K si intersecano in sei punti. Allora K è una componente comune a D e D', come prima un assurdo. Per il lemma precedente si ha che X impone condizioni indipendenti alle cubiche ovvero $\dim(\mathbf{I}(X)_3)=\dim(\mathrm{Ker}(r_X(3)))=10-8=2$. Quindi D e D' costituiscono una base di $\mathbf{I}(X)_3$. Possiamo scrivere ogni cubica contenente X come $F=\alpha D+\beta D'$, in particolare $F(p_9)=\alpha D(p_9)+\beta D'(p_9)=0$ quindi F passa anche per p_9. . □

Capitolo 7

Legge di gruppo sopra le cubiche lisce di $\mathbb{P}^2$

«Le combinazioni utili sono precisamente quelle più belle, intendo quelle maggiormente in grado di incantare. Tale incanto è la sensibilità speciale che tutti i matematici conoscono, ma di cui il profano è così ignorante che spesso è tentato di sorriderci su.»

Jules Henri Poincaré (1854-1912)

Vogliamo ora definire su una cubica liscia C di $\mathbb{P}^2$ una legge di composizione interna + in modo che (C,+) risulti essere un gruppo abeliano. Troveremo poi delle formule d'addizione esplicite per i punti sulla cubica.

7.1 Legge di gruppo

Sia $C \subseteq \mathbb{P}^2$ una cubica liscia e sia R una retta di $\mathbb{P}^2$. Dalla versione debole del teorema di Bezout sappiamo che $C \cap R$ consta di tre punti contati con molteplicità. Dobbiamo perciò distinguere tre casi:

1. $C \cap R$ consta di tre punti distinti.

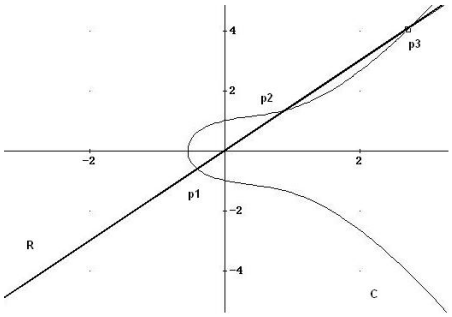

Figura 7.1: Caso I - Intersezione su tre punti distinti

2. R è tangente a C e C∩R consta di due punti distinti.

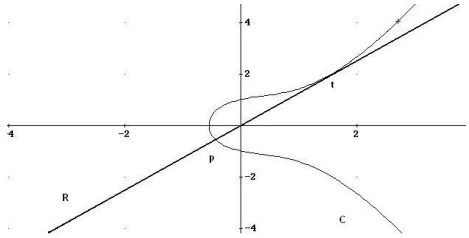

Figura 7.2: Caso II - Intersezione su due punti

3. R è una tangente di flesso per C, C∩R consta di un solo punto p e i(C,R,p)=3, ovvero p è un flesso di C.

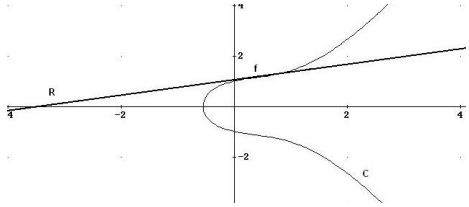

Figura 7.3: Caso III - Intersezione su un punto di molteplicità tre

Introduciamo il terzo punto. Siano a e b due punti sulla cubica C e sia R la retta per a e b. Il terzo punto è l'ulteriore intersezione della retta R con C e si indica con [ab]. Osserviamo che il punto a è un punto di flesso se e solo se [aa]=a.
Fissiamo ora su C un punto O che chiameremo origine e definiamo una legge di composizione interna.

Definizione 81. *Siano p,q due punti di C, allora p+q:=[O,[pq]], cioè p+q è il terzo punto di C∩R dove R è la retta generata da O e da [pq].*

Abbiamo così definito la legge di composizione interna C×C→C che manda (p,q)→p+q.

Lemma 26. *Con le notazioni precedenti si ha:*

1. *Per ogni (p,q)∈C^2, p+q=q+p.*
2. *Per ogni p∈C, p+O=O+p=p.*
3. *Per ogni p∈C, esiste -p∈C tale che p+(-p)=(-p)+p=O.*

Dimostrazione:1) La retta R può essere vista come R=[pq]=[qp] perciò [qp]=[pq] e [O,[qp]]=[O,[pq]]. Dunque p+q=[O,[pq]]∩C=[O,[qp]]∩C=q+p.
2) La retta [Op] interseca ulteriormente C in [Op]. Ora la retta [O[Op]] coincide

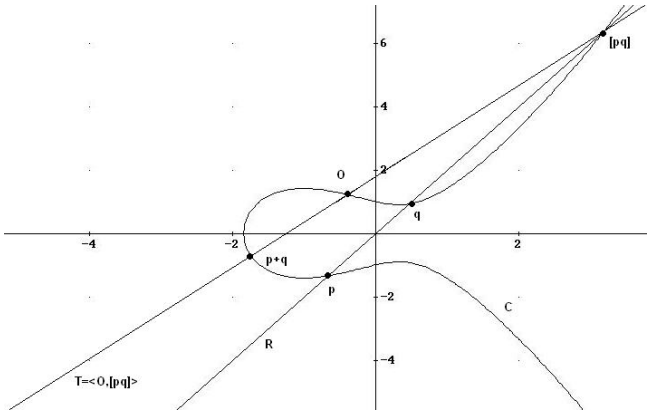

Figura 7.4: Somma di due punti su una cubica

con [Op] perchè hanno i punti O e p in comune. Quindi la terza intersezione tra [O,[Op]] è proprio p ovvero O+p=p. Da 1) sappiamo poi che p+O=O+p=p.
3)La cubica C è liscia, in particolare O è un punto liscio ed esiste quindi la tangente T a C in O. Sia q=[OO] il terzo punto di T∩C. Per ogni punto p∈C poniamo -p=[pq]. Ora la retta [p,-p] coincide con [p,q] quindi [-pp]=q e la retta [q,O] è proprio la tangente T che interseca C in O con molteplicità due. Vediamo così che p+(-p)=-p+p=O. □

A questo punto resta da dimostrare che la legge è associativa ovvero che per ogni (a,b,c)∈C^3 si ha a+(b+c)=(a+b)+c. Ci limitiamo al caso in cui i punti considerati sono distinti. La dimostrazione nel caso generale necessita della teoria degli schemi. Per la dimostrazione completa si può ricorrere ad un argomento di densità, ovvero osservando che i punti fatti intervenire nella dimostrazione dell'associatività sono tutti distinti per un sottoinsieme denso della cubica e argomentando che alla luce di questo la legge può essere estesa su tutta la curva.

Calcoliamo s'=(a+b)+c e t'=(b+c)+a=a+(b+c). In ognuna delle due costruzioni compaiono quattro rette. Riportiamo in figura la prima costruzione. Chiamiamo poi q,q',t,t' i punti delle seconda costruzione corrispondenti a r,r',s,s'.
Nella prima costruzione abbiamo le rette L1=[abr], L2=[cr's], L3=[r'Or],

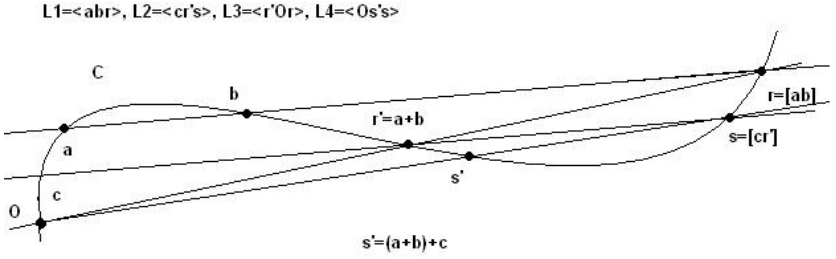

Figura 7.5: Associatività della somma su una cubica

L4=[Os's]. Analogamente nella seconda costruzione abbiamo le quattro rette

D1=[bcq], D2=[aq't], D3=[q'Oq], D4=[Ot't]. Vogliamo dimostrare che s'=t'. Chiaramente basta mostrare che s=t.
Siano ora F=L1∪L2∪D3 e G=D1∪D2∪L3 due cubiche. Si ha:
F∩C={a,b,c,r,r',q',O,q,s} e G∩C={a,b,c,r,r',q',O,q,t}.
Gli otto punti a,b,c,r,r',q',O,q sono otto dei nove punti dell'intersezione F∩C. Per il paradosso di Cramer (Proposizione 41 - Capitolo 6) ogni cubica passante per questi otto punti deve necessariamente passare per il nono punto s. In particolare G deve passare per s e perciò s=t.

