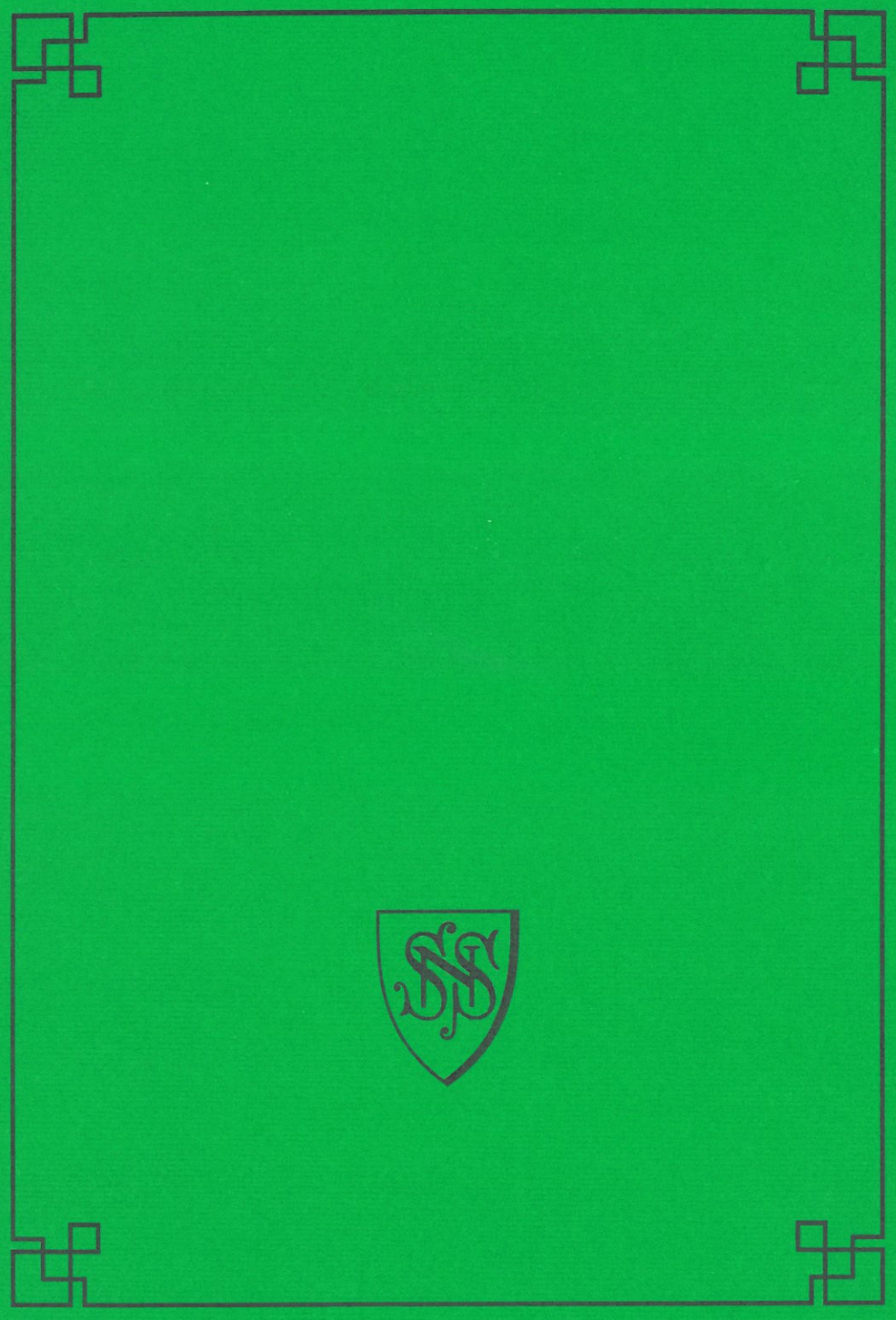


M. Manetti Corso introduttivo alla Geometria Algebrica

Marco Manetti

Corso introduttivo alla Geometria Algebrica

APPUNTI

SCUOLA NORMALE SUPERIORE
PISA

Marco Manetti

Corso introduttivo alla Geometria Algebrica

APPUNTI

SCUOLA NORMALE SUPERIORE
1998

Indice

Presentazione

Queste note raccolgono il materiale preparato per il corso di Geometria Algebrica 1997-98 tenuto presso la Scuola Normale Superiore.

Tale corso era rivolto a studenti del terzo anno del corso di laurea in Matematica, si richiedeva pertanto una buona conoscenza dei corsi istituzionali del primo biennio, in particolare dei corsi di Algebra e Geometria.

L' obbiettivo principale del corso era quello di illustrare alcuni risultati che risalgono ad oltre 100 anni fa e che sono all'origine di quel ramo della matematica che oggi viene comunemente chiamato Geometria Algebrica. Pur mantenendo un linguaggio moderno ed il necessario rigore, ho preferito, nei limiti del possibile, dimostrazioni che utilizzano le tecniche algebriche disponibili all'epoca.

Tra i possibili approcci alla materia ho scelto quello puramente algebrico; per evitare le tentazioni topologiche ed analitico-complesse lavoreró su di un campo arbitrario $\mathbb{K}$ (sempre infinito e quasi sempre algebricamente chiuso). Suggerisco però al lettore di farsi sempre un'idea intuitiva, aiutandosi con delle figure e se necessario introducendo concetti estranei alle note, di quello che succede sui numeri reali e complessi.

L'undicesimo ed ultimo capitolo raccoglie invece alcune lezioni del corso di Geometria Algebrica 1995-96 (corso propedeutico allo studio dell'aritmetica delle curve ellittiche); per la comprensione di quest'ultimo capitolo è richiesta una conoscenza di base di Algebra Commutativa.

Alle note ho aggiunto alcuni esercizi (circa 450) molti dei quali decisamente non banali, alcuni asterischi indicano il livello di difficoltà: si tratta naturalmente di una valutazione del tutto personale che riflette in pieno le difficoltà che ho trovato nel risolverlo al momento dell'inserimento dei singoli esercizi nelle note; il simbolo (**?) sta ad indicare un esercizio del quale non conosco alcuna ragionevole dimostrazione che utilizzi il materiale esposto nelle note (fino a quel punto).

Gli esercizi complementari (che possono essere tralasciati ad una prima lettura) sono raccolti in apposite sezioni.

Commenti, suggerimenti e segnalazioni di errori sono benvenuti.

I. Richiami di Algebra e Geometria

In questo primo capitolo saranno richiamate, in modo estremamente conciso, alcune nozioni basilari di algebra e geometria proiettiva allo scopo di facilitare il lettore e di fissare le notazioni. Per una trattazione più dettagliata e dimostrazioni complete rimandiamo ai testi base di algebra e geometria [He], [G-R-T], [La], [Enr].

Attenzione: Salvo avviso contrario, in queste note tutti gli anelli sono commutativi con unità e tutti i campi sono infiniti.

1. Anelli ed ideali

Con il termine anello intenderemo sempre un anello commutativo con identità. Assumeremo che il lettore abbia familiarità con le nozioni di dominio di integrità, di campo e di caratteristica di un campo.

Dato un dominio di integrità A, il campo delle frazioni di A è il campo F formato dalle classi di equivalenza delle frazioni $\frac{a}{b}$, $a, b \in A$, $b \neq 0$ ove $\frac{a}{b} \sim \frac{c}{d}$ se e solo se $ad = bc$. Le operazioni di somma e prodotto in F sono definite nel modo "naturale" $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$.

Per definizione, la caratteristica di un domino di integrità è la caratteristica del suo campo delle frazioni; se A è un dominio di caratteristica $p > 0$, l'applicazione $x \to x^p$ è un omomorfismo iniettivo di A in sé detto **morfismo di Frobenius**.

Un dominio di integrità si dice **perfetto** se ha caratteristica 0 oppure se ha caratteristica $p > 0$ ed il morfismo di Frobenius è surgettivo.

Sia A un dominio di integrità, un elemento $a \in A$ si dice **irriducibile** se non è invertibile e ogniqualvolta $a = bc$ con b, c due elementi in A ne segue che uno è invertibile. Un elemento non invertibile $a \in A$ si dice **primo** se ogniqualvolta a divide bc si ha che a divide almeno uno dei due elementi b, c. È facile dimostrare che ogni primo è irriducibile, il viceversa è generalmente falso. Un dominio di integrità si dice a **fattorizzazione unica** se:

i) Ogni elemento non zero di A è o invertibile oppure si può scrivere come prodotto di un numero finito di elementi irriducibili.

ii) Gli elementi irriducibili di cui al punto i) sono unicamente determinati, a meno dell'ordine e di moltiplicazione per invertibili.

Dato un anello A ed $E \subset A$ un sottoinsieme, denotiamo con $(E) \subset A$ il più piccolo ideale di A contenente E. Si dimostra facilmente che ogni elemento di (E) si può scrivere come una combinazione lineare finita di elementi di E a coefficienti in A. Diremo che un insieme E è un **insieme di generatori** dell'ideale $I \subset A$ se $I = (E)$, l'ideale I si dice **finitamente generato** se ammette un insieme finito di generatori; si dice **principale** se è generato da un solo elemento, cioè se $I = (a)$, $a \in A$.

Dato un insieme totalmente ordinato V, una famiglia $\{I_v\}$, $v \in V$, di ideali in A si dice una **catena ascendente** se $I_v \subset I_w$ quando $v \leq w$. Una catena ascendente di ideali I_v si dice **stazionaria** se esiste $v_0 \in V$ tale che $I_v = I_{v_0}$ per ogni $v \geq v_0$.

Un anello si dice **locale** se contiene un solo ideale massimale.

ESERCIZIO 1: Sia I un ideale massimale di un anello A. A è locale se e solo se $1 - a$ è invertibile per ogni $a \in I$.

Infine un ideale I si dice **irriducibile** se per ogni coppia J_1, J_2 di ideali tali che $I = J_1 \cap J_2$ si ha che $I = J_1$ oppure $I = J_2$.

Un ideale P si dice **primo** se $ab \in P$ implica che $a \in P$ oppure $b \in P$.

ESERCIZIO 2: Ogni ideale primo è irriducibile, il viceversa è generalmente falso.

Dato un ideale $I \subset A$ si definisce il **radicale** di I come

$$\sqrt{I} = \{a \in A \,|\, a^n \in I \text{ per } n >> 0\}$$

Un ideale radicale è un ideale I tale che $I = \sqrt{I}$, gli ideali primi sono radicali.

ESERCIZIO 3: Sia $I \subset A$ ideale, provare che $\sqrt{I}$ è l'intersezione di tutti gli ideali primi che contengono I. (Sugg. Sia $f \notin \sqrt{I}$ fissato e sia $\mathcal{A}$ la famiglia degli ideali radicali che non contengono f. Gli elementi massimali di $\mathcal{A}$ sono ideali primi)

Sia ora $B = (b_{ij})$ una matrice quadrata di ordine n a coefficienti in un anello A. In analogia con quanto fatto per le matrici a coefficienti in un campo si definisce il determinante di B nel modo seguente

$$det(B) = \sum_{\sigma \in \Sigma_n} (-1)^\sigma b_{1\sigma(1)} \cdots b_{n\sigma(n)}$$

dove Σ_n è il gruppo simmetrico delle permutazioni di $\{1, ..., n\}$ e $(-1)^\sigma$ è la segnatura di σ.

Continuano a valere le seguenti proprietà:

1) Sviluppo di Laplace.

Se B^{ij} è il determinante della matrice di ordine $n-1$ ottenuto da B togliendo la i-esima riga e la j-esima colonna vale

$$det(B) = \sum_{j=1}^{n} (-1)^{i+j} b_{ij} B^{ij} = \sum_{i=1}^{n} (-1)^{i+j} b_{ij} B^{ij}$$

2) Moltiplicando una riga od una colonna di B per un elemento $a \in A$ anche $det(B)$ viene moltiplicato per a.

3) $det(B)$ non cambia se ad una colonna viene aggiunto un multiplo di un'altra colonna. Lo stesso per le righe.

4) Se B possiede due colonne uguali $det(B) = 0$.

5) Vale il teorema di Binet: $\det(AB) = \det A \det B$.

Come esempio di applicazione delle precedenti regole calcoliamo il determinante della matrice di Vandermonde; proviamo per induzione su n che

$$V(x_0, ..., x_n) = \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_0 & x_1 & \dots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \dots & x_n^{n-1} \\ x_0^n & x_1^n & \dots & x_n^n \end{vmatrix} = \prod_{i>j} (x_i - x_j)$$

Si consideri infatti il polinomio $p(t) = \prod_{j=0}^{n-1} (t - x_j) = t^n + \sum_{i=0}^{n-1} a_i t^i$, sommando all'ultima riga della matrice di Vandermonde la combinazione lineare a coefficienti a_i delle rimanenti righe si ottiene

$$V(x_0, ..., x_n) = \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_0 & x_1 & \dots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \dots & x_n^{n-1} \\ p(x_0) & p(x_1) & \dots & p(x_n) \end{vmatrix}$$

Dato che $p(x_i) = 0$ per ogni $i < n$ si ha $V(x_0, ..., x_n) = p(x_n) V(x_0, ..., x_{n-1})$.

Sia $\tilde{B} = (\tilde{b}_{ij})$ la matrice di coefficienti $\tilde{b}_{ij} = (-1)^{i+j} B^{ji}$, allora se I indica la matrice identità, dallo sviluppo di Laplace segue immediatamente che

$$B \cdot \tilde{B} = \tilde{B} \cdot B = det(B) \cdot I \quad \text{prodotto righe per colonne}$$

La matrice $\tilde{B}$ viene detta **matrice aggiunta** di B.

ESERCIZIO 4: Sia $B = (b_{ij})$ una matrice le cui colonne sono linearmente dipendenti su A, provare che $det(B)$ è un divisore di 0.

Un anello A si dice **graduato** se esiste una decomposizione $A = \oplus_{d=0}^{\infty} A_d$ che rispetta l'addizione e tale che $A_n A_m \subset A_{n+m}$; gli elementi di $A_d \subset A$ si dicono **omogenei**

di grado d. Un ideale I di un anello graduato A si dice **omogeneo** se ogniqualvolta $a \in I$ accade che anche tutte le componenti omogenee di a appartengono a I, in altre parole I è omogeneo se e solo se $I = \oplus(I \cap A_d)$; si dimostra facilmente che un ideale è omogeneo se e solo se è generato da elementi omogenei.

Se A è un dominio di integrità graduato, $f, g \in A$ e fg è omogeneo allora anche f e g sono omogenei: infatti se $f = f_n + f_{n+1} + ... + f_N$, $g = g_r + g_{r+1} + ... + g_R$ sono le scomposizioni in componenti omogenee con $f_n, f_N, g_r, g_R \neq 0$ si ha $fg = f_N g_R + f_n g_r +$ combinazione lineare di elementi omogenei di gradi strettamente compresi fra $n+r$ e $N+R$. Siccome f è omogeneo deve necessariamente essere $n+r = N+R$ e quindi $n = N, r = R$.

2. Anelli di polinomi

Richiamiamo in questo paragrafo le proprietà fondamentali degli anelli di polinomi, supporremo che il lettore abbia familiarità con la nozione di grado e di polinomio monico.

Se A è un anello indicheremo con $A[x_1, ..., x_n]$ l'anello dei polinomi a coefficienti in A nelle indeterminate $x_1, ..., x_n$. Proprietà caratterizzante di $A[x_1, ..., x_n]$ è che per ogni omomorfismo di anelli $\phi: A \to B$ e per ogni n-upla $b_1, ..., b_n \in B$ esiste unica una estensione di ϕ ad un omomorfismo $\hat{\phi}: A[x_1, ..., x_n]$ tale che $\hat{\phi}(x_i) = b_i$.

Se A è un dominio a fattorizzazione unica, un polinomio $f \in A[t]$ si dice **primitivo** se i coefficienti di f non hanno fattori comuni. Ricordiamo i ben noti

Lemma 2.1.(di Gauss) *Sia A un dominio a fattorizzazione unica con campo delle frazioni $\mathbb{K}$.*

Il prodotto di polinomi primitivi è primitivo; in particolare se $f, g \in A[t]$, f primitivo e f divide g in $\mathbb{K}[t]$ allora f divide g in $A[t]$ e $A[t]$ è un dominio a fattorizzazione unica.

Lemma 2.2.(Divisione Euclidea) *Sia A dominio di integrità e $p \in A[x]$ un polinomio monico di grado $n > 0$. Per ogni $f \in A[x]$ esistono unici $g, r \in A[x]$ con r di grado $< n$ tali che $f = gp + r$.*

Lemma 2.3.(regola di Ruffini) *Sia A un dominio di integrità, $f \in A[x]$ e $a \in A$ tale che $f(a) = 0$ allora $(x - a)$ divide f, in particolare esistono in A al più $deg(f)$ radici.*

ESERCIZIO 5: Dimostrare 2.1, 2.2 e 2.3.

Dal lemma 2.3 segue il seguente criterio di cui faremo uso in seguito: se A è un dominio di integrità infinito ed $f \in A[t]$ allora $f = 0$ se e solo se $f(a) = 0$ per infiniti $a \in A$.

Sia n un intero positivo fissato, un multiindice $I = (i_1, ..., i_n)$ è un elemento di $\mathbb{N}^n$; il **grado** di I è $|I| = i_1 + ... + i_n$; il **peso** di I è $w(I) = i_1 + 2i_2 + ... + ni_n$. Similmente si definisce il grado ed il peso di un monomio nelle indeterminate $x_0, ..., x_n$. Un polinomio si dice **omogeneo** se tutti i monomi hanno lo stesso grado, **isobaro** se hanno lo stesso peso.

Il ragionamento usato nella sezione 1 mostra che i fattori irriducibili di un polinomio omogeneo (risp. isobaro) sono omogenei (risp. isobari).

Un ideale $I \subset A[x_0, ..., x_n]$ si dice **omogeneo** se è generato da polinomi omogenei.

Lemma 2.4. *Sia A un dominio infinito e sia $f \in A[x_1, ..., x_s]$. f è omogeneo di grado n se e solo se*

$$f(tx_1, ..., tx_s) = t^n f(x_1, ..., x_s)$$

per ogni $t \in A$.

Dim. Se f è omogeneo la relazione precedente è evidente. Viceversa scriviamo $f = f_0 + f_1 + ... + f_N$ con f_i omogeneo di grado i, il polinomio $P = f_0 + tf_1 + ... + t^N f_N - t^n f \in A[x_1, ..., x_s, t]$ si annulla per infiniti valori di $t \in A \subset A[x_1, ..., x_s]$ e quindi deve necessariamente essere $f_n = f$ e $f_i = 0$ per $i \neq n$. □

Lemma 2.5. *Un ideale $I \subset \mathbb{K}[x_1, ..., x_n]$ è omogeneo se e solo se $f(tx_1, ..., tx_n) \in I$ per ogni $f \in I$, $t \in \mathbb{K}$.*

Dim. esercizio (Sugg. Vandermonde). □

Dato un qualsiasi anello A, per ogni $i = 1, ..., s$ esiste una unica applicazione

$$\frac{\partial}{\partial x_i}: A[x_1, ..., x_s] \to A[x_1, ..., x_s]$$

che soddisfa le seguenti 4 regole:

1) $\frac{\partial}{\partial x_i}(a) = 0$ per ogni $a \in A$.
2) (additività) $\frac{\partial}{\partial x_i}(b_1 + b_2) = \frac{\partial}{\partial x_i}(b_1) + \frac{\partial}{\partial x_i}(b_2)$ per ogni $b_1, b_2 \in A[x_1, ..., x_s]$.
3) (Leibnitz) $\frac{\partial}{\partial x_i}(b_1 b_2) = b_1 \frac{\partial}{\partial x_i}(b_2) + b_2 \frac{\partial}{\partial x_i}(b_1)$ per ogni $b_1, b_2 \in A[x_1, ..., x_s]$.
4) $\frac{\partial}{\partial x_i}(x_j) = \delta_{ij}$ delta di Kronecker.

Si vede facilmente che $\frac{\partial}{\partial x_i}$ è ben definita e unica. Più in generale dato un morfismo di anelli $A \to B$, una applicazione $d: B \to B$ che soddisfa le precedenti condizioni 1), 2) e 3) si dice una **A-derivazione**. Se $A = \mathbb{R}$ le applicazioni $\frac{\partial}{\partial x_i}$ coincidono con le usuali derivate parziali.

ESERCIZIO 6: Sia $E: A[x_1, ..., x_s] \to A[x_1, ..., x_s]$ l'unica applicazione additiva (che soddisfa cioè la condizione 2)) tale che $E(f) = nf$ per ogni polinomio f omogeneo di grado n, provare che E è una A-derivazione detta **derivazione di Eulero**.

Lemma 2.6. *Sia A un dominio perfetto a fattorizzazione unica e $f \in A[x_1,...,x_s]$. f possiede un fattore multiplo di grado positivo se e solo se $f, \frac{\partial}{\partial x_1}(f),..., \frac{\partial}{\partial x_s}(f)$ hanno un fattore comune di grado positivo.*

Dim. Se h^2 divide f, segue immediatamente dalla regola di Leibnitz che h divide tutte le derivate parziali. Viceversa sia $f = f_1 f_2 ... f_n$ con f_i fattori irriducibili distinti e si assuma per assurdo che f_1 abbia grado positivo e divida tutte le derivate parziali di f. Di nuovo per Leibnitz segue che f_1 divide $\frac{\partial}{\partial x_i}(f_1)$ per ogni i e quindi siccome il grado della derivata è strettamente inferiore deve essere necessariamente $\frac{\partial}{\partial x_i}(f_1) = 0$ per ogni i.

Basta quindi dimostrare che se f è irriducibile di grado positivo allora possiede una derivata parziale non nulla.

L'asserzione è evidente in caratteristica 0, se la caratteristica è $p > 0$ e le derivate parziali sono nulle allora $f \in A[x_1^p,...,x_s^p]$; siccome A è perfetto, f appartiene all'immagine del morfismo di Frobenius $A[x_1,...,x_s] \to A[x_1,...,x_s]$ e quindi esiste $h \in B$ tale che $f = h^p$. □

Lemma 2.7.(Formula di Eulero) *Se $f \in A[x_1,...,x_s]$ è omogeneo di grado n vale*

$$nf = \sum_{i=1}^{s} x_i \frac{\partial f}{\partial x_i}.$$

Dim. Induzione su n. Se $n = 0$ $f \in A$ e la formula è chiara.

Sia $n > 0$ e supponiamo la formula vera per polinomi omogenei di grado $n-1$; per linearità basta provare la formula nel caso in cui f è un monomio, si può quindi scrivere $f = x_j f'$ per qualche $j = 1,...,s$ e f' omogeneo di grado $n-1$.

Quindi per induzione

$$\sum_{i=1}^{s} x_i \frac{\partial f}{\partial x_i} = \sum_{i=1}^{s} x_j x_i \frac{\partial f'}{\partial x_i} + x_j f' = (n-1) x_j f' + x_j f' = n x_j f' = nf$$

□

Una **serie formale** a coefficienti in A nelle indeterminate $x_1,...,x_n$ è una espressione del tipo

$$\phi = \sum_I a_I x^I \qquad a_I \in A, \quad I \in \mathbb{N}^n$$

dove si è posto $x^I = x_1^{i_1} x_2^{i_2} ... x_n^{i_n}$; chiaramente un polinomio può essere pensato come una serie formale in cui $a_I \neq 0$ per al più un numero finito di multiindici. Con le ben note regole di somma e di prodotto di Cauchy le serie formali formano un anello commutativo $A[[x_1,...,x_n]]$.

È talvolta utile considerare $A[x_1,...,x_n]$ come un sottoanello di $A[[x_1,...,x_n]]$. Ad esempio sia $a \in A$, allora $1 - ta \in A[t]$ è invertibile in $A[[t]]$ con inverso $\sum_{i \geq 0} a^i t^i$; si deduce immediatamente che $1 - at$ è invertibile in $A[t]$ se e solo se a è nilpotente.

