Geometria ed Algebra delle curve piane

Alessandro Verra

10 Settembre 2009

Sia k un *campo* e siano $X_1, \ldots, X_n$ coordinate sullo *spazio affine* k^n.
La *geometria algebrica* ha come scopo lo studio dei sottoinsiemi

$$S \subset k^n$$

definiti da un sistema di equazioni polinomiali

$$F_1 = \cdots = F_s = 0$$

a coefficienti in k.
Preciseremo tra poco la nozione di campo, per il momento ci basti pensare a k come ad uno dei seguenti insiemi numerici:

$$\mathbf{Q} \quad , \quad \mathbf{R} \quad , \quad \mathbf{C}$$

scegliendo quello che piú ci piace.

Il caso piú semplice di tutta la geometria algebrica é quello in cui le equazioni $F_1 \dots F_s$ che definiscono S sono *lineari*.

Il *teorema di Rouché-Capelli* descrive completamente la situazione.

il teorema ci dice quando esistono soluzioni. Esso ci dice inoltre che, in tal caso, S é descritto da *equazioni parametriche lineari*

$$X_1 = f_1(t_1, \dots, t_{n-r}) \ \dots X_n = f_n(t_1, \dots, t_{n-r})$$

che definiscono una corrispondenza biunivoca tra i punti di S e k^{n-r}.

Un altro caso relativamente trattabile é quello in cui

$$S \subset k^n$$

é definito da *una sola equazione di grado due*. S viene chiamata *quadrica* di k^n, in particolare *conica* se $n = 2$ e *superficie quadrica* se $n = 3$.

L' equazione di S é

$$F = a_{00} + \sum_{j=1\ldots n} a_{0j}X_j + \sum_{1\leq i,j\leq n} a_{ij}X_iX_j$$

e ad essa é associata una matrice simmetrica di ordine $n+1$

$$A = (a_{ij}), \quad 0 \leq i,j \leq n.$$

Utilizzando A si puó riscrivere F in modo conveniente e descrivere S.

Infatti

$$F = a_{00} + \sum_{j=1\ldots n} a_{0j}X_j \ + \ (X_1 \ \ldots \ X_n)\, A_0 \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix},$$

dove $A_0 = (a_{ij}),\ \ 1 \leq i,j \leq n$ é matrice simmetrica. Quindi

$$A_0 = {}^tPDP$$

dove $D = (c_{ii})$ é una matrice diagonale e P una matrice invertibile. Ponendo $\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = P \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$ e $(b_{01} \ldots b_{0n}) = (a_{01} \ldots a_{0n})P^{-1}$ si ha

$$F = a_{00} + b_{01}Y_1 + \cdots + b_{0n}Y_n + c_{11}Y_1^2 + \cdots + c_{nn}Y_n^2,$$

S potrá essere studiato su tale equazione. Si tratta del primo passo della

riduzione in forma canonica della equazione di una quadrica di k^n.

Il rango $r_0 = r(A_0)$ descrive una proprietá intrinseca a F:
Sia

$$F = G + d_1 L_1^2 + \cdots + d_s L_s^2$$

dove $L_1 \ldots L_s$ *sono forme lineari e deg* $G \leq 1$, *allora* $s \geq r_0$.

Ad esempio in k^2 il valore di r_0 distingue le *coniche a centro* ($r_0 = 2$) da quelle non a centro ($r_0 = 1$), degeneri o non degeneri.

La classificazione delle quadriche di k^n é un risultato acquisito. Almeno nel caso di $\mathbf{R}^2$ esso risale all' epoca greca e poi ellenistica.
Su $\mathbf{R}^2$ é poi possibile definire la distanza tra punti nel modo standard e procedere alla classificazione delle coniche a meno di isometrie, ovvero di corrispondenze biunivoche di $\mathbf{R}^2$ che preservino la distanza.

Ellisse, Parabola , Iperbole sono nomi greci a noi ben noti:

$$\frac{X^2}{a^2} + \frac{Y^2}{b^2} = 1 \ , \ Y = -4pX^2 \ , \ \frac{X^2}{a^2} - \frac{Y^2}{b^2} = 1.$$

Il procedimento applicato ad una sola equazione di grado due é senz'altro utile per descrivere le soluzioni un sistema di equazioni polinomiali

$$F_1 = \cdots = F_s = 0 :$$

(1) *riscrivere le equazioni in una forma conveniente*,
(2) *eliminare le equazioni non necessarie*.

Purtroppo tale programma é raramente praticabile e quasi mai sufficiente per sviluppare una conoscenza matematica profonda degli insiemi definiti da tali equazioni.

Per questo motivo la geometria algebrica ha una posizione centrale in matematica ed incrocia molte altre discipline che le sono necessarie e utili: dall' algebra alla teoria dei numeri, dall' analisi alla topologia.

Ritroveremo tale aspetto, in forma elementare, nelle pagine successive.

In matematica questioni elementari possono essere di difficoltá estrema. La geometria algebrica non fa eccezione e giá lo studio delle coniche del piano affine $\mathbf{Q}^2$ basterebbe a rivelarlo. In proposito si consiglia il non troppo difficile ma istruttivo studio delle seguenti coniche di $\mathbf{Q}^2$:

$$X^2 + Y^2 = 1 \ , \ X^2 + Y^2 = 2 \ , \ X^2 + Y^2 = 3.$$

Sia poi $C_n \subset \mathbf{Q}^2$, $n \geq 3$, la curva di equazione

$$X^n + Y^n = 1.$$

Forse é superfluo ricordare che lo studio di tale equazione costituisce il celeberrimo *problema di Fermat*. Fermat aveva affermato che le uniche soluzioni erano quelle ovvie in cui una delle coordinate é zero:

mirabilem demontrationem inveni.

Sarebbero passati *tre secoli* prima che questa affermazione potesse essere dimostrata dai matematici Andrew Wiles e Richard Taylor nel 1994.

$\star$ *Varietá algebriche affini*

Sia k un campo, indicheremo con $k[X_1 \dots X_n]$ l' anello dei polinomi a coefficienti in k nelle variabili $X_1 \dots X_n$:

Definizione

Una varietá algebrica affine $V \subset k^n$ é l'insieme delle soluzioni di un sistema di equazioni $F_1 = \dots F_s = 0$, dove $F_1 \dots F_s \in k[X_1 \dots X_n]$.

Terminologia

- *Diremo che V é una varietá definita su k,*
- *$W \subset V$ é una sottovarietá di V se é una varietá affine,*
- *$U \subset V$ é un aperto di Zariski se $V - U$ é una sottovarietá di V.*
- *$S \subset V$ é denso se $S \cap U \neq \emptyset$ per ogni aperto di Zariski $U \neq \emptyset$.*

Definizione

Una varietá V si dice irriducibile se

$$U_1 \cap U_2 \neq \emptyset$$

per ogni coppia (U_1, U_2) di suoi aperti di Zariski .

$\star$ Per motivi tecnici supporremo d' ora in poi che V sia irriducibile, salvo avviso del contrario.
Le varietá irriducibili costituiscono la maggior parte dei casi interessanti e che qui interessano.

Esempi/Esercizi

Determinare quali sono le coniche irriducibili di $\mathbf{R}^2$ e di $\mathbf{C}^2$.

⋆ *Campi*

Gli insiemi $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ con le usuali operazioni sono esempi di campi.

Definizione

Un campo é un insieme k sul quale siano definite due operazioni, dette somma e prodotto di k, tali che:

- *somma e prodotto sono associative e commutative,*
- *esistono gli elementi neutri di somma e prodotto, indicati con* 0 *e* 1,
- $\forall x \in k$ *esiste l' opposto rispetto alla somma, indicato con* $-x$,
- $\forall x \in k, x \neq 0$, *esiste l' inverso rispetto al prodotto, indicato con* $\frac{1}{x}$,
- *distributiva del prodotto rispetto alla somma.*

$\forall x, y \in k$ la loro somma si indica con $x + y$ e il loro prodotto con xy. Sia nx la somma di x $n > 0$ volte: supporremo sempre che $nx = 0 \Rightarrow x = 0$.