Rimane così definita sulla cubica liscia C una struttura di gruppo.

Osservazione 21. *Ogni cubica liscia di $\mathbb{P}^2$ ha di certo un punto di flesso (Lemma 18 - Capitolo 5). Se fissiamo l'origine su un punto di flesso allora O'=[OO]=O perciò -a=[O'a]=[Oa].*

Lemma 27. *Sia O un punto di flesso della cubica liscia C, allora:*

1. *Per ogni (P,Q,U)∈C^3 P+Q+U=O se e solo se P,Q,U sono allineati.*
2. *P è un punto di flesso se e solo se 3P=O.*
3. *Se P,Q sono due flessi allora anche il terzo punto U=[PQ] è un flesso.*

Dimostrazione: 1) Supponiamo che sia P+Q+U=O, allora -U=P+Q quindi [OU]=-U=P+Q=[O[PQ]] ovvero P,Q,U sono allineati. Viceversa supponiamo che i tre punti siano allineati. Allora [PQ]=U da cui P+Q=[O[PQ]]=[OU]= =-U essendo O un flesso, ovvero P+Q+U=O.
2) Supponiamo che P sia un flesso allora [PP]=P, quindi 2P=P+P=[O[PP]]=[OP]=-P da cui 3P=2P+P=O. Se invece 3P=O, poichè 2P=P+P=[O[PP]] e -P=[OP], da 2P=-P segue che [O[PP]]=[OP] ovvero [PP]=P e quindi P è un flesso.
3) Siano P,Q due flessi. Abbiamo P+Q+[PQ]=O per 1) allora 3(P+Q+[PQ])=O da cui 3[PQ]=O e per 2) concludiamo che [PQ] è un flesso. □

7.2 Formule d'addizione su una cubica liscia

Sia C una cubica liscia di $\mathbb{P}^2(\mathbb{C})$. Possiamo scriverla nella forma di Legendre come $Y^2Z=X^3+aX^2+bXZ^2+cZ^3$. Nella carta affine U_Z la curva è data da $y^2=x^3+ax^2+bx+c$. Inoltre C è liscia perciò le sue derivate parziali non devono mai annullarsi su uno stesso punto ovvero il polinomio $p(x,y)=y^2-x^3-ax^2-bx-c$ non deve avere radici multiple e quindi il suo discriminante $D(p)=-4a^3c+a^2b^2+18abc-4b^3-27c^2\neq 0$.
Calcoliamo lo spazio tangente di Zariski alla cubica affine C nel suo punto p=(0,1). Posto $P(X,Y,Z)=Y^2Z-X^3-aX^2-bXZ^2-cZ^3$, si ha che Z=0 è tangente a C in p=(0,1,0). Infatti $P(X,Y,0)=-X^3=0$ se e solo se X=0, vediamo che Z=0 e C si intersecano in p con molteplicità tre quindi p=(0,1,0) è un punto di flesso. Notiamo esplicitamente che p non è singolare infatti $P_Z(0,1,0)=1$.
Per il teorema di Bezout debole la cubica proiettiva C interseca la retta all'infinito Z=0 in tre punti contati con molteplicità. Come abbiamo visto c'è un unico punto d'intersezione, il flesso p=(0,1,0) con molteplicità tre. Espliciti-amo la struttura di gruppo su C prendendo l'origine O=p. Sappiamo che C è

il completamento proiettivo della curva affine di equazione $p(x,y)=y^2-x^3-ax^2-bx-c$. Possiamo allora riguardare C in $\mathbb{P}^2$ come l'insieme $\{(x,y)\in\mathbb{C}^2$ tali che $p(x,y)=0\}\cup\{O\}$.
Sia ora $p\in\mathbb{C}^2$ denotiamo con $(x(p),y(p))$ le sue coordinate. Il nostro scopo è stabilire delle relazioni per le coordinate di P+Q,-P e 2P, dove P,Q sono punti della cubica C.
Sia $p\neq O$ un punto di C, sia poi R la retta generata da P e O, essendo O un flesso il terzo punto di $R\cap C$ è -P. La retta R è la retta verticale passante per P ovvero la retta di equazione $x=x(P)$. Essendo C simmetrica rispetto all'asse delle x si ha:

Lemma 28. *Sia P=(x(P),y(P)) un punto di C diverso da O allora -P=(x(P),-y(P)).*

Consideriamo ora la **somma di due punti distinti** sulla cubica. Siano $P=(x_1,y_1)$, $P'=(x_2,y_2)$ due punti distinti di C. Posto $[PP']=(x_3,y_3)$ allora P+P' è il terzo punto di $R\cap C$ dove R è la retta generata da O e [PP'], quindi $P+P'=(x_3,-y_3)$. Sia $y=mx+q$ l'equazione della retta D per P e P'(nel caso in cui D sia verticale P=-P' e P+P'=O). Si ha $m=(y_1-y_2)/(x_1-x_2)$ (se $x_1=x_2$ allora $P=\pm P'$). Il punto [PP'] è il terzo punto di $D\cap C$, tale intersezione è data da:
$y^2=(mx+q)^2=x^3+ax^2+bx+c$ da cui $m^2x^2+2mxq+q^2-x^3-ax^2-bx-c=0$ ovvero $x^3+x^2(a-m^2)+x(b-2q)+c-q^2=0$.
Questa equazione è verificata da P,P' e [PP'], perciò:
$x^3+x^2(a-m^2)+x(b-2q)+c-q^2=(x-x_1)(x-x_2)(x-x_3)=x^3-x^2(x_1+x_2+x_3)+x(x_1x_2x_2x_3+x_1x_3)-x_1x_2x_3$. Allora deve essere $a-m^2=-x_1-x_2-x_3$ da cui $x_3=m^2-a-x_1-x_2$.
Sappiamo poi che $y_1=mx_1+q$ e $y_2=mx_2+q$ perciò $q=y_1-mx_1=y_2-mx_2$. Infine ricaviamo y_3 dalla relazione $y_3=mx_3+q$. Per riassumere vale il segunte:

Lemma 29. *Siano $P=(x_1,y_1)$ e $P'=(x_2,y_2)$ due punti distinti di C a distanza finita. Allora $P+P'=(x,y)$ è il punto di coordinate:*
$x=m^2-a-x_1-x_2$;
$y=-mx-q$;
dove $m=(y_1-y_2)/(x_1-x_2)$ e $q=y_1-mx_1=y_2-mx_2$.

Ricaviamo ora la **formula di duplicazione**. Sia $P=(x_1,y_1)$ un punto di C, cerchiamo le coordinate di 2P=P+P. Consideriamo la retta tangente a C in P che avrà equazione $-(x-x_1)f'(x_1)+(y-y_1)2y_1=0$. La tangente è verticale se e solo se 2P=O. Se $y_1\neq 0$ la tangente avrà equazione del tipo $y=mx+q$ con $m=f'(x_1)/2y_1=(3x_1^2+2ax_1+b)/2y_1$. Cerchiamo le intersezioni tra la tangente e C, come prima vale l'equazione $y^2=(mx+q)^2=x^3+ax^2+bx+c$ da cui $m^2x^2+2mxq+q^2-x^3-ax^2-bx-c=0$ ovvero $x^3+x^2(a-m^2)+x(b-2q)+c-q^2=0$. Tale equazione è verificata da P con molteplicità due e da $[PP]=(x_{2p},-y_{2p})$. Possiamo scrivere $x^3+x^2(a-m^2)+x(b-2q)+c-q^2=(x-x_1)^2(x-x_{2p})=x^3-x^2(2x_1x_{2p})+x(x_1^2+2x_1x_{2p})-x_{2p}x_1^2$.
Da cui $x_{2p}=m^2-a-2x_1$. Possiamo ora ricavare y_{2p} dalla relazione $-y_{2p}=mx_{2p}+q$.
Abbiamo visto che:

Lemma 30. *Sia $P=(x,y)$ un punto di C a distanza finita allora le coordinate del punto 2P sono:*
$x(2P)=f'(x)^2/4f(x)-a-2x$ e $y(2P)=-mx(2P)-q$, con $m=f'(x)/2y$ e $q=y-mx$.
Se $y=0$ allora $2P=O$.