ESERCIZIO 7: Siano $d_1, d_2 : A[x_1,...,x_s] \to A[x_1,...,x_s]$ due A-derivazioni, allora $d_1 = d_2$ se e solo se $d_1(x_i) = d_2(x_i)$ per ogni $i = 1,...,s$.

ESERCIZIO 8: Sia $A = \mathbb{K}[x,y,z]/(xy - z^2)$, provare che A è un dominio di integrità, $z \in A$ è irriducibile ma non è primo. (Sugg. A è un anello graduato).

ESERCIZIO 9: Sia $f \in A[x_1,...,x_s]$ e $g_1,...,g_s \in A[t]$, provare che

$$\frac{\partial}{\partial t} f(g_1(t),...,g_s(t)) = \sum_{i=1}^{s} \frac{\partial f}{\partial x_i}(g_1(t),...,g_s(t)) \frac{\partial g_i}{\partial t}(t)$$

ESERCIZIO 10: Provare che in $A[x_1,...,x_s]$ gli operatori $\frac{\partial}{\partial x_i}$ commutano tra loro.

ESERCIZIO 11: Sia $A \to B$ un morfismo di anelli e siano $f, g, h : B \to B$ A-derivazioni. Provare che:

i) $f + g$, bf sono A-derivazioni per ogni $b \in B$.

ii) $[f,g] = f \circ g - g \circ f$ è una A-derivazione.

iii) $[f \circ g, h] = f \circ [g,h] + [f,h] \circ g$.

ESERCIZIO 12: (*) (Lo Pfaffiano).

Nel seguito sia R un dominio a fattorizzazione unica di caratteristica $\neq 2$ e F il suo campo delle frazioni.

i) Sia $A = (A^{ij})$ una matrice simmetrica $n \times n$ di rango 1 a coefficienti in R, dimostrare che esistono $a, p_1,...,p_n \in R$ tali che $MCD(p_1,...,p_n) = 1$ e $A^{ij} = a p_i p_j$.

Sia $R = \mathbb{Z}[a_{ij}]$, $1 \leq i < j \leq n$ e sia $A = (A_{ij})$ la matrice antisimmetrica tale che $A_{ij} = a_{ij}$ se $i < j$ e A^{ij} la sua aggiunta. Provare che:

ii) Se n è dispari A ha rango $n-1$, A^{ij} è simmetrica di rango 1 e $MCD(A^{ij}) = 1$. Per i punti precedenti si può scrivere $A^{ij} = a p_i p_j$. Mostrare che necessariamente $a = 1$, il vettore $(p_1,...,p_n)$ è unicamente determinato a meno del segno e vale $\sum_j A_{ij} p_j = 0$ per ogni $i = 1,...,n$. I polinomi p_i sono detti gli Pfaffiani della matrice A.

iii) Se $n = 2d$ è pari allora A ha rango n ed esiste $Pf \in R$ tale che $\det A = Pf^2$, Pf si dice lo Pfaffiano della matrice A.

Si provi inoltre che: Pf è omogeneo di grado d e se il peso di a_{ij} è $i + j$ Pf è pure isobaro di peso $d(n+1)$. Si provi infine che Pf è irriducibile. (Sugg. Si usi la omogeneità di Pf e si consideri la specializzazione $A_{ij} = A_{ji} = 0$ se $i > d$ oppure se $j < d$.)

iv) Sia $\mathbb{K}$ un campo di caratteristica 0, V uno spazio vettoriale su $\mathbb{K}$ di dimensione $n = 2d$ e $e_1,...,e_n$ una base di V. Data una matrice antisimmetrica $A = A_{ij}$ con Pfaffiano $Pf(A)$ si consideri la forma

$$\eta = \frac{1}{2} \sum_{i,j} A_{ij} e_i \wedge e_j$$

Si provi che

$$\frac{1}{n!}\eta^{\wedge d} = Pf(A)e_1 \wedge ..... \wedge e_n.$$

(Sugg. Esiste una matrice B tale che $\eta = Be_1 \wedge Be_2 + Be_e \wedge Be_4 + \ldots + Be_{n-1} \wedge Be_n$.)

v) Scrivere esplicitamente lo Pfaffiano di una matrice antisimmetrica 4×4.

ESERCIZIO 13: Ricordiamo che una $\mathbb{K}$-algebra si dice finitamente generata se è isomorfa ad un quoziente di un'algebra di polinomi in un numero finito di variabili.

Sia $R \subset \mathbb{K}[x,y]$ la sottoalgebra generata da tutti i monomi xy^a, $a \geq 0$; si dimostri che R non è finitamente generata.

ESERCIZIO 14: Sia $A(t)$ una matrice quadrata a coefficienti in $\mathbb{K}[t]$, se r è la dimensione su $\mathbb{K}$ del nucleo di $A(0)$ allora t^r divide il determinante di $A(t)$.

3. Moduli

Sia A un anello, un **A-modulo** è il dato di un gruppo abeliano M e di un prodotto $A \times M \to M$ tale che:

1) $a(m_1 + m_2) = am_1 + am_2$ per ogni $a \in A$, $m_1, m_2 \in M$.
2) $(a_1 + a_2)m = a_1m + a_2m$ per ogni $a_1, a_2 \in A$, $m \in M$.
3) $(ab)m = a(bm)$ per ogni $a, b \in A$, $m \in M$.
4) $1m = m$, $0m = 0$ per ogni $m \in M$.

Dato un A-modulo M, un ideale $I \subset A$ ed un sottoinsieme $E \subset M$ denotiamo con $IE \subset M$ l'insieme delle combinazioni lineari finite di elementi di E a coefficienti in I. Chiaramente IE è chiuso per la somma e per il prodotto per scalare.

Dato un A-modulo M un sottogruppo $N \subset M$ si dice un **sottomodulo** se $AN \subset N$. Dati due sottomoduli $N_1, N_2 \subset M$, gli insiemi $N_1 \cap N_2$ e $N_1 + N_2 = \{n_1 + n_2 | n_i \in N_i\}$ sono sottomoduli. Se $N \subset M$ è un sottomodulo e $I \subset A$ è un ideale allora IN è un sottomodulo.

Se $N \subset M$ è un sottomodulo il gruppo quoziente M/N possiede una struttura naturale di A-modulo.

Un insieme di generatori per M è un sottoinsieme $E \subset M$ tale che $M = AE$. Un modulo finitamente generato è un modulo che ammette un insieme finito di generatori. Per i moduli finitamente generati vale il seguente:

Teorema 3.1.(Lemma di Nakayama) *Sia A un anello, $I \subset A$ un ideale, M un A-modulo finitamente generato e $N \subset M$ un sottomodulo. Se $IM + N = M$ allora esiste $a \in I$ tale che $(1-a)M \subset N$.*

Dim. Sia $e_1, ..., e_r$ un insieme finito di generatori di M, dato che $IM + N = M$ si può scrivere per ogni $i = 1, .., r$, $e_i = \sum a_{ij}e_j + n_i$ con $a_{ij} \in I$ e $n_i \in N$. Se B è la matrice di coefficienti $B_{ij} = \delta_{ij} - a_{ij}$ si può scrivere la precedente relazione come un prodotto righe per colonne

$$B \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} = \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix}$$

Moltiplicando a sinistra entrambi i membri per la matrice aggiunta di B si ottiene $\det(B)e_i \in N$ per ogni $i = 1, ..., r$ e quindi $\det(B)M \subset N$. Basta adesso osservare che $1 - \det(B) \in I$. □

Corollario 3.2. *Sia $R \subset A$ l'intersezione di tutti gli ideali massimali e M un A-modulo finitamente generato, se $RM = M$ allora $M = 0$.*

Dim. Poniamo $N = 0$ nel teorema 3.1, esiste $a \in R$ tale che $(1-a)M = 0$. Dato che a appartiene a R, $1 - a$ non appartiene a nessun ideale massimale e quindi è invertibile. □

Un applicazione di $f: M \to N$ tra due moduli si dice A-lineare o un morfismo di moduli se $f(a_1m_1 + a_2m_2) = a_1f(m_1) + a_2f(m_2)$. È evidente che $\ker f = \{m \in M \,|\, f(m) = 0\}$ e $\operatorname{im} f = f(M) \subset N$ sono sottomoduli; si definisce il conucleo $\operatorname{coker} f = N/\operatorname{im} f = N/f(M)$.

Corollario 3.3. *Sia A un anello, M un A-modulo finitamente generato e $f: M \to M$ un morfismo surgettivo di moduli. Allora f è anche iniettivo e quindi un isomorfismo.*

Dim. L'endomorfismo f permette di considerare M come $A[t]$-modulo tale che $tm = f(m)$. Per ipotesi $(t)M = M$ e quindi esiste $g \in A[t]$ tale che $(1 - gt)M = 0$. Sia $m \in \ker(f)$, allora $0 = (1 - gt)m = m - gf(m) = m$ e quindi f è iniettiva. □

Ogni anello A è un A-modulo in modo banale, i sottomoduli di A corrispondono agli ideali. Un modulo si dice **libero** se è isomorfo ad una somma diretta di A-moduli isomorfi ad A. Il modulo A^r è libero ed è generato da r elementi e non di meno. Infatti un A-modulo M può essere generato da r elementi se e e solo se esiste un morfismo surgettivo di moduli $A^r \to M$. Lasciamo per esercizio la verifica che se $f: A^s \to A^r$ è surgettivo allora $s \geq r$.

4. Spazi proiettivi

Sia $\mathbb{K}$ un campo e V uno spazio vettoriale su $\mathbb{K}$; definiamo il **proiettivizzato** di V

$$\mathbb{P}(V) = (V - \{0\})/\sim, \qquad v \sim w \iff v = \lambda w, \quad \lambda \in \mathbb{K} - \{0\}$$

Lo spazio $\mathbb{P}(V)$ è in bigezione naturale con l'insieme dei sottospazi vettoriali di dimensione 1 (rette) di V.

Se V ha dimensione finita definiamo la dimensione di $\mathbb{P}(V)$, $\dim \mathbb{P}(V) = \dim V - 1$.

Dato un vettore $v \in V$, $v \neq 0$ si è soliti denotare con $[v] \in \mathbb{P}(V)$ la classe corrispondente.

Chiameremo $\mathbb{P}^n_{\mathbb{K}} = \mathbb{P}(\mathbb{K}^{n+1})$ **spazio proiettivo** di dimensione n sul campo $\mathbb{K}$. In assenza di ambiguità sul campo $\mathbb{K}$ scriveremo più semplicemente $\mathbb{P}^n$.

Se $W \subset V$ è un sottospazio lineare si ha $\mathbb{P}(W) \subset \mathbb{P}(V)$, chiameremo $\mathbb{P}(W)$ **sottospazio proiettivo** di $\mathbb{P}(V)$. Se $W \subset V$ è un iperpiano diremo che $\mathbb{P}(W)$ è un **iperpiano** di $\mathbb{P}(V)$. Infine si definisce lo spazio proiettivo duale $\mathbb{P}(V)^\vee = \mathbb{P}(V^\vee)$, è chiaro che $\mathbb{P}(V)^\vee$ è in bigezione naturale con gli iperpiani di V (e quindi di $\mathbb{P}(V)$).

Se $W_1, W_2 \subset V$ sono sottospazi scriveremo $\mathbb{P}(W_1) + \mathbb{P}(W_2) = \mathbb{P}(W_1 + W_2)$; in altri termini se $H_1, H_2 \subset \mathbb{P}(V)$ sono sottospazi proiettivi allora $H_1 + H_2$ è il più piccolo sottospazio proiettivo di $\mathbb{P}(V)$ che li contiene. Se $p, q \in \mathbb{P}(V)$ sono punti distinti scriveremo talvolta $\overline{pq}$ per denotare $p + q$, la retta proiettiva congiungente p e q.

Definizione 4.1. Una applicazione $\phi\colon \mathbb{P}(V) \to \mathbb{P}(W)$ si dice una **proiettività** se è indotta per passaggio al quoziente da una applicazione **lineare iniettiva** $f\colon V \to W$; scriveremo in tal caso $\phi = [f]$. Un **isomorfismo proiettivo** è una proiettività bigettiva.

È un facile esercizio osservare che date $f, g\colon V \to W$ lineari iniettive vale $[f] = [g]$ se e solo se esiste $a \in \mathbb{K} - 0$ tale che $f = ag$.

Se V ha dimensione finita ogni proiettività $\mathbb{P}(V) \to \mathbb{P}(V)$ possiede una proiettività inversa, denotiamo con $PGL(V) = Aut(\mathbb{P}(V))$ il gruppo delle proiettività di $\mathbb{P}(V)$ in sé. Per definizione esiste un omomorfismo surgettivo di gruppi $GL(V) \to PGL(V)$ che ha come nucleo i multipli dell'identità.

Chiameremo **sistema di coordinate omogenee** su $\mathbb{P}(V)$ un qualsiasi sistema di coordinate lineari su V. Se $\mathbb{P}(V)$ ha dimensione finita n, la scelta di un sistema di coordinate omogenee definisce un isomorfismo proiettivo $\mathbb{P}(V) = \mathbb{P}^n$ e quindi permette di rappresentare ogni punto $p \in \mathbb{P}(V)$ come $p = [a_0, ..., a_n]$ con i numeri $a_i \in \mathbb{K}$ non tutti nulli. Tale rappresentazione non è unica ma vale $[a_0, ..., a_n] = [b_0, ..., b_n]$ se e solo se esiste $\lambda \in \mathbb{K} - 0$ tale che $b_i = \lambda a_i$ per ogni i.

Si consideri adesso una decomposizione in somma diretta di sottospazi $V = K \oplus W$ e sia $\pi\colon V \to W$ la proiezione sul secondo fattore. Per passaggio al quoziente otteniamo una mappa $[\pi]\colon \mathbb{P}(V) - \mathbb{P}(K) \to \mathbb{P}(W)$ detta **proiezione** su $\mathbb{P}(W)$ di **centro** $\mathbb{P}(K)$. Da un punto di vista più geometrico se $p \in \mathbb{P}(V) - \mathbb{P}(K)$ allora $[\pi](p)$ è il punto di intersezione di $\mathbb{P}(W) \subset \mathbb{P}(V)$ e di $\mathbb{P}(K) + p$.

Lo spazio proiettivo $\mathbb{P}(V/K)$ può essere pensato come l'insieme dei sottospazi proiettivi di $\mathbb{P}(V)$ di dimensione $\dim_{\mathbb{K}} K$ che contengono $\mathbb{P}(K)$; in tale interpretazione l'isomorfismo naturale $\mathbb{P}(W) \to \mathbb{P}(V/K)$ associa al punto $p \in \mathbb{P}(W)$ il sottospazio $\mathbb{P}(K) + p$.

Definizione 4.2. s punti $p_0, ..., p_s \in \mathbb{P}^n$ si dicono *proiettivamente indipendenti* se il sottospazio generato $p_0 + ... + p_s$ ha dimensione esattamente s.

Definizione 4.3. Un insieme $p_0, ..., p_{n+1} \in \mathbb{P}^n$ si dice un **sistema di riferimento** se per ogni i fissato i punti p_j, $j \neq i$ sono proiettivamente indipendenti.

Ad esempio tre punti distinti di $\mathbb{P}^1$ e e quattro punti di $\mathbb{P}^2$, tre a tre non allineati, sono sistemi di riferimento.

Valgono i ben noti:

Lemma 4.4. *Sia V spazio vettoriale di dimensione $n+1$ e $p_0, ..., p_{n+1} \in \mathbb{P}(V)$ un sistema di riferimento. Allora esiste una base $e_0, ..., e_n \in V$, unica a meno di omotetie, tale che $p_i = [e_i]$ per $i = 0, ..., n$ e $p_{n+1} = [e_0 + e_1 + ... + e_n]$.*

Corollario 4.5. *Dati due sistemi di riferimento $p_0, ..., p_{n+1}$, $q_0, ..., q_{n+1}$ di $\mathbb{P}^n$ esiste unica una proiettività $\phi \in PGL(n+1)$ tale che $\phi(p_i) = q_i$ per ogni i.*

ESERCIZIO 15: Dimostrare 4.4 e 4.5.

Fissiamo un sistema di coordinate omogenee $x_0, ..., x_n$ su $\mathbb{P}^n$, possiamo allora scrivere $\mathbb{P}^n = \mathbb{A}^n_0 \cup H_0$ dove $\mathbb{A}^n_0 = \{[x_0, ..., x_n] \,|\, x_0 \neq 0\}$ è la "parte affine" e $H_0 = \{[x_0, ..., x_n] \,|\, x_0 = 0\}$ è "l'iperpiano all'infinito".

L'applicazione $\mathbb{K}^n \to \mathbb{A}^n_0$, $(a_1; ..., a_n) \to [1, a_1, ..., a_n]$ è bigettiva e determina una struttura di spazio affine di dimensione n su $\mathbb{A}^n_0$. Non è difficile mostrare che il sottogruppo di $Aut(\mathbb{P}^n)$ delle proiettività che preservano la decomposizione $\mathbb{P}^n = \mathbb{A}^n_0 \cup H_0$ coincide con il gruppo delle trasformazioni affini di $\mathbb{A}^n_0$.

Per $n = 1$ possiamo scrivere $\mathbb{P}^1 = \mathbb{K} \cup \{\infty\}$ dove $\mathbb{K} = \{[1, t] \,|\, t \in \mathbb{K}\}$ e $\infty = [0, 1] = [1, \infty]$.

Ogni proiettività ϕ di $\mathbb{P}^1$ è rappresentata da una matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad ad - bc \neq 0$$

e quindi $\phi([x_0, x_1]) = [ax_0 + bx_1, cx_0 + dx_1]$ che, nella coordinata affine t diventa

$$\phi(t) = \frac{a + bt}{c + dt} \qquad ad - bc \neq 0$$

ESERCIZIO 16: Determinare le proiettività di $\mathbb{C} \cup \{\infty\}$ che preservano i seguenti sottospazi:

$\mathbb{R} = \{x+iy \,|\, y = 0\}$, $H = \{x+iy \,|\, y > 0\}$, $\overline{H} = \{x+iy \,|\, y \geq 0\}$, $\Delta = \{x+iy \,|\, x^2+y^2 < 1\}$, $\overline{\Delta} = \{x+iy \,|\, x^2+y^2 \leq 1\}$.

Dati 4 punti distinti $p_1, ..., p_4 \in \mathbb{P}^1$ esiste unica una proiettività $\phi \in Aut(\mathbb{P}^1)$ ed un elemento $\lambda \in \mathbb{K} - \{0, 1\}$ tale che

$$\phi(p_1) = 0, \quad \phi(p_2) = \infty, \quad \phi(p_3) = 1, \quad \phi(p_4) = \lambda$$

Dunque λ dipende solo dalla quaterna ordinata $p_1,..,p_4$ ed è invariante per proiettività.

Definizione 4.6. Il valore $\lambda = (p_1p_2p_3p_4)$ si dice **birapporto** della quaterna ordinata $p_1,..,p_4$.

È evidente che esiste una proiettività che trasforma l'una nell'altra due quaterne ordinate di punti di $\mathbb{P}^1$ se e solo se le due quaterne hanno lo stesso birapporto. Il nome birapporto è motivato dalla seguente

Proposizione 4.7. *Siano $p_1 = [x_1, y_1]$,..,$p_4 = [x_4, y_4]$ punti distinti di $\mathbb{P}^1$, allora vale la formula*

$$(p_1p_2p_3p_4) = \frac{x_1y_3 - x_3y_1}{x_2y_3 - x_3y_2} : \frac{x_1y_4 - x_4y_1}{x_2y_4 - x_4y_2}$$

che, in coordinate affini diventa, se $p_i \in \mathbb{K}$

$$(p_1p_2p_3p_4) = \frac{p_1 - p_3}{p_2 - p_3} : \frac{p_1 - p_4}{p_2 - p_4}$$

Il gruppo simmetrico su 4 elementi Σ_4 agisce sulla quaterna $p_1,...p_4$ permutando gli indici; è naturale chiedersi come agisce Σ_4 sul birapporto.

Definizione 4.8. Il **gruppo trirettangolo** è il sottogruppo $\Gamma_4 \subset \Sigma_4$ formato dall'identità e dalle tre permutazioni di ordine 2

$$\sigma_1 = (2,1,4,3), \quad \sigma_2 = (3,4,1,2), \quad \sigma_3 = (4,3,2,1)$$

Lemma 4.9. *Il birapporto di una quaterna di punti distinti di $\mathbb{P}^1$ è invariante per l'azione del gruppo trirettangolo. Se $bir(p_1,p_2,p_3,p_4) = \lambda$, sotto l'azione del gruppo simmetrico il birapporto assume i valori*

$$\lambda, \quad \frac{1}{\lambda}, \quad 1-\lambda, \quad 1-\frac{1}{\lambda}, \quad \frac{1}{1-\lambda}, \quad \frac{\lambda}{\lambda-1}$$

Dim. Esercizio. □

In generale le sei espressioni di λ in 4.9 forniscono valori distinti in $\mathbb{K}$, si hanno tuttavia le seguenti eccezioni:

1) Caratteristica $\neq 2$ e $\lambda = -1, 2, \frac{1}{2}$. In questo caso la quaterna è detta **armonica.**
2) Caratteristica $\neq 3$, $\xi^2 - \xi + 1 = 0$ e $\lambda = \xi, \xi^{-1}$. In questo caso la quaterna è detta **equianarmonica.**

ESERCIZIO 17: Siano date $L_1,...,L_n \subset \mathbb{P}^n = \mathbb{A}^n_0 \cup H_0$ rette. Si assuma che nessuna delle rette L_i è contenuta in H_0 e sia $p_i = L_i \cap H_0$. Per ogni i esiste una rappresentazione parametrica della retta $L_i \cap \mathbb{A}^n_0$

$$L_i = \{ [1, a_{i1}t + b_{i1}, ..., a_{in}t + b_{in}] \mid t \in \mathbb{K} \}$$

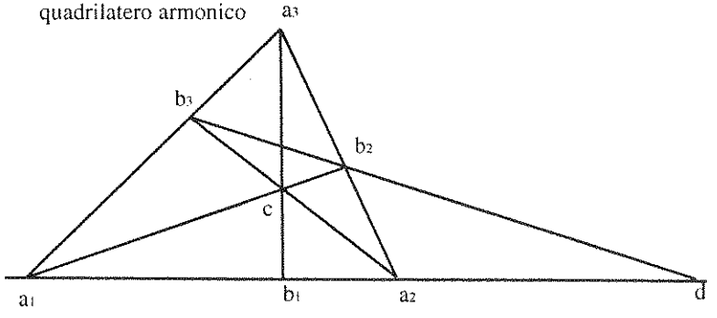
Provare che $p_1,....p_n$ sono proiettivamente indipendenti se e solo se $\det(a_{ij}) \neq 0$.

ESERCIZIO 18: (*) Sia $\mathbb{K}$ algebricamente chiuso di caratteristica $\neq 2$ e siano date $L_1,...,L_4 \subset \mathbb{P}^3$ rette. Provare che esiste una retta in $\mathbb{P}^3$ che le interseca tutte. (Sugg. Se $L_i \cap L_j \neq \emptyset$ è facile. Altrimenti si prendano coordinate omogenee tali che $L_4 = \{x_0 = x_1 = 0\}$, $L_1 = \{x_2 = x_3 = 0\}$, l'iperpiano all'infinito $H_0 = \{x_0 = 0\}$ e si consideri il fascio di piani $F_t = \{x_1 = tx_0\}$, $t \in \mathbb{K}$. Ad un certo punto servirà l'esercizio precedente.)

ESERCIZIO 19: $\mathbb{K}$ campo infinito, per ogni $n \geq 5$ esiste un insieme $S \subset \mathbb{P}^1$ di n elementi tale che se $\phi \in Aut(\mathbb{P}^1)$ e $\phi(S) \subset S$ allora $\phi = Id$.