Definizione

Due campi si dicono isomorfi se esiste tra di essi una corrispondenza biunivoca compatibile con le operazioni di somma e prodotto.

$\star$ *Sottocampi ed estensioni*

Si noti che

$$\mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$$

e che le operazioni su un campo sono indotte dalle operazioni su quello successivo.

Definizione

Siano $k \subset K$ due campi. Diremo che k é un sottocampo di K se le operazioni di k sono indotte su k dalle operazioni tra elementi di K.

$\star$ *Funzioni razionali su V*

Definizione

Un germe di funzione razionale su V é una fuzione $\frac{p}{q} : U \longrightarrow k$ tale che

- *U é un aperto di Zariski denso,*
- *$p, q \in k[X_1 \dots X_n]$ e $q(x) \neq 0, \forall x \in U$.*

Definizione

Due germi di funzioni razionali $\frac{p_1}{q_1} : U_1 \longrightarrow k$ e $\frac{p_2}{q_2} : U_2 \longrightarrow k$ si dicono coincidenti se coincidono su $U_1 \cap U_2$.

$\star$ La relazione di coincidenza é una relazione di equivalenza.

Definizione

Una funzione razionale $f : V \dashrightarrow k$ é una classe di coincidenza di germi di funzioni razionali su V. Il dominio di $f : V \dashrightarrow k$ é l' insieme

$$D = \bigcup U,$$

dove $(\frac{p}{q}, U)$ varia nella classe di coincidenza $f : V \dashrightarrow k$.

Una funzione razionale $f : V \dashrightarrow k$ determina una funzione vera e propria

$$f_D : D \to k.$$

$\forall x \in D$, $\exists$ un germe $\frac{p}{q} : U \to k \ / \ x \in U$. Per definizione $f_D(x) = \frac{p(x)}{q(x)}$. La linea tratteggiata di $f :\dashrightarrow k$ indica che V non é necessariamente il dominio di f.

In pratica

$f : V \dashrightarrow k$ si studia considerando un suo germe $\frac{p}{q} : U \to k$.

$\star$ *Il campo delle funzioni razionali di* V

Indicheremo con

$$k(V)$$

l' insieme delle funzioni razionali $f : V \dashrightarrow k$. Su $k(V)$ si possono definire le usuali operazioni di somma e prodotto di funzioni. Siano $\frac{p_1}{q_1} : U_1 \longrightarrow k$ e $\frac{p_2}{q_2} : U_2 \longrightarrow k$ germi delle funzioni razionali $fg \in k(V)$:

Definizione

- $f + g : V \dashrightarrow k$ *é la classe di coincidenza di* $\frac{p_1}{q_1} + \frac{p_2}{q_2} : U_1 \cap U_2 \longrightarrow k$,
- $fg : V \dashrightarrow k$ *é la classe di coincidenza di* $\frac{p_1 q_1}{q_2 p_2} : U_1 \cap U_2 \longrightarrow k$.

$\star$ *Il campo delle funzioni razionali su* k^n

Sia $V = k^n$, segue facilmente dalla definizione che il campo delle funzioni razionali $f : k^n \dashrightarrow k$ non é altro che il campo delle funzioni razionali in n variabili e cioé il campo dei quozienti dell' anello di polinomi $k[X_1 \dots X_n]$:

$$k(k^n) = k(X_1 \dots X_n).$$

Osservazione

Nonostante le apparenze $k(V)$ *non* é per costruzione un sottocampo di $k(X_1 \dots X_n)$: c' é di mezzo la relazione di equivalenza che entra in gioco nella definizione di $k(V)$.

⋆ *Mappe razionali e birazionali*

Siano $V \subset k^n$ e $W \subset k^m$ varietá affini. Un *germe di mappa razionale da V a W* é una funzione $\phi_U : U \to W$ definita dalle equazioni

$$Y_1 = f_1 \ldots Y_m = f_m$$

dove $f_1 \ldots f_m \in k(V)$ e $U \subset V$ é un aperto di Zariski. Diremo che $\phi_1 : U_1 \to W$ e $\phi_2 : U_2 \to W$ coincidono se $\phi_1/U_1 \cap U_2 = \phi_2/U_1 \cap U_2$. La relazione di coincidenza é una relazione di equivalenza.

Definizione

Una mappa razionale $\phi : V \dashrightarrow W$ é una classe di coincidenza di germi di mappe razionali da V a W.
Il dominio di ϕ é l' insieme $D = \bigcup U$, al variare di $\phi_U : U \to W$ nella classe di coincidenza

In pratica

Una mappa razionale $\phi : V \dashrightarrow W$ va pensata come una m-upla $(f_1, \ldots, f_m)$ di fuzioni razionali su V tali che $(f_1(x), \ldots, f_m(x)) \in W$ per ogni punto $x \in V$ nel quale $f_1 \ldots f_m$ siano regolari.

Esempi/Esercizi

- *Ogni funzione $\alpha : k^n \to k^m$ definita da polinomi. $D = k^n$.*
- *$\beta : k^2 \dashrightarrow k^2$ definita da $Y_1 = \frac{1}{X_1}$, $Y_2 = \frac{1}{X_2}$.*
- *Provare che β é biunivoca tra due aperti di Zariski.*
- *$\gamma : k \to k^3$ di equazioni $X = 2, Y = t^4, Z = 1$. Determinare $\gamma(k)$.*
- *$\delta : V \dashrightarrow k$, dove γ é definita da $T = \frac{Y}{X}$ e V é la curva di equazione*

$$Y^2 - X^2 = X^3.$$

- *Determinare il dominio di δ.*

Definizione

Una mappa razionale $\phi : V \dashrightarrow W$ si dice birazionale se ammette una mappa razionale inversa i.e. se esiste $\psi : W \dashrightarrow V$ tale che $\psi \cdot \phi = id_V$ e $\psi \cdot \phi = id_V$.

Proposizione

Una mappa razionale $f : V \dashrightarrow W$ é birazionale se e solo determina una corrispondenza biunivoca tra due aperti di Zariski non vuoti di V e W.

Proposizione

$\phi : V \dashrightarrow V$ é birazionale se e solo se i campi $k(V)$ e $k(W)$ sono isomorfi.

Esempi/Esercizi

La nozione di mappa birazionale é particolarmente importante. Verificare quali mappe sono birazionali negli esempi/esercizi precedenti.

$\star$ *Dimensione*

Se $k = \mathbf{R}$ la nozione di dimensione di una varietá algebrica mantiene in parte il suo significato intuitivo: *linee e superfici in dimensione 1 e 2...*
La dimensione puó essere definita in termini algebrici. Ció ha molte analogie la definizione di dimensione di uno spazio vettoriale:

Esempi/Esercizi

- $k(V)$ *contiene* k *ed é uno spazio vettoriale su* k
- $k(V)$ *non ha dimensione finita su* k*, salvo se* V *é un punto.*

C' é qualche analogia con il caso delle estensioni $\mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$:

Esempi/Esercizi

- $\mathbf{R}$ *non ha dimensione finita su* $\mathbf{Q}$*: se no* $\mathbf{R}$ *sarebbe numerabile.*
- $\mathbf{C}$ *ha dimensione due su* $\mathbf{R}$*:* $\forall z \in \mathbf{C}$, $z = a + ib$ *con* $a, b \in \mathbf{R}$.

Osservazione

Siano $k \subset K$ una estensione di campi e $f_1 \dots f_s \in K$ possiamo studiare:

- *la dipendenza o indipendenza lineare su k di $f_1 \dots f_s$ di K.*
- *la dipendenza o indipendenza algebrica su k di $u_1 \dots u_s$.*

Definizione

$f_1 \dots f_s$ si dicono algebricamente indipendenti su k se l'unico polinomio $F \in k[X_1, \dots, X_n]$ tale che $F(f_1, \dots, f_s)$ é quello a coefficienti nulli.

L' analogia con la nozione di indipendenza lineare di vettori é evidente.

Definizione

K ha grado di trascendenza d su k se d é il massimo numero di elementi di K che sono algebricamente indipendenti su k.