7.3 Punti razionali delle cubiche lisce

Abbiamo messo una struttura di gruppo sulle cubiche lisce di $\mathbb{P}^2(\mathbb{C})$. Una cubica può avere punti razionali, cioè punti a coordinate intere. Lo studio delle soluzioni razionali di equazioni polinomiali a coefficienti interi è oggetto dell'aritmetica diofantea. Un famoso problema di questa branca della matematica è la congettura di Fermat: *"Non esiste una terna di interi (X,Y,Z) con XYZ≠0 soluzione dell'equazione polinomiale $X^n+Y^n=Z^n$ per n≥3"*. Questo problema venne risolto da Wiles nel 1995.

Definizione 82. *Un punto di $\mathbb{P}^2(\mathbb{C})$ è razionale se e solo se ammette delle coordinate intere. Una curva C di $\mathbb{P}^2(\mathbb{C})$ è definita su $\mathbb{Q}$ se ammette un'equazione F(X,Y,Z)=0 con F(X,Y,Z)∈$\mathbb{Q}$[X,Y,Z]. Si denota con C($\mathbb{Q}$) l'insieme dei punti razionali della curva C.*

Data una cubica liscia E, definita su $\mathbb{Q}$, non si conosce nessun algoritmo per stabilire se E($\mathbb{Q}$) sia o meno vuoto. Supporremo quindi che la cubica E abbia un punto razionale e che tale punto sia un flesso. Supponiamo che E sia data da un equazione del tipo $y^2=x^3+ax^2+bx+d$ con a,b,d∈$\mathbb{Q}$. Se scriviamo a=p/q, b=m/n, d=s/t abbiamo $y^2=x^3+(p/q)x^2+(m/n)x+(s/t)$. Posto M=m.c.m.(q,n,t) possiamo scrivere $My^2=x^3+Ax^2+Bx+C$ con A,B,C∈$\mathbb{Z}$ e posto $My^2=Y^2$ si ha $Y^2=X^3+aX^2+bX+c$ con a,b,c∈$\mathbb{Z}$. Inoltre essendo la cubica liscia sappiamo che il discriminante $D=-4a^3c+a^2b^2+18abc-4b^3-27c^2\neq 0$. Il punto all'infinito O=(0,1,0) è un punto razionale per la cubica E. Allora l'insime dei punti razionali di E è costituito dal punto all'infinito O e dai punti a distanza finita ovvero E($\mathbb{Q}$)={(x,y)∈$\mathbb{Q}^2$ tali che $y^2=f(x)$}∪{O}. Vediamo allora che risolvere l'equazione diofantea $y^2=f(x)$ è equivalente a determinare E($\mathbb{Q}$) e questo è equivalente a trovare le soluzioni intere di $Y^2Z=X^3+aX^2Z+bXZ^2+cZ^3$.

Proposizione 42. *E($\mathbb{Q}$) è un sottogruppo di E($\mathbb{C}$).*

Dimostrazione: Sappiamo che O∈E($\mathbb{Q}$). Siano P,Q∈E($\mathbb{Q}$). Usiamo ora le formule esplicite per l'aritmetica su una cubica liscia ricavate in precedenza. Scriviamo $P=(x_p,y_p)$ e $Q=(x_q,y_q)$ con $x_p,y_p,x_q,y_q\in\mathbb{Q}$. Sappiamo che $-Q=(x_q,-y_q)$ e quindi anche -Q è razionale. Ora $P-Q=P+(-Q)=(x,y)$ è dato da: $x=m^2-a-x_p-x_q$ e $y=-mx-q$, con $m=(x_p-x_q)/(y_p-y_q)$ e $q=y_p-mx_p$. Vediamo così che m è razionale essendo rapporto di razionali. Dal fatto che $\mathbb{Q}$ è sottogruppo di $\mathbb{C}$ deriva che x è razionale. Inoltre mx_p è razionale perchè prodotto di razionali, quindi q è razionale e ancora y=-mx-q è razionale. □

Consideriamo ad esempio la curva di Fermat definita da $X^3+Y^3=Z^3$. Grazie al teorema di Wiles possiamo concludere che gli unici punti razionali di F sono (1,0,1), (1,-1,0) e (0,1,1) ovvero F($\mathbb{Q}$)={(1,0,1);(1,-1,0);(0,1,1)}.

Più in generale sia X una curva ellittica su un campo K algebricamente chiuso. Supponiamo che X possa essere definita tramite un'equazione f(X,Y,Z)=0 a coefficienti in un campo k contenuto nel campo K, diciamo allora che X è definita si k.
A questo punto è evidente, grazie alla natura geometrica della legge di composizione su X, che l'insieme X(k) dei punti di X a coordinate in k è un sottogruppo del gruppo su X.
In particolare se K=$\mathbb{C}$ e k=$\mathbb{Q}$ possiamo supporre f(X,Y,Z) a coefficienti in $\mathbb{Z}$

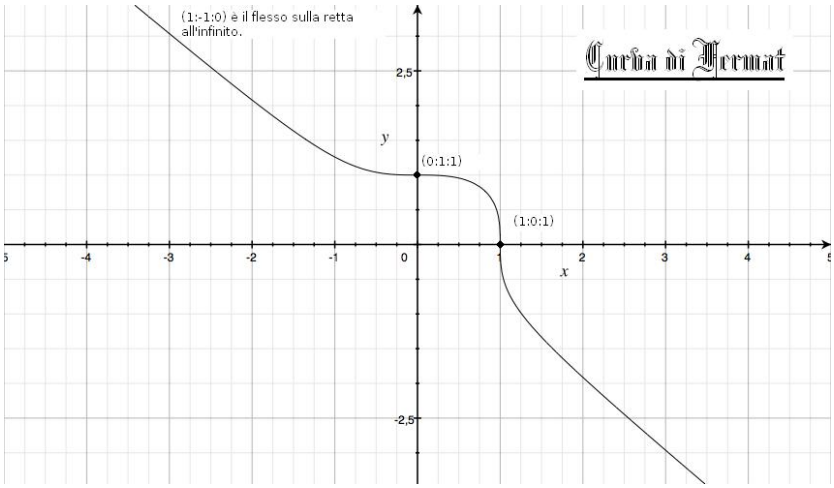

Figura 7.6: Curva di Fermat

avendo su $\mathbb{P}^2$ delle coordinate omogenee. Ci riduciamo così a cercare le soluzioni intere dell'equazione cubica diofantea f(X,Y,Z)=0.
Il teorema di Mordell da' un'informazione importante rigurado al gruppo X($\mathbb{Q}$), afferma infatti che X($\mathbb{Q}$) è un gruppo abeliano finitamente generato.
Un altro importante risultato è dovuto a Faltings. Se C è una curva liscia in $\mathbb{P}^2(\mathbb{C})$ di grado d$\geq$4 definita da un' equazione a coefficienti interi, allora C ha un numero finito di punti razionali.
Grazie a questo teorema possiamo affermare che l'equazione di Fermat $X^n+Y^n=Z^n$ ha al più un numero finito di soluzioni intere per ogni n$\geq$4.

Capitolo 8

Varietà Abeliane

«Una realtà completamente indipendente dallo spirito che la genera, la vede, o la sente, è un'impossibilità; un mondo talmente esterno a noi che, anche se esistesse, ci sarebbe per sempre inaccessibile.»