ESERCIZIO 20: Sia $p \in \mathbb{P}^n$ e $G \subset Aut(\mathbb{P}^n)$ il sottogruppo delle proiettività ϕ tali che $\phi(H) \subset H$ per ogni iperpiano H contenente p. Provare che G agisce transitivamente sull'insieme degli iperpiani di $\mathbb{P}^n$ che non contengono p.

ESERCIZIO 21: (quadrilatero armonico)
Caratteristica $\neq 2$. Siano $a_1, a_2, a_3 \in \mathbb{P}^2$ non allineati e $b_2 \in \overline{a_2a_3}$, $b_3 \in \overline{a_3a_1}$ tali che $b_i \neq a_j$ per ogni i,j. Siano c il punto di intersezione di $\overline{a_1b_2}$ e $\overline{a_2b_3}$; b_1 il punto di intersezione di $\overline{a_1a_2}$ e $\overline{a_3c}$; d il punto di intersezione di $\overline{a_1a_2}$ e $\overline{b_2b_3}$ (vedi figura). Provare che $(a_1a_2b_1d) = -1$. (Sugg. fissare un sistema di coordinate omogenee tali che $a_1 = [0,0,1]$, $a_2 = [2,0,1]$, $d = [1,0,0]$, $a_3 = [0,1,0]$ e provare che $b_1 = [1,0,1]$.)



5. Esercizi complementari

ESERCIZIO 22: (*) Un dominio di integrità è a fattorizzazione unica se e solo se sono soddisfatte entrambe le seguenti condizioni:

i) Ogni elemento irriducibile è primo.

ii) Ogni catena ascendente di ideali principali è stazionaria.

ESERCIZIO 23: Sia V uno spazio vettoriale su di un campo $\mathbb{K}$ e sia $f: V \to V$ una applicazione lineare fissata. Dato comunque un polinomio $p \in \mathbb{K}[t]$ si può considerare l'endomorfismo $p(f): V \to V$.

Sia ora $P = (p_{ij})$ una matrice quadrata di ordine n a coefficienti in $\mathbb{K}[t]$; alla matrice P si può associare una applicazione lineare $P(f): V^n \to V^n$ ponendo $P(f)(v_1, ..., v_n) = (w_1, ..., w_n)$ dove $w_i = \sum_j p_{ij}(f)v_j$.

Si osservi che se $P(f)(v_1, ..., v_n) = 0$ allora $0 = \tilde{P} \cdot P(f)(v_1, ..., v_n)$ e quindi $\det(P(f))v_i = \det P(f)v_i = 0$.

Cosa succede se $v_1, ..., v_n$ è una base di V, (a_{ij}) è la matrice che rappresenta f in tale base e $p_{ij} = a_{ij} - \delta_{ij}t$?

ESERCIZIO 24: Ogni dominio di integrità finito è un campo.

ESERCIZIO 25: I campi finiti sono perfetti, dimostrare che in ogni caratteristica positiva esistono campi non perfetti e domini perfetti che non sono campi.

ESERCIZIO 26: Provare che il polinomio $x^3 + 2x^2 + 2x - 88$ non ha radici razionali positive.

ESERCIZIO 27: Differenziare la relazione $t^n f(x_1, ..., x_s) = f(tx_1, ..., tx_s)$ e riottenere la formula di Eulero.

ESERCIZIO 28: Provare che non esistono $\mathbb{R}$-derivazioni nonbanali su $\mathbb{C}$. Più in generale se A è un dominio perfetto, $f \in A[t]$ irriducibile, allora non esistono A-derivazioni su $A[t]/(f)$.

ESERCIZIO 29: Un dominio a fattorizzazione unica A è perfetto se e solo se per ogni $f \in A[t]$ irriducibile, $\dfrac{df}{dt} \neq 0$.

ESERCIZIO 30: Sia A un anello commutativo, $f = a_0x^n + \ldots + a_n \in A[x]$. Provare che:

a) f è nilpotente se e solo se a_i è nilpotente per ogni i.

b) f è invertibile se e solo se a_n è invertibile e $a_0, .., a_{n-1}$ sono nilpotenti.

ESERCIZIO 31: Sia $A \to B$ un morfismo di anelli, $a, b \in B$ e siano $D, D': B \to B$ A-derivazioni; allora vale

$$[aD, bD'] = ab[D, D'] + aD(b)D' - bD'(a)D$$

ESERCIZIO 32: Sia $\mathbb{Q} \to A$ un morfismo di anelli, $D: A \to A$ una $\mathbb{Q}$-derivazione e sia $x \in A$ tale che $Dx = 1$ e $\cap_{i=1}^{\infty}(x^i) = 0$. Provare che x non è un divisore di 0.

ESERCIZIO 33: Sia A un anello commutativo con 1 e siano

$$R = \{x \in A | 1 + xy \text{ invertibile per ogni } y \in A\}$$

$$N = \sqrt{0} = \{x \in A | x \text{ nilpotente }\}, \quad E(A) = \{x \in A | \, x^2 = x\}$$

Provare che:

i) R, N sono ideali e $N \subset R$.

ii) Sia $I \subset R$ ideale, $a \in A$. Provare che a è invertibile in A se e solo se la sua proiezione è invertibile in A/I.

iii) (*) Sia $I \subset A$ ideale e $\alpha: E(A) \to E(A/I)$ la proiezione al quoziente. Se $I \subset R$ allora α è iniettiva; se $I \subset N$ allora α è bigettiva.

(Sugg.: provare che nella surgettività di α non è restrittivo supporre I principale a quadrato nullo; mostrare inoltre che $1 - 2x$ è invertibile in $\mathbb{Z}[x]/(x^2 - x)$.)

ESERCIZIO 34: Un polinomio $p = \sum a_I x^I$ si dice quasiomogeneo se esistono interi positivi $d_1, ..., d_n$ tali che la somma $d(I) = \sum_j i_j d_j$ è costante sull'insieme dei multiindici $I = (i_1, ..., i_n)$ per cui $a_I \neq 0$. Enunciare e provare l'analogo della formula di Eulero per i polinomi quasiomogenei.

ESERCIZIO 35: Sia B matrice $n \times n$ a coefficienti in un anello A, $\tilde{B}$ la matrice aggiunta e v, w vettori di A^n. Provare che per ogni vettore riga v e vettore colonna w vale

$$v\tilde{B}w = \det \begin{pmatrix} B & w \\ v & 0 \end{pmatrix}$$

ESERCIZIO 36: (Teorema di Macaulay)

Sia $\mathbb{K}$ un campo di caratteristica 0, $S = \mathbb{K}[x_1, ..., x_n] = \oplus S_d$ dove S_d denota lo spazio vettoriale dei polinomi omogenei di grado d.

Denotiamo $\partial_i = \dfrac{\partial}{\partial x_i}: S \to S$, $i = 1, .., n$, le derivate parziali e con $T = \mathbb{K}[\partial_1, ..., \partial_n] = \oplus T_d$ dove T_d è lo spazio vettoriale degli operatori differenziali omogenei di grado d; si noti che le naturali applicazioni bilineari $S_d \times T_d \to \mathbb{K}$ sono nondegeneri.

Data $f \in S_n$, $f \neq 0$, si definisce $f^{\perp} = \{D \in T | \, Df = 0\}$. Provare:

i) $f^{\perp}$ è un ideale omogeneo di T.

ii) Se $g \in T$ è omogeneo e $f^{\perp} = g^{\perp}$ allora $g = af$, $a \in \mathbb{K}$.

Si denoti $I_d = f^{\perp} \cap T_d$, per il punto 1) $f^{\perp} = \oplus I_d$. Sia $A = T/f^{\perp} = \oplus A_d$ dove $A_d = T_d/I_d$. Provare:

iii) $A_n = \mathbb{K}$ e $A_d = 0$ per ogni $d > n$.

iv)

$$\text{Zoccolo}(A) := \{a \in A | \, aA_d = 0 \, \forall d > 0\} = A_n.$$

v) Viceversa ogni ideale omogeneo $I \subset T$ tale che l'anello $A = T/I$ soddisfa le precedenti condizioni iii) e iv) è del tipo $f^{\perp}$ per qualche $f \in S_n$. (Sugg. I è unicamente determinato da I_n).

ESERCIZIO 37: Dato un A-modulo M si consideri $B = A \oplus M$ dotato delle operazioni $(a, m) + (b, n) = (a + b, m + n)$, $(a, m)(b, n) = (ab, an + bm)$. Provare che B è un anello

ESERCIZIO 38: Si consideri l'anello $B = \mathbb{K}[x, y]/(x - y^2)$.

1) Si provi che B è un $\mathbb{K}[x]$-modulo libero di rango 2 ed un $\mathbb{K}[y]$-modulo libero di rango 1.

2) Siccome $\mathbb{K}[x]$ è isomorfo a $\mathbb{K}[y]$ e due moduli liberi isomorfi hanno lo stesso rango ne segue che 1=2; dove sta l'errore?

ESERCIZIO 39: Se $\phi\colon \mathbb{P}^n - K \to H$ è una proiezione e $L \subset \mathbb{P}^n$ è un sottospazio proiettivo tale che $K \cap L = \emptyset$ allora la restrizione $\phi\colon L \to H$ è una proiettività tale che $\phi(p) = p$ per ogni $p \in L \cap H$: viceversa ogni proiettività $\psi\colon L \to H$ tale che $\psi(p) = p$ per ogni $p \in L \cap H$ è ottenuta come restrizione di una opportuna proiezione (di centro non necessariamente K). Discutere se il risultato continua ad essere vero sugli spazi proiettivi definiti su corpi noncommutativi (per questo si consiglia di analizzare il caso H, L rette in $\mathbb{P}^2$).

ESERCIZIO 40: Siano $L, H \subset \mathbb{P}^2$ rette distinte, $p = L \cap H$ e $\phi\colon L \to H$ una proiettività tale che $\phi(p) \neq p$. Provare che ϕ è composizione di due proiezioni. (Sugg. considerare la retta $\phi(p) + \phi^{-1}(p)$.)

ESERCIZIO 41: Discutere la validità di 4.5 su corpi noncommutativi. In particolare si determini il sottogruppo di $PGL(2)$ che lascia fissi tre punti distinti di $\mathbb{P}^1$.

ESERCIZIO 42: Sia $\lambda \in \mathbb{K} - \{0, 1\}$ fissato, $L \subset \mathbb{P}^2$ retta, $\pi\colon \mathbb{P}^2 - o \to L$ proiezione di centro $o \notin L$. Definiamo $\phi\colon \mathbb{P}^2 \to \mathbb{P}^2$ nel modo seguente:

$\phi(o) = o$ e $\phi(p) = p$ per ogni $p \in L$; se $p \neq o$ e $p \notin L$ si pone $r = \pi(p)$, $\phi(p) = q$ dove $q \in o + p$ è l'unico punto tale che $(orpq) = \lambda$.

Provare che ϕ è una proiettività.

ESERCIZIO 43: (rapporto semplice)

Siano $a, b, c \in \mathbb{A}^n$ punti allineati con $b \neq c$, esistono quindi unici un vettore $v \in \mathbb{K}^n$ ed uno scalare $t \in cam$ tali che $b = c + v$, $a = c + tv$. Chiameremo $t = (abc) = \dfrac{a-c}{b-c}$ **rapporto semplice** della terna.

Provare che se $f\colon \mathbb{A}^n \to \mathbb{A}^m$ è una applicazione affine tale che $f(b) \neq f(c)$ allora vale la relazione $(f(a)f(b)f(c)) = (abc)$.

ESERCIZIO 44: (rapporti plurisezionali)

Sia $n \geq 2$ e $a_1, ..., a_n, b_1, ..., b_n \in \mathbb{P}^1$, $b_i \neq a_{i+1}$ si definisce il rapporto n-sezionale

$$(a_1a_2...a_nb_1b_2...b_n) = \prod_{i=1}^{n}(a_ia_{i+1}b_i) = \prod_{i=1}^{n}\frac{a_i^0b_i^1 - a_i^1b_i^0}{a_{i+1}^0b_i^1 - a_{i+1}^1b_i^0}$$

dove si è posto $a_{n+1} = a_1$, $b_{n+1} = b_1$ e $a_i = [a_i^0, a_i^1]$, $b_i = [a_i^0, a_i^1]$ sono le rappresentazioni in coordinate omogenee. Provare che è invariante per proiettività e che se $b_n = b_{n-1}$ allora $(a_1a_2...a_nb_1b_2...b_n) = (a_1a_2...a_{n-1}b_1b_2...b_{n-1})$.

Se invece $a_1, ..., a_n \in \mathbb{P}^2$ e $b_i \in \overline{a_ia_{i+1}}$, $b_i \neq a_{i+1}$ per ogni $i = 1, .., n$, preso un punto $p \in \mathbb{P}^2$ non appartenente all'unione delle rette $\overline{a_ia_{i+1}}$ si definisce $(a_1a_2...a_nb_1b_2...b_n)$

come il rapporto plurisezionale delle rispettive immagini in $\mathbb{P}^1$ tramite la proiezione di centro p. Si provi che si tratta di una buona definizione e che quindi il rapporto plurisezionale è invariante per proiettività. (Sugg. Siano p, q due centri di proiezione e prendere coordinate affini tali che $\overline{pq}$ è la retta all'infinito. Non è restrittivo assumere che $\overline{pq}$ non contenga nessun punto a_i; si scriva quindi $(a_1a_2...a_nb_1b_2...b_n)$ come un prodotto di rapporti semplici.)

ESERCIZIO 46: (Teorema di Menelao, (I sec. d.c.))

Siano $a_1, a_2, a_3 \in \mathbb{P}^2$ i vertici di un triangolo e $b_i \in \overline{a_ia_{i+1}}$ punti distinti dai vertici. Provare che b_1, b_2, b_3 sono allineati se e solo se $(a_1a_2a_3b_1b_2b_3) = 1$ (Sugg. considerare $\overline{b_1b_2}$ come retta all'infinito).

ESERCIZIO 47: (Teorema di Ceva, 1678)

Siano $a_1, a_2, a_3 \in \mathbb{P}^2$ non allineati e $b_i \in \overline{a_ia_{i+1}}$ punti distinti dai vertici. Provare che le rette $L_i = \overline{a_ib_{i+1}}$ sono concorrenti se e solo se $(a_1a_2a_3b_1b_2b_3) = -1$ (Sugg. Sia p un punto generico contenuto nella retta $\overline{b_2b_3}$ e si consideri la proiezione di centro p sulla retta $\overline{a_1a_2}$).

ESERCIZIO 48: Sia $\mathbb{K}$ algebricamente chiuso e $\phi \in Aut(\mathbb{P}^1)$ di ordine finito non divisibile per la caratteristica di $\mathbb{K}$. Provare che ϕ ha esattamente due punti fissi

ESERCIZIO 49: (caratteristica $\neq 2$) Una quaterna ordinata $p_1, ..., p_4$ di punti distinti di $\mathbb{P}^1$ definisce un omomorfismo iniettivo di gruppi $h\colon \Gamma_4 \to PGL(2, \mathbb{K}) = Aut(\mathbb{P}^1)$ caratterizzato dalla proprietà che per ogni permutazione $\sigma \in \Gamma_4$ vale $h(\sigma)(p_i) = p_{\sigma(i)}$. Provare che non esiste alcun sollevamento di h ad un omomorfismo $\Gamma_4 \to GL(2, \mathbb{K})$. (Sugg. Non è restrittivo assumere $\mathbb{K}$ algebricamente chiuso; si prenda una coordinata affine tale che la quaterna sia $1, -1, a, -a$ con $a \neq \pm 1$.)

ESERCIZIO 50: Trovare una elemento di ordine 2 di $PGL(2, \mathbb{Q})$ che non si rappresenta con elementi di ordine finito di $GL(2, \mathbb{Q})$

ESERCIZIO 51: Sia $G = \mathbb{K} - 0$ il gruppo moltiplicativo, $n \geq 2$ un intero e si assuma che esista un sottogruppo finito $H \subset G$ di ordine d tale che G è generato da H e dalle potenze n-esime di elementi di G. Sia inoltre h il massimo divisore di n non divisibile dalla caratteristica di $\mathbb{K}$.

Per ogni sottogruppo finito $\Gamma \subset PGL(n, \mathbb{K})$ di ordine m esiste un sottogruppo finito $\Gamma' \subset GL(n, \mathbb{K})$ di ordine $\leq hdm$ che si mappa surgettivamente su Γ tramite la proiezione naturale $GL(n, \mathbb{K}) \to PGL(n, \mathbb{K})$.

ESERCIZIO 52: Una quaterna di punti distinti di $\mathbb{P}^1$ è equianarmonica se e solo se il birapporto è invariante per l'azione del gruppo alterno A_4.

ESERCIZIO 53: Il gruppo simmetrico Σ_4 contiene esattamente tre sottogruppi di ordine 8 (2-Sylow) tra loro coniugati e isomorfi al gruppo diedrale D_4. Provare che una quaterna

è armonica se e solo se il birapporto è invariante per l'azione di un sottogruppo di ordine 8 di Σ_4.

ESERCIZIO 54: Si consideri l'applicazione $f:\mathbb{P}^1\to\mathbb{P}^n$, definita in coordinate omogenee da $f([x_0,x_1])=[x_0^n,x_0^{n-1}x_1,....,x_1^n]$. Provare che se $p_0,..,p_{n+1}$ sono punti distinti di $\mathbb{P}^1$ allora $f(p_0),...,f(p_{n+1})$ è un sistema di riferimento su $\mathbb{P}^n$

ESERCIZIO 55: Si consideri il piano $\mathbb{R}^2$ con la metrica euclidea usuale, per ogni $p\in\mathbb{R}^2$ sia $F_p\simeq\mathbb{P}^1_{\mathbb{R}}$ il fascio di rette per il punto p. Verificare che l'applicazione $F_p\to F_p$ che manda ogni retta nella sua perpendicolare è una proiettività. Tale proiettività è chiamata *involuzione degli angoli retti.*

ESERCIZIO 56: (Luogo polare)
Sia $o\in\mathbb{P}^1$ e G un insieme di n punti distinti $p_1,....,p_n$ di $\mathbb{P}^1$. Si definisce il luogo polare di o rispetto a G come l'insieme dei punti $q\in\mathbb{P}^1$ che in coordinate affini soddisfano la condizione

$$\sum_{i=1}^{n}(oqp_1)=\sum_{i=1}^{n}\frac{o-p_1}{q-p_1}=0$$

Scrivere la precedente relazione in funzione delle coordinate omogenee di $o,p_1,...,p_n,q$ e mostrare che la definizione del luogo polare non dipende dalla scelta del sistema di coordinate omeogenee scelto. Provare inoltre che se $o=\infty$ e $p_1,...,p_n\in\mathbb{K}$ sono le radici di un polinomio monico f di grado n allora il luogo polare di ∞ rispetto a $p_1,...,p_n$ è l'insieme delle radici della derivata f' di f.

II. Forme binarie

Uno dei settori trainanti della geometria algebrica nel periodo 1840-1890 è stato senza dubbio la teoria algebrica degli invarianti. In questo capitolo ripercorriamo alcune delle principali conquiste di quel periodo, culminate con i teoremi della base e degli zeri di Hilbert, studiando gli invarianti di forme binarie.
Riprendendo la terminologia usata all'epoca useremo il termine forma (binaria, ternaria, etc..) per indicare un polinomio omogeneo (in due, tre, etc.. variabili).
Supporremo per semplicità $\mathbb{K}$ campo di caratteristica 0 o sufficientemente alta (rispetto ai gradi dei polinomi considerati).

1. Risoluzione per radicali dell'equazione di terzo grado

In questo paragrafo $\mathbb{K}$ denota un campo algebricamente chiuso di caratteristica $\neq 2,3$.
Sia $f(x)=x^3+3a_1x^2+3a_2x+a_3$, essendo $\mathbb{K}$ algebricamente chiuso si può scrivere

$$f(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3),\qquad \alpha_i\in\mathbb{K}$$

A meno di sostituire x con $x-a_1$ si può tranquillamente assumere $a_1=0$ e quindi

$$f(x)=x^3+3a_2x+a_3$$

Esistono tre casi in cui l'equazione $f(x)=0$ è particolarmente semplice da risolvere:

1) Se $a_2=0$, allora $x=\sqrt[3]{-a_3}$.
2) Se $a_3=0$, allora $x=0,\sqrt{-3a_2}$.
3) Se f e $f'=3(x^2+a_2)$ hanno un fattore comune allora l'equazione si riduce ad una equazione di secondo grado.

Assumiamo quindi di non essere in nessuno dei tre casi precedenti, in particolare f possiede tre radici distinte.
È buona regola, di fronte a equazioni di qualsiasi tipo e grado, cercare le simmetrie del sistema, cioè i gruppi di trasformazioni che lasciano invariato (nella sostanza) il sistema di equazioni.

Su $\mathbb{K}$ è naturale considerare i seguenti gruppi:

1) Trasformazioni lineari; sono le trasformazioni del tipo $x \to \lambda x$, si vede subito che f è invariante per una tale trasformazione se e solo se $a_2 = 0, \lambda^3 = 1$ oppure $a_3 = 0, \lambda^2 = 1$ oppure $a_2 = a_3 = 0$.

2) Trasformazioni affini; sono le trasformazioni del tipo $x \to \lambda x + \eta$, si vede subito che f può essere invariante solo se $\eta = 0$, cioè solo se la trasformazione è lineare.

3) Trasformazioni proiettive; sono le trasformazioni del tipo

$$x \to \frac{ax+b}{cx+d} \qquad ad \neq bc.$$

Una tale proiettività agisce sul proiettivizzato dello spazio vettoriale dei polinomi di grado $\leq n$ e trasforma la classe $[g(x)]$ di grado n in

$$\left[g\left(\frac{ax+b}{cx+d}\right)(cx+d)^n \right].$$

Siccome le tre radici di f sono distinte, esiste una unica proiettività ψ tale che $\psi(\alpha_1) = \alpha_2$, $\psi(\alpha_2) = \alpha_3$, $\psi(\alpha_3) = \alpha_1$. Evidentemente $\psi^3 = Id$ e f è un autovettore per l'azione di ψ sullo spazio dei polinomi di terzo grado, per le ipotesi fatte su f sappiamo che ψ non è una affinità, cioè il punto all'infinito non è un punto fisso di ψ. Siano $n, m \in \mathbb{K}$ i punti fissi di ψ. I due polinomi $x - n$, $x - m$ sono entrambi autovettori per l'azione di ψ e, detti λ_1, λ_2 i rispettivi autovalori, si ha $\lambda_1^3 = \lambda_2^3$.
Siccome $n \neq m$ esiste un polinomio $g(y)$ di grado al più tre tale che

$$f(x) = g\left(\frac{x-n}{x-m}\right)(x-m)^3$$

e tale che g è un autovettore per l'azione $y \to \xi y$, dove ξ è una radice primitiva tripla di 1. Dunque $g(y)$ deve essere necessariamente del tipo $ay^3 + b$, abbiamo quindi dimostrato la seguente

Proposizione 1.1. *Sia f un polinomio di terzo grado con radici distinte e siano n, m i punti fissi della proiettività che induce una permutazione ciclica delle radici di f.*
Esistono allora due costanti a, b tali che $f(x) = a(x-n)^3 + b(x-m)^3$.

Da tale risultato è facile ricavare la formula risolutiva dell'equazione di terzo grado, abbiamo infatti

$$x^3 + 3a_2x + a_3 = t(x-n)^3 + (1-t)(x-m)^3$$

che equivale al sistema

$$\begin{cases} tn = (t-1)m \\ tn^2 + (1-t)m^2 = a_2 \\ tn^3 + (1-t)m^3 = -a_3 \end{cases}$$

che, essendo $n - m \neq 0$ si riconduce facilmente al sistema

$$\begin{cases} tn = (t-1)m \\ nm = -a_2 \\ n + m = -\dfrac{a_3}{a_2} \end{cases}$$

Si tratta di un sistema di secondo grado simmetrico dal quale si può ricavare n , m e t.