Se tale massimo non esiste si dice che K ha grado di trascendenza infinito su k. In caso contrario che K ha grado di trascendenza finito.

Sia V una varietá algebrica integra:

Theorem

$k(V)$ ha grado di trascendenza finito su k.

Definizione

La dimensione di V é il grado di trascendenza di $k(V)$ su k.

La dimensione di V si indica co *dim* V.

Esempi/Esercizi

Provare che k^n ha dimensione n e cioé che $k(X_1 \dots X_n)$ ha grado di trascendenza n su k.

Una *curva algebrica* é una varietá algebrica di dimensione uno.

Una *superficie algebrica* é una varietá di dimensione due.

Uno spazio vettoriale E su k di dimensione d é caratterizzato dal fatto che esiste un isomorfismo di spazi vettoriali

$$\phi : E \to k^d.$$

Esiste una caratterizzazione simile per una varietá algebrica V definita su k e di dimensione d?

$dim\ V = d$ se e solo se esiste una mappa razionale genericamente finita

$$\phi : V \dashrightarrow k^d.$$

Una mappa razionale $\phi : V \dashrightarrow W$ si dice *genericamente finita* se:

$$\forall\ y \in U,\ f^{-1}(x) \text{ é un insieme non vuoto e finito.}$$

su un aperto Zariski non vuoto $U \subset W$.

⋆ *Spazi proiettivi*

Lo studio nello spazio affine non é sempre sufficiente per comprendere gli aspetti piú profondi dela geometria delle varietá algebriche. Lo spazio affine stesso é dotato in piú modi di una mappa iniettiva naturale

$$a : k^n \longrightarrow \mathbf{P}_k^n$$

in uno spazio di natura diversa, dove molte proprietá globali delle varietá algebriche diventano piú chiare e visibili. Si tratta dello spazio proiettivo di dimensione n su k che ora descriveremo in velocitá.

Definizione

Sia E uno spazio vettoriale su k dim $E > 0$. Lo spazio proiettivo di E é l'insieme $\mathbf{P}(E)$ dei sottospazi vettorali di dimensione uno di S.

$\star$ *Coordinate proiettive o omogenee*

Salvo eccezioni lavoreremo con lo spazio proiettivo di k^{n+1}, indicato con

$$\mathbf{P}_k^n$$

Ogni punto $p \in \mathbf{P}_k^n$ é una retta vettoriale. I punti p sono $n+1$-uple

$$(cl_o, \ldots, cl_n)k^{n+1}$$

dove $(l_0, \ldots, l_n) \neq (0, \ldots, 0)$ genera p e $c \in k$. p é determinato da ogni suo generatore cioé da ogni $n+1$-upla $(cl_0, \ldots, cl_n)$ con $c \neq 0$.

Definizione

p ha coordinate proiettive $(l_0 : \cdots : l_n)$ se $(l_0, \ldots, l_n)$ é un generatore di p.

Osservazione

Le coordinate proiettive di p non sono univocamente determinate da p:
$(l_0 : \cdots : l_n)$ e $(cl_0 : \cdots : cl_n)$ sono entrambe coordinate di p se $c \neq 0$.
Le coordinate proiettive sono determinate a meno di un fattore $c \neq 0$.

$\star$ *Ricoprimento affine standard di* $\mathbf{P}^n$

Siano $(Z_0 : \cdots : Z_n)$ coordinate proiettive su $\mathbf{P}^n_k$, definiamo

$$k^n_i := \{z \in \mathbf{P}^n_k \ / \ z_i \neq 0\}, \quad i = 0 \ldots n.$$

e consideriamo la mappa $a_i : k^n_i \longrightarrow k^n$ definita dalle equazioni

$$X_j = \frac{Z_j}{Z_i}, \quad j = 0 \ldots i-1 \ , \ X_{j-1} = \frac{Z_j}{Z_i}, \quad j = i+1 \ldots n+1,$$

dove $(X_1 \ldots X_n)$ sono coordinate su k^n. a_i é biunivoca e inoltre

$$\mathbf{P}^n_k = \bigcup_{i=0\ldots n} k^n_i.$$

Definizione

La famiglia $\{k^n_i, \ i = 0 \ldots n\}$ *é il ricoprimento affine standard di* $\mathbf{P}^n_k$.

$\star$ $\mathbf{P}^n_k$ é ricoperto *in modo naturale* da tali spazi affini k^n_i, $i = 0 \ldots n$.

⋆ *Completamento proiettivo e varietá proiettive*

Sia $V \subset k^n$ una varietá algebrica affine, definita dalle equazioni

$$F_1(X_1, \ldots, X_n) = \cdots = F_s(X_1, \ldots, X_n) = 0.$$

Posto $X_j = \frac{Z_j}{Z_0}$, $j = 1 \ldots n$, identifichiamo k^n con $k_0^n \subset \mathbf{P}_k^n$. Dopo di che i punti di $\mathbf{P}_k^n - k_0^n$ vanno pensati come *punti all'infinito* di k^n.
Sostituendo X_j con $\frac{Z_j}{Z_0}$ in F_m e moltiplicando per $Z_0^{deg\ F_m}$ otteniamo *polinomi omogenei* $\overline{F}_m(Z_0, \ldots, Z_n)$, $m = 1 \ldots s$.
Su k_o^n essi annullano esattamente le coordinate proiettive dei punti di V. Su $\mathbf{P}_k^n - k_0^n$ essi annullano eventualmente altri punti *all' infinito.*

Definizione

Il completamento proiettivo $\overline{V}$ *di* V *é il sottoinsieme di* $\mathbf{P}_k^n$ *definito da*

$$\overline{F}_1(Z_0, \ldots, Z_n) = \cdots = \overline{F}_s(Z_0, \ldots, Z_n) = 0.$$

Le equazioni da utilizzare su $\mathbf{P}_k^n$ sono necessariamente omogenee.

Definizione

Una varietá algebrica proiettiva $V \subset \mathbf{P}_k^n$ é un sottoinsieme definito da equazioni polinomiali omogenee

$$\overline{F}_1(Z_0, \ldots, Z_n) = \cdots = \overline{F}_s(Z_0, \ldots, Z_n) = 0.$$

Intuitivamente possiamo dire che una varietá proiettiva puó essere vista, (in molti modi poiché le carte affini su $\mathbf{P}_k^n$ sono piú di una), *come una varietá affine completata della sua parte all' infinito.*
Solitamente, per fissare le abitudini, lavoreremo sulla carta affine k_0^n di $\mathbf{P}_k^n$ considerando i punti con coordinata $Z_0 = 0$ come punti all' infinito. Dal punto di vista formale, la scelta di una o di un altra carta affine é indifferente.

Esempi/Esercizi

- *Determinare il completamento proiettivo delle seguenti ellisse, iperbole e parabola*

$$X_1^2 + X_2^2 = 1 \ , \ X_1 - X_2 = 1 \ , \ X_2 = X_1^2$$

di $\mathbf{R}^2$. *Determinare i punti sulla retta all' infinito* $Z_0 = 0$.

- *Sia* $C \subset \mathbf{P}^2_{\mathbf{R}}$ *la conica proiettiva di equazione*

$$Z_1^2 + Z_2^2 - 2Z_1Z_0 - 2Z_2Z_0 + Z_0^2 = 0.$$

Descrivere le tre coniche affini $\Gamma_i = C \cap \mathbf{R}^2_i, i = 0, 1, 2$, *determinate da* C *sulle carte affini standard di* $\mathbf{P}^2_{\mathbf{R}}$. *Indicare i punti all' infinito.*

Le nozioni considerate per varietá affini si definiscono in modo del tutto analogo per varietá proiettive. Per le nozioni di sottovarietá e di aperto di Zariski basta sostituire l' aggettivo affine con l' aggettivo proiettivo.

Sia $X \subset \mathbf{P}_k^n$ una varietá proiettiva. Un *germe di funzione razionale* é una funzione $\frac{\overline{p}}{\overline{q}} : U \longrightarrow k$ dove $\overline{p}, \overline{q} \in k[Z_0 \dots Z_n]$ sono omogenei e di grado uguale e $U \subset X$ é un aperto di Zariski. Le definizioni di campo $k(X)$ delle funzioni razionali e mappa razionale seguono di conseguenza.