Jules Henri Poincaré (1854-1912)

Nella prima parte di questo capitolo viene introdotto lo spazio tangente ad una varietà algebrica X in un suo punto x, al fine di dimostrare alcune proprietà sui punti lisci e singolari delle varietà. Vengono poi dimostrate alcune importanti proprietà riguardo alle varietà abeliane. In particolare mostriamo che una varietà associata a un gruppo algebrico è sempre liscia, che una varietà abeliana è sempre commutativa e che due varietà abeliane isomorfe come varietà algebriche sono isomorfe anche come gruppi. L'ultima parte mostra che la legge di gruppo sulle curve ellittiche può essere rivista attraverso la teoria delle funzioni ellittiche, in particolare usando alcune proprietà di una delle più semplici funzioni ellittiche non costanti, la $\wp$ di Weierstrass. Grazie alla $\wp$ associeremo ad un toro complesso una curva ellittica.

8.1 Punti lisci e punti singolari sulle varietà algebriche

Vogliamo ora dimostrare alcuni importanti teoremi sulle varietà abeliane. Per fare questo è necessario introdurre la nozione di spazio tangente a una varietà algebrica X in un suo punto x.
Definiamo lo spazio tangente a X in x come l'insieme delle rette per il punto $x \in X$ tangenti alla varietà X. Riguardiamo $X \subseteq \mathbb{A}^n$ e fissiamo $x=(0,...,0)$. Allora la generica retta L passante per x è della forma $L=\{ta$ tali che $t \in K\}$ con $a \neq 0$ punto fissato in $\mathbb{A}^n$. Al fine di studiare l'intersezione $X \cap L$ supponiamo che la varietà X sia definita dall'ideale $I=(F_1,...,F_m)$. Allora $X \cap L$ è dato dalle equazioni $F_1(ta)=...=F_m(ta)=0$. Stiamo ora considerando polinomi nella sola variabile t, le loro radici comuni sono le radici del loro massimo fattore comune. Supponiamo che sia $f(t)=hcf\{F_1(ta),...,F_m(ta)\}=A\prod(t-a_i)^{ki}$. I valori $t=a_i$ corrispondono ai punti di intersezione tra X e L. Osserviamo che ad ogni a_i è associata una molteplicità k_i che viene interpretata geometricamente come la

molteplicità dell'intersezione tra la retta L e la varietà X nel punto corrispondente ad a_i. Notiamo che poichè 0∈X∩L, una delle radici di f(t) è t=0. Possiamo ora dare la seguente definizione.

Definizione 83. *La molteplicità dell'intersezione di una retta L con una varietà X nel punto x=0 è la molteplicità di t=0 come radice del polinomio f(t)=hcf{F_1(ta),...,F_m(ta)}.*

Vediamo allora che la molteplicità dell'intersezione è la più grande potenza di t che divide tutti gli F_i(ta). Tale molteplicità è certamente maggiore o uguale ad 1, poichè 0∈X∩L. Se gli F_i(ta) sono identicamente nulli si assume la molteplicità come $+\infty$.
Osserviamo inoltre che f(t)=hcf{F_1(ta),...,F_m(ta)}=hcf{F(ta) tali che F∈I}. Infatti se f(t) è il massimo fattore che divide tutti gli F_i(ta), f(t) divide certamente ogni F(ta) con F∈I ed è anche il massimo a fare ciò perchè in particolare gli F_i∈I. Se viceversa f(t) è il massimo fattore che divide tutti gli F(ta)∈I a maggiore ragione sarà il massimo a dividere gli F_i(ta). Vediamo così che la molteplicità dell'intersezione non dipende dai generatori di I che abbiamo scelto. Possiamo dare ora la seguente definizione.

Definizione 84. *Una retta L è tangente alla varietà X nel punto x=0 se ha intersezione di molteplicità maggiore o uguale a 2 con X nel punto x=0.*

Osserviamo ora che poichè 0∈X ogni polinomio F_i(T) ha termine costante nullo. Per i=1,...,m, scriviamo F_i=L_i+G_i dove L_i è il termine lineare e G_i è costituito dai termini di grado maggiore o uguale a 2. Allora F_i(at)=L_i(at)+G_i(at)=tL_i(a)+G_i(at).
Ora i G_i(at) sono divisibili per t^2, quindi F_i è divisibile per t^2 se e solo se L_i(a)=0 per i=1,...,m. Allora possiamo riscrivere la relazione di tangenza come

$$L_1(a)=...=L_m(a)=0.$$

Diamo ora la definizione di spazio tangente.

Definizione 85. *Il luogo geometrico di tutti i punti appartenti alle rette tangenti a X in x si dice spazio tangente a X in x e viene denotato con T_xX.*

Il nostro prossimo obiettivo è mostrare che se f:X→Y è un isomorfismo tra varietà algebriche allora lo spazio tangente a X in x e lo spazio tangente a Y in f(x) sono isomorfi. Per fare questo tradurremo la nozione di spazio tangente in termini dell'anello dello coordinate K[X].
Se F(T_1,...,T_N) è un polinomio e x=(x_1,...,x_N) un punto, allora F può essere espresso in serie di Taylor come

$$F(T)=F(x)+F^1(T)+...+F^k(T),$$

Dove F^i è un polinomio omogeneo di grado i nelle variabili T_j-x_j. La forma lineare F^1 è il differenziale di F in x e viene denotato con d_xF, abbiamo

$$d_xF=\sum_{i=1}^{N}(\partial F/\partial T_i)(x)(T_i\text{-}x_i).$$

Valgono allora le relazioni: $d_x(F+G)=d_xF+d_xG$ e $d_x(FG)=d_xFG+Fd_xG$.
Attraverso le nuove relazioni possiamo scrivere lo spazio tangente a x in X tramite il sistema lineare

$$d_xF_1=...=d_xF_m=0 \text{ o } \sum_{i=1}^{N}(\partial F_j/\partial T_i)(x)(T_i\text{-}x_i)=0 \text{ per } j=1,...,m,$$

dove $I=(F_1,...,F_m)$ è l'ideale di definizione della varietà X.
Supponiamo che $g\in K[X]$ sia definita restringendo un polinomio G alla varietà X. Poniamo $d_xg=d_xG$. Ci chiediamo ora se d_xg dipende dal polinomio G scelto. Poichè $I=(F_1,...,F_m)$ se $F\in I$ allora $F=P_1F_1+...+P_mF_m$. Ora poichè $d_x(P_iF_i)=d_xP_iF_i+P_id_xF_i$ e $F_i(x)=0$, abbiamo che $d_xF=P_1(x)d_xF_1+...+P_m(x)d_xF_m$. Da $d_xF_1=...=d_xF_m=0$ si ha che $d_xF=0$ su T_x per ogni $F\in I$. Allora se definiamo d_xg come la restrizione della forma lineare d_xG a T_x abbiamo una mappa che manda ogni funzione $g\in K[X]$ in una ben definita forma lineare d_xg su T_x.

Definizione 86. *La forma lineare d_xg appena definita di dice differenziale di g in x.*

Abbiamo ora un morfismo $d_x:K[X]\to T_x^*$, dove T_x^* è lo spazio vettoriale delle forme lineari su T_x. Poichè $d_xa=0$ per ogni $a\in K$ è sufficiente studiare la mappa $d_x:M_x\to T_x^*$, dove $M_x=\{f\in K[X]$ tali che $f(x)=0\}$. Notiamo che M_x è un ideale di K[X]. Infatti $0\in M_x$, se $u,v\in M_x$ allora $(u-v)(x)=u(x)-v(x)=0$ ovvero $u-v\in M_x$ e se $f\in K[X]$ e $u\in M_x$ allora $(fu)(x)=f(x)u(x)=0$, ovvero $fu\in M_x$.