Le radici di f sono quindi le radici dell'equazione

$$\left(\frac{x-n}{x-m}\right)^3 = \frac{t-1}{t} = \frac{n}{m}$$

che si calcolano esattamente e sono

$$\alpha_i = \frac{m\sqrt[3]{n} - n\sqrt[3]{m}}{\sqrt[3]{n} - \sqrt[3]{m}}$$

ESERCIZIO 1: Se f possiede una radice multipla la precedente equazione risolutiva degenera alla forma $\alpha_i = \dfrac{0}{0}$.

Nel capitolo sulle curve piane ridurremo l'equazione di quarto grado ad una di terzo grado (equazione risolvente) ed a due equazioni di secondo grado. È ben noto che per polinomi di grado ≥ 5 non esiste la risolubilità per radicali.

Un problema intermedio (rispetto al problema della risolubilità delle equazioni) è il seguente:

Dati due polinomi $f(x), g(x)$ di grado n, esiste una proiettività ψ che trasforma le radici di f nelle radici di g?

Tale problema ha perfettamente senso per ogni $n \geq 4$ ed è perfettamente risolubile anche se in caso di risposta positiva non esiste nessuna formula in grado di determinare ψ. Di tale problema inizieremo ad occuparci a partire dal prossimo paragrafo.

ESERCIZIO 2: Sia f un polinomio di grado 4 senza radici multiple, Allora f è autovettore per almeno tre proiettività distinte ψ_1, ψ_2, ψ_3 tali che $\psi_i^2 = Id$.

2. Invarianti e Covarianti di forme binarie

Abbiamo appena avuto un efficace esempio di come la geometria della retta proiettiva si applica allo studio delle equazioni polinomiali $f(x) = 0$. In tale contesto è utile considerare al posto dei polinomi le forme binarie.

Definizione 2.1. Una **forma binaria** di grado n è un polinomio omogeneo di grado n in due variabili.

Le forme binarie di grado n formano uno spazio vettoriale V_n di dimensione $n+1$ su $\mathbb{K}$. Per ragioni di convenienza notazionale, che appariranno più chiare in seguito, scriviamo ogni forma binaria nel modo seguente:

$$f(x_0,x_1)=a_0x_0^n+\binom{n}{1}a_1x_0^{n-1}x_1+\ldots+\binom{n}{i}a_ix_0^{n-i}x_1^i+\ldots+a_nx_1^n$$

dove $a_0,\ldots,a_n\in V_n^\vee=\mathrm{Hom}_{\mathbb{K}}(V_n,\mathbb{K})$ sono le coordinate di f. Esiste una naturale applicazione bilineare $V_a\times V_b\to V_{a+b}$ data dalla moltiplicazione.

Per ogni $n\geq 0$ esiste un isomorfismo naturale fra V_n e lo spazio vettoriale dei polinomi di grado $\leq n$ in una variabile x. Data una $f\in V_n$, la sua disomogeneizzazione $f(x,1)$ è un polinomio di grado $\leq n$. Viceversa dato un polinomio $p(x)$ di grado $\leq n$, la sua omogeneizzazione è la forma binaria definita da

$$f(x_0,x_1)=x_1^np\left(\frac{x_0}{x_1}\right)$$

da questo isomorfismo segue immediatamente che, se $\mathbb{K}$ è algebricamente chiuso, ogni forma binaria è il prodotto di forme binarie di grado 1 e che quindi ogni forma binaria non nulla di grado n possiede esattamente n radici (contate con molteplicità) su $\mathbb{P}^1=\mathbb{P}(V_1^\vee)$.

È inoltre chiaro che le radici di $f(x,1)$ sono esattamente le radici di $f(x_0,x_1)$ che stanno nella parte affine $\{x_1\neq 0\}$ di $\mathbb{P}^1$.

Lemma 2.2. *Due forme binarie non nulle hanno le stesse radici nella chiusura algebrica di $\mathbb{K}$, contate con molteplicità, se e solo se sono proporzionali.*

Dim. Evidente. □

Si noti che il lemma 2.2 definisce una bigezione fra $\mathbb{P}^n=\mathbb{P}(V_n)$ ed il quoziente di $(\mathbb{P}^1)^n$ per l'azione del gruppo simmetrico Σ_n.

Ogni isomorfismo lineare $\psi\colon V_1\to V_1$ induce in modo naturale una proiettività $[\psi]$ di $\mathbb{P}^1=\mathbb{P}(V_1^\vee)$, più precisamente se $p\in\mathbb{P}^1$ è il punto di coordinate omogenee $[p_0,p_1]$ si definisce $[\psi](p)$ come la radice di $\psi(p_1x_0-p_0x_1)$.

Ogni proiettività si ottiene in questo modo e $[\psi_1]=[\psi_2]$ se e solo se ψ_1 e ψ_2 sono proporzionali.

ESERCIZIO 3: Sia $\mu_n\subset\mathbb{C}$ l'insieme delle radici n-esime di 1, determinare il gruppo delle proiettività ϕ di $\mathbb{P}^1_{\mathbb{C}}$ tali che $\phi(\mu_n)=\mu_n$.

Tramite la base canonica x_0,x_1 di V_1 si definisce un isomorfismo tra $GL(2,\mathbb{K})$ ed il gruppo degli automorfismi lineari di V_1

$$\begin{pmatrix}a&c\\b&d\end{pmatrix}x_0=ax_0+bx_1,\quad\begin{pmatrix}a&c\\b&d\end{pmatrix}x_1=cx_0+dx_1$$

L'azione di $GL(2,\mathbb{K})$ si estende in modo unico ad una azione sinistra su V_n in modo compatibile con i prodotti $V_a\times V_b\to V_{a+b}$. Se $f\in V_n$ e g è il suo disomogeneizzato si ha

$$\begin{pmatrix}a&c\\b&d\end{pmatrix}f(x_0,x_1)=f(ax_0+bx_1,cx_0+dx_1)\quad\begin{pmatrix}a&c\\b&d\end{pmatrix}g(x)=g\left(\frac{ax+b}{cx+d}\right)(cx+d)^n$$

Ogni polinomio $p(a_0,\ldots,a_n)$ può essere pensato come una funzione $p\colon V_n\to\mathbb{K}$, esiste allora una ovvia azione destra di $GL(2,\mathbb{K})$ su $\mathbb{K}[a_0,\ldots,a_n]$ data da

$$p^A(f)=p(Af),\qquad A\in GL(2,\mathbb{K}),\quad p\in\mathbb{K}[a_0,\ldots,a_n],\quad f\in V_n$$

Esempio 2.3. Se

$$n=2,\quad p=a_0a_2-a_1^2,\quad A=\begin{pmatrix}a&c\\b&d\end{pmatrix}$$

si ha allora $p^A=p\det^2A=\det A^2$, infatti

$$p^A(a_0x_0^2+2a_1x_0x_1+a_2x_1^2)=p(a_0(ax_0+bx_1)^2+2a_1(ax_0+bx_1)(cx_0+dx_1)+a_2(cx_0+dx_1)^2)$$

$$=(a_0a^2+2a_1ac+a_2c^2)(a_0b^2+2a_1bd+a_2d^2)-(a_0ab+a_1(ad+bc)+a_2cd)^2$$

$$=(a_0a_2-a_1^2)(ad-bc)^2=p(a_0x_0^2+2a_1x_0x_1+a_2x_1^2)\det A^2$$

Si noti che $a_0a_2-a_1^2=0$ se e solo se f ha una radice doppia.

Definizione 2.4. Un polinomio $p(a_0,\ldots,a_n)$ si dice una **forma covariante** su V_n di peso m se per ogni $A\in GL(2,\mathbb{K})$ vale $p^A=p\det^mA$.

L'esempio 2.3 mostra che $a_0a_2-a_1^2$ è un covariante su V_2 di peso 2. Si noti che ogni covariante è costante sulle orbite di $SL(2,\mathbb{K})$, in particolare le uniche forme covarianti su V_1 sono le costanti.

Proposizione 2.5. *Sia $p(a_0,\ldots,a_n)$ una forma covariante di peso m su V_n. Allora p è omogeneo di grado $\frac{2m}{n}$ ed isobaro di peso m.*

In particolare ogni monomio di p contiene un fattore a_i per qualche $i\geq\frac{n}{2}$.

Dim. Vale $p^A=p\det A^m$ per ogni matrice A diagonale. Sia $A=diag(\alpha,\beta)$ e sia $q=a_0^{i_0}\ldots a_n^{i_n}$ un monomio di grado $d=i_0+\ldots+i_n$ e peso $m=i_1+2i_2+\ldots+ni_n$. Vale $\det A=\alpha\beta$ e $q^A=q\alpha^{dn-m}\beta^m$ e quindi q può comparire in p solo se $dn-m=m$. Si noti infine che la condizione $dn=2m$ implica necessariamente $i_s>0$ per qualche $s\geq\frac{n}{2}$. □

ESERCIZIO 4: Provare che un polinomio omogeneo $p\in\mathbb{K}[a_0,\ldots,a_n]$ è un covariante se e solo se $p^A=p$ per ogni $A\in SL(2,\mathbb{K})$.

ESERCIZIO 5: Se p è una forma covariante di peso m allora vale $p(a_n, a_{n-1}, ..., a_0) = (-1)^m p(a_0, ..., a_n)$.

ESERCIZIO 6: Una forma non nulla

$$f(x_0, x_1) = a_0 x_0^n + \binom{n}{1} a_1 x_0^{n-1} x_1 + ... + \binom{n}{i} a_i x_0^{n-i} x_1^i + ... + a_n x_1^n$$

possiede una radice di molteplicità n se e solo se

$$rango \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = 1.$$

Un polinomio $p \in \mathbb{K}[a_0, ..., a_n]$ si dice SL-invariante se $p^A = p$ per ogni $A \in SL(2, \mathbb{K})$: i polinomi SL-invarianti formano una sottoalgebra $R \subset \mathbb{K}[a_0, ..., a_n]$, per l'esercizio precedente R coincide con la sottoalgebra generata delle forme covarianti. Chiameremo R **algebra dei covarianti** su V_n.

Corollario 2.6. *Sia p un covariante su V_n e sia $f \in V_n$. Se f possiede una radice di molteplicità $> \frac{n}{2}$ allora $p(f) = 0$.*

Dim. Siccome p è covariante basta dimostrare che $p(Af) = 0$ per qualche $A \in GL(2, \mathbb{K})$, non è quindi restrittivo supporre che f abbia in 0 una radice di molteplicità d con $2d > n$. Quindi x_0^d divide f e $a_s = 0$ per ogni $s > n - d$, basta allora applicare 2.5. □

È utile osservare che p è un covariante di peso m se e solo se $p^A = p \det^m A$ per ogni A appartenente ad un insieme fissato di generatori di $GL(2, \mathbb{K})$. Un conveniente insieme di generatori è dato dall'unione dei seguenti tre insiemi:

i) Matrici diagonali $x_i \to \lambda_i x_i$, $i = 0, 1$.

ii) Inversione $x_0 \to x_1$, $x_1 \to x_0$.

iii) Traslazioni $x_0 \to x_0 + a x_1$, $x_1 \to x_1$.

Dimostreremo in seguito il tutt'altro che evidente fatto che è sufficiente verificare la covarianza per le diagonali e le traslazioni.

Usiamo adesso il teorema sulle funzioni simmetriche (vedi esercizi) per costruire in modo intuitivo (ma poco rigoroso) alcuni covarianti non banali su V_n per ogni $n \geq 2$; si assuma per semplicità $\mathbb{K} = \mathbb{R}, \mathbb{C}$.

Siano $\alpha_1, ..., \alpha_n$ le radici di un polinomio $f(x) = a_0 x^n + n a_1 x^{n-1} + ... + a_n$, si assuma $a_0 a_n \neq 0$ e si consideri

$$D = \prod_{i \neq j} (\alpha_i - \alpha_j)$$

Si tratta di una polinomio simmetrico in $\alpha_1, ..., \alpha_n$ e quindi si può scrivere $D = D(\sigma_1, ..., \sigma_n)$ dove $\sigma_i = (-1)^i \binom{n}{i} \frac{a_i}{a_0}$ indica la i-esima funzione simmetrica elementare.

Dimostriamo adesso che $\Delta = a_0^{2(n-1)} D$ è un polinomio in $a_0, ..., a_n$ covariante di peso $n(n-1)$ su V_n. $\Delta(f)$ viene detto **discriminante** di f.

La dimostrazione completa e rigorosa che Δ è un polinomio , cioè che non contiene potenze di a_0 al denominatore sarà data nel capitolo III: si tratta comunque di un fatto abbastanza ovvio dal punto di vista intuitivo, infatti per ogni polinomio monico fissato $g(x)$ di grado $n-1$ con radici $\beta_1, ..., \beta_{n-1}$, esiste una costante C dipendente da g tale che posto $f(x) = (a_0 x - 1) g(x)$ vale $\Delta(f) = C a_0^{2(n-1)} \prod_{i=1}^{n-1} (a_0^{-1} - \beta_i)^2$ e quindi esiste finito il limite di $\Delta(f)$ per $a_0 \to 0$.

La covarianza di Δ rispetto alle traslazioni è automatica, rimane da verificare la covarianza rispetto alle matrici diagonali ed all'inversione.

Sia $A = diag(\lambda, \xi)$, allora $A(x_0 - \alpha_i x_1) = \lambda x_0 - \alpha_i \xi x_1$ e quindi A trasforma la radice α_i in $\lambda^{-1} \xi \alpha_i$, mentre trasforma il coefficiente a_0 in $\lambda^n a_0$, ne segue che

$$\Delta^A = \Delta (\lambda^{-1} \xi)^{n(n-1)} \lambda^{2n(n-1)} = \Delta \det A^{n(n-1)}$$

L'inversione manda α_i in α_i^{-1} e a_0 in a_n, dunque

$$\Delta^A = a_n^{2(n-1)} \prod_{i \neq j} \frac{(\alpha_i - \alpha_j)}{\alpha_i \alpha_j} = \Delta$$

dove nell'ultima uguaglianza abbiamo fatto uso della relazione $a_n = a_0 \alpha_1 ..... \alpha_n$.

Siccome le $f \in V_n$ con $a_0 a_n \neq 0$ sono un aperto denso la relazione $\Delta(Af) = \Delta(f) \det A^{n(n-1)}$ vale per ogni f, A e quindi Δ è un covariante.

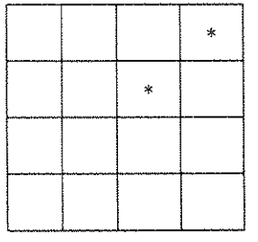
Usando la stessa idea si possono costruire altri covarianti di peso multiplo di n, diamo qui solo l'algoritmo di costruzione lasciando per esercizio le verifiche di covarianza.

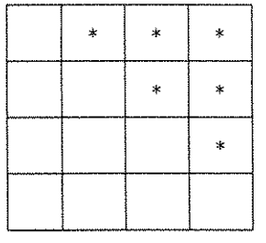
Si consideri una tabella quadrata di lato n $T = \{(i, j) \in \mathbb{N}^2 | 1 \leq i, j \leq n\}$ e sia $S \subset T$ un sottoinsieme con le seguenti proprietà:

1) Se $(i, j) \in S$ allora $i < j$.

2) Detto r_i (risp.: c_i) il numero di elementi di S sulla i-esima riga (risp.: colonna) allora $r_i + c_i = m$ non dipende da i.

Le seguenti due tabelle forniscono due esempi di tali insiemi per $n = 4$





Un covariante di peso nm è allora dato da

$$\Delta_S = a_0^{2m} \sum_{\sigma \in \Sigma_n} \prod_{(i,j)\in S} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)})^2$$

Si noti che Δ_S non è identicamente nullo, come si vede considerando un polinomio a radici razionali distinte.

Con un conto che omettiamo si calcola il discriminante di una forma di terzo grado che, a meno di uno scalare, vale

$$\Delta = a_0^2 a_3^2 - 3a_1^2 a_2^2 + 4a_1^2 a_3 + 4a_0 a_2^3 - 6a_0 a_1 a_2 a_3.$$

Dati due covarianti P, Q su V_n dello stesso peso, $Q \neq 0$, il quoziente $\dfrac{P}{Q}$ si dice un **invariante razionale** su V_n. Se $U \subset V_n$ è l'insieme delle forme f tali che $Q(f) \neq 0$ allora $AU \subset U$ per ogni $A \in GL(2, \mathbb{K})$ ed è definita una funzione

$$\frac{P}{Q}: U \to \mathbb{K} \qquad \frac{P}{Q}(f) = \frac{P(f)}{Q(f)}$$

con le proprietà:

i) $\dfrac{P}{Q}(Af) = \dfrac{P}{Q}(f)$ per ogni $A \in GL(2, \mathbb{K})$.

ii) $\dfrac{P}{Q}(\lambda f) = \dfrac{P}{Q}(f)$ per ogni $\lambda \in \mathbb{K}^*$.

Le proprietà i) e ii) implicano tra l'altro che se $f, g \in U$ ed esiste una proiettività di $\mathbb{P}^1$ che trasforma gli zeri di f (contati con molteplicità) negli zeri di g allora $\dfrac{P}{Q}(f) = \dfrac{P}{Q}(g)$.

Proposizione 2.7. *L'algebra dei covarianti su V_2 e V_3 è generata dal discriminante.*

Dim. Consideriamo il caso V_3, la dimostrazione nel caso V_2 è sostanzialmente identica. Sia P un covariante, esistono allora interi positivi r, s tali che P^r, Δ^s hanno lo stesso peso e quindi $\phi = \dfrac{P^r}{\Delta^s}$ è un invariante razionale. Detto $U = \{f | \Delta(f) \neq 0\}$ si ha che $f \in U$ se e solo se f possiede tre radici distinte; siccome due terne su $\mathbb{P}^1$ sono sempre proiettivamente equivalenti ϕ è uguale su U ad una costante c. Basta adesso osservare che Δ è irriducibile e che $\Delta(P^r - c\Delta^s) = \Delta P^r - c\Delta^{s+1}) = 0$. □

ESERCIZIO 7: Le funzioni simmetriche elementari $\sigma_1, .., \sigma_n \in \mathbb{Z}[x_1, ..., x_n]$ sono definite dalla relazione $t^n + \sum \sigma_i t^{n-i} = \prod (t + x_i)$.

Sia $f \in \mathbb{Z}[x_1, ..., x_n]$ simmetrica di peso m e sia $f = f_0 + ... + f_m$ la decomposizione in componenti isobare. Provare che ogni monomio di f_m è del tipo $ax_1^{i_1} x_2^{i_2} ... x_n^{i_n}$ con $i_1 \leq i_2 \leq ... \leq i_n$ e quindi che esiste un polinomio g tale che $f_m(x_1, ..., x_n) = g(y_1, ..., y_n)$ dove $y_i = x_i x_{i+1} .. x_n$ e che la funzione $f - g(\sigma_n, \sigma_{n-1}, ..., \sigma_1)$ è simmetrica di peso $< m$. Dedurre che $\sigma_1, .., \sigma_n$ generano la sottoalgebra delle funzioni simmetriche.

3. Il metodo simbolico di Cayley-Aronhold

Sia V_d lo spazio vettoriale delle forme binarie di grado d, V_d è uno spazio vettoriale su $\mathbb{K}$ di dimensione $d+1$, definiamo l'isomorfismo standard $V_d \simeq \mathbb{K}^{d+1}$ associando alla $d+1$-upla $(a_0, ..., a_d)$ la forma

$$a_0 x_0^d + \binom{d}{1} a_1 x_0^{d-1} x_1 + ... + \binom{d}{i} a_i x_0^{d-i} x_1^i + ... a_d x_1^d.$$

Esistono degli ovvi morfismi $V_a \times V_b \to V_{a+b}$ dati dalla moltiplicazione; si noti che negli isomorfismi standard l'elevazione a potenza $V_1 \to V_d$ si rappresenta come

$$(t_0, t_1) \to (t_0^d, t_0^{d-1} t_1, ..., t_0^{d-i} t_1^i, ..., t_1^d).$$

In particolare ogni applicazione lineare $F: V_d \to \mathbb{K}$ induce una applicazione $\tilde{F}: V_1 \to \mathbb{K}$, $\tilde{F}(p) = F(p^d)$, omogenea di grado d.

Viceversa, ogni $\tilde{G}: V_1 \to \mathbb{K}$ omogenea di grado d è indotta da una unica applicazione lineare $G: V_d \to \mathbb{K}$. Infatti si ha $\tilde{G}(\alpha_0 x_0 + \alpha_1 x_1) = \tilde{g}(\alpha_0, \alpha_1)$ con $\tilde{g}$ polinomio omogeneo di grado d, detto $a_i = \alpha_0^{d-i} \alpha_1^d$ si ha $\tilde{g}(\alpha_0, \alpha_1) = g(a_0, ..., a_d)$ con g omogeneo di grado 1. Se si pone $G(\sum a_i \binom{d}{i} x_0^{d-i} x_1^d) = g(a_0, ..., a_d)$ si verifica immediatamente che $G(p^d) = \tilde{G}(p)$ per ogni $p \in V_1$.

Si prova similmente che l'applicazione $F \to \tilde{F}$ definisce un isomorfismo di spazi vettoriali.

Si consideri adesso uno spazio vettoriale V di dimensione finita, data una $\hat{F}: V^d \to \mathbb{K}$ multilineare simmetrica si definisce in modo naturale una $F: V \to \mathbb{K}$ omogenea di grado d ponendo $F(v) = \hat{F}(v, ..., v)$. Il procedimento $\hat{F} \to F$ prende il nome di **restituzione**.

Viceversa, data una $F: V \to \mathbb{K}$ omogenea di grado d e $v_1, ..., v_d \in V$ esiste unico un polinomio omogeneo simmetrico f di grado d tale che

$$F(\lambda_1 v_1 + ... + \lambda_d v_d) = f(\lambda_1, ..., \lambda_d)$$

per ogni $\lambda_1, ... \lambda_d \in \mathbb{K}$.

Si può quindi definire $\hat{F}(v_1, ..., v_d)$ come il coefficiente di $\lambda_1 .... \lambda_d$ in f diviso per $d!$.

L'operazione $F \to \hat{F}$ si chiama **polarizzazione**.

Proposizione 3.1. *La polarizzazione è l'inverso della restituzione: in particolare $\hat{F}$ è multilineare simmetrica.*

Dim. Chiaramente $\hat{F}$ è simmetrica, per dimostrare la multilinearità basta dimostrare che $\hat{F}(aw_1 + bw_2, v_2, ..., v_d) = a\hat{F}(w_1, v_2, ..., v_d) + b\hat{F}(w_2, v_2, ..., v_d)$.

Sia $c_i = d!\hat{F}(w_i, v_2, ..., v_d)$, $i = 1, 2$, dal fatto che F è omogeneo di grado d segue che il coefficiente di $\lambda_2...\lambda_d$ in $F(aw_1 + bw_2 + \lambda_2 v_2 + ... + \lambda_d v_d)$ è una forma lineare in a e b che deve necessariamente essere $c_1 a + c_2 b$.

Basta adesso notare che, per ogni d-upla $z_1, ..., z_d \in V$ $d!\hat{F}(z_1, ..., z_d)$ può essere definito come il coefficiente di $\lambda_2...\lambda_d$ in $f(1, \lambda_2, ..., \lambda_d) = F(z_1 + \lambda_2 z_2 + ... + \lambda_d z_d)$ e quindi $\hat{F}(aw_1 + bw_2, v_2, ..., v_d) = c_1 a + c_2 b$.