Sia $X_0 = k_0^n \cap X$, passando in coordinate affini $X_i = \frac{Z_i}{Z_0}$, $\frac{\overline{p}}{\overline{q}}$ definisce un germe di funzione razionale $\frac{p}{q} : U \cap X_0 \longrightarrow k$ su X_0. In tal modo ogni $f : X \dashrightarrow k$ determina una funzione razionale $f_0 : X_0 \dashrightarrow k$ e viceversa. Di fatto $k(X)$ e $k(X_0)$ possono essere considerati come lo stesso campo,

$$k(X) = k(X_0),$$

i cui elementi ammettono descrizioni diverse: con coordinate affini o proiettive. Definendo la dimensione di X come grado di trascendenza di $k(X)$, ne segue $dim\ X = dim\ X_0$.

Diamo un cenno di due dimostrazioni del seguente

Teorema

Ogni curva algebrica C é birazionale ad una curva piana.

Per via algebrica:
Sia $\phi : C \to k^2$ una mappa razionale non costante definita da

$$X = p \ , \ \ Y = q$$

dove $p, q \in k(C)$. Poiché $dim\ C = 1$ p e q sono algebricamente dipendenti in $k(C)$. Quindi esiste $F \in k[X, Y]$ *non nullo* tale che $F(p, q) = 0$. Eliminando fattori non necessari si puó supporre che

$$D := \phi(C) = \{F(X, Y) = 0\}.$$

'E possibile una scelta conveniente di p, q. Ció segue dal teorema dell' elemento primitivo che riformuliamo ad hoc per $k(C)$:

Theorem

Sia p algebricamente indipendente su $k(C)$. Allora esiste $q \in k(C)$ tale che $1, q, \ldots, q^{d-1}$ é una base di $k(C)$ come spazio vettoriale su $k(p)$.

Sia ϕ definita da p, q scelti come nel teorema, consideriamo la funzione

$$\phi^* : k(D) \to k(C)$$

che a $h \in k(D)$ associa $h \cdot \phi := \phi^*(h)$. Si ha $\phi^*(X) = p$ e $\phi^*(Y) = q$.

Poiché $1 \ldots q^{d-1}$ é una base di $k(C)$ su $k(p)$, per ogni $f \in k(C)$ si ha

$$f = c_0 + c_1 q + \cdots + c_{d-1} q^{d-1} = \phi^*(c_0(X) + c_1(X)Y + \cdots + c_{d-1} Y^{-1}).$$

Ma allora $\phi^*(k(D)) = k(C)$ e ció equivale a che $\phi : C \dashrightarrow D$ sia birazionale.

Per via geometrica:
Tra le piú semplici mappe razionali ci sono le proiezioni lineari

$$\pi : k^n \dashrightarrow k^2$$

definite da equazioni lineari. Per $n = 3$ π avrá equazioni

$$aX_1 + bX_2 + cX_3 + d = Y_1 \ , \ eX_1 + fX_2 + gX_3 + h = Y_2.$$

Sia $y \in k^2$: $\pi^{-1}(y) := L_y$ é una retta. Sia $C \subset k^3$ e $D = \pi(C)$:

$\pi : C \to D$ birazionale $\iff L_y \cap C = \{y\}$, y punto generico su C.

In altri termini: L_y é secante ma non multisecante a C.

Esempi/Esercizi

Si verifichi che tale proprietá é soddisfatta per la curva i cui punti hanno coordinate (t, t^2, t^4) *in* k^3*, ma non per tutte le possibili scelte di* π*.*

Supponiamo di avere una curva algebrica proiettiva $C \subset \mathbb{P}^2_k$.

Che cosa é la forma di C?

L' intuzione reale suggerisce che C ha la forma di una linea curva.
Prendiamo una C definita da una facile equazione $F \in \mathbf{Z}[X_0, X_1, X_2]$

$$X_1^2 + X_2^2 = X_0^2$$

e studiamone la forma nel caso di $k = \mathbf{Q},\ \mathbf{R},\ \mathbf{C}$. Sia

$$\Gamma_k = C \cap k_0^2.$$

Γ_k é la parte *non all' infinito* di C di equazione,

$$X^2 + Y^2 = 1,$$

$(X = \frac{X_1}{X_0},\ Y = \frac{X_1}{X_0})$.

Che cosa é la forma di Γ_k?

.

$k = \mathbf{Q}$: *Le terne pitagoriche.*
Le equazioni parametriche razionali di $\Gamma_{\mathbf{Q}}$ ne descrivono i punti:

$$X = \frac{1 - t^2}{1 + t^2} \ , \ \frac{2t}{1 + t^2}$$

Le soluzioni della equazione sono le coppie ordinate di numeri razionali $(\frac{a}{c}, \frac{b}{c})$ tali che

$$a^2 + b^2 = c^2.$$

Una terna di interi (a, b, c) come sopra si chiama terna pitagorica.

Esempi/Esercizi

Provare che una delle due coniche ha infiniti punti e l' altra nessuno.

$$X^2 + Y^2 = 2 \ , \ X^2 + Y^2 = 3.$$

$k = \mathbf{R}$ La circonferenza
In questo caso chiedersi quale é la forma di $\Gamma_{\mathbf{R}}$ é piú giustificato ed é coerente con la nostra intuizione di esseri viventi in uno spazio affine reale ed euclideo.

Su $\mathbf{R}^2$ abbiamo la nozione standard di distanza. Fissata questa distanza s, la forma di $\Gamma_{\mathbf{R}}$ é quella della circonferenza di raggio di lunghezza 1.

$k = \mathbf{C}$: *La sfera*

Le novitá, in un certo senso, nascono con il caso complesso. Osserviamo quanto segue:

(1) C interseca la retta *all' infinito* $\{X_0 = 0\}$ nei due punti *ciclici*

$$I_1 = (0 : 1 : i) \ , \ I_2 = (0 : 1 : -i).$$

(2) $\Gamma_{\mathbf{C}}$ é la curva proiettiva C privata dei dei suoi due punti I_1, I_2.

$k = \mathbf{C}$
(3) Per descrivere $\Gamma_{\mathbf{C}}$ possiamo cercare di ricorrere all' intuizione reale seppur in quattro dimensioni.

X, Y sono coordinate complesse dunque possiamo porre

$$X = a + ib \ , \ Y = c + id \quad \text{dove } (a, b, c, d) \in \mathbf{R}^4$$

In $\mathbf{R}^4$ otteniamo allora due equazioni che descrivono $\Gamma_{\mathbf{C}}$:

$$a^2 + c^2 - b^2 - d^2 = 1 \ , \ ab + cd = 0.$$

Che cosa é il sottoinsieme di $\mathbf{R}^4$ definito da queste due equazioni?

$k = \mathbf{C}$

Consideriamo in $\mathbf{C}^2$ il fascio di rette paralle

$$Y = iX + t, \quad t = t_1 + it_2 \in \mathbf{C}.$$

La retta $L_t = \{Y = iX + t\}$ interseca $\Gamma_{\mathbf{C}}$ nel punto di coordinate

$$X = \frac{1 - t^2}{2t} + t = , \ Y = \frac{1 - t^2}{2it}.$$

Tali uguaglianze sono le equazioni di una mappa razionale

$$\psi : \mathbf{C} \dashrightarrow \Gamma_{\mathbf{C}}$$

che risulta biunivoca tra $\mathbf{C} - \{O\}$ e $\Gamma_{\mathbf{C}}$.

$k = \mathbf{C}$
(a, b, c, d) si scrive in funzione di (t_1, t_2) usando le equazioni di ψ:

$$a = , \ b = , \ c = , \ d = .$$

Identificando $\mathbf{C}$ con coordinata $t = t_1 + it_2$ e $\mathbf{R}^2$ con coordinate (t_1, t_2) possiamo considerare ψ come una mappa razionale

$$\psi : \mathbf{R}^2 \dashrightarrow \Gamma_{\mathbf{C}} \subset \mathbf{R}^4$$

biunivoca tra $\mathbf{R}^2 - \{O\}$ e $\Gamma_{\mathbf{C}}$.