Proposizione 43. *La mappa d_x definisce un isomorfismo di spazi vettoriali tra M_x/M_x^2 e T_x^*.*

Dimostrazione: Sia f una forma lineare su T_x. Certamente f è indotta da una qualche funzione lineare F su $\mathbb{A}^N$ e $d_xF=f$. Abbiamo così mostrato che l'applicazione è suriettiva. Supponiamo ora $x=(0,...,0)$ e che $g\in M_x$ con $d_xg=0$. Supponiamo poi che g sia indotta da un polinomio $G\in K[T_1,...,T_N]$. Allora la forma lineare d_xG è nulla su T_x, perciò è combinazione lineare delle forme che definiscono T_x. Possiamo scrivere $d_xG=a_1d_xF_1+...+a_md_xF_m$. Poniamo ora $G_1=G-a_1d_xF_1-...-a_md_xF_m$. Per come è definito G_1 non ha termini di grado 0 o 1 nelle variabili $T_1,...,T_N$ e quindi $G_1\in(T_1,...,T_N)^2$. Inoltre $G_1(x)=G(x)=g(x)$ per ogni $x\in X$, e quindi $g\in(t_1,...,t_N)^2$ dove $t_i=T_{i|X}$. Ora dal fatto che $M_x=(t_1,...,t_N)$ segue la tesi. □

Lo spazio vettoriale M_x/M_x^2 si dice spazio cotangente a X in x. Ora T_x è isomorfo al suo duale T_x^* che per la proposizione precedente è isomorfo a M_x/M_x^2. Quindi abbiamo un isomorfismo tra T_x è M_x/M_x^2. Ovvero lo spazio tangente e lo spazio cotangente ad una varietà X nel punto x sono isomorfi.
Siano ora X e Y due varietà algebriche e $F:X\to Y$ una mappa regolare. Allora F induce una mappa $f:K[Y]\to K[X]$ e si ha $f(M_{F(X)})\subseteq M_x$ e $f(M_{F(X)}^2)\subseteq M_x^2$, quindi F induce una mappa $f:M_{F(X)}/M_{F(X)}^2\to M_x/M_x^2$. Per la proposizione precedente T_x e $T_{F(x)}$ sono isomorfi rispettivamente a M_x/M_x^2 e a $M_{F(x)}/M_{F(x)}^2$. Abbiamo così una mappa $T_x\to T_{F(x)}$ detta differenziale di F in x e denotata con d_xF. Ora se $G:Y\to Z$ è un'altra mappa regolare allora il differenziale $d_x(G\circ F)=d_xG\circ d_xF$. Inoltre se $F:X\to X$ è l'identità allora il differenziale di F è l'identita su T_x per ogni $x\in X$.
Tutto questo ci dice che sotto un isomorfismo tra varietà gli spazi tangenti in punti corrispondenti sono isomorfi. In particolare spazi tangenti in punti corrispondenti hanno la stessa dimensione.

Definizione 87. *Una varietà X si dice liscia nel punto $x\in X$ se $dim(T_x)=dim(X)$. In caso contrario X si dice singolare in x.*

Proposizione 44. *Siano X e Y due varietà algebriche isomorfe è $F:X\to Y$ un isomorfismo. Allora X è liscia in x se e solo se Y è liscia in F(x).*

Dimostrazione: L'isomorfismo F tra X e Y induce un isomorfismo f tra gli spazi tangenti T_x e $T_{F(x)}$ che quindi hanno la stessa dimensione. Ora X è liscia in x se e solo se dim(X)=dim(T_x). Ma per ipotesi dim(X)=dim(Y). Quindi X è liscia in x se e solo se dim(Y)=dim($T_{F(x)}$), se e solo se Y è liscia in F(x). □

Al fine di dimostrare la prossima proposizione assumiamo il seguente fatto del quale non diamo la dimostrazione.
Ogni varietà quasi affine Y, con dim(Y)=n, è birazionalmente equivalente ad un'ipersuperficie di $\mathbb{A}^{n+1}$.

Proposizione 45. *Sia Y una varietà quasi-affine, l'insieme dei punti non singolari di Y contiene un aperto non vuoto.*

Dimostrazione: Cominciamo col supporre che Y=$\mathbf{V}$(F) sia un'ipersuperficie di $\mathbb{A}^n$, quindi F è un polinomio non costante e irriducibile. Sappiamo che y∈Y è singolare se e solo se tutte le derivate parziali F'$_i$(y)=(∂F/∂T$_i$)(y) sono nulle. Quindi i punti singolari di Y formano un chiuso di Y. Se ogni punto di Y è singolare allora le derivate parziali si annullano su Y ovvero F'$_i$∈$\mathbb{I}$(Y)=(F), dunque F divide F'$_i$. Se la variabile X$_i$ compare in F allora deg$_{Xi}$(F'$_i$)<deg$_{Xi}$(F) e quindi deve essere F'$_i$=0. Ora se char(K)=0 e tutte le derivate parziali sono nulle si ha che F è costante e siamo arrivati ad una contraddizione. Se char(K)=p interi positivo, F'$_i$=0 implica che F è un polinomio in X_i^p. Poichè questo vale per ogni i prendendo delle radici p-esime dei coefficienti di F (K algebricamente chiuso), abbiamo F=G^p, assurdo perchè F è irriducibile. La proposizione risulta provata nel caso delle ipersuperfici. Se ora Y è una varietà quasi-affine qualsiasi sappiamo che esiste un'ipersuperficie Z di $\mathbb{A}^n$ e due aperti U⊆Y, V⊆Z, e un isomorfismo f:U→V. Grazie alla prima parte della dimostrazione sappiamo che l'insieme dei punti lisci di Z è un aperto non vuoto W di Z. Poichè Z è irriducibile anche V∩W è un aperto non vuoto. Quindi f^{-1}(V∩W) è un aperto costituito da punti lisci di Y. □

Proposizione 46. *Sia Y una varietà quasi-affine. Per ogni t∈$\mathbb{A}$ posto Y_t={y∈Y tali che dim(T_yY)≥t} si ha che Y_t è chiuso rispetto alla topologia di Zariski in Y.*

Dimostrazione: Sia $\mathbb{I}$(Y)=(P$_1$,...,P$_m$) e sia J(y) la matrice Jacobiana dei P$_i$ nel punto y. Ora dim(T_yY)≥t se e solo se rango(J(y))≤n-t se e solo se tutti i minori di ordine n-t+1 di J(y) sono nulli. Quindi Y_t è l'intersezione di Y con $\mathbf{V}$(M$_1$,...,M$_i$,...) dove gli M$_i$ sono i minori di ordine n-t+1 della matrice Jacobiana J(P$_1$,...,P$_m$). □

Proposizione 47. *Sia Y una varietà quasi-affine. Allora per ogni y∈Y dim(T_yY)≥dim(Y). In particolare Sing(Y), insieme dei punti singolari di Y, è un chiuso proprio di Y.*

Dimostrazione: Sia dim(Y)=n, sappiamo dalla proposizione precedente che Y_n è un chiuso di Y e che Y_n contiene un aperto di punti non singolari, quindi Y_n=Y. Questo significa che per ogni y∈Y si ha dim(T_yY)=dim(Y) oppure dim(T_yY)>dim(Y). Sappiamo che l'insieme dei punti singolari è chiuso in Y ed è un chiuso proprio perchè l'insieme dei punti lisci di Y contiene sempre un aperto non vuoto. □

8.2 Gruppi algebrici e varietà abeliane

Definizione 88. *Un gruppo algebrico è una varietà algebrica V con una legge di composizione interna + tale che:*

- *(V,+) sia un gruppo;*
- *la mappa $\chi: V \to V$ definita da $\chi(v)=-v$ sia un'applicazione regolare;*
- *la mappa $\tau: V \times V \to V$ definita da $\tau(v_1,v_2)=v_1+v_2$ sia un'applicazione regolare.*

Definizione 89. *Un gruppo algebrico A su una varietà proiettiva viene detto una varietà abeliana.*

Diamo alcuni esempi di gruppi algebrici.

1. La retta affine $\mathbb{A}^1$ con la somma usuale tra le coordinate dei punti e la varietà $\mathbb{A}^1$-(0) con la moltiplicazione tra le coordinate dei punti.