Indichiamo con R l'operatore di restituzione e con P quello di polarizzazione. Data una $F: V \to \mathbb{K}$ omogenea di grado d e $v \in V$ si ha $F(\lambda_1 v + ... + \lambda_d v) = (\lambda_1 + ... + \lambda_d)^d F(v)$ ed il coefficiente di $\lambda_1...\lambda_d$ in $(\lambda_1 + ... + \lambda_d)^d$ è esattamente $d!$, questo prova che $R \circ P = Id$.

Viceversa sia $\hat{F}$ multilineare simmetrica e siano $v_1, ...v_d \in V$ fissati, detto $w = \lambda_1 v_1 + ... + \lambda_d v_d$ si ha

$$\hat{F}(w, ..., w) = \hat{f}(\lambda_1, ..., \lambda_d)$$

per un opportuno polinomio omogeneo $\hat{f}$, essendo $\hat{F}$ simmetrica il coefficiente di $\lambda_1...\lambda_d$ in $\hat{f}$ è esattamente $d!\hat{F}(v_1, ..., v_d)$, questo prova che $P \circ R = Id$. □

Si noti che le operazioni di polarizzazione e restituzione commutano con le azioni naturali di $GL(V)$.

Ritorniamo agli spazi V_d, un ragionamento analogo al precedente mostra che esiste una bigezione naturale fra le

$$\phi: V_d \times ... \times V_d \to \mathbb{K} \quad \text{multilineari simmetriche}$$

e le

$$\tilde{\phi}: V_1 \times ... \times V_1 \to \mathbb{K} \quad \text{multiomogenee simmetriche di grado } d$$

La bigezione è data dalla relazione $\tilde{\phi}(p_1, ..., p_s) = \phi(p_1^d, ..., p_s^d)$. Riassumendo abbiamo trovato un procedimento che, partendo da una $\tilde{F}: V_1^s \to \mathbb{K}$ multiomogenea simmetrica di grado d, si passa da una $\hat{F}: V_d^s \to \mathbb{K}$ multilineare simmetrica e si arriva ad una $F: V_d \to \mathbb{K}$ omogenea di grado s. Se inoltre $\tilde{F}$ è $SL(2, \mathbb{K})$-invariante anche F lo è.

In concreto, se $v_i = \alpha_i x_0 + \beta_i x_1$, $i = 1, ..., s$ si ha $\tilde{F}(v_1, ..., v_s) = \tilde{f}(\alpha_1, \beta_1, ..., \alpha_s, \beta_s)$ con $\tilde{f}$ polinomio multiomogeneo simmetrico di grado d.

Per passare da $\tilde{F}$ a $\hat{F}$ si opera la sostituzione $a_{ij} = \alpha_i^{d-j}\beta_i^j$ e si ha $\tilde{f}(\alpha_i, \beta_i) = \hat{f}(a_{ij})$.

Infine si pone $a_j = a_{ij}$ e si ottiene $f(a_0, ..., a_d) = \hat{f}(a_{ij})$ con f polinomio omogeneo di grado s, e usando l'isomorfismo standard si ha infine

$$F(\sum a_i \binom{d}{i} x_0^{d-i} x_1^d) = f(a_0, ..., a_d)$$

Come esempio costruiamo alcune forme covarianti su V_4 di grado $s \leq 3$ ottenute partendo da dei covarianti $\tilde{F}: V_1^s \to \mathbb{K}$ multiomogenei simmetrici di grado 4.

Per $s = 1$ non ci sono covarianti di peso positivo, ciò segue immediatamente dal fatto che $V_1 - \{0\}$ è una orbita per l'azione di $SL(2, \mathbb{K})$.

Per $s = 2$ un covariante naturale è dato da

$$g_2 = \frac{1}{2}\begin{vmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{vmatrix}^4$$

Per $s = 3$ abbiamo

$$g_3 = \frac{1}{6}\begin{vmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{vmatrix}^2 \begin{vmatrix} \alpha_2 & \alpha_3 \\ \beta_2 & \beta_3 \end{vmatrix}^2 \begin{vmatrix} \alpha_3 & \alpha_1 \\ \beta_3 & \beta_1 \end{vmatrix}^2$$

I covarianti g_2, g_3 sono detti di **Eisenstein.**

Applicando il procedimento descritto si ha

$$g_2 = \frac{1}{2}(\alpha_1\beta_2 - \alpha_2\beta_1)^4 = \frac{1}{2}(\alpha_1^4\beta_2^4 - 4\alpha_1^3\beta_1\alpha_2\beta_2^3 + 6\alpha_1^2\beta_1^2\alpha_2^2\beta_2^2 - 4\alpha_1\beta_1^3\alpha_2^3\beta_2 + \beta_1^4\alpha_2^4)$$

$$g_2 = \frac{1}{2}(a_{10}a_{24} - 4a_{11}a_{23} + 6a_{12}a_{22} - 4a_{13}a_{21} + a_{14}a_{20})$$

$$g_2 = \frac{1}{2}(a_0a_4 - 4a_1a_3 + 6a_2^2 - 4a_3a_1 + a_4a_0) = a_0a_4 - 4a_1a_3 + 3a_2^2$$

Si noti che da questa ultima espressione non è affatto evidente la covarianza di g_2.

Prima di affrontare il calcolo esplicito di g_3 osserviamo che, essendo in ogni monomio la somma dei gradi di α_i e β_i uguale a 4 possiamo disomogeneizzare il tutto ponendo $\alpha_i = 1$.

Si ha quindi

$$6g_3 = (\beta_1 - \beta_2)^2(\beta_2 - \beta_3)^2(\beta_3 - \beta_1)^2$$

Dopo aver scritto i 27 addendi di g_3 bisogna sostituire il monomio $\beta_1^i\beta_2^j\beta_3^k$ con $a_ia_ja_k$, si ottiene quindi una grande semplificazione da cui

$$g_3 = a_0a_2a_4 - a_0a_3^2 + 2a_1a_2a_3 - a_2^3 - a_1^2a_4$$

Come prima non è affatto evidente da questa ultima espressione che si tratti di un covariante. Un piccolo aiuto può venire osservando che g_2 e g_3 sono rispettivamente, a meno di costanti moltiplicative, lo Pfaffiano ed il determinante delle matrici

$$\begin{pmatrix} 0 & a_0 & 2a_1 & 3a_2 \\ -a_0 & 0 & a_2 & 2a_3 \\ -2a_1 & -a_2 & 0 & a_4 \\ -3a_2 & -2a_3 & -a_4 & 0 \end{pmatrix} \qquad \begin{pmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{pmatrix}$$

Lemma 3.2. *I covarianti $g_2, g_3 \in \mathbb{K}[a_0, ..., a_4]$ sono algebricamente indipendenti su $\mathbb{K}$.*

Dim. Sia $P=\sum_{i=0}^{s} c_i g_2^{\beta_i} g_3^{\gamma_i}$ con $c_i \neq 0$ per ogni i, dobbiamo dimostrare che $P \neq 0$ in $\mathbb{K}[a_0,...,a_4]$. A meno di permutare gli indici si può supporre che per ogni $i>0$ vale $\beta_0+\gamma_0 > \beta_i+\gamma_i$ oppure che $\beta_0+\gamma_0=\beta_i+\gamma_i$, $\gamma_0>\gamma_i$.
Si vede facilmente che il coefficiente in P di $a_0^{\beta_0+\gamma_0}a_4^{\beta_0}a_3^{2\gamma_0}$ è uguale a $\pm c_0$ che è non nullo. □

Vedremo più avanti che g_2 e g_3 generano l'algebra dei covarianti di V_4.
Sia $f \in V_4$ senza radici multiple e sia $x=\frac{x_0}{x_1}$ una coordinata affine sulla retta proiettiva. Con una opportuna proiettività possiamo mandare una radice all'infinito ed il baricentro delle altre 3 nello 0, dunque f è proiettivamente equivalente ad una forma binaria del tipo $4a_1x^3+4a_3x+a_4$, $a_1\neq 0$. A meno di moltiplicare f per uno scalare possiamo supporre $a_1=1$, si ottiene quindi la **forma canonica** delle forme binarie di grado 4 senza radici multiple

$$4x^3-px-q, \qquad a_0=a_2=0,\ a_1=1,\ a_3=-\frac{p}{4},\ a_4=-q$$

Si ha quindi $g_2=a_0a_4-4a_1a_3+3a_2^2=p$, $g_3=a_0a_2a_4-a_0a_3^2+2a_1a_2a_3-a_2^3-a_1^2a_4=q$ da cui si deduce il

Teorema 3.3. *Ogni forma binaria f di grado 4 a radici distinte con covarianti g_2, g_3 è equivalente alla forma di equazione non omogenea*

$$4x^3-g_2x-g_3.$$

Dim. Evidente. □

Teorema 3.4. *Sia $f\in V_4$. Allora f possiede radici multiple se e solo se $(g_2^3-27g_3^2)(f)=0$.*

Dim. Se f possiede una radice multipla allora f è equivalente ad una forma binaria in cui $a_0=a_1=0$, per tale forma si ha $g_2=3a_2^2$, $g_3=-a_2^3$ e quindi $g_2^3=27g_3^2$.
Viceversa se f non ha radici multiple il polinomio $p(x)=4x^3-g_2x-g_3$ non ha radici in comune con la sua derivata $p'(x)=12x^2-g_2$, cioè

$$0\neq p\left(\pm\sqrt{\frac{g_2}{12}}\right)=\pm\left(\frac{g_2}{27}\right)^{\frac{3}{2}}-g_3$$

e quindi $27g_3^2\neq g_2^3$. □

Si definisce l'invariante j di una forma binaria di grado 4 come

$$j=1728\frac{g_2^3}{g_2^3-27g_3^2}$$

Il motivo del coefficiente $1728=12^3$ è motivato dalla teoria delle curve ellittiche su campi di caratteristica 2 e 3, cf. [Sil].

ESERCIZIO 8: Provare che $g_2^3-27g_3^2$ differisce per una costante moltiplicativa dal discriminante Δ

Corollario 3.5. *Due forme binarie di grado 4 a radici distinte sono equivalenti se e solo se hanno lo stesso invariante j.*

Dim. Siano $f_1,f_2\in V_4$ senza radici multiple con lo stesso invariante j, non è restrittivo supporre f_1,f_2 in forma canonica

$$f_1=4x^3-p_1x-q_1, \quad f_2=4x^3-p_2x-q_2$$

in tali forme l'uguaglianza dell'invariante j equivale alla relazione $p_1^3q_2^2=p_2^3q_1^2$.
Dimostriamo che esiste $t\in\mathbb{K}^*$ tale che $f_2(x)=t^3f_1(t^{-1}x)$ o in termini equivalenti che $p_2=t^2p_1$, $q_2=t^3q_1$. Se $p_1=0$ allora $q_1\neq 0$ e dunque anche $p_2=0$ e t esiste. Se $p_1\neq 0$ allora anche $p_2\neq 0$ e con un t opportuno si può assumere $p_1=p_2$ e quindi $q_1=\pm q_2$, basta quindi considerare $t=\pm 1$. □

Data una quaterna non ordinata di punti $Q=\{p_1,...p_4\}\subset\mathbb{P}^1$, $p_i\neq p_j$, è ben definito $j(Q)$ come l'invariante j di una forma binaria che ha come zeri esattamente $p_1,..,p_4$, il corollario 3.5 afferma che due quaterne non ordinate sono proiettivamente equivalenti se e solo se hanno lo stesso invariante j. Dunque j ha la stessa funzione che ha il birapporto rispetto alle quaterne ordinate di punti.

Proposizione 3.6. *Una quaterna non ordinata Q di punti distinti è:*

i) Armonica se e solo se $g_3=0$ (Salmon, 1859).

ii) Equianarmonica se e solo se $g_2=0$ (Painvin, 1861).

Dim. I covarianti g_2 e g_3 di $4x(x-1)(x-\lambda)$ sono

$$g_2=\frac{4}{3}(\lambda^2-\lambda+1)m \quad g_3=\frac{4}{27}(\lambda+1)(\lambda-2)(2\lambda-1)$$

□

ESERCIZIO 9: Siano $\alpha_1,\alpha_2,\alpha_3$ le radici di $4x^3-g_2x-g_3$, si provi che

$$g_2^3-27g_3^2=16(\alpha_1-\alpha_2)^2(\alpha_2-\alpha_3)^2(\alpha_3-\alpha_1)^2$$

ESERCIZIO 10: Sia $f(x)=x(x-1)(x-\lambda)$, $\lambda\neq 0,1$, vale allora

$$j(f)=2^8\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$$

ESERCIZIO 11: Sia $j\in\mathbb{K}$ e sia λ una radice di

$$f(\lambda)=2^8(\lambda^2-\lambda+1)^3-j\lambda^2(\lambda-1)^2=0$$

allora le sei radici di f contate con molteplicità sono esattamente

$$\lambda, \quad \frac{1}{\lambda}, \quad 1-\lambda, \quad 1-\frac{1}{\lambda}, \quad \frac{1}{1-\lambda}, \quad \frac{\lambda}{\lambda-1}$$

Mostrare inoltre che f possiede radici multiple se e solo se $j = 0, 1728$. Confrontare il presente risultato con i possibili birapporti di una quaterna non ordinata di punti.

4. Finita generazione dell'algebra dei covarianti

Abbiamo visto che in generale una sottoalgebra di $\mathbb{K}[a_0, ...a_n]$ non è finitamente generata, in questa sezione mostreremo che l'algebra dei covarianti è finitamente generata. Per fare ciò abbiamo bisogno di caratterizzare i covarianti su V_n come soluzioni di certe equazioni differenziali.

Lemma 4.1. *Il gruppo $GL(2,\mathbb{K})$ è generato dalle matrici diagonali e dalle matrici triangolari aventi 1 sulla diagonale.*

Dim. Basta osservare che

$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

e ricordarsi che $GL(2)$ è generato dalle matrici triangolari inferiori e dalla matrice che rappresenta l'inversione. □

Per ogni $t \in \mathbb{K}$ definiamo

$$h(t) = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \quad d(t) = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \quad \delta(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$

(naturalmente $h(t)$ viene definita solo per $t \neq 0$)

Proposizione 4.2. *Sia $P \in \mathbb{K}[a_0, ..., a_n]$ omogeneo di grado d ed isobaro di peso $\frac{1}{2}nd$. Allora P è un covariante se e solo se $P^{d(t)} = P^{\delta(t)} = P$ per ogni $t \in \mathbb{K}$.*

Dim. Le condizioni sul grado e sul peso equivalgono alla covarianza di P rispetto al sottogruppo delle matrici diagonali. □

Studiamo adesso l'invarianza rispetto alle matrici triangolari inferiori $d(t)$ (traslazioni), per quelle superiori basterà scambiare x_0 con x_1 e a_i con a_{n-i}.

Si noti che $(P+Q)^{d(t)} = P^{d(t)} + Q^{d(t)}$, $(P^{d(t)})^{d(s)} = P^{d(t+s)}$.

Sia S_d lo spazio vettoriale dei polinomi omogenei di grado d in $a_0, ..., a_n$, si osserva facilmente che S_d è stabile per l'azione di $GL(2,\mathbb{K})$, in particolare esiste una applicazione polinomiale

$$\mathbb{K} \times S_d \to S_d, \quad (t, P) \to P^{d(t)}$$

È possibile interpretare t come una indeterminata e quindi $P^{d(t)} \in \mathbb{K}[a_0, ..., a_n, t]$, $P^{d(0)} = P$ e si può scrivere lo sviluppo di Taylor rispetto a t

$$P^{d(t)} = P + tP' + \frac{1}{2}t^2P'' + ... + \frac{1}{d!}t^dP^{(d)}$$

dove $P^{(i)} \in S_d$ e $P' = \frac{\partial}{\partial t}P^{d(t)}_{|t=0}$.

Lemma 4.3. *Nelle notazioni precedenti $P^{d(t)} = P$ per ogni $t \in \mathbb{K}$ se e solo se $P' = 0$.*

Dim. Una implicazione è ovvia, si assuma $P' = 0$, per ogni $c \in \mathbb{K}$ vale

$$P^{d(c+t)} = (P^{d(t)})^{d(c)} = P^{d(c)} + \frac{1}{2}(P'')^{d(c)}t^2 + ...$$

Dunque $\frac{\partial}{\partial t}P^{d(t)}_{|t=c} = 0$ e siccome c è arbitrario ne segue che $P^{d(t)}$ non dipende da t. □

Siccome $P^b(a_0, ..., a_n) = P(a_0^b, ..., a_n^b)$ e

$$a_i^{d(t)} = a_i + \binom{n}{i}^{-1}\binom{n}{i-1}(n-i+1)ta_{i-1} + ...$$

Si ha dunque $a_i' = ia_{i-1}$ e per la regola di derivazione della funzione composta

$$P' = \sum_{i=0}^{n}\frac{\partial P}{\partial a_i}a_i' = \sum_{i=0}^{n} ia_{i-1}\frac{\partial P}{\partial a_i}$$

La precedente relazione si può scrivere come $P' = DP$ dove D è l'operatore differenziale lineare del primo ordine

$$D = \sum_{i=0}^{n} ia_{i-1}\frac{\partial}{\partial a_i}$$

Scambiando x_0 con x_1 e a_i con a_{n-i} l'operatore D si trasforma nell'operatore

$$\Delta = \sum_{i=0}^{n} ia_{n-i+1}\frac{\partial}{\partial a_{n-i}} = \sum_{i=0}^{n}(n-i)a_{i+1}\frac{\partial}{\partial a_i}$$

Scriviamo $S_d = \oplus S_{d,m}$ dove $S_{d,m}$ è il sottospazio vettoriale dei polinomi isobari di peso m. Si noti che $S_{d,m} \neq 0$ se e solo se $0 \leq m \leq nd$ e che $DS_{d,m} \subset S_{d,m-1}$, $\Delta S_{d,m} \subset S_{d,m+1}$. È inoltre conveniente introdurre un operatore $H: S_{d,m} \to S_{d,m}$, $HP = (nd - 2m)P$. Si estende poi per linearità H, D, Δ ad operatori definiti su $\mathbb{K}[a_0, ..., a_n]$, si verifica facilmente che H, D, Δ sono $\mathbb{K}$-derivazioni e per i risultati precedenti un polinomio P appartiene all'algebra dei covarianti se e solo se $HP = DP = \Delta P = 0$.

Lemma 4.4. *Valgono le seguenti regole di commutazione:*

1) $[D,\Delta]=D\Delta-\Delta D=H$.

2) $[H,D]=2D$.

3) $[H,\Delta]=-2\Delta$.

Dim. Dimostriamo solo 1), la dimostrazione di 2) e 3) è simile ed è lasciata per esercizio.

Essendo $[D,\Delta]$ ed H derivazioni basta verificare la relazione sui generatori a_i, in tal caso vale

$$[D,\Delta]a_i=D(n-i)a_{i+1}-\Delta i a_{i-1}=((i+1)(n-i)-i(n-i+1))a_i=(n-2i)a_i=Ha_i.$$

□

Nota: La maggior parte dei lettori avrà riconosciuto in 4.4 le regole di commutazione dell'algebra di Lie $sl(2)$ [Hu].

Sullo spazio degli operatori differenziali lineari agisce l'operatore T di inversione geometrica $x_i\to x_{1-i}, a_i\to a_{n-i}$, si osserva facilmente che $TD=\Delta$, $T\Delta=D$, $TH=-H$.

Siano $D^k\colon S_{d,m}\to S_{d,m-k}$, $\Delta^k\colon S_{d,m}\to S_{d,m+k}$ le iterate di D e Δ.

Lemma 4.5. *Per ogni* $k>0$ *vale*

1) $[D^k,\Delta]=D^{k-1}(kH+k(k-1))$

2) $[D,\Delta^k]=\Delta^{k-1}(kH-k(k-1))$

Dim. Basta dimostrare 1), il punto 2) segue da 1) applicando l'inversione geometrica T. Se $k=1$ ritroviamo esattamente il lemma 4.4. Usando induzione su k e la regola di Leibnitz per la derivata di Lie

$$[AB,C]=A[B,C]+[A,C]B$$

si ottiene

$$[D^{k+1},\Delta]=D^k[D,\Delta]+[D^k,\Delta]D=$$

$$=D^kH+D^{k-1}(kH+k(k-1))D=D^k((k+1)H+(k+1)k).$$

□

Siamo adesso in grado di dimostrare il

Teorema 4.6. *$P\in S_d$ è covariante se e solo se soddisfa due delle seguenti tre condizioni:*

1) $HP=0$.

2) $DP=0$.

3) $\Delta P=0$.

Dim. Basta dimostrare che due condizioni implicano la terza.

2)+3)$\Rightarrow$ 1) segue subito da $[D,\Delta]=H$.

1)+2)$\Rightarrow$ 3). Siccome $HP=0$ P è isobaro di peso $m=\frac{1}{2}nd$, dato che $S_{d,m+i}=0$ se $i>m$ esiste un intero $k>0$ tale che $\Delta^kP=0$ $\Delta^{k-1}P\neq 0$. Vale allora $0=[D,\Delta^k]P=\Delta^{k-1}k(k-1)P$ da cui segue $k=1$.

1)+3)$\Rightarrow$ 2). Sia $HP=\Delta P=0$, vale quindi $H(TP)=D(TP)=0$ e per il punto precedente $\Delta(TP)=0$ da cui $DP=0$. □

Lemma 4.7. *Sia* $m=\frac{1}{2}nd$, $k\geq 0$ *e* $Q\in S_{d,m-k}$ *tale che* $DQ=0$. *Per ogni* $i=0,\dots,k$ *vale*

$$D^i\Delta^kQ=\frac{(k+i)!}{(k-i)!}\Delta^{k-i}Q$$

Si noti che nella formula non appare il peso.

Dim. Induzione su i, per $i=0$ non c'è nulla da dimostrare.

$$D^{i+1}\Delta^kQ=\frac{(k+i)!}{(k-i)!}D\Delta^{k-i}Q=\frac{(k+i)!}{(k-i)!}\Delta^{k-i-1}((k-i)H-(k-i)(k-i-1))Q=$$

$$=\frac{(k+i)!}{(k-i)!}(k-i)\Delta^{k-i-1}((nd-2(m-k))-(k-i-1))Q=\frac{(k+i)!}{(k-i)!}(k-i)(k+i+1)\Delta^{k-i-1}Q$$

□

Proposizione 4.8. *Siano* $Q,P_1,\dots,P_r$ *forme covarianti su* V_n *di peso* $q,m_1,\dots,m_r$ *e siano* $A_1,\dots,A_r\in\mathbb{K}[a_0,\dots,a_n]$ *tali che* $Q=\sum A_iP_i$.

Esistono allora covarianti $B_1,\dots,B_r$ *di peso* $q-m_1,\dots,q-m_r$ *tali che* $Q=\sum B_iP_i$.

Dim. Non è restrittivo supporre gli A_i omogenei ed isobari di peso $q-m_i$, cioè $HA_i=0$ per ogni i.

Usando induzione su r basta dimostrare che si può trovare una espressione del tipo $Q=\sum B_iP_i$ con B_1 covariante, fatto questo si sostituisce Q con $Q-B_1P_1$. Dimostriamo che tale espressione esiste per induzione sul minimo intero k tale che $D^{k+1}A_1=0$, se $k=0$ allora A_1 è un covariante e non c'è nulla da dimostrare.

Se $k>0$ sia $R=D^kA_1$, per il lemma 4.7 vale

$$D^k\Delta^kR=(2k)!R\qquad D^k(A_1-\frac{1}{(2k)!}\Delta^kD^kA_1)=0$$

Essendo Q,P_i covarianti, per la regola di Leibnitz vale

$$0=\Delta^kD^k(\sum A_iP_i)=\sum(\Delta^kD^kA_i)P_i$$

e quindi

$$Q=\sum_{i=1}^{r}(A_i-\frac{1}{(2k)!}\Delta^k D^k A_i)P_i$$

Si può adesso applicare l'ipotesi induttiva su k e trovare una espressione con A_1 covariante. □

Possiamo adesso dimostrare il teorema principale della sezione

Teorema 4.9.(Gordan 1868) *L'algebra dei covarianti su V_n è finitamente generata su $\mathbb{K}$.*

Nota. La dimostrazione originale di Gordan e le semplificazioni dei contemporanei erano basate sul metodo simbolico e sulla rappresentazione dei covarianti come funzioni simmetriche delle differenze delle radici (cf. [Hilb],[K-R]). Di tali dimostrazioni sopravvive oggi un fondamentale lemma sulla geometria dei coni poliedrali (vedi esercizi).

