Teoria delle curve algebriche

Vitturi Alvise

Università degli studi di Padova

27 Settembre 2010

Argomenti della tesi

- Concetti introduttivi di algebra (corso di algebra commutativa).
- Spazio affine (corso di algebra commutativa).
- Spazio proiettivo.
- Molteplicità.
- Molteplicità di intersezione.
- Teorema di Bézout.
- Singolarità.
- Teorema di Riemann Roch.
- Introduzione ai codici.

Spazio affine

Definizione

K^n si chiama spazio affine.

Definizione

Se I è un ideale di $K[X_1, ..., X_n]$, un elemento di K^n si dice zero di I se è zero di ogni polinomio appartenente a I.

Definizione

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

Da una varietà algebrica V si definisce $\mathcal{I}(V)$ come l'ideale di tutti i polinomi che si annullano in V. Si ha che $\mathcal{I}(\mathcal{V}(I)) \supseteq I$.

Nullstellensatz

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

Teorema(Nullstellensatz)

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

Osservazione

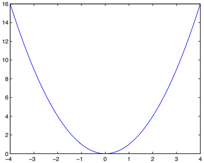
Se I è ideale primo di $K[X_1, ..., X_n]$, allora

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

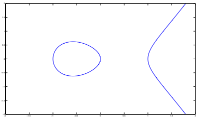
Questo corollario del Nullstellensatz può essere interpretato come un criterio di appartenenza. Se F si annulla su $\mathcal{V}(I)$, allora $F \in I$.

Definizione

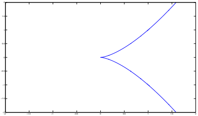
Sia $\mathcal{V}(F)$ una curva, $P = (a, b)$. P è chiamato un punto semplice (sottovarietà semplice) se $F_X(P) \neq 0$ o $F_Y(P) \neq 0$. La curva $F_X(P)(X - a) + F_Y(P)(Y - b)$ viene detta linea tangente (nel caso di P semplice). Un punto che non è semplice viene detto singolare.



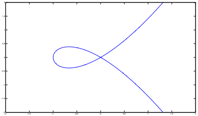
(a) `(semplice)`



(b) `(semplice)`



(c) `(singolare)`



(d) `(singolare)`

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

Spazio proiettivo

Definizione

Si definisce spazio poiettivo di dimensione n l'insieme:

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

dove ~ è la relazione di equivalenza così definita:

$$((x_1, \ldots., x_{n+1}), (y_1, \ldots.., y_{n+1})) \in_\sim se(y_1, \ldots.., y_{n+1}) = \lambda(x_1, \ldots., x_{n+1})$$

per qualche $\lambda \in K$.

Definizione

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

Definizione

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

Definizione

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

Proposizione

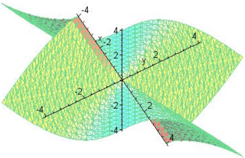
Ogni polinomio $P \in B[X_1, \ldots\ldots, X_n]$ *ha un' unica scrittura* $P = P_0 + P_1 + \cdots + P_d$ *dove* P_i *sono tutti polinomi omogenei di grado* i.

Da un polinomio si può ottenere il suo polinomio omogeneo, viceversa da un polinomio omogeneo si può definire il suo polinomio demogeneizzato. Questo e utile per legare lo spazio proiettivo a quello affine.

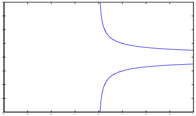
Esempio

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

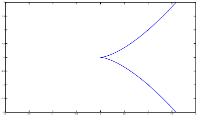
1. $\mathcal{V}_a((YZ^2 - 1))$.
2. $\mathcal{V}_a((Z^2 - X^3))$.
3. $\mathcal{V}_a((Y - X^3))$.



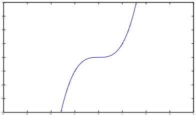
(a) cubica



(b) prima



(c) seconda



(d) terza

Figura: Le tre varietà affini.

Bézout

Teorema (Bézout)

Siano F, G due curve piane proiettive senza componenti in comune di grado m,n rispettivamente. Allora

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

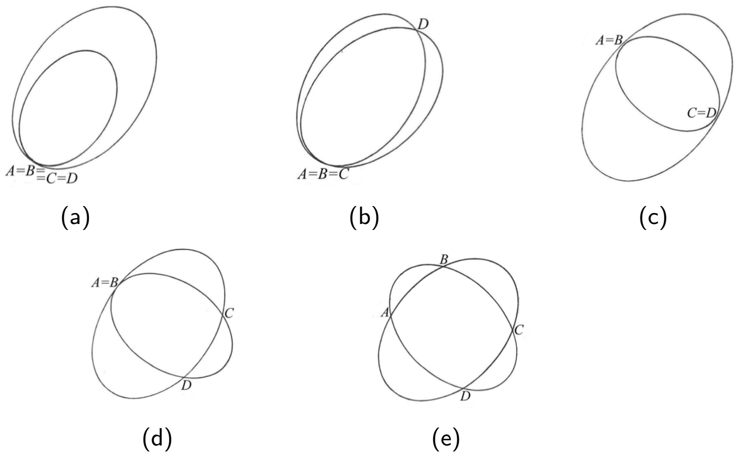


Figura: Esempi Bézout.

Singolarità

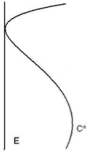
Definizione

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

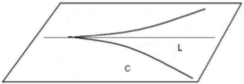
La classificazione appena data è di importanza fondamentale

Proposizione

Sia C una curva piana proiettiva irriducibile con tutti i punti multipli ordinari (tutti con tangenti distinte). Allora esiste una curva C' non singolare e un morfismo birazionale f da C' a C.(esiste analogo nel caso affine).

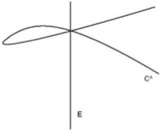


(a)

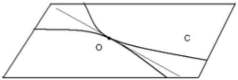


(b)

Figura: Curva con singolarità eliminabile.



(a)



(b)

Figura: Curva che non verifica le ipotesi del teorema.

Teorema

Sia C una curva proiettiva (anche non del piano). Allora esiste una curva proiettiva X non singolare e un morfismo birazionale f da X a C. Il teorema afferma anche che se esiste un altra applicazione $f' : X' \to C$ questa è tale per cui $X \cong X'$.

Codici

Teorema (Riemann-Roch)

Sia W un divisore canonico di X. Allora per ogni divisore D,

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

Definizione

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

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

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

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

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

o anche:

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

Definizione

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

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

Esempio

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

$$B = P_0 + \cdots P_6$$

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

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