2. Le cubiche lisce di $\mathbb{P}^2$ con la legge di composizione interna definita nel capitolo precedente. Infatti abbiamo visto che se C è una cubica liscia allora (C,+) è un gruppo.
   Inoltre sappiamo che dato un punti $P \in C$ di coordinate (X,Y) si ha che -P=(X,-Y) ovvero la mappa χ:V→V della definizione è data da $\chi((X,Y))=(X,-Y)$ e evidentemente è una mappa regolare.
   Infine la mappa τ:V×V→V è data da $\tau(P_1,P_2)=P_1+P_2=(X,Y)$, dove:
   $X=(\frac{Y1-Y2}{X1-X2})^2$-a-$X_1$-$X_2$ e
   $Y=-\frac{Y1-Y2}{X1-X2}((\frac{Y1-Y2}{X1-X2})^2$-a-$X_1$-$X_2)$-$Y_1+\frac{Y1-Y2}{X1-X2}X_1$.
   Quindi indicati con $P_1=(X_1,Y_1)$ e $P_2=(X_2,Y_2)$ due punti distinti su C si ha:

$$\tau(P_1,P_2)=(X,Y), \text{ con}$$
$$X=((Y_1-Y_2)^2-(a+X_1+X_2))/(X_1-X_2)^2 \text{ e}$$
$$Y=((Y_1-Y_2)(X_1(X_1-X_2)^2-(Y_1-Y_2)^2-(a+X_1+X_2))/(X_1-X_2)^3$$

Possiamo supporre $X_1 \neq X_2$, infatti in caso contrario avremmo $P_1=\pm P_2$. Se $P_1=-P_2$ allora $P_1+P_2=O$. Qundi la funzione τ è regolare su C.
Consideriamo ora il caso $P_1=P_2$. Dalla formula di duplicazione abbiamo:

$$\tau(P_1,P_1)=(f'(X_1)^2/4f(X_1)-a-2X_1, -m(f'(X_1)^2/4f(X_1)-a-2X_1)-q)$$
$$\text{con } m=f'(X_1)/2f(X_1) \text{ e } q=f(X_1)-mX_1.$$

Anche in questo caso l'applicazione τ risulta regolare perchè $Y_1=f(X_1)\neq 0$. Infatti se $Y_1=0$ abbiamo visto che la tangente in P_1 a C è verticale e allora $2P_1=O$. Più brevemente si può concludere che χ e τ sono mappe regolari grazie **al principio delle costruzioni algebro-geometriche**. Infatti nella costruzione geometrica della legge di gruppo in sostanza abbiamo considerato intersezioni tra curve algebriche ovvero operazioni geometriche che possono essere tradotte in linguaggio algebrico. Abbiamo così definito sulle curve ellittiche una struttura di gruppo algebrico. Possiamo perciò concludere che **le curve ellittiche sono varietà abeliane di dimensione uno in** $\mathbb{P}^2$.

Teorema 13. *La varietà associata a un gruppo algebrico G è non singolare.*

Dimostrazione: Per ogni h∈G consideriamo la mappa F_h:G→G, che manda g↦h+g. Per la definizione di gruppo algebrico si ha che F_h è un automorfismo della varietà G. Per ogni g_1,g_2∈G abbiamo F(g_1)=g_2 se prendiamo h=g_2-g_1. Sappiamo che un punto singolare è invariante sotto un isomorfismo (Proposizione 44). Allora se G avesse un punto singolare g ogni punto di G risulterebbe essere singolare, assurdo perchè Sing(G) è un chiuso proprio di G (Proposizione 47). Concludiamo che ogni punto di G è liscio. □

Enunciamo ora un lemma necessario in seguito senza darne una dimostrazione[1].

Lemma 31. *Siano X e Y due varietà algebriche con X varietà proiettiva, e sia f:X× Y→Z una famiglia di applicazioni da X in una varietà Z di base Y. Supponiamo che esista y_0∈Y tale che f(X×y_0)=z_0∈Z sia un punto. Allora f(X×y) è un punto per ogni y∈Y.*

Teorema 14. *Una varietà abeliana è sempre commutativa.*

Dimostrazione: Consideriamo una famiglia di mappe da G in G di base G date da f(g,h)=-g+h+g. Per h=0_G abbiamo f(g,0_G)=0_G e allora per il lemma precedente f(G,h) è un punto per ogni h. Quindi f(g,h)=f(0_G,h)=h. Vediamo così che -g+h+g=h ovvero h+g=g+h per ogni g,h∈G e quindi G è un gruppo abeliano.

□

Teorema 15. *Se F:G→H è una mappa regolare tra una varietà abeliana G e un gruppo algebrico H, allora F(g)=F(0_G)+f(g) dove f:G→H è un morfismo di gruppi.*

Dimostrazione: Poniamo f(g)=-F(0_G)+F(g) e consideriamo la seguente famiglia di mappe da G in H e di base G:

T:G×G→H date da T(g',g)=f(g')+f(g)-f(g'+g).

Notiamo che f(0_G)=0_H dunque T(G,0_G)=0_H. Per il lemma T(G,g) è un singolo punto per ogni g∈G ovvero T(g',g) non dipende da g'. Posto g'=0_G si ha che T(g',g)=T(0_G,g)=0_H dunque f(g')+f(g)-f(g'+g)=0_H ovvero f(g'+g)=f(g')+f(g) ed f è un morfismo di gruppi. □

Teorema 16. *Se due varietà abeliane sono isomorfe come varietà allora sono isomorfe come gruppi.*

Dimostrazione: Sia F:X→Y l'isomorfismo tra la varietà abeliane X e Y. Possiamo riguardare F come una mappa regolare tra la varietà X e il gruppo algebrico Y. Per il teorema precedente F induce un isomorfismo di gruppi f:X→Y. Sappiamo inoltre che f(x)=-F(0_X)+F(x)=A+F(X), dove A=-F(0_X) è costante. Vediamo allora che essendo F biettiva anche f lo è, dunque f:X→Y è un isomorfismo di gruppi. □

[1] Per la dimostrazione del lemma si veda I.Shafarevich - Basic Algebraic Geometry, pag.191.

8.3 Funzione $\wp$ di Weierstrass e legge di gruppo sulle curve ellittiche

Consideriamo ora il campo dei numeri complessi $\mathbb{C}$. Siano v_1,$v_2 \in \mathbb{C}$ linearmente indipendenti su $\mathbb{R}$, il reticolo generato da v_1 e v_2 è

$$\Gamma=\{pv_1+qv_2 \text{ tali che } p,q\in\mathbb{Z}\}.$$

Sia f una funzione meromorfa e sia P_f l'insieme dei suoi periodi.

Teorema 17. *Una funzione ellittica rispetto a* Γ *è una funzione meromorfa tale che* $P_f \cup \{0\} \supseteq \Gamma$.

Consideriamo ora la serie $(1/z^2)+\sum_{p,q\in\mathbb{Z}}(1/(z\text{-}pv_1\text{-}qv_2)^2)\text{-}(1/(pv_1+qv_2)^2)$, si ha che tale serie converge in norma su $\mathbb{C}$ e in particolare converge uniformemente. Poniamo

$$\wp(z)=(1/z^2)+\sum_{p,q\in\mathbb{Z}}(1/(z\text{-}pv_1\text{-}qv_2)^2)\text{-}(1/(pv_1+qv_2)^2).$$

La funzione così definita è la $\wp$ di Weierstrass. Tale funzione è meromorfa e ha poli nei punti di Γ. Si dimostra che $\wp$ e $\wp$' appartengono al campo delle funzione ellittiche su Γ e che inoltre $E(\Gamma)=\mathbb{C}(\wp,\wp')$ ovvero $E(\Gamma)$ è il campo generato dalle funzioni $\wp$ e $\wp$' relative al reticolo Γ.
Inoltre la $\wp$ può essere riguardata come funzione inversa dell'integrale ellittico

$$u=\int_y^\infty (1/(4v^3\text{-}Av\text{-}B)^{1/2})dv, \text{ con A,B costanti.}$$

ovvero $y=\wp(u)$.
Le propietà per noi più importanti della $\wp$ sono le seguenti[2]:

- La $\wp$ di Weierstarss soddisfa ad un teorema di addizione e in particolare alla relazione determinantale

$$\text{Det}\begin{pmatrix} \wp(z) & \wp'(z) & 1 \\ \wp(y) & \wp'(y) & 1 \\ \wp(z+y) & -\wp'(z+y) & 1 \end{pmatrix}=0$$