La dimostrazione che presentiamo si deve sostanzialmente a David Hilbert e si basa sul seguente risultato la cui dimostrazione verrà data nel prossimo paragrafo.

Teorema 4.10.(Della base di Hilbert, 1890) *Ogni ideale di $\mathbb{K}[a_0,...,a_n]$ è finitamente generato.*

Dimostrazione di 4.9. Sia $I\subset\mathbb{K}[a_0,...,a_n]$ l'ideale generato dai covarianti di peso positivo, per il teorema della base di Hilbert I è generato da un numero finito $P_1,...,P_r$ di covarianti.

Sia Q un covariante di peso q, dimostriamo per induzione su q che si può scrivere Q come un polinomio nei P_i a coefficienti in $\mathbb{K}$. Se $q\leq 0$ allora Q è una costante. Se $q>0$ allora $Q\in I$ ed esistono $A_1,...,A_r\in\mathbb{K}[a_0,...,a_n]$ tali che $Q=\sum A_iP_i$. Per la proposizione 4.8 si può scrivere $Q=\sum B_iP_i$ dove ogni B_i è un covariante di peso $<q$ e quindi un polinomio nei P_i. □

Sia $s_n(d,m)$ la dimensione di $S_{d,m}$ e sia $w_n(d,m)$ la dimensione dello spazio vettoriale dei covarianti di peso m e grado d

Teorema 4.11. *Vale*

$$w_n(d,m)=\begin{cases}s_n(d,m)-s_n(d,m-1) & \text{se } 2m=nd,\\ 0 & \text{altrimenti}\end{cases}$$

Dim. Basta dimostrare che se $2m=nd$ allora $D\colon S_{d,m}\to S_{d,m-1}$ è surgettiva. Dimostriamo per induzione decrescente su k che $D^k\colon S_{d,m}\to S_{d,m-k}$ è surgettiva per ogni $k\geq 0$. Se $k>m$ il risultato è banale. Un semplice ragionamento di algebra lineare mostra che D^k è surgettiva se:

1) D^{k+1} è surgettiva.

2) l'immagine di D^k contiene il nucleo di $D\colon S_{d,m-k}\to S_{d,m-k-1}$. La 1) è vera per induzione mentre la 2) segue immediatamente dal lemma 4.7. □

Corollario 4.12. *Sia $2m=nd$, allora $w_n(d,m)$ è il coefficiente di x^m nello sviluppo in serie di*

$$(1-x)\prod_{i=1}^{d}\frac{(1-x^{n+i})}{(1-x^i)}.$$

Dim. Sia

$$\prod_{i=1}^{d}\frac{(1-x^{n+i})}{(1-x^i)}=\sum_{h=0}^{\infty}c_hx^h$$

vale allora

$$(1-x)\prod_{i=1}^{d}\frac{(1-x^{n+i})}{(1-x^i)}=\sum_{h=0}^{\infty}(c_h-c_{h-1})x^h$$

e basta quindi dimostrare che per ogni $h\geq 0$ vale $c_h=s_n(d,h)$.

Sia

$$\phi(x,y)=\prod_{i=0}^{n}(\sum_{h=0}^{\infty}(x^iy)^h)=\prod_{i=0}^{n}\frac{1}{(1-x^iy)}$$

È chiaro che $\phi(x,y)=\sum_{d,m}s_n(d,m)y^dx^m$, infatti il coefficiente di x^my^d nello sviluppo di ϕ coincide con il numero dei multiindici $(i_0,...,i_n)$ di grado d e peso m. Si ha

$$(1-y)\phi(x,y)=\prod_{i=1}^{n}\frac{1}{(1-x^iy)}=(1-x^{n+1}y)\prod_{i=1}^{n+1}\frac{1}{(1-x^iy)}=(1-x^{n+1}y)\phi(x,xy)$$

Da tale equazione ne segue che, scrivendo $\phi(x,y)=\sum G_i(x)y^i$, vale $G_0=1$ e

$$(1-y)\sum G_i(x)y^i=(1-x^{n+1}y)\sum G_i(x)x^iy^i$$

ed eguagliando i coefficienti di y^i

$$G_i-G_{i-1}=G_ix^i-G_{i-1}x^{n+i}$$

per induzione si deduce quindi che

$$G_i(x)=\frac{(1-x^{n+i})}{(1-x^i)}G_{i-1}=\prod_{j=1}^{i}\frac{(1-x^{n+i})}{(1-x^i)}.$$

In particolare $G_d(x)=\sum c_hx^h$ e la dimostrazione è conclusa. □

Nei prossimi esempi useremo la seguente notazione: se $f(x)=\sum a_ix^i$ è una serie di potenze denoteremo $\{f(x)\}_{x^i}=a_i$.

Esempio 4.13. Applichiamo il corollario 4.12 per calcolare $w_4(d,2d)$

$$w_4(d,2d)=\left\{(1-x)\prod_{i=1}^{d}\frac{(1-x^{4+i})}{(1-x^i)}\right\}_{x^{2d}}=$$

$$=\left\{\frac{(1-x^{d+1})(1-x^{d+2})(1-x^{d+3})(1-x^{d+4})}{(1-x^2)(1-x^3)(1-x^4)}\right\}_{x^{2d}}$$

Possiamo manipolare la formula togliendo termini che non influenzano il coefficiente di x^{2d},

$$w_4(d,2d)=\left\{\frac{1-x^{d+1}-x^{d+2}-x^{d+3}-x^{d+4}}{(1-x^2)(1-x^3)(1-x^4)}\right\}_{x^{2d}}$$

$$w_4(d,2d)=\left\{\frac{1}{(1-x^2)(1-x^3)(1-x^4)}\right\}_{x^{2d}}-\left\{\frac{x(1+x+x^2+x^3)}{(1-x^2)(1-x^3)(1-x^4)}\right\}_{x^d}$$

dove abbiamo usato l'ovvio fatto che $\{x^a\phi(x)\}_{x^b}=\{\phi(x)\}_{x^{b-a}}$. Siccome $1-x^4=(1-x)(1+x+x^2+x^3)$ si ha

$$w_4(d,2d)=\left\{\frac{1}{(1-x^2)(1-x^3)(1-x^4)}\right\}_{x^{2d}}-\left\{\frac{x}{(1-x^2)(1-x^3)(1-x)}\right\}_{x^d}$$

$$w_4(d,2d)=\left\{\frac{1}{(1-x^2)(1-x^3)(1-x^4)}-\frac{x^2}{(1-x^2)(1-x^4)(1-x^6)}\right\}_{x^{2d}}$$

$$w_4(d,2d)=\left\{\frac{1+x^3-x^2}{(1-x^2)(1-x^4)(1-x^6)}\right\}_{x^{2d}}$$

Siccome nello sviluppo del denominatore compaiono solo potenze pari di x si può togliere x^3 dal numeratore e si ottiene la formula finale

$$w_4(d,2d)=\left\{\frac{1}{(1-x^4)(1-x^6)}\right\}_{x^{2d}}=\{(a,b)\in\mathbb{N}^2|4a+6b=2d\}$$

Ricordiamo che i covarianti $g_2^ag_3^b$ sono linearmente indipendenti e dalla formula precedente segue che quelli di grado d sono esattamente $w_4(d,2d)$, quindi g_2,g_3 generano l'algebra dei covarianti di V_4.

ESERCIZIO 12: Sia $n=2d$ e sia $a_{ij}=a_{i+j}$, $0\le i,j\le d$, mostrare che $P=\det(a_{ij})$ è un covariante non banale su V_n (Sugg. provare direttamente che $P'=0$).

ESERCIZIO 13: Sia $n=4d$ e sia $a_{ij}=(j-i)a_{i+j-1}$, $0\le i,j\le 2d+1$, mostrare che lo Pfaffiano di a_{ij} è un covariante non banale su V_n (Sugg. vedi esercizio precedente).

Proposizione 4.14. *Siano $Q\in\mathbb{K}[a_0,...,a_n]$, $f_1,...,f_s\in V_n$, $c_1,...,c_s\in\mathbb{K}$ tali che $Q(Af_i)=Q^A(f_i)=c_i$ per ogni $A\in SL(2,\mathbb{K})$, $i=1,...,s$.*
Esiste allora un SL-invariante P tale che $P(f_i)=c_i$ per ogni $i=1,...,s$.

Dim. Sia $Q=\sum Q_l$ dove $HQ_l=lQ_l$, si verifica facilmente che $Q^{h(t)}=\sum t^lQ_l$ e quindi per ogni $A\in SL(2,\mathbb{K})$ fissato vale

$$Q^{h(t)}(Af_i)=\sum t^lQ_l(Af_i)=c_i$$

da cui ne segue che $Q_0(Af_i)=c_i$ e si può dunque supporre $Q=Q_0$, $HQ=0$.
Dalla definizione di D e Δ si ha per ogni $P\in\mathbb{K}[a_0,...,a_n]$, $f\in V_n$

$$DP(f)=\frac{\partial}{\partial t}_{|t=0}P(d(t)f)\quad \Delta P(f)=\frac{\partial}{\partial t}_{|t=0}P(\delta(t)f)$$

da cui si deduce che $DQ(f_i)=0$, $\Delta Q(f_i)=0$ e per induzione su k $\Delta^kD^kQ(f_i)=0$.
Sia k il più piccolo intero positivo tale che $D^{k+1}Q=0$, posto $\hat{Q}=Q-\frac{1}{(2k)!}\Delta^kD^kQ$, vale $D^k(\hat{Q})=0$ e $\hat{Q}(Af_i)=c_i$. La dimostrazione si conclude con la solita induzione decrescente su k. □

ESERCIZIO 14: Si provi che ogni fattore irriducibile di un covariante è covariante.

ESERCIZIO 15: Sia $f(x,y)$ una forma binaria di grado n su $\mathbb{C}$. Provare che $f=(ax+by)^n$ se e solo se il determinante Hessiano di f è nullo.

5. Anelli Noetheriani

In questa sezione dimostreremo il teorema della base di Hilbert. Per future applicazioni è conveniente inquadrare il teorema in un ambito più astratto di quello considerato precedentemente.

Definizione 5.1. Un anello in cui ogni ideale è finitamente generato si dice **Noetheriano**.

Lemma 5.2. *Per un anello A le seguenti condizioni sono equivalenti:*

1) A è Noetheriano.
2) Ogni catena ascendente di ideali in A è stazionaria.
3) Ogni famiglia di ideali di A contiene un elemento massimale.

Dim. 1) $\Rightarrow$ 2). Sia I_v, $v\in V$ una catena ascendente di ideali e sia $I=\cup I_v$. L'ideale I è finitamente generato diciamo da $a_1,...,a_n$; se $a_i\in I_{v_i}$ allora detto w il massimo di $v_1,..,v_n$ si ha che $I\subset I_w\subset I_v\subset I$ per ogni $v\ge w$ e quindi la catena è stazionaria.
2)$\Rightarrow$3). Applicazione standard del lemma di Zorn, i dettagli sono lasciati per esercizio al lettore.
3)$\Rightarrow$1). Sia I un ideale e sia $J\subset I$ un elemento massimale della famiglia degli ideali finitamente generati contenuti in I, dimostriamo che $J=I$. Sia $a\in I$ allora l'ideale

$J + (a) \subset I$ è ancora finitamente generato e per la massimalità di J si deve avere $a \in J$. □

Emmy Noether (figlia di Max) è stata la prima a introdurre nel 1923 la nozione di catena ascendente di ideali ed a studiare la classe degli anelli, oggi chiamati in suo onore, Noetheriani.

I campi e gli anelli ad ideali principali sono tutti Noetheriani.

Teorema 5.3.(Della base di Hilbert) *Se A è Noetheriano allora anche $A[x]$ è Noetheriano.*

Dim. Dato un polinomio $f \in A[x]$ di grado $r \geq 0$ chiameremo coefficiente direttore di f il coefficiente di x^r in f, è ovvio che $f, xf, x^2f, ...$ hanno tutti lo stesso coefficiente direttore.

Sia $I \subset A[x]$ un ideale e per ogni $m \geq 0$ sia $J_m \subset A$ l'insieme dei coefficienti direttori dei polinomi di grado m. Si osserva immediatamente che J_m è un ideale e che $J_m \subset J_{m+1}$ per ogni m. Per ipotesi A è Noetheriano, dunque gli ideali J_m sono tutti finitamente generati e la catena $\{J_m\}$ è stazionaria.

Sia $N > 0$ tale che $J_m = J_N$ per ogni $m \geq N$ e per ogni $i = 0, ..., N$ siano $f_1^i, ..., f_j^i \in I$ polinomi di grado i i cui coefficienti direttori generano J_i. Sia $H \subset I$ l'ideale generato dai polinomi f_j^i, $i = 0, .., N$, e proviamo che $H = I$. Sia infatti $f \in I$ e scriviamo $f = h + g$ con $h \in H$ e g di grado minimo e si assuma per assurdo $g \neq 0$. Sia $r = \min(\deg(g), N)$, il coefficiente direttore di g appartiene a J_r e quindi esistono $a_1, ..., a_j \in A$ tali che, detto $s = \deg(g) - r$, il polinomio $g - (a_1 f_1^r - ... - a_j f_j^r)x^s$ ha grado minore del grado di g. Dato che $\sum a_i f_i^r \in H$ l'assurdo è servito. □

È lecito chiedersi se vale anche il viceversa del teorema, la risposta è si come si vede dalla seguente

Proposizione 5.4. *Sia A un anello Noetheriano e I un ideale. Allora l'anello quoziente A/I è Noetheriano.*

Dim. Sia $\pi: A \to A/I$ la proiezione al quoziente, una catena ascendente di ideali $\{J_v\} \subset A/I$ è stazionaria se e solo se la catena $\{\pi^{-1}(J_v)\} \subset A$ è stazionaria. □

Corollario 5.5. *Per ogni campo $\mathbb{K}$ e per ogni ideale $I \subset \mathbb{K}[x_1, ..., x_n]$ l'anello $\mathbb{K}[x_1, ..., x_n]/I$ è Noetheriano.*

Dim. Evidente. □

ESERCIZIO 16: Sia A un anello Noetheriano , $E \subset A$ un sottoinsieme. Provare che esiste un sottoinsieme finito $E_0 \subset E$ tale che $(E) = (E_0)$.

ESERCIZIO 17: Sia A un anello Noetheriano e $f: A \to A$ un endomorfismo surgettivo di anelli. Provare che f è un isomorfismo.

ESERCIZIO 18: (Moduli Noetheriani)

Un modulo si dice **Noetheriano** se ogni suo sottomodulo è finitamente generato. Si provi:

1) Sia M un modulo e $N \subset M$ un sottomodulo; M è Noetheriano se e solo se N e M/N sono Noetheriani.
2) Se M, N sono Noetheriani allora $M \oplus N$ è Noetheriano.
3) Se A è un anello Noetheriano ogni A-modulo finitamente generato è Noetheriano.

(Sugg. ogni modulo finitamente generato è quoziente di un modulo libero di rango finito).

6. Esercizi complementari

ESERCIZIO 19: Classificare (in caratteristica 0) i polinomi f di grado n tali che

$$nff'' = (n-1)(f')^2$$

ESERCIZIO 20: (*) Una applicazione olomorfa fra due varietà complesse $f: X \to Y$ si dice una immersione chiusa se è propria, iniettiva ed ha differenziale iniettivo in ogni punto.

Siano $f_0, f_1, f_2 \in \mathbb{C}[x_0, x_1]$ omogenei di grado 3 senza zeri comuni, si provi che l'applicazione $f: \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$, $f([x_0, x_1]) = [f_0(x_0, x_1), f_1(x_0, x_1), f_2(x_0, x_1)]$ non è una immersione chiusa (Sugg. usare 1.1).

ESERCIZIO 21: (**) Sia $\mathbb{K}$ un campo di caratteristica $\neq 2$ e $A \subset \mathbb{K}[x_0, ..., x_n]$ la sottoalgebra delle funzioni invarianti per l'azione del gruppo alterno A_{n+1}. Provare che A è generata dalle funzioni simmetriche elementari e dal determinante della matrice di Vandermonde.

(Sugg. Per ogni $a \geq 0$ scriviamo

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ x_0^{a+1} & x_1^{a+1} & \dots & x_n^{a+1} \\ x_0^{a+2} & x_1^{a+2} & \dots & x_n^{a+2} \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{a+n} & x_1^{a+n} & \dots & x_n^{a+n} \end{vmatrix} = P_a(x_0, ..., x_n) - D_a(x_0, ..., x_n)$$

dove P_a e D_a indicano le somme dei termini presenti nello sviluppo del determinante, relativi alle permutazioni di segnatura pari e dispari rispettivamente. Provare dapprima che A è generata dalle funzioni simmetriche e dalle funzioni D_a, $a \geq 0$.)

ESERCIZIO 22: Determinare un insieme di generatori della sottoalgebra di $\mathbb{Q}[x_0, .., x_3]$ delle funzioni invarianti per l'azione del gruppo trirettangolo.

ESERCIZIO 23: Un modo alternativo per dimostrare che ogni covariante $p(a_0,...,a_4)$ di grado d su V_4 si può scrivere come polinomio in g_2, g_3 è il seguente:

i) Se d è dispari allora $p(x^3-x)=0$.

ii) Se $d=2h$, a meno di sostituire p con $p-cg_2^h$ per un opportuna costante c si può supporre $p(x^3-x)=0$.

iii) Se $p(x^3-x)=0$ allora g_3 divide p.

(Sugg. Siccome $-4g_3=4a_2^3-h_2a_2-h_3$, con $h_2,h_3\in\mathbb{K}[a_0,a_1,a_3,a_4]$, per la divisione euclidea si può scrivere $p=qg_3+r$ con r di grado ≤ 2 rispetto alla variabile a_2. Immergere $\mathbb{K}$ in una chiusura algebrica e provare che $(g_2^3-27g_3^2)(h_2^3-27h_3^2)r=0$).

ESERCIZIO 24: (*) Mostrare che

$$w_2(d,d)=\left\{\frac{1}{(1-x^2)}\right\}_{x^d},\quad w_3(d,\frac{3}{2}d)=\left\{\frac{1}{(1-x^4)}\right\}_{x^d}$$

(Sugg. vedi [Hilb])

ESERCIZIO 25: Caratterizzare $s_n(d,m)$ come il numero di sottotabelle S di una tabella rettangolare $n\times d$ tali che:

a) S contiene m elementi.

b) Se $(i,j)\in S$ allora $(h,l)\in S$ per ogni $h\leq i$, $l\leq j$.

Dedurne la *legge di reciprocità di Hermite* $s_n(d,m)=s_d(n,m)$, $w_n(d,m)=w_d(n,m)$.

Nota: Una sottotabella S definita come sopra viene detta anche *Diagramma di Young.*

ESERCIZIO 26: Dimostrare la legge di reciprocità di Hermite utilizzando il corollario 4.12.

ESERCIZIO 27: (Il lemma di Gordan)

Un sottoinsieme $C\subset\mathbb{R}^n$ si dice un cono se $0\in C$ e se per ogni numero reale $t>0$, $tC=C$. Si denoti $x\cdot y$ il prodotto scalare usuale in $\mathbb{R}^n$. Un cono C si dice poliedrale se esiste un insieme finito di vettori $y_1,...,y_r$ tali che $C=\{x|x\cdot y_i\geq 0\,\forall i=1,..,r\}$. Un cono si dice poliedrale razionale se in aggiunta i vettori y_i possono essere scelti a coordinate razionali.

Dato un cono C si definisce il cono duale

$$C^\vee=\{x\in\mathbb{R}^n|x\cdot y\geq 0\,\forall y\in C\}$$

Dimostrare:

i) C cono, allora $C^\vee$ è chiuso e convesso.

ii) (Hahn-Banach) Se C è un cono chiuso e convesso allora $C=C^{\vee\vee}$.

iii) Sia C cono poliedrale razionale, allora $C^\vee$ è poliedrale razionale.

iv) Dato un cono C sia $\mathbb{K}[C]\subset\mathbb{K}[x_1,x_1^{-1},...,x_n,x_n^{-1}]$ la sottoalgebra generata dai monomi x^I, $I\in C\cap\mathbb{Z}^n$. Se C è poliedrale razionale allora $\mathbb{K}[C]$ è finitamente generata.

ESERCIZIO 28: Una forma binaria f si dice:

instabile se $P(f)=0$ per ogni covariante P di grado positivo. (il termine instabile è recente, la denominazione precedente era *nullform*).

semistabile se non è instabile.

stabile se è semistabile e se $\{A\in SL(2,\mathbb{K})|Af=f\}$ è un sottogruppo finito.

Si diano esempi di forme stabili, instabili e semistabili nonstabili. Si classifichi inoltre le forma di grado ≤ 4 secondo le precedenti definizioni. (si noti che la proposizione 4.14 cade a fagiolo nello studio della instabilità di forme binarie)

ESERCIZIO 29: (I Cumulanti).

Sia $\mathbb{K}$ algebricamente chiuso di caratteristica 0 e sia V lo spazio affine dei polinomi monici di grado n nella variabile x.

Dato $f=\prod_{i=1}^n(x-\lambda_i)=x^n-\sigma_1x^{n-1}+...+(-1)^n\sigma_n$ si definisce per ogni $k\geq 0$

$$s_k=\frac{1}{n}\sum_{i=1}^n\lambda_i^k=s_k(\sigma_1,...,\sigma_n),\qquad s_0=1,s_1=\frac{1}{n}\sigma_1$$

$$\sum_{k=1}^\infty c_k\frac{t^k}{k}=\log(\sum_{k=0}^\infty s_k\frac{t^k}{k!})$$

Si provi che per ogni $k\geq 2$, $c_k(\sigma_1,...,\sigma_n)$ è un covariante per l'azione naturale su V del gruppo delle affinità di $\mathbb{K}$ in sé.

ESERCIZIO 30: Provare che non esistono covarianti di grado 3 su V_{22}

ESERCIZIO 31: Siano $f,g\in V_2$ forme binarie di grado 2 senza zeri comuni e sia $J=f_1g_2-f_2g_1\in V_2$ il loro Jacobiano. Provare che le radici di $fJ\in V_4$ formano una quaterna armonica.

ESERCIZIO 32: Sia A un anello e V la famiglia degli ideali di A che non sono finitamente generati. Se $V\neq\emptyset$, i.e. se A non è Noetheriano, allora V contiene elementi massimali rispetto all'inclusione. Inoltre i massimali di V sono ideali primi. (Sugg. Se I è un ideale, $xy\in I$ e $J\subset I$ un ideale tale che $I+(x)=J+(x)$ vale $I=J+x(I:(x))$.)

ESERCIZIO 33: Sia A un anello Noetheriano che contiene $\mathbb{Q}$ come subanello e sia G un gruppo finito di automorfismi di A. Provare che l'anello degli invarianti $A^G\subset A$ è Noetheriano. (Sugg. Operatore di media).

ESERCIZIO 34: Sia A un anello locale Noetheriano con ideale massimale m. Se $m^n=m^{n+1}$ per qualche intero $n\geq 0$ allora $m^n=0$.