Le funzioni reali di variabili reali t_1, t_2 che definiscono ψ sono continue e lo sono anche quelle che definiscono ψ^{-1}:

Proposizione

$\mathbf{R}^2 - \{O\}$ *e* $\Gamma_{\mathbf{C}}$ *sono omeomorfi o topologicamente equivalenti.*

Preciseremo in seguito.

$k = \mathbf{C}$
Sia ora $\Sigma \subset \mathbf{R}^3(t_1, t_2, t_3)$ una sfera appoggiata in $S := (0, 0, 0)$ sul piano $t_3 = 0$ e sia $N = (0, 0, 1)$. La *proiezione stereografica*

$$\pi : \Sigma - \{N\} \to \mathbf{R}^2.$$

di centro N. π é biunivoca quindi lo é anche

$$\psi \cdot \pi : \Sigma - \{N, S\} \leftrightarrow \Gamma_{\mathbf{C}}$$

$\Gamma_{\mathbf{C}}$ é topologicamente equivalente a una sfera bucata in due punti.
C si ottiene da $\Gamma_{\mathbf{C}}$ aggiungendo i due punti *all' infinito* I_1 e I_2.
Ció suggerisce quanto segue:

Teorema

C é topologicamente una sfera 2-dimensionale Σ.

Procediamo con una curva $C \subset \mathbf{P}^2_{\mathbf{C}}$ definita da una equazione omogenea $F \in \mathbf{Z}[X_0, X_1, X_2]$. Indicheremo con C_k la curva definita dalla equazione F in $\mathbf{P}^2_k$, $k = \mathbf{Q}, \mathbf{R}$. Si noti che

$$\mathbf{P}^2_{\mathbf{Q}} \subset \mathbf{P}^2_{\mathbf{R}} \subset \mathbf{P}^2_{\mathbf{C}}$$

e che

$$C_{\mathbf{R}} = \mathbf{P}^2_{\mathbf{R}} \cap C \ , \ C_{\mathbf{Q}} = \mathbf{P}^2_{\mathbf{Q}} \cap C.$$

Possiamo dire che $\Gamma_{\mathbf{R}}$ é la l' insieme dei *punti reali* di C e che $C_{\mathbf{Q}}$ e l' insieme dei suoi *punti razionali.*
Successivamente daremo qualche informazione sull' insieme $C_{\mathbf{Q}}$.
Per capire la forma della curva reale $C_{\mathbf{R}}$, di quella complessa C sarebbe necessario introdurre qualche nozione di topologia.

Definizione

Uno spazio topologico separato é un insieme $S \neq \emptyset$ sul quale é fissato un ricoprimento $\mathcal{U}$ con le seguenti proprietá:
(1) l'unione di elementi di $\mathcal{U}$ appartiene a $\mathcal{U}$,
(2) l'intersezione di un insieme finito di elementi di $\mathcal{U}$ appartiene a $\mathcal{U}$,
(3) $\forall x_1, x_2 \in S$, $x_1 \neq x_2$, esistono $U_1, U_2 \in \mathcal{U}$ tali che:

$$x_1 \in U_1 \ , \ x_2 \in U_2 \ , \ U_1 \cap U_2 = \emptyset.$$

Gli elementi di $\mathcal{U}$ si dicono *aperti* di S e i loro complementari *chiusi.*

Definizione

(1) Una funzione $f : S \to T$ tra due spazi topologici si dice continua se la controimmagine di ogni aperto di T é un aperto di S,
(2) Se f é biunivoca e f^{-1} é continua si dice che f é un omeomorfismo. In tal caso i due spazi si dicono omeomorfi o topologicamente equivalenti.

Ancora qualche definizione:

- *S é connesso se non esistono due aperti non vuoti A_1, A_2 tali che $A_1 \cap A_2 = \emptyset$ e $A_1 \cup A_2 = S$.*
- *S é compatto se ogni successione $x_n,\ n \in \mathbf{N}$ di punti di S converge i.e. esiste $l \in S$ tale che: per ogni aperto A contenente l esiste n_0 tale che $x_n \in A,\ \forall n > n_o$.*
- *Un sottospazio topologico é un sottoinsieme non vuoto $T \subset S$ la cui famiglia di aperti é $\mathcal{U}_T := \{U \cap T,\ U$ aperto di $S\}$.*

Piú che gli spazi topologici ci interessano le varietá topologiche:

Definizione

Una varietá topologica V di dimensione d é uno spazio topologico separato tale che: per ogni $x \in V$ esiste un aperto A contenente x e omemorfo a $\mathbf{R}^d$.

Esempi/Esercizi

- $k = \mathbf{R}$, $\mathbf{C}$
- *Topologia standard su* k^d*: gli aperti sono i polidischi*

$$U(C, r) := \{t = (t_1, \ldots, t_n) \in k^d \ / \ \sqrt{\sum_{j=1\ldots d} \mid t_j - c_j \mid^2} < r\},$$

le loro unioni e le loro intersezioni finite.

- *Topologia standard su* $\mathbf{P}^n_k$*: gli aperti sono*
  - $k^n_0, \ldots, k^n_n$*,*
  - gli aperti della topologia standard su k^n_j*,*
  - le unioni ed intersezioni finite dei precedenti insiemi.

Esempi/Esercizi

- $k = \mathbf{R}, \mathbf{C}$
- $\mathbf{P}^n_{\mathbf{R}}$ *é una varietá topologica di dimensione* n,
- $\mathbf{P}^n_{\mathbf{C}}$ *é una varietá topologica di dmensione* $2n$,
- *una sfera* $S^2 \subset \mathbf{R}^3$ *é una varietá topologica,*
- S^2 *é omeomorfa a* $\mathbf{P}^1_{\mathbf{C}}$,
- *descrivere* $\mathbf{P}^2_{\mathbf{R}}$, *(piano proiettivo reale / bottiglia di Klein)*
- *il toro* $T \subset \mathbf{R}^3$ *é una superficie topologica.*

Teorema

Sia S una varietá topologica compatta e connessa di dimensione uno. Allora S é topologicamente equivalente a una circonferenza reale.

Teorema

Sia S una superficie topologica connessa e compatta. Allora S é topologicamente equivalente ad una delle seguenti superfici:

- *la sfera S^2,*
- *il toro T*
- *il piano proiettivo reale $\mathbf{P}^2_{\mathbf{R}}$*
- *la somma connessa di g tori*
- *la somma connessa di g piani proiettivi reali.*

Definizione

Il genere g di S é il numero dei suoi 'manici' o 'buchi'.

Continuiamo il nostro studio di $C \subset \mathbf{P}^2_k$, con $k = \mathbf{Q}, \mathbf{R}, \mathbf{C}$ e avendo assegnato $F \in k[X_0, X_1, X_2]$ come equazione di C.

$\star$ *D'ora i poi diremo che C ha grado d se tale é il grado di F.*

Per $k = \mathbf{R}, \mathbf{C}$ la curva C é un sottospazio della varietá topologica $\mathbf{P}^n_k$:

Per $k = \mathbf{R}, \mathbf{C}$ é la curva C una varietá topologica?

Preliminarmente ricordiamo che $p \in k^2_0$ si dice *punto singolare di C* se

$$F(p) = \frac{\partial F}{\partial X}(p) = \frac{\partial F}{\partial Y}(p) = 0$$

$(X = \frac{X_1}{X_0}\ ,\ Y = \frac{X_2}{X_0})$. Tale condizione equivale alla seguente

$$\frac{\partial F}{\partial X_0}(p) = \frac{\partial F}{\partial X_1}(p) = \frac{\partial F}{\partial X_2}(p)$$

sostituendo ora X_0, X_1, X_2 con le coordinate proiettive di p.

Definizione

p é un punto singolare di C se $\frac{\partial F}{\partial X_i}(p) = 0, \quad i = 0, 1, 2.$

Equivalentemente, per ogni carta affine standard k_j^n a cui p appartenga, p annulla l' equazione in coordinate affini di C e le sue derivate parziali.