- La funzione $\wp(z)$ di Weierstrass soddisfa all'equazione differenziale

$$(\wp')^2=4(\wp)^3\text{-}A\wp\text{-}B \text{ dove A,B sono costanti.}$$

Posto $\wp'=y$ e $\wp=x$ abbiamo l'equazione $y^2=4x^3\text{-}Ax\text{-}B$, che definisce una cubica parametrizzata da $(\wp,\wp')$.
Se ora reinterpretiamo tale curva come ottenuta per deomogeneizzazione dell'equzione di una curva piana proiettiva abbiamo, $y=Y/Z$ e $x=X/Z$. Da cui $(Y/Z)^2=4(X/Z)^3\text{-}A(X/Z)\text{-}B$ ovvero $Y^2Z=4X^3\text{-}AXZ^2\text{-}BZ^3$, che è l'equazione di una curva ellittica.
Ora i punti della cubica $y^2=4x^3\text{-}Ax\text{-}B$ sono della forma $(x,y,1)=(\wp(z),\wp'(z),1)$.
Grazie al teorema d'addizione per la $\wp(z)$, sappiamo che vale la seguente relazione determinantale

[2]Per un approfondimento sulla funzione $\wp$ di Weierstrass e per la dimostrazione delle proprietà enunciate si veda Serge Lang - Elliptic Functions.

$$\mathrm{Det}\begin{pmatrix} \wp(z) & \wp'(z) & 1 \\ \wp(y) & \wp'(y) & 1 \\ \wp(z+y) & -\wp'(z+y) & 1 \end{pmatrix}=0$$

e quindi i punti $P_1=(\wp(z),\wp'(z),1)$, $P_2=(\wp(y),\wp'(y),1)$ e $P_{1,2}=(\wp(z+y),-\wp'(z+y))$ sulla cubica sono allineati. La cubica che stiamo considerando è simmetrica rispetto all'asse delle ascisse, $P_{1,2}$ non è altro che il terzo punto. Se fissiamo l'origine O sul punto all'infinito (0:1:0) della cubica e poniamo $P_1+P_2=P_S$ dove P_S è il simmetrico di $P_{1,2}$ rispetto all'asse delle ascisse, ovvero la terza interzezione della retta per O e $P_{1,2}$ con la cubica riotteniamo la struttura di gruppo definita sulle curve ellittiche nel capitolo precedente.

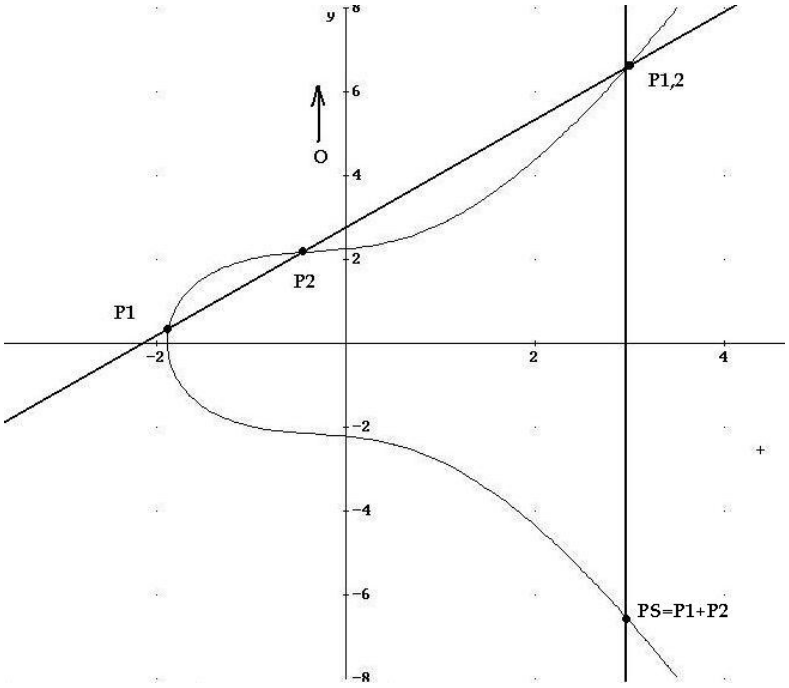

Figura 8.1: Legge di composizione sulla cubica attraverso la funzione $\wp$

8.4 Curve ellittiche e tori complessi

Consideriamo la seguente definizione:

Definizione 90. *Una varietà complessa di dimensione uno si dice una superfice di Riemann. Una superfice di Riemann compatta è una varietà topologica di dimensione due, compatta e orientabile.*

Consideriamo ancora le curve ellittiche come caso particolare di varietà abeliane. Come sappiamo il genere di un curva piana proiettiva e irriducibile è

$$g=\frac{(n-1)(n-2)}{2}$$

dove n è il grado della curva. Una curva ellittica è una curva piana di genere uno.
E' noto che le varietà topologiche compatte e orientabili di dimensione due sono classificate dal loro genere g. Infatti tali varietà sono omeomorfe ad una sfera con g manici dove g è un numero naturale.
Consideriamo ora una curva ellittica. Possiamo visulizzare la sua traccia reale ma non possiamo fare lo stesso per la sua traccia complessa che vive in uno spazio quadridimensionale. Tuttavia possiamo considerarne la superfice di Riemann che può essere immersa in uno spazio tridimensionale. Consideriamo la cubica definita da $y^2=x^3-x$. La sua traccia reale è riportata in figura.

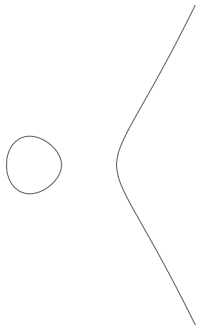

Figura 8.2: Traccia reale della cubica $y^2=x^3-x$

La funzione di variabile complessa associata alla cubica è $f(z)=\sqrt{z^3-z}$. Notiamo esplicitamente che la funzione che stiamo considerando è algebrica, sappiamo dalla teoria generale sulle superfici di Riemann[3] che vale la seguente proposizione:

Proposizione 48. *Sia* $\boldsymbol{A}$ *una funzione analitica. La superfice di Riemann associata ad* $\boldsymbol{A}$ *è compatta se e solo se* $\boldsymbol{A}$ *è algebrica.*

Per quanto detto la superfice associata alla cubica deve essere compatta e pertanto omeomorfa ad una sfera con g=1 manici avvero ad un toro complesso. Infatti sulla sfera di Riemann $\mathbb{C}^\infty$ la funzione algebrica $f(z)=\sqrt{z^3-z}$ ha quattro punti di diramazione. Tale funzione da luogo a due rami distinti ovvero a due copie distinte di $\mathbb{C}$ che però si intersecano in z=0, z=1, z=-1 e $z=\infty$ che sono punti di diramzione di ordine k=2.
Consideriamo il caso z=0. Poniamo $\xi=z^3-z$. Per z in un intorno dello zero si ha che anche $\xi\in S(0,r)$ e abbiamo $F(\xi)=\xi$, vediamo allora che z=0 è punto di diramazione ordinaria per f, perchè la funzione F ottenuta per sostituzione da f risulta olomorfa in un intorno dello zero.
Consideriamo ora $z=\infty$. Posto $z^3-z=1/\xi^2$ si ha $F(\xi)=1/\xi$. Se z è in un intorno di ∞ allora ξ è in un intorno dello zero. Dunque $z=\infty$ è un punto di diramazione algebrica semplice per f perchè abbiamo ottenuto per F uno sviluppo in serie di Laurent troncato alla prima potenza negativa di ξ.
Per z=1 e z=-1 si ha rispettivamente $F(\xi)=\xi-1$ e $F(\xi)=\xi+1$ e quindi entrambi risultano essere punti di diramazione ordinaria. Possiamo visualizzare la superfice di Riemann associata alla curva tagliando ognuna delle due copie di $\mathbb{C}^\infty$

[3]Per una trattazione approfondita della teoria sulle superfici di Riemann si veda Farkas, Kra - Riemann Surfaces.

lungo due archi che congiungono i punti di diramazione è incollandone i bordi. La superfice che otteniamo è proprio un toro.
Si dimostra che se due curve sono birazionalmente equivalenti allora sono isomorfe. Notiamo che la curva considerata non è razionale infatti abbiamo visto che la cubica è omeomorfa ad un toro mentre $\mathbb{P}^1$ essendo una retta e quindi una curva di grado uno e genere g=0 è omeomorfo ad una sfera.