ESERCIZIO 35: (Metodo di Hermite per l'integrazione delle funzioni razionali)

Siano $\alpha_1,...,\alpha_r\in\mathbb{K}$ e $a_1,...,a_r$ interi positivi. Per ogni $p(t)\in\mathbb{K}[t]$ la funzione razionale

$$\frac{p(t)}{\prod_{i=1}^r(t-\alpha_i)^{a_i}}$$

si scrive in modo unico come somma di un polinomio e di una combinazione lineare delle funzioni razionali $1/(t-\alpha_i)^j$, $i=1,...,r$, $1 \leq j \leq a_i$.
(Sugg. Sia $d=\sum a_i$, $f(t)=\prod(t-\alpha_i)^{a_i}$, provare che le m funzioni razionali $1/(t-\alpha_i)^j$ sono linearmente indipendenti in $\mathbb{K}(t)$ e generano il sottospazio delle funzioni razionali g/f con g polinomio di grado $< m$.)

ESERCIZIO 36: $(*)$ $\mathbb{K}$ campo di caratteristica 0. Dati $n+1$ polinomi $f_0,...,f_n \in \mathbb{K}[x]$ sia $W \in \mathbb{K}[x]$ il relativo determinante Wronskiano,

$$W=\left|\frac{\partial^i f_j}{\partial x^i}\right| \quad i,j=0,...,n$$

Provare che $W=0$ se e solo se $f_0,...,f_n$ sono linearmente dipendenti in $\mathbb{K}[x]$. (Sugg. Se i polinomi sono linearmente indipendenti e d_i è il grado di f_i non è restrittivo assumere $d_0<d_1<...<d_n$: provare che la derivata $(d_0+...+d_n)$-esima di W è diversa da 0.

III. Teoria elementare dell'eliminazione

Nello studio delle soluzioni di un sistema di equazioni algebriche

$$f_i(x_1,...,x_n)=0 \quad i=1,...,m \quad f_i \in \mathbb{K}[x_1,...,x_n]$$

è naturale cercare di manipolare algebricamente il sistema in modo da ottenere nuove equazioni di più facile comprensione, un caso tipico è il metodo di riduzione a forma triangolare dei sistemi di equazioni lineari.
È generalmente utile considerare, insieme alle equazioni $f_i=0$, delle equazioni $g_j=\sum h_{ji}f_i=0$ tali che nei polinomi g_j alcune delle variabili $x_1,..,x_n$ non compaiono. Le ricette per esplicitare, se esistono, i polinomi g_j nei quali alcune variabili sono state eliminate fanno parte della teoria dell'eliminazione.
Più precisamente la teoria dell'eliminazione si occupa del seguente problema:
Dato un anello A ed un ideale $I \subset A[x_1,...,x_n]$ determinare elementi non banali $I \cap A = I^c$.
Lo strumento fondamentale della teoria dell'eliminazione è il risultante con il quale si riesce a dare una risposta più che soddisfacente al problema precedente nel caso in cui $n=1$ e I è generato da due elementi. Il risultante sarà inoltre lo strumento tecnico più usato nel resto di queste note.

1. Il risultante di due polinomi

Sia A un anello e m,n due interi positivi fissati. Indichiamo con $M \subset A[x]$ il sottomodulo libero dei polinomi di grado $\leq n+m-1$. Ogni elemento $p \in M$ si può rappresentare come un vettore riga $p=(a_0,...,a_{n+m-1})$ se $p=\sum a_i x^{n+m-1-i}$.
Dati $p_0,...,p_{n+m-1} \in M$, $p_i=(a_{i,0},...,a_{i,n+m-1})$ è possibile considerare la matrice $\Delta=(a_{i,j})$ ed il suo determinante $J(p_0,...,p_{n+m-1})=\det\Delta$.
Siano Δ^i i vettori colonna della matrice Δ, si ha

$$P=\begin{pmatrix} p_0 \\ p_1 \\ \vdots \\ p_{n+m-1} \end{pmatrix}=\Delta^0 x^{n+m-1}+\Delta^1 x^{n+m-2}+...+\Delta^{n+m-1}$$

Siccome il determinante J non cambia se lo si calcola in $A[x]$ anziché in A si può scrivere

$$J = \det(\Delta^0, ..., \Delta^{n+m-1}) = \det(\Delta^0, ..., \Delta^{n+m-2}, P)$$

Lo sviluppo di Laplace rispetto all'ultima colonna ci da la seguente

Proposizione 1.1. *Esistono $c_0, ..., c_{n+m-1} \in A$ tali che*

$$J(p_0, ..., p_{n+m-1}) = c_0 p_0 + ... + c_{n+m-1} p_{n+m-1}$$

Si consideri adesso due polinomi $f, g \in A[x]$

$$f(x) = a_0 x^n + a_1 x^{n-1} + ... + a_n, \quad g(x) = b_0 x^m + b_1 x^{m-1} + ... + b_m$$

e si definisce il risultante (n,m)-esimo di f e g

$$R_{n,m}(f,g) = J(x^{m-1}f, x^{m-2}f, ..., f, x^{n-1}g, ..., g)$$

Il risultante $R(f,g)$ di f e g è per definizione il risultante (n,m)-esimo in cui $n = \deg(f)$, $m = \deg(g)$.
In altri termini $R_{n,m}(f,g) = \det Sy_{n,m}(f,g)$ dove $Sy_{n,m}(f,g)$ è la matrice quadrata di ordine $n+m$

$$Sy_{n,m}(f,g) = \begin{pmatrix}
a_0 & a_1 & \dots & \cdot & \cdot & \cdot & \dots & \cdot & a_n & & & \\
 & a_0 & \dots & \cdot & \cdot & \cdot & \dots & \cdot & \cdot & a_n & & \\
 & & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \\
 & & & a_0 & a_1 & a_2 & \dots & \cdot & \cdot & \cdot & \dots & a_n \\
b_0 & b_1 & \dots & \cdot & b_m & & & & & & & \\
 & b_0 & \dots & \cdot & \cdot & b_m & & & & & & \\
 & & \ddots & \vdots & \vdots & \vdots & \ddots & & & & & \\
 & & & b_0 & b_1 & b_2 & \dots & b_m & & & & \\
 & & & & b_0 & b_1 & \dots & \cdot & b_m & & & \\
 & & & & & b_0 & \dots & \cdot & \cdot & b_m & & \\
 & & & & & & \ddots & \vdots & \vdots & \vdots & \ddots & \\
 & & & & & & & b_0 & b_1 & b_2 & \dots & b_m
\end{pmatrix} \tag{1.2}$$

Proposizione 1.3. *Vale:*

a) $R_{n,m}(f,g) = (-1)^{nm} R_{m,n}(g,f)$.

b) Se $b_0 = 0$ *allora* $R_{n,m}(f,g) = a_0 R_{n,m-1}(f,g)$.

c) $R(x^n, g) = g(0)^n$.

d) Si assuma $n \geq m$ *e sia* h *un polinomio di grado* $\leq n-m$, *allora*

$$R_{n,m}(f,g) = R_{n,m}(f + hg, g).$$

e) $R(xf,g) = g(0)R(f,g)$, $R_{n,m}(af,bg) = a^m b^n R_{n,m}(f,g)$ *per ogni* $a, b \in A$.

f) Esistono $F, G \in A[x]$ *polinomi di grado* $\leq n-1$, $\leq m-1$ *rispettivamente tali che* $R_{n,m}(f,g) = Gf + Fg$, *in particolare* $R(f,g)$ *appartiene all'ideale generato da* f *e* g.

g) Se f *è monico di grado* n *e* a_{ij} *è la matrice quadrata di ordine* n *a coefficienti in* A *tale che*

$$x^i g = h_i f + \sum_{j=0}^{n-1} a_{ij} x^j, \qquad h_i \in A[x], \qquad i = 0, ..., n-1$$

allora $R(f,g) = \det(a_{ij})$. *In particolare per* f *monico fissato il risultante* $R(f,g)$ *dipende solo dalla classe di* g *in* $A[x]/(f)$.

Dim. a), b), c), d) ed e) seguono da 1.2 e dalle proprietà elementari del determinante mentre f) è una conseguenza immediata della proposizione 1.1.
Per il punto g) basta osservare che se m è il grado di g allora ogni polinomio $h_i f$ è una combinazione lineare a coefficienti in A di $f, xf, ..., x^{m-1}f$. È dunque possibile sommare ad ognuna delle ultime n righe della matrice $Sy_{n,m}(f,g)$ dei multipli delle prime m righe in modo tale che diventi una matrice della forma

$$\begin{pmatrix} T & * \\ 0 & a_{ij} \end{pmatrix}$$

con T matrice triangolare superiore di ordine m con i coefficienti della diagonale tutti uguali a 1. □

La matrice $Sy_{n,m}(f,g)$ si dice matrice di Sylvester della coppia (f,g) e l'espressione del risultante come determinante di $Sy_{n,m}(f,g)$ viene detta formula di Sylvester.
Il risultante è chiaramente funtoriale in A, più precisamente se $\phi: A \to B$ è un omomorfismo di anelli, ϕ si estende in modo ovvio ad un omomorfismo $\phi: A[x] \to B[x]$ tale che $\phi(x) = x$ e vale $R(\phi(f), \phi(g)) = \phi(R(f,g))$.

Proposizione 1.4. (invarianza per traslazione) *Per ogni* $a \in A$ *vale* $R(f(x-a), g(x-a)) = R(f(x), g(x))$.

Dim. Sia $M_d \subset A[x]$ il modulo dei polinomi di grado $\leq d-1$, M_d possiede una base canonica $1, x, ..., x^{d-1}$ ed il risultante è esattamente il determinante dell'applicazione $M_m \oplus M_n \to M_{n+m}$ $(p,q) \to fp + gq$ calcolato rispetto alle basi canoniche.
Basta quindi osservare che l'isomorfismo di traslazione $T_a: A[x] \to A[x]$, $T_a(x) = x-a$, $T_a(b) = b$ se $b \in A$ preserva i sottomoduli M_d e su ciascuno di essi si rappresenta con una matrice triangolare con tutti 1 sulla diagonale ed ha quindi determinante 1. □

Corollario 1.5. *Se* $f = a_0 \prod_{i=1}^{n}(x-\alpha_i)$ *allora* $R_{n,m}(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i)$ *e quindi se* $g = b_0 \prod_{i=1}^{m}(x-\beta_i)$ *vale*

$$R_{n,m}(f,g) = a_0^m b_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j)$$

In particolare valgono le relazioni di bilinearità

$$R_{n+n',m}(ff',g) = R_{n,m}(f,g)R_{n',m}(f',g), \quad R_{n,m+m'}(f,gg') = R_{n,m}(f,g)R_{n,m'}(f,g').$$

Dim. Per la proposizione 1.3 non è restrittivo supporre $a_0 = 1$, dimostriamo che vale $R_{n,m}(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i)$ per induzione su n; se $n = 0$ non c'è nulla da dimostrare, sia $n > 0$ e scriviamo $f = (x-\alpha_1)f'$ per la proposizione precedente

$$R_{n,m}(f,g) = R_{n,m}((x-\alpha_1)f'(x), g(x)) = R_{n,m}(xf'(x+\alpha_1), g(x+\alpha_1))$$

e per 1.3 si ha dunque

$$R_{n,m}(f,g) = g(\alpha_1)R_{n-1,m}(f'(x+\alpha_1), g(x+\alpha_1)) = g(\alpha_1)R_{n-1,m}(f'(x), g(x))$$

Le relazioni di bilinearità sono chiaramente funtoriali, si può quindi assumere senza perdita di generalità che $A = \mathbb{Z}[a_i, a_i', b_i]$ dove a_i, a_i', b_i sono indeterminate che rappresentano i coefficienti di f, f' e g. Dunque non è restrittivo assumere A dominio di integrità. Basta adesso immergere A in una chiusura algebrica del suo campo delle frazioni per avere la completa riducibilità di f, f', g, e quindi la dimostrazione della bilinearità come conseguenza immediata della rapprentazione di R come funzione della differenza delle radici. □

Corollario 1.6. *Sia* A *un dominio a fattorizzazione unica,* $f, g \in A[x]$, *allora* f *e* g *possiedono un fattore comune di grado positivo se e solo se* $R(f,g) = 0$.

Dim. Sia $\mathbb{K}$ la chiusura algebrica del campo delle frazioni di A, è allora ben noto che f e g hanno un fattore comune di grado positivo se e solo se hanno una radice comune in $\mathbb{K}$, la tesi segue immediatamente da 1.5. □

ESERCIZIO 1: Si dia una dimostrazione alternativa di 1.6 che utilizzi il punto 1.3.f).

ESERCIZIO 2: Siano $f(x,y), g(x,y)$ polinomi omogenei non nulli a coefficienti in un campo $\mathbb{K}$ di gradi rispettivi n, m. Provare che f e g hanno un fattore comune se e solo se $R_{n,m}(f(x,1), g(x,1)) = 0$.

Mostrare inoltre che per ogni $A \in SL(2,\mathbb{K})$ $R_{n,m}(Af, Ag) = R_{n,m}(f,g)$.

ESERCIZIO 3: Sia A dominio a fattorizzazione unica, $f, g \in A[x]$ polinomi di grado n, m rispettivamente; mostrare che f e g hanno un fattore comune di grado $\geq k > 0$, $k \leq n, m$ se e solo se la matrice $(x^{m-k-1}f, ..., f, x^{n-k-1}g, ..., g)$ non ha rango massimo.

ESERCIZIO 4: (k-risultanti)

Sia A un dominio a fattorizzazione unica e $f, g \in A[x]$ di grado n, m rispettivamente. Per ogni $k \geq 0$ si definisce il k-risultante $R_k(f,g)$ come il determinante della matrice quadrata di ordine $n+m-2k$ ricavata eliminando dalla matrice di Sylvester $Sy_{n,m}(f,g)$ le righe $1, 2, ..., k, m+1, ..., m+k$ e le colonne $1, 2, .., k, n+m, n+m-1, ..., n+m-k+1$. Provare che f e g hanno un fattore comune di grado $> k$ se e solo se $R_0(f,g) = R_1(f,g) = ... = R_k(f,g) = 0$. (Sugg. Induzione su k, la condizione $R_k(f,g) = 0$ equivale all'esistenza di due polinomi A_k, B_k di grado $< m-k, n-k$ rispettivamente tali che $A_k f + B_k g$ ha grado $< k$.)

ESERCIZIO 5: Calcolare esplicitamente il risultante di due polinomi di secondo grado.

Proposizione 1.7. $R_{n,m}(f,g)$ *è isobaro di peso* nm.

Dim. Sia Δ la matrice di Sylvester (1.2), moltiplicare a_i e b_i per t^i equivale a eseguire nell'ordine le seguenti operazioni:

1) moltiplicare per t^i la i-esima colonna di Δ.

2) dividere per t^i la i-esima riga di Δ se $i \leq m$.

3) dividere per t^{i-m} la i-esima riga di Δ se $i > m$.

Alla fine il determinate di Δ risulta moltiplicato per t^e dove

$$e = \sum_{i=1}^{n+m} i - \sum_{i=1}^{m} i - \sum_{i=1}^{n} i = nm.$$

□

Lemma 1.8. *Sia* A *un dominio di integrità e* $0 \neq P \subset A[x]$ *un ideale primo tale che* $P \cap A = 0$. *Sia* $\mathbb{K}$ *il campo delle frazioni di* A *e sia* $P^e \subset \mathbb{K}[x]$ *l'ideale generato da* P. *Allora* P^e *è un ideale primo e* $P^e \cap A[x] = P$.

Dim. Si vede facilmente che $P^e = \{\frac{p}{a} | p \in P, a \in A - \{0\}\}$. Si assuma che $\frac{p_1}{a_1}\frac{p_2}{a_2} \in P^e$ con $p_i \in A[x]$, $a_i \in A$. Allora esiste $a \in A - \{0\}$ tale che $ap_1p_2 \in P$ e siccome $P \cap A = 0$ deve essere $p_1 \in P$ oppure $p_2 \in P$; questo prova che P^e è primo.

Sia $q \in P^e \cap A[x]$, come sopra esiste $a \in A$, $a \neq 0$ tale che $aq \in P$ e quindi $q \in P$. □

Lemma 1.9. *Siano* A, $P \subset A[x]$ *come nel lemma 1.8. Per ogni* $g \notin P$ *esiste* $f \in P$ *tale che* $R(f,g) \neq 0$.

Dim. Per il lemma 1.8 esiste $f \in P$ irriducibile in $\mathbb{K}[x]$ tale che $P^e = (f) \subset \mathbb{K}[x]$. Essendo $g \notin P^e$ si ha $R(f,g) \neq 0$. □

Teorema 1.10. *Sia* A *anello,* $P \subset A[x]$ *ideale primo,* $Q = A \cap P$ *e* $g \notin P$.
Se $P \neq Q[x]$ *allora esiste* $f \in P$ *tale che* $R(f,g) \notin Q$.

Dim. Siccome $Q[x] \subset P$ l'immagine di P in $(A/Q)[x] = A[x]/Q[x]$ è un ideale primo che soddisfa le ipotesi del Lemma 1.9. □

Corollario 1.11. *Siano $P_1 \subset P_2 \subset A[x]$ ideali primi tali che $1 \notin P_2$ e P_1 contiene un polinomio monico. Allora $P_1 \cap A = P_2 \cap A$ se e solo se $P_1 = P_2$.*

Dim. Sia $Q = P_1 \cap A = P_2 \cap A$, siccome Q è un ideale proprio $Q[x]$ non contiene polinomi monici. Se per assurdo esistesse $g \in P_2 - P_1$, allora per il Teorema 1.10 esisterebbe $f \in P_1$ tale che $R(f,g) \notin Q$ in contraddizione con il fatto che $R(f,g) \in (f,g) \subset P_2$. □

2. Il discriminante

Per semplicità espositiva consideriamo il caso in cui A è un dominio di integrità perfetto oppure di caratteristica sufficientemente alta, lasciando le possibili generalizzazioni al lettore interessato.

Dato un polinomio $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n \in A[x]$ $a_0 \neq 0$ e la sua derivata formale $f'(x) = na_0x^{n-1} + ... + a_{n-1}$ si osserva che la prima colonna della matrice di Sylvester della coppia f, f' è divisibile per a_0, esiste dunque unico un elemento $\Delta(f) \in A$ detto **discriminante** di f, tale che

$$\Delta(f) = \frac{1}{a_0}R(f,f') = \frac{1}{a_0}R(f',f).$$

Se A è un dominio a fattorizzazione unica, segue da 1.6 che f possiede un fattore multiplo se e solo se $\Delta(f) = 0$. Come conseguenza immediata di 1.7 abbiamo che se $A = \mathbb{K}[a_0, ..., a_n]$, il discriminante è un polinomio omogeneo di grado $2n-2$ ed isobaro di peso $n(n-1)$.

Siccome la derivazione rispetto ad x ed il risultante commutano con le traslazioni $x \to x - a$ si ha $\Delta(f(x)) = \Delta(f(x-a))$ per ogni $a \in A$, dai risultati del capitolo II segue dunque che Δ è un covariante. Per confrontare la definizione di Δ con quella data nel capitolo II come funzione delle differenze delle radici scriviamo

$$f = a_0\prod_{i=1}^{n}(x-\alpha_i), \quad f' = a_0\sum_{i=1}^{n}\prod_{j\neq i}(x-\alpha_j)$$

da cui $f'(\alpha_i) = a_0\prod_{j\neq i}(\alpha_i - \alpha_j)$ e per 1.5

$$\Delta(f) = a_0^{-1}R(f,f') = a_0^{n-2}\prod_{i=1}^{n}f'(\alpha_i) = a_0^{2n-2}\prod_{i\neq j}(\alpha_i-\alpha_j)$$

Naturalmente se $\beta_1, ..., \beta_{n-1}$ sono le radici della derivata f' vale anche la formula $\Delta(f) = n^n a_0^{n-1}\prod f(\beta_i)$.

Esempio 2.1. $f = ax^2 + 2bx + c$ allora $-\frac{b}{a}$ è la radice di f' e si ha $\Delta(f) = 2^2af(-\frac{b}{a}) = 4(ac-b^2)$.

Esempio 2.2. $f = x^3 - px - q$, le radici di f' sono $\pm\sqrt{\frac{p}{3}}$ e quindi il discriminante vale $\Delta = 27f(\sqrt{\frac{p}{3}})f(-\sqrt{\frac{p}{3}}) = 27q^2 - 4p^3$.

Esempio 2.3. Per 1.3. si ha $\Delta(x^n + a) = n^n a^{n-1}$.

Un possibile modo per calcolare $\Delta(f)$ con f monico è quello di applicare l'algoritmo euclideo per determinare il massimo comune divisore fra f e f' e poi moltiplicare per uno scalare in modo da avere la precedente relazione soddisfatta. Ad esempio se $f = x^4 + cx^2 + bx + a$ si ha $27\Delta(f) = 4(c^2+12a)^3 - (2c^3 - 72ac + 27b^2)^2$.

ESERCIZIO 6: Calcolare il discriminante di un binomio.

ESERCIZIO 7: Sia $f \in A[x]$ di grado n, $g = nf - xf'$; provare che $R_{n-1,n-1}(g,f') = n^{n-1}\Delta(f)$.

3. Il teorema degli zeri di Hilbert (Nullstellensatz)

Sia $\mathbb{K}$ un campo (infinito) fissato e $\mathbb{A}^n = \mathbb{K}^n$ lo spazio affine su $\mathbb{K}$ di dimensione n. L'anello $P = \mathbb{K}[x_1, ..., x_n]$ può essere pensato come l'algebra delle funzioni polinomiali su $\mathbb{A}^n$ a valori in $\mathbb{K}$, mentre ogni sottoinsieme $E \subset P$ può essere pensato come un insieme di equazioni algebriche nelle variabili $x_1, ..., x_n$; è quindi naturale considerare il **luogo di zeri** di E dato da

$$V(E) = \{(a_1, ..., a_n) \in \mathbb{A}^n \mid f(a_1, ..., a_n) = 0 \ \forall f \in E\}$$

Dalla definizione appare chiaro che se (E) è l'ideale generato da E allora E ed (E) hanno lo stesso luogo di zeri, $V(E) = V((E))$, e quindi non è restrittivo considerare esclusivamente luoghi di zeri di ideali di P. (Il motivo della lettera V è motivato dall'inglese "to vanish").

Definizione 3.1. Un sottoinsieme X di $\mathbb{A}^n$ si dice **algebrico** se è del tipo $V(I)$ per qualche ideale $I \subset P$.

Non tutti i sottoinsiemi di $\mathbb{A}^n$ sono algebrici, ad esempio un sottoinsieme proprio di $\mathbb{A}^1$ è algebrico se e solo se è finito.

Le seguenti proprietà sono di immediata verifica:

1) $V(0) = \mathbb{A}^n$, $V(P) = \emptyset$.
2) Se $I \subset J$ ideali allora $V(J) \subset V(I)$.
3) Per ogni ideale I, $V(I) = V(\sqrt{I})$.

4) Dati I, J ideali $V(IJ) = V(I) \cup V(J)$.

5) Data una famiglia qualsiasi $\{I_\alpha\}$ di ideali $V(\sum I_\alpha) = \cap V(I_\alpha)$.

Le proprietà 1), 4) e 5) mostrano che i sottoinsiemi algebrici di $\mathbb{A}^n$ sono i chiusi di una topologia detta **topologia di Zariski.**

ESERCIZIO 8: Provare che la topologia di Zariski è T_1 ma non T_2.

Dato un qualsiasi sottoinsieme $X \subset \mathbb{A}^n$ denotiamo con $\overline{X}$ la chiusura di X nella topologia di Zariski. Se si definisce

$$I(X) = \{f \in P | f(a) = 0 \quad \forall a \in X\}$$

si vede facilmente che $V(I(X)) = \overline{X}$. La corrispondenza $X \to I(X)$ soddisfa inoltre le proprietà:

6) $I(\emptyset) = P$, $I(\mathbb{A}^n) = 0$.

7) Se $X \subset Y$ allora $I(Y) \subset I(X)$.

8) Per ogni X, $I(X) = \sqrt{I(X)}$, $X \subset V(I(X))$.

9) Per ogni ideale $J \subset P$ vale $\sqrt{J} \subset I(V(J))$.