$\star$ *L'insieme dei punti singolari si indica con Sing C.*

Sia $p = (p_1, p_2) \in Sing\ C \cap k_0^2$, lo sviluppo in serie di Taylor dá

$$F(X - p_1, Y - p_2) = F_m + F_{m+1} + \cdots + F_d$$

dove $F_m \ldots F_d$ sono omogenei in $(X - p_1), (Y - p_2)$, $m \geq 2$ e $F_m \neq 0$.

$\star$ *p si dice punto singolare di molteplicitá m.*

Il *Teorema delle funzioni implicite* e la conoscenza di $Sing\ C$ portano la risposta, nei casi sia reale che complesso, alla domanda posta:

$$Quando\ C \subset \mathbf{P}^2_k\ é\ una\ varietá\ topologica?$$

Teorema

- $k = \mathbf{R}$: $C - Sing\ C$ *é una varietá topologica di dimensione uno*
- $k = \mathbf{C}$: $C - Sing\ C$ *é una varietá topologica di dimensione due,*

Inoltre: $C \subset \mathbf{P}^2_k$ é *compatto.* Se $k = \mathbf{C}$ allora $C - Sing\ C$ é *connesso.*

$k = \mathbf{R}$

Sia $p \in C - Sing\ C$. Supponiamo $p = (p_1, p_2)$ in coordinate affini X, Y. p non é singolare dunque non annulla ogni derivata parziale di F:

$$\frac{\partial F}{\partial Y}(p) \neq 0.$$

Per il teorema delle funzioni implicite esiste una funzione C^∞

$$\phi : (p_1 - a, p_1 + a) \to (p_2 - b, p_2 + b)$$

invertibile e tale che

$$C \cap (p_1 - a, p_1 + a) \times (p_2 - b, p_2 + b)$$

é l'insieme U_p dei punti $(t, \phi(t))$, $t \in (p_1 - a, p_1 + a)$. A_p é un aperto di C contenente p. U_p é omeomorfo a un intervallo aperto reale mediante

$$\Phi : U_p \to (p_2 - b, p_2 + b)$$

che a $(t, \phi(t))$ associa $\phi(t)$.

$k = \mathbf{C}$
Il caso compesso é del tutto simile: esiste un teorema delle funzioni implicite. Esso dice che esiste una funzione analitica

$$\phi : D(p_1, a) \to D(p_2, b),$$

invertibile e tale che l' insieme

$$C \cap D(p_1, a) \times D(p_2, b) = \{(t, \phi(t), t \in D(p_1, a)\}$$

é omeomorfo al disco aperto $D(p_2, b) \subset \mathbf{C}$, via la funzione Φ definita come sopra.

(* $D(c, r)$ indica il disco aperto $\{t \in \mathbf{C} \ / \ \mid t - c \mid < r\} \subset \mathbf{C} = \mathbf{R}^2$)

$\star$ *Topologia delle curve piane reali o complesse*

Traiamo qualche conclusione sulla topologia di C. Supporremo $Sing\ C = \emptyset$, quindi C é una varietá topologica compatta.

$k = \mathbf{R}$

L' unica varietá topologica compatta e connessa di dimensione 1 é S^1 che chiameremo qui *circuito*. C é unione di circuiti disgiunti e questi sono in numero finito a causa della compattezza di C. Sia d il grado di C:

Quanti sono i circuiti di C ?

Teorema (Teorema di Harnack)

Il numero dei circuiti di $\Gamma_{\mathbf{R}}$ *é limitato dal valore* $g + 1$ *dove*

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

$k = \mathbf{C}$
C é una superficie topologica compatta e connessa. Quindi é topologicamente equivalente ad una delle superfici elencate.

A quali di esse puó essere omeomorfa C?

A quelle cosiddette orientabili:

- *La sfera S^2,*
- *il toro T,*
- *la somma connessa di g tori.*

Rimane il caso *Sing* $C \neq \emptyset$: che cosa si puó dire in questo caso?

Teorema

Sia C *una curva definita su* $k = \mathbf{R}, \mathbf{C}$. *Allora esiste una curva proiettiva*

$$N \subset \mathbf{P}_k^r$$

tale che:
(1) N *é birazionale a* C,
(2) come sottospazio di $\mathbf{P}_k^r$ N *é una varietá topologica.*
(3) $k = \mathbf{R}$: N *é unione di u nuero finito di circuiti disgiunti,*
(4) $k = \mathbf{C}$: N *é una superficie topologica orientabile.*

(*) La nozione di punto singolare puó essere definita per ogni curva C. Pi'u in generale esiste sempre una curva proiettiva N birazionale a C e *non singolare* i.e. tale che *Sing* $N = \emptyset$.
$\star$ N si dice *normalizzazione di* C.

Sia C una curva e sia $B(C)$ l' insieme di tutte le curve *birazionali* a C:

Esistono proprietá comuni alle curve di $B(C)$ *?*

La risposta viene insieme dall'algebra e dalla topologia.

Algebra: Sia $D \in B(C)$ piana e proiettiva di grado m e sia

$$g(D) := \frac{1}{2}(m-1)(m-2) - \sum_{p \in Sing\ D} \delta_p. \ (*)$$

Teorema

$g(D)$ é costante al variare di D in $B(C)$.

(*) δ_p é un intero positivo ben definito, $\forall p \in Sing\ D$. $Sing\ D$ é finito.

Topologia: Sia $k = \mathbf{C}$. In $B(C)$ il sottoinsieme delle curve proiettive$N$ che sono varietá topologiche (compatte e connesse) é costituito da superfici topologiche dello stesso genere. Sia

$$g(N) := \text{ il genere topologico di } N.$$

Anche questo carattere numerico é allora un dato associato a $B(C)$ e o a sue singole curve. La conclusione é quella attesa:

Teorema

$g(N) = g(D)$, *qualunque sia la curva proiettiva* $D \in B(C)$.

Definizione

Il genere geometrico $g(C)$ di una curva (proiettiva) C é il valore

$$g(D) = \frac{1}{2}(m-1)(m-2) - \sum_{p \in Sing\ D} \delta_p$$

di una qualunque curva proiettiva piana birazionale a C.

- *Se C é una curva proiettiva complessa $g(C)$ é il genere topologico della sua normalizzazione N,*
- *(teorema di Harnack) il numero di circuiti di C é al piú $g+1$, dove g é il genere geometrico della complessificata (*) di C*

$\star$ Nel seguito studieremo in concreto curve di genere zero ed uno.

(*) La complessificata $X \subset \mathbf{P}^n_{\mathbf{C}}$ di $C \subset \mathbf{P}^n_{\mathbf{R}}$ é la curva proiettiva complessa formata dai punti le cui coordinate soddisfano le equazioni di C.

Definizione

Una curva C, definita su k, si dice razionale se é birazionale a k.

Poiché k e $\mathbf{P}^1_k$ sono birazionali il genere di una curva razionale é zero. Un esempio di curva razionale lo abbiamo giá incontrato: $X^2 + Y^2 = 1$ che ha equazioni parametriche birazionali

$$X = \frac{1 - t^2}{2t} + t = , \ Y = \frac{1 - t^2}{2it}.$$

sono equazioni parametriche birazionali di $X^2 + Y^2 = 1$ In realtá

Proposizione

Ogni conica C contenente almeno un punto non singolare é razionale. Qualunque sia il campo su cui essa sia definita.