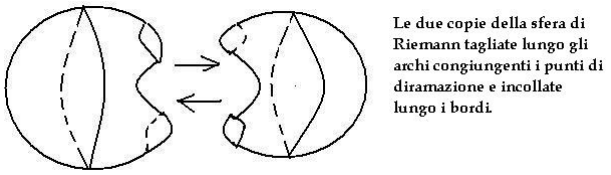

Figura 8.3: Le due copie della sfera di Riemann opportunamente tagliate

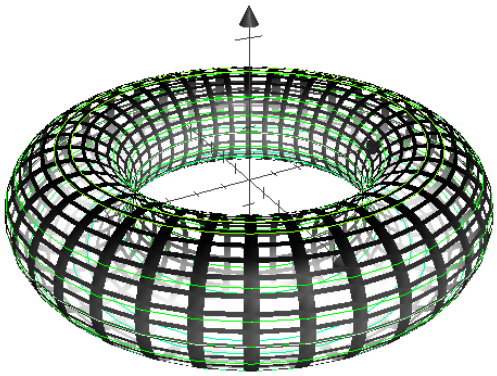

Figura 8.4: Toro complesso

Notiamo che lo studio fatto per la nostra particolare cubica vale in generale per ogni cubica liscia. Sappiamo infatti che ogni cubica liscia pùo essere scritta in forma di Weierstrass come $Y^2Z=X^3+aX^2Z+bZ^3$ e che il discriminante del polinomio $P(x)=x^3+ax^2+b$ è non nullo. Dunque la funzione di variabile complessa $f(z)=\sqrt{P(z)}$, $z\in\mathbb{C}$, presenterà quattro punti di diramazione distinti situati nei tre zeri di P(z) e in $z=\infty$. Perciò la superfice di Riemann ad essa associata sarà ancora un toro.

Vogliamo ora formalizzare quanto detto. Consideriamo ancora la funzione $\wp$ di Weierstrass che sappiamo essere una funzione ellittica rispetto ad un reticolo Γ generato dai suoi periodi primitivi e avente poli esattamente nei punti di Γ.

Notiamo che $\Gamma=\mathbb{Z}v_1+\mathbb{Z}v_2$ è il gruppo additivo libero generato da v_1 e v_2 e in particolare è un sottogruppo normale di $\mathbb{C}$. Ha senso allora considerare il quoziente $\mathbb{C}/\Gamma$. Notiamo che $\mathbb{C}/\Gamma$ è dotato:

- di una struttura di gruppo abeliano ereditata dal gruppo additivo di $\mathbb{C}$.
- della struttura di superfice di Riemann compatta con la topologia quoziente su $\mathbb{C}$. Infatti se per ogni $y\in\mathbb{C}/\Gamma$ consideriamo un $x\in\mathbb{C}$ e un intorno di U_x di x, che contenga al più un punto di Γ allora si ha che la collezione degli U_x forma un atlante per $\mathbb{C}/\Gamma$ se si prendono come mappe di transizione l'identità o la traslazione.

Il quoziente $T=\mathbb{C}/\Gamma$ si dice un toro complesso. Si ha che T è una varietà complessa di dimensione uno e la sua struttura complessa è determinata dal fatto che la proiezione canonica $\Pi:\mathbb{C}\longrightarrow\mathbb{C}/\Gamma$ è olomorfa. Topologicamente $\mathbb{C}/\Gamma$ è un $\mathbf{S}^1\times\mathbf{S}^1$. Infatti ogni punto di $\mathbb{C}$ ha un rappresentante nel paralellogramma generato da v_1 e v_2, detto parallelogramma fondamentale, se identifichiamo i lati opposti del paralellogramma percorsi nella medesima direzione otteniamo proprio un toro.

Sappiamo ora che la $\wp$ e la $\wp$' soddisfano alla relazione $(\wp')^2=4\wp^3+A\wp+B$.

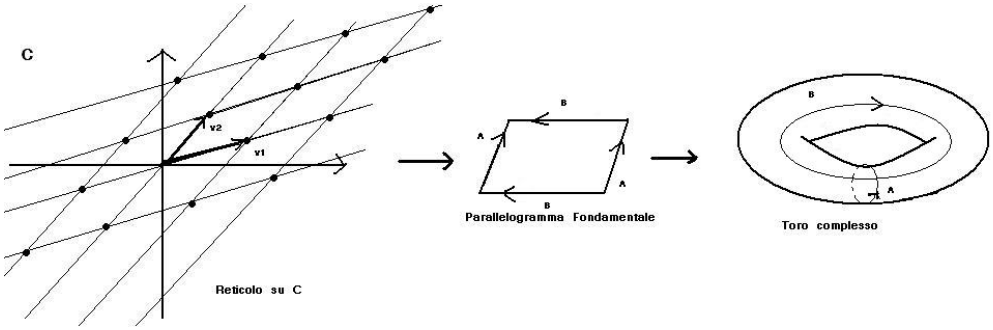

Figura 8.5: Costruzione del toro complesso

Inoltre in T abbiamo identificato tutti i punti di $\mathbb{C}$ sui quali $\wp$ e $\wp$' assumono lo stesso valore. Tenendo conto di queste osservazioni si dimostra che

Proposizione 49. *La mappa*

$$\Theta: T\longrightarrow\mathbb{P}^2 \text{ che manda } [z]\longmapsto(\wp(z):\wp'(z):1)$$

è un'immersione olomorfa del toro complesso T in $\mathbb{P}^2$ *che ha per immagine la curva ellittica di equazione* $Y^2Z=4X^3+AXZ^2+BZ^3$.

Allora una curva ellittica è isomorfa ad un toro complesso. Riassumendo dopo aver dato la definizione di varietà abeliana abbiamo verificato che le curve ellittiche appartengono a questa particolare classe di varietà e abbiamo definito su tali curve una struttura di gruppo algebrico prima dal punto di vista della geometria algebrica e poi usando strumenti dell'analisi complessa. Poi si è introdotto il genere di una curva algebrica, piana e proiettiva. Abbiamo osservato che il genere può essere riguardato attraverso la sua connotazione topologica e che ad una curva ellittica è possibile associare un toro complesso attraverso la teoria delle superfici di Riemann.

Bibliografia

[1] Claudia Menini, Freddy Van Oystaeyen, *Abstract Algebra a Comprehensive Treatment*. New York, M.Dekker (2004).

[2] Czes Kosniowski, *Introduzione alla topologia algebrica*. Zanichelli (1979).

[3] Edoardo Sernesi, *Geometria I*. Bollati-Boringhieri.

[4] Edoardo Sernesi, *Geometria II*. Bollati-Boringhieri.

[5] Farkas, Kra, *Riemann Surfaces*. Springer.

[6] I. Shafarevich, *Algebraic Geometry I*. Springer-Verlang.

[7] I. Shafarevich, *Basic Algebraic Geometry, vol 1*. Springer-Verlang.

[8] Joe Harris, *Algebraic Geometry - A first course*. Springer-Verlang.

[9] Makoto Namba, *Geometry of Projective Algebraic Curves*. New York, M.Dekker (1984).

[10] Michael Artin, *Algebra*. Bollati-Boringhieri.

[11] Philippe Ellia, *Appunti di geometria I*. Pitagora Ed.

[12] Philippe Ellia, *Appunti di geometria algebrica*.

[13] R. Hartshorne, *Algebraic Geometry*. Springer (1977).

[14] Serge Lang, *Abelian Varieties*. Interscience Pubishers, INC., New York. Interscience Pubishers LTD., London (1959).

[15] Serge Lang, *Algebra*. Addison-Wesley Publishing Company (1984).

[16] Serge Lang, *Algebra Lineare*. Bollati-Boringhieri.

[17] Serge Lang, *Elliptic Functions*. Springer.

[18] Thomas W. Hungerford, *Algebra*. Springer (1974).

[19] Walter Rudin, *Analisi reale e complessa*. Bollati-Boringhieri.