⋆ *Quali curve ammettono equazioni parametriche razionali?*

Esempi/Esercizi

- *Curve monoidali.* Una curva monoidale C é il luogo degli zeri di un polinomio irriducibile $F(X_0, \ldots, X_2) = X_0A + B$, dove A e B sono omogenei di grado $d-1$ e d in X_1, X_2.
  C é razionale: l'equazione di C in k_0^2 é $A(X,Y) + B(X,Y) = 0$, dove A e B hanno gradi $d-1$ e d. Si consideri il fascio di rette $Y = tX$ e si determini la intersezione della retta $Y = tX$ con C. Si otterra' l'origine O e il punto p_t di coordinate
  $$X = -\frac{B(1,t)}{A(1,t)}\ , Y = -t\frac{B(1,t)}{A(1,t)}.$$

Esempi/Esercizi

- *Cubica nodata o folium di Descartes.* L' equazione é $Y^2 - X^2 = X^3$. Equazioni parametriche birazionali:

$$X = t^2 - 1, Y = t(t^2 - 1).$$

  Determinare la forma del folium di Descartes e dove la mappa non é biunivoca.
- Cubica con cuspide ordinaria. L' equazione é $Y^2 = X^3$. Determinare le equazioni parametriche. Verificare che queste determinano un omeomorfismo tra C e $\mathbf{P}^1_k$. Dedurre, nel caso $k = \mathbf{C}$, che C é omeomorfa alla sfera S^2.
- Provare che non esistono cubiche con due punti singolari distinti o con un punto singolare p di molteplicitá ≥ 3.

Esempi/Esercizi

- *Quartiche con tre punti doppi.* Non sempre basta considerare un fascio di rette per un punto singolare per determinare equazioni parametriche razionali di una curva. Si consideri ad esempio i $\mathbf{P}^2_{\mathbf{C}}$ la quartica di equazione

$$X_1^2X_2^2 + X_0^2X_2^2 + X_0^2X_1^2 = 0.$$

Si verifichi che C ha tre punti doppi ordinari, e nessuna altra singolaritá, in $(1:0:0)$, $(0:1:0)$, $(0:0:1)$. Si dimostri che C é birazionale alla curva piana $X_0^2 + X_1^2 + X_2 = 0$. Se ne deduca che C é razionale.

Esempi/Esercizi

- *Quartiche razionali di vario tipo.* Si trovino equazioni parametriche razionali per i bifogli e la lemniscata di Bernoulli definiti dalle seguenti equazioni:
  (1) bifoglio $(X^2 + Y^2)^2 - 8XY = 0$,
  (2) bifoglio aperto $(X^2 - Y^2)^2 - XY = 0$
  (3) lemniscata di Bernoulli $X^2 + Y^2)^2 - XY = 0$

Proposizione

Ogni curva C di genere zero é razionale.

Lo schema di una delle possibili dimostrazioni é coerente con gli esempi nei quali abbiamo utilizzato un fascio di rette passante per un punto singolare allo scopo di *mettere in corrispondenza birazionale le rette del fascio con i punti di C.* Non si usa piú un fascio di rette $Y = tX$ ma un fascio di curve piane passante per opportuni punti di C.
La discussione sulle curve razionali ci porta in modo naturale a un' altra questione: sia

$$\psi : k \to C$$

una mappa razionale dominante non birazionale. Esistono semplici esempi di queste mappe. *Basta prendere equazioni parametriche birazionali qualsiasi in t e sostituire t con u^m, $m \geq 2$.*

Definizione

Una varietá algebrica V si dice unirazionale se ammette equazioni parametriche razionali ovvero una mappa razionale dominante $\phi : k^d \to V$.

Una curva unirazionale é razionale?

La risposta fu data nel 1876 dal matematico e astronomo Jacob Lueroth.

Theorem (Teorema di Lueroth)

Ogni curva unirazionale é razionale.

Sono dunque equivalenti, per concludere, le seguenti condizioni:

- *C ha genere zero,*
- *C é birazionale a k,*
- *C ammette equazioni parametriche razionali.*

Da genere uno in poi nessuna curva ammette equazioni parametriche razionali!

Abbiamo studiato una serie di curve piane algebriche: sia nel piano proiettivo reale sia nel piano proiettivo complesso, trascurando in parte il caso del piani proiettivo sui razionali $\mathbf{P}^2_{\mathbf{Q}}$. Rimedieremo ora in parte, senza trascurare lo studio delle curve considerate nel caso reale e complesso.
Una cubica *non singolare*

$$C \subset \mathbf{P}^2_k$$

ha genere geometrico 1 per la formula del genere, dunque non é razionale.
(1) Nel caso $k = \mathbf{C}$ sappiamo che C é topologicamente un toro.
(2) Nel caso $k = \mathbf{R}$ il teorema di Harnack ci dice che C ha al piú 2 circuiti.
(3) Nel caso $k = \mathbf{Q}$ avremo modo di discutere alcuni aspetti interessanti.

Se $k = \mathbf{R}$ o $k = \mathbf{C}$ é possibile scrivere l' equazione di una conica in forma canonica, traendo qualche vantaggio. 'E possibile fare qualcosa di simile per le cubiche, il risultato si chiama *forma normale* o forma di Weierstrass della equazione di C. Qualunque sia il campo k consideriamo il sistema lineare completo $\mathbb{P}$ delle cubiche $C \subset \mathbf{P}^2_k$ é la seguente

$$c_0 Z_0^3 + c_1 Z_0^2 Z_2 + c_2 Z_0^2 Z_1 + c_3 Z_0 Z_2^2 + c_4 Z_0 Z_1^2 + c_5 Z_0 Z_1 Z_2 + c_6 Z_1^3 + c_7 Z_2^3 + c_8 Z_1^2 Z_2 + c_9 Z_1 Z_2^2 = 0.$$

In esso consideriamo il sottosistema lineare $\mathbb{P}_{3O}$ delle cubiche per le quali il punto $O = (1 : 0 : 0)$ é un punto di flesso con tangente inflessionale la retta all' infinito

$$\{Z_0 = 0\}.$$

Definizione

$p \in C$ é un punto di flesso con tangente inflessionale la retta L se l' indice di intersezione tra C e L in p é uguale a 3.

Per una cubica C questo equivale a dire che $C \cap L = \{p\}$. Imponendo questa condizione a C nel caso in cui L ha equazione $Z_0 = 0$ vediamo che essa é soddisfatta se e solo se $c_9 = c_8 = c_7 = 0$. $\mathbb{P}_{3O}$ é dunque il sistema lineare delle curve di equazione

$$c_0 Z_0^3 + c_1 Z_0^2 Z_2 + c_2 Z_0^2 Z_1 + c_3 Z_0 Z_2^2 + c_4 Z_0 Z_1^2 + c_5 Z_0 Z_1 Z_2 + c_6 Z_1^3 = 0.$$

Quelle che ci interessano sono quelle non singolari. Passando in coordinate affini X, Y su k_0^2 l' equazione diventa

$$c_0 + c_1 Y + c_2 X + c_3 Y^2 + c_4 X^2 + c_5 XY = -c_6 X^3.$$

D' altra parte l' espressione a sinistra dell' uguaglianza é l'equazione di una conica affine. Pertanto possiamo riscriverla eliminando il prodotto misto XY ovvero:

$$c_0 + c_1 Y + c_2 X + c_3 Y^2 + c_4 X^2 + c_5 XY = a + bX' + cY' + dX'^2 + eY'^2$$

dove X' e Y' sono opportuni *polinomi lineari omogenei in X e Y*. Sostituendo X con X' e Y con Y' l' equazione affine di C diventa

$$a + bX' + cY' + dX'^2 + eY'^2 = -c_6 X'^3.$$

Se $e = 0$ C diventa, come di é giá osservato, una curva razionale con un punto doppio all' infinito. Non é il nostro caso, quindi $e \neq 0$. Con un facile lavoro possiamo porre

$$Y' = Y'' + \frac{c}{2e} \ , \ X'' = X'$$

nel caso $d = 0$, oppure

$$Y' = Y'' + \frac{c}{2e} \ , \ X' = X'' + \frac{b}{2d}$$

nel caso $d \neq 0$.

Otterremo allora la seguente forma della equazione di C:

$$(a - \frac{c^2}{4e^2} - f) + dX''^2 + c_6X''^3 = eY''^2,$$

dove $f = \frac{b^2}{4d^2}$ se $d \neq 0$ e $f = 0$ se $d = 0$. Abolendo $''$ e indicando in modo piú semplice i coefficienti concludiamo che l'equazione di C nel piano k_0^2 é

$$Y^2 = \alpha X^3 + \beta X^2 + \gamma$$

dove $\alpha, \beta, \gamma \in k$.

Possiamo chiamare tale equazione *forma normale generalizzata* della equazione affine di C. Abbiamo dunque provato il seguente

Theorem

Sia $C \subset \mathbf{P}^2_k$ una cubica non singolare. Se esiste un punto di flesso su C allora la sua equazione si puó scrivere in forma normale come segue:

$$Y^2 = \alpha X^3 + \beta X^2 + \gamma.$$

Si noti che $\alpha \neq 0$. Esaminiamo la situazione nei casi $k = \mathbf{C},\ \mathbf{R},\ \mathbf{Q}$:

(1) $k = \mathbf{C}$. Per il teorema fondamentale dell' algebra il polinomio $\alpha X^3 + \beta X^2 + \gamma$ ha una radice complessa λ. Per il teorema di Ruffini

$$\alpha X^3 + \beta X + \gamma = \alpha(X - \lambda)Q(X)$$

dove $Q(X)$ ha grado due e coefficienti complessi e coefficiente direttore 1. Allora $Q(X) = (X - r_1)(X - r_2)$ con $r_1, r_2 \in \mathbf{C}$. Le tre radici r, r_1, r_2 sono distinte: in caso contrario C sarebbe singolare.'E possibile determinare p e q in modo tale che

$$pr_1 + q = 0\ ,\ \ pr_2 + q = 1.$$

Il sistema ammette una e una sola soluzione poiché $r_1 \neq r_2$.

Ponendo infine

$$Y = \frac{Y'}{\sqrt{\alpha}} \ , \ X = \frac{X' - q}{p}$$

possiamo riscrivere l' equazione nella forma nota come

Forma normale di Weierstrass:

$$Y'^2 = X'(X' - 1)(X' - \lambda).$$

(2) $k = \mathbf{R}$. $\alpha X^3 + \beta X^2 + \gamma$ é un polinomio di grado 3 a coefficienti reali. 'E noto che esso ha *almeno* una radice reale λ. Per il teorema di Ruffini

$$Y^2 = \alpha(X - \lambda)Q(X)$$

dove $Q(X)$ é un polinomio di grado due a coefficienti reali. Se Q ha due radici reali distinte r_1, r_2 possiamo procedere come nel caso precedente. Possiamo porre

$$Y = \frac{Y'}{\sqrt{\alpha}} \ , \ X = \frac{X' - q}{p}$$

se $\alpha > 0$ oppure

$$Y = \frac{Y'}{\sqrt{-\alpha}} \ , \ X = \frac{X' - q}{p}$$

se $\alpha < 0$. Infine l'equazione si riscrive nella forma

$$Y^2 = \mp X'^2(X' - 1)(X' - \lambda).$$

Lo studio del grafico di questa curva piana reale porta alla seguente conclusione:

⋆ *C ha due circuiti, uno é un ovale limitato e simmetrico rispetto all' intervallo* $[0,1]$ *dell' asse X. L'altro é illimitato e si chiude all'infinito nel punto di flesso O. Continuando la descrizione osserviamo che $Q(X)$ non ha una radice doppia: se no C sarebbe singolare. L' ultima possibilitá rimasta é che $Q(X)$ abbia solo radici complesse e non reali. In questo caso abbiamo una sola possibilitá di migliorare ancora l' equazione: poniamo $X' = (X - \lambda)$ e $Y' = \frac{Y}{\sqrt{\alpha}}$ o $Y' = \frac{Y}{\sqrt{\alpha}}$ a seconda che sia $\alpha > 0$ o $\alpha < 0$. Allora*

$$Y'^2 = \mp X'^2 Q(X').$$

⋆ *In questo caso C ha un solo circuito che si chiude all' infinito nel punto di flesso O.*

Tutta la descrizione precedente riguarda una cubica non singolare dotata di un punto di flesso O con tangente inflessionale la retta all' infinito. Che cosa si puó dire per le altre cubiche? Non é troppo difficile dimostrare il seguente teorema, anche se per brevitá la dimostrazione é omessa:

Theorem

Sia $k = \mathbf{C}$ o sia $k = \mathbf{R}$. Allora C ha un punto di flesso.

Sia p tale punto di flesso. Con una semplice sostituzione

$$\begin{pmatrix} Z_0 \\ Z_1 \\ Z_2 \end{pmatrix} = M \begin{pmatrix} Z_0' \\ Z_1' \\ Z_2' \end{pmatrix}$$

é possibile fare in modo che, nelle nuove coordinate $(Z_0' : Z_1' : Z_2')$ il punto p sia il punto $(1 : 0 : 0)$ e la tangente inflessionale sia $Z_0' = 0$. *Dopo avere effettuato questa sostituzione di variabili la descrizione della curva C é esattamente quella precedente.*

(3) $k = \mathbf{Q}$ Veniamo ora al caso di una cubica del piano proiettivo sui razionali.

- *'E possibile che non ci siano punti di flesso?*
- *C puó essere un insieme vuoto o finito?*
- *Come descrivere i punti di C se C é un insieme infinito?*

Per quanto riguarda le prime due domande la risposta é positiva. In particolare, per quanto riguarda la seconda, osserviamo che il primo caso del teorema di Fermat riguarda la cubica di $\mathbf{P}^2_{\mathbf{Q}}$ di equazione affine

$$X^3 + Y^3 = 1.$$

Eulero ha dimostrato che le uniche soluzioni razionali di questa equazione sono $(1, 0)$ e $(0, 1)$. Passando in coordinate proiettive i punti di C sono tre: $(1 : 1 : 0)$, $(1 : 0 : 1)$, $(0 : 1 : -1)$. Si tratta di un insieme finito e di tre punti di flesso. Possono comunque essere fatti molti altri esempi in cui non ci sono punti o non ci sono flessi.

Il caso $k = \mathbf{Q}$ riguarda *l'aritmetica delle cubiche piane,* in altre parole quella che viene chiamata *l' aritmetica delle curve ellittiche.*
Per definizione una curva ellittica é una curva di genere geometrico uno. Si dimostra che essa é sempre birazionale ad una cubica piana.

Diversamente dalle altre curve, le cubiche

$$C \subset \mathbf{P}_k^n$$

hanno una particolare ricchezza, di tipo algebrico e geometrico insieme. Qualunque sia il campo k é possibile infatti considerare su C una *operazione di somma* dei punti di C dotata di particolare importanza e significato. Tale operazione di somma si puó definire nello stesso modo qualunque sia il campo k su cui si sta lavorando. A condizione naturalmente che la cubica C sia non vuota. Questa operazione ci porta, nel caso $k = \mathbf{Q}$, a costruire eventualmente altri punti non appena se ne conosca qualcuno.

Supponiamo ad esempio che sia $P \in C$ e indichiamo con nP la somma di P con se stesso n volte. L' insieme

$$\mathbf{N}P := \{nP,\ n \geq 1\}$$

ci fornirá altri punti di C, a meno che P non sia il punto O che é lo zero di questa somma. In qualche caso potrá succedere che tale insieme, nonostanze le apparenze, sia finito. L' operazione in questione infatti porta in certi casi ad avere $nP = O$ e in tal caso l' insieme $\mathbf{N}P$ si riduce alla successione di punti $P, 2P, \ldots, (n-1)P, O$ e poi si ripete tal quale.

Vediamo di descrivere, per un campo k qualsiasi ma prenderemo come esempio su cui lavorare il caso $k = \mathbf{R}$, l'operazione di somma che si definisce su una cubica. Poi enunceremo alcuni teoremi che usano tale somma per dire quacosa sui punti di una cubica

$$C \subset \mathbf{P}^2_{\mathbf{Q}}.$$

$\star$ *La somma sulla cubica*

Indicheremo con $\oplus$ l'operazione di somma su una cubica C.

Teorema (Teorema di Mordell)

Sia $C \subset \mathbf{P}^2_{\mathbf{Q}}$ *una cubica. Se l' insieme dei punti di* C *non é vuoto esistono* r *punti*

$$P_1 \dots P_r \in C$$

tali che $\forall P \in C$*:*

$$P = m_1 P_1 \oplus \cdots \oplus m_r P_r$$

con $m_1 \dots m_r \in \mathbf{Z}$.