L'inclusione del punto 9) è in generale propria, ad esempio se $\mathbb{K} = \mathbb{R}$, $n = 1$ e $J = (x^2 + 1)$ allora $V(J) = \emptyset$ e $I(V(J)) = P \neq \sqrt{J}$.

L'obiettivo di questo paragrafo è di dimostrare gli importantissimi

Teorema 3.2.(degli zeri di Hilbert, forma debole) *Se $\mathbb{K}$ è algebricamente chiuso e $J \subset P$ è un ideale, vale $V(J) = \emptyset$ se e solo se $1 \in J$.*

Teorema 3.3.(degli zeri di Hilbert, forma forte) *Se $\mathbb{K}$ è algebricamente chiuso allora per ogni ideale $J \subset P$ vale $\sqrt{J} = I(V(J))$.*

Dimostrazione di 3.2. Se $1 \in J$ è ovvio che il luogo di zeri di J è l'insieme vuoto, supponiamo quindi $1 \notin J$ e proviamo che $V(J)$ è non vuoto. Si può inoltre supporre $J \neq 0$.

Se $n = 1$, J è principale e quindi $J = (f)$ e $V(J)$ è l'insieme delle radici di f. Siccome f non è invertibile deve avere grado positivo e quindi possiede radici.

Sia $n > 1$ e supponiamo il teorema vero in $\mathbb{A}^{n-1}$. Sia $F \in J$, $F \neq 0$, non è restrittivo supporre F polinomio monico rispetto a x_n; sia infatti $m > 0$ il grado di F e F_m la componente omogenea di grado m di F. Essendo $\mathbb{K}$ infinito esistono $b_1, ...b_{n-1} \in \mathbb{K}$ tali che $F_m(b_1, ..., b_{n-1}, 1) \neq 0$, a meno di effettuare il cambio lineare di coordinate $x_n \to x_n$, $x_i \to x_i - b_i x_n$ ed eventualmente moltiplicando F per uno scalare si può supporre $b_i = 0$ per ogni i e $F_m(0, ..., 0, 1) = 1$. In queste condizioni si ha

$$F = x_n^m + \sum_{i=1}^{m} h_i(x_1, .., x_{n-1}) x_n^{m-i}$$

Assumiamo quindi F polinomio monico rispetto alla variabile x_n e si consideri l'ideale $J^c = J \cap \mathbb{K}[x_1, ..., x_{n-1}]$, per l'ipotesi induttiva $V(J^c) \neq \emptyset$, detta quindi $\pi: \mathbb{A}^n \to \mathbb{A}^{n-1}$ la proiezione sulle prime $n-1$ coordinate è sufficiente dimostrare che $\pi(V(J)) = V(J^c)$.

Se $(a_1, ..., a_n) \in V(J)$ allora $f(a_1, ..., a_n) = 0$ per ogni $f \in J^c$ e quindi $(a_1, .., a_{n-1}) \in V(J^c)$.

Viceversa si consideri un punto $(a_1, ..., a_{n-1}) \in V(J^c)$ e sia $M \subset P$ l'ideale generato da $x_1 - a_1, ..., x_{n-1} - a_{n-1}$. Siccome $V(J + M) = V(J) \cap V(M) \subset V(M) = \pi^{-1}(a_1, ..., a_{n-1})$ basta dimostrare che $V(J + M)$ è non vuoto.

Mostriamo per prima cosa che $1 \notin J + M$: sia infatti per assurdo $1 = f + \sum (x_i - a_i) g_i$ per qualche $f \in J$. $g_i \in P$; allora $f(a_1, ..., a_{n-1}, t) = 1$ per ogni $t \in \mathbb{K}$ e quindi se

$$f(x_1, ..., x_{n-1}, t) = \sum f_i(x_1, ..., x_{n-1}) t^i$$

deve essere $f_0(a_1, ..., a_{n-1}) = 1$ e $f_i(a_1, ..., a_{n-1}) = 0$ per ogni $i > 0$.

Si consideri adesso il risultante $R = R(F, f) \in J^c$ calcolato rispetto alla variabile x_n. Vale $R = \det Sy(F, f)$, dove $Sy(F, f)$ è la matrice di Sylvester della coppia F, f.

Siccome $Sy(F, f)(a_1, ..., a_{n-1})$ è una matrice triangolare superiore con tutti 1 sulla diagonale si ha $R(F, f)(a_1, ..., a_{n-1}) = 1$ in contraddizione con l'appartenenza a J^c, dunque $1 \notin J + M$.

Si consideri adesso l'omomorfismo surgettivo $\phi: \mathbb{K}[x_1, ..., x_n] \to \mathbb{K}[t]$, $\phi(x_n) = t$, $\phi(x_i) = a_i$, è chiaro che $M = \ker \phi$ e quindi che $\phi^{-1}(\phi(J)) = J + M$. Dato che $1 \notin J + M$ ne segue che $\phi(J)$ è un ideale proprio e quindi esiste $a_n \in \mathbb{K}$ tale che per ogni $f \in J$ vale $f(a_1, ..., a_n) = \phi(f)(a_n) = 0$. □

Per uso futuro enunciamo in un lemma a parte una conseguenza della precedente dimostrazione

Lemma 3.4. *Sia $\mathbb{K} = \overline{\mathbb{K}}$, $J \subset \mathbb{K}[x_1, ..., x_n]$ un ideale, $J^c = J \cap \mathbb{K}[x_1, ..., x_{n-1}]$ e $\pi: \mathbb{A}^n \to \mathbb{A}^{n-1}$ la proiezione sulle prime coordinate.*

Se esiste $F \in J$ monico rispetto a x_n (e.g. se $\deg_{x_n} F = \deg F$) allora $\pi: V(J) \to V(J^c)$ è chiusa e surgettiva.

Dim. La surgettività è dimostrata sopra, sia $X \subset V(J)$ un chiuso di Zariski, allora $X = V(I(X))$ e $J \subset I(X)$, in particolare $F \in I(X)$ e $\pi(X) = V(I(X)^c)$. □

Corollario 3.5. *Se $\mathbb{K} = \overline{\mathbb{K}}$ gli ideali massimali di $P = \mathbb{K}[x_1, ..., x_n]$ sono tutti e soli gli ideali del tipo $I(p)$, $p \in \mathbb{A}^n$. Esiste dunque una bigezione naturale fra $\mathbb{A}^n$ e l'insieme degli ideali massimali di P.*

Dim. Sia $M \subset P$ massimale e $p \in V(M)$ allora $M \subset I(p)$ da cui $M = I(p)$. Viceversa se $p \in \mathbb{A}^n$ e $I(p) \subset M$ con M massimale si ha, per quanto visto sopra $I(p) \subset M = I(q)$ da cui $\{q\} \subset \{p\}$ e quindi $p = q$. □

Dimostrazione di 3.3. Siccome $X = V(J) = V(\sqrt{J})$ si può supporre senza perdita di generalità che $J = \sqrt{J}$ cioè che $S = P/J$ non possieda elementi nilpotenti. Dobbiamo dimostrare che se $F \notin J$ allora esiste $x \in X$ tale che $F(x) \neq 0$.

Sia F come sopra fissato, $\alpha: P \to S$ la proiezione al quoziente, $f = \alpha(F)$. Si noti che $1 - tf$ è invertibile in $S[[t]]$ con inverso $\sum_{i=0}^{\infty} t^i f^i$ e quindi $1 - tf$ è invertibile in $S[t]$ se e solo se f è nilpotente. Per ipotesi S è ridotto e quindi $(1 - tf)$ è un ideale proprio di $S[t]$ e $J, 1 - tF$ generano un ideale proprio di $\mathbb{K}[x_1, ..., x_n, t]$.

Per la forma debole del teorema degli zeri esistono $a_0, ..., a_n, t_0$ tali che $g(a_0, ..., a_n) = 0$ per ogni $g \in J$ e $1 - t_0 F(a_0, ..., a_n) = 0$. Dunque $x = (a_0, ..., a_n) \in X$ e $F(x) \neq 0$. □

Corollario 3.6. *Sia $\mathbb{K} = \overline{\mathbb{K}}$, $f, g \in \mathbb{K}[x_1, ..., x_n]$ con f irriducibile, se $V(f) \subset V(g)$ allora f divide g.*

Dim. Per il teorema degli zeri $g \in I(V(f)) = \sqrt{(f)} = (f)$. □

Ricordiamo che un ideale $I \subset \mathbb{K}[x_1, ..., x_n]$ si dice omogeneo se è generato da polinomi omogenei, se $S_d \subset \mathbb{K}[x_1, ..., x_n]$ è il sottospazio dei polinomi omogenei di grado d si verifica facilmente che I è omogeneo se e solo se $I = \oplus(I \cap S_d)$.

Sia infine $0 = (0, ..., 0) \in \mathbb{A}^n$, si noti che se I omogeneo e $V(I) \neq \emptyset$ allora $0 \in V(I)$.

Corollario 3.7. (Teorema degli zeri omogeneo) *Sia $\mathbb{K} = \overline{\mathbb{K}}$ e $I \subset \mathbb{K}[x_1, ..., x_n]$ ideale omogeneo proprio. Allora $V(I) = \{0\}$ se e solo se esiste $d > 0$ tale che $S_d \subset I$.*

Dim. Se $S_d \subset I$ allora $x_i^d \in I$, $x_i \in \sqrt{I}$ e quindi $V(I) = V(\sqrt{I}) = \{0\}$.

Viceversa se $V(I) = \{0\}$ per il teorema degli zeri $\sqrt{I} = I(\{0\}) = (x_1, ..., x_n)$. Esiste dunque $d > 0$ tale che $x_i^d \in I$ per ogni i e quindi $S_{dn-n+1} \subset I$. □

ESERCIZIO 9: Sia $\pi: \mathbb{A}^2 \to \mathbb{A}^1$ la proiezione sulla prima coordinata. Nella topologia di Zariski, è π chiusa? è π aperta?.

4. Esercizi complementari

ESERCIZIO 10: Sia $f \in A[x]$ un polinomio monico, allora per ogni $g, h \in A[x]$ vale $R(f, g) = R(f, g + hf)$.

ESERCIZIO 11: Provare che $R_{n,m}(f(x), g(x)) = \pm R_{n,m}(x^n f(x^{-1}), x^m g(x^{-1}))$.

ESERCIZIO 12: Sia A un dominio di integrità e $f, g \in A[x]$, $s \in (f, g) \cap A$; si provi che $s^3 \in (f^2, g^2) \cap A$ mentre $R(f^2, g^2) = R(f, g)^4$. Si deduca che in generale il risultante non genera l'ideale contratto $(f, g) \cap A$.

ESERCIZIO 13: Sia $Sy(f, g)$ la matrice di Sylvester di due forme binarie f, g, di gradi n, m. Provare che se f, g hanno un fattore comune di grado r allora la dimensione del nucleo di $Sy(f, g)$ è almeno r.

ESERCIZIO 14: Esistono altre rappresentazioni del risultante, qui ne proponiamo due come esercizi, per suggerimenti vedi [GKZ] p. 401.

i) Data una serie formale $\phi = \sum r_i x^i$ si definiscono le matrici di Toeplitz $S_{n,m}(\phi) = (a_{ij})$ con $a_{ij} = r_{n+j-i}$, $1 \leq i, j \leq m$. Siano $f, g \in A[x]$ con $f(0) = 1$ e $\phi = \frac{g}{f} \in A[[x]]$, si provi $\det S_{n,m}(\phi) = R_{n,m}(f, g)$.

ii) (Formula di Bézout-Cayley) Sia $n = m$ e sia

$$\frac{f(x)g(y) - g(x)f(y)}{x - y} = \sum_{i,j=0}^{n-1} c_{ij} x^i y^j$$

Provare che $R_{n,n}(f, g) = \det(c_{ij})$.

ESERCIZIO 15: Siano $I_1, ..., I_r \in \mathbb{N}^n$ multiindici distinti e $\mathbb{K}$ un campo infinito. Mostrare che l'immagine di $\mathbb{K}^n \to \mathbb{K}^r$, $x \to (x^{I_1}, ..., x^{I_r})$ contiene una base dello spazio vettoriale $\mathbb{K}^r$.

ESERCIZIO 16: (Sistemi risultanti).

Sia A un dominio a fattorizzazione unica e $f, g_1, ..., g_r \in A[x]$ polinomi, $a_1, ..., a_r$ indeterminate e sia $R \in A[a_1, ..., a_r]$ il risultante dei polinomi $f, a_1 g_1 + ... + a_r g_r$.

Vale $R = 0$ se e solo se i polinomi $f, g_1, ..., g_r$ hanno un fattore comune di grado positivo. Si provi inoltre che i coefficienti di $R(a_1, ..., a_r)$ appartengono a $A \cap (f, g_1, ..., g_r)$.

ESERCIZIO 17: Per un polinomio monico a coefficienti reali senza radici multiple determinare la relazione tra il segno del discriminante, il grado del polinomio ed la classe di resto modulo 4 del numero di radici reali. In particolare si provi che se il grado è 3 allora f possiede tre radici reali distinte se e solo se $\Delta(f) < 0$.

ESERCIZIO 18: Provare che se f, g hanno gradi n, m allora vale la formula di polarizzazione

$$R(f, g)^2 = (-1)^{nm} \frac{\Delta(fg)}{\Delta(f)\Delta(g)}.$$

ESERCIZIO 19: Sia $f = \sum a_i x^{n-i} y^i$ un polinomio omogeneo di grado n e f_x, f_y le derivate di f rispetto a x e y rispettivamente. Vale allora

$$R_{n,n-1}(f, f_x) = \frac{a_0}{n^{n-2}} R_{n-1,n-1}(f_x, f_y), \qquad \Delta(f) = \frac{1}{n^{n-2}} R_{n-1,n-1}(f_x, f_y).$$

ESERCIZIO 20: Sia $I \subset \mathbb{K}[x_1, .., x_n]$ un ideale proprio, $\mathbb{K} \subset L$ una estensione di campi e $I^e \subset L[x_1, .., x_n]$ l'estensione di I. Mostrare che $1 \notin I^e$.

ESERCIZIO 21: Sia $I \subset \mathbb{K}[x_1, .., x_n]$ un ideale proprio, mostrare che esiste una estensione finita di campi $\mathbb{K} \subset L$ tale che $V(I^e) \neq \emptyset$.

ESERCIZIO 22: Se $\mathbb{K} \subset L$ è una estensione di campi e L è una $\mathbb{K}$-algebra finitamente generata allora L è una estensione algebrica finita di $\mathbb{K}$. (sugg. Sia $L = \mathbb{K}[x_1, ..., x_n]/I$, mostrare che esiste un omomorfismo di $\mathbb{K}$ algebre $\phi: \mathbb{K}[x_1, ..., x_n] \to \overline{\mathbb{K}}$ tale che $\phi(I) = 0$.)

ESERCIZIO 23: (*) Siano $f, g \in \mathbb{K}[x, y]$ omogenei di grado d senza fattori comuni. Provare che $S_n \subset (f, g)$ se e solo se $n \geq 2d - 1$, (sugg. usare 1.3.f).

Nota. Esiste una generalizzazione del risultato a polinomi in un numero arbitrario di variabili, in particolare vale il seguente:

Teorema 3.8: *Sia $I \subset \mathbb{K}[x_0, ..., x_n]$ ideale omogeneo generato da $n+1$ polinomi omogenei di gradi $d_0, ..., d_n$. Se $\sqrt{I} = (x_0, ..., x_n)$ allora la dimensione di $S_h \cap I$ dipende solo da $h, n, d_0, ..., d_n$ e non da I. In particolare $S_d \subset I$ se e solo se $d \geq \sum d_i - n$.*

La dimostrazione di tale risultato richiede strumenti troppo avanzati per queste note (complesso di Koszul) e quindi la omettiamo.

ESERCIZIO 24: Dimostrare che in 3.8 non è restrittivo supporre $\mathbb{K}$ algebricamente chiuso.

ESERCIZIO 25: Nelle notazioni di 3.8, siano $V \subset S_a$, $W \subset S_b$ sottospazi vettoriali e $\mu: V \otimes W \to S_{a+b}$ la mappa di moltiplicazione $\mu(f \otimes g) = fg$. Provare che il rango di μ è $\geq \dim V + \dim W - 1$.

ESERCIZIO 26: Teorema di Hopf.

i) (*) Siano A, B, C spazi vettoriali di dimensione finita su un campo algebricamente chiuso con $\dim A = 2$ e $\mu: A \otimes B \to C$ lineare e separatamente iniettiva, cioè tale che se $a, b \neq 0$ allora $\mu(a \otimes b) \neq 0$. Provare che $\dim C > \dim B$. (Sugg. Sia per assurdo $\mu: A \otimes B \to B$ come sopra, e_1, e_2 una base di A, $f_i(b) = \mu(e_i \otimes b)$ e si consideri gli endomorfismi $\lambda f_1 + \eta f_2$, $[\lambda, \eta] \in \mathbb{P}^1$.)

ii) (**?) Lo stesso del punto i) con A di dimensione arbitraria.

iii) Se vale $\dim C = \dim A + \dim B - 1$ nel teorema di Hopf allora per ogni $c \in C$ esistono a, b tali che $c = \mu(a \otimes b)$. Si deduca che se $\mathbb{K}$ non è algebricamente chiuso il teorema di Hopf è falso su $\mathbb{K}$.

ESERCIZIO 27: (Lemma di Gieseker).

Sia $I \subset \mathbb{K}[x, y]$ un ideale omogeneo e sia $I_d = I \cap S_d$. Se $I_d \neq fS_h$ per qualche $h \leq d$, $f \in S_{d-h}$ allora $\dim I_{d+1} \geq \dim I_d + 2$.

(Sugg. Sia $f_0, ..., f_n$ una base di I_d tale che $f_i = x^{r_i} g_i$ con $g_i(0, 1) = 1$ e $r_i < r_{i+1}$ per ogni $i = 0, ..., n$. Si consideri l'insieme $A = \{i \mid g_n \not| g_i\} \cup \{i | r_{i+1} \geq r_i + 2\}$, se $A \neq \emptyset$ sia $s \in A$ massimo e si provi che $yf_0, xf_0, ..., xf_s, yf_{s+1}, xf_{s+1}, ..., xf_n$ sono linearmente indipendenti.)

ESERCIZIO 28: Siano $f, g, q \in \mathbb{K}[x]$ polinomi senza fattori comuni di grado n, n, m rispettivamente con $m < n$. Si provi che $R(f + \lambda q, g + \mu q) \in \mathbb{K}[\lambda, \mu]$ è un polinomio di

grado $\leq n$. (Sugg. Non è restrittivo supporre $\mathbb{K}$ algebricamente chiuso, si consideri allora gli omomorfismi $\mathbb{K}[\lambda, \mu] \to \mathbb{K}[t]$ dati da $\lambda \to at$, $\mu \to bt$, $a, b \in \mathbb{K}$.)

ESERCIZIO 29: (Implicitizzazione delle curve razionali nel piano)

Dati $f, g, q \in \mathbb{K}[t]$ polinomi senza fattori comuni provare che l'insieme

$$C = \{\left(\frac{f(t)}{q(t)}, \frac{f(t)}{q(t)}\right) \mid t \in \mathbb{K}, q(t) \neq 0\}$$

è definito da una equazione polinomiale. (Sugg. esercizio precedente).

ESERCIZIO 30: (*) (Teorema di Lüroth: versione geometrica (1875))

Sia $\mathbb{K}$ campo algebricamente chiuso, $F(x, y) \in \mathbb{K}[x, y]$ con le seguenti proprietà:

a) La relazione $a \sim b$ se e solo se $(a, b) \in V(F) \subset \mathbb{K}^2$ è una relazione di equivalenza su $\mathbb{K}$.

b) F è combinazione lineare di monomi $x^a y^b$ con $a, b \leq n$.

c) Esiste $x_0 \in \mathbb{K}$ tale che il polinomio $F(x_0, y) \in \mathbb{K}[y]$ possiede n radici semplici distinte.

Provare che esistono $f, g \in \mathbb{K}[t]$ di grado $\leq n$ tali che $F(x, y) = f(x)g(y) - f(y)g(x)$.

(Suggerimento. Svolgere nell'ordine i seguenti punti:

1) Non è restrittivo supporre che F non contenga fattori del tipo $x - a$, $y - b$.

2) Il polinomio F è ridotto e $F(x, y) = \delta F(y, x)$, $\delta^2 = 1$.

3) Esistono n punti distinti $a_1, ..., a_n \in \mathbb{K}$ tali che $F(a_i, y) = C_i F(a_1, y)$ per opportune costanti $C_2, ..., C_n \in \mathbb{K}$.

4) Sia $V \subset \mathbb{K}[y]$ il sottospazio vettoriale dei polinomi di grado $n + 1$, dimostrare che l'immagine dell'applicazione $\mathbb{K} \to V$, $a \to F(a, y)$, è contenuta in un piano $P \subset V$.

5) Sia f, g una base di P. Per ogni $a \in \mathbb{K}$ esistono costanti α, β tali che $F(a, y) = \alpha f(y) - \beta g(y)$. Se $g(a)f(a) \neq 0$ esiste una costante C_a tale che $F(a, y) = C_a(g(a)f(y) - f(a)g(y))$.

6) Utilizzare la simmetria di F (punto 2) per mostrare che $C_a = C$ non dipende da a.)

ESERCIZIO 31: (*) Siano $p, q \in \mathbb{K}[x]$ di grado $\leq n$ tali che $ap + bq$ abbia n radici distinte per qualche $a, b \in \mathbb{K}$. Si ponga $\phi = \frac{p}{q} \in \mathbb{K}(x)$, $F(x, y) = p(x)q(y) - p(y)q(x)$ e

$$\Sigma = \Sigma(F) = \{\frac{r(x)}{s(x)} \mid F(x, y) \text{ divide } r(x)s(y) - r(y)s(x)\}$$

Provare che $\Sigma = \mathbb{K}(\phi)$ e che $\Sigma \subset \mathbb{K}(x)$ è una estensione di grado n.

(Sugg. provare nell'ordine i seguenti punti:

1) Σ è un campo contenente $\mathbb{K}(\phi)$.

2) l'estensione $\mathbb{K}(\phi) \subset \mathbb{K}(x)$ ha grado $\leq n$.

3) l'estensione $\Sigma \subset \mathbb{K}(x)$ ha grado $\geq n$.)

ESERCIZIO 32: (*) (Teorema di Lüroth: versione algebrica)

Sia $\mathbb{K}$ algebricamente chiuso, $f_1,...,f_d \in \mathbb{K}(x)$ $f_i = \frac{p_i}{q_i}$, $p_i, q_i \in \mathbb{K}[x]$ senza fattori comuni e $F_i(x,y) = p_i(x)q_i(y) - p_i(y)q_i(x)$ e F il massimo comune divisore di $F_1,...,F_d$.
Se il polinomio F_1 soddisfa le ipotesi della versione geometrica allora anche F le soddisfa e vale $\mathbb{K}(f_1,...,f_n) = \Sigma(F) = \mathbb{K}(\phi)$ per qualche $\phi \in \mathbb{K}(x)$.
(Sugg. sia $g(\lambda) \in \mathbb{K}(f_1,...,f_n)[\lambda]$ il polinomio minimo di x, dato che g divide i polinomi $p_i(\lambda) - f_i q_i(\lambda)$ si deduca, come in [Wa, p. 150] che g divide F e quindi il grado di g è minore o uguale del grado di F. Si utilizzi quindi l'esercizio precedente.)

ESERCIZIO 33: (Il discriminante di una estensione algebrica)
Sia $\mathbb{K} \subset L$ una estensione algebrica finita di campi di caratteristica 0. Sia n il grado dell'estensione e siano $\sigma_1,...,\sigma_n$ gli automorfismi di L che fissano $\mathbb{K}$.
Dato $a \in L$ si denoti con $Tr(a) \in \mathbb{K}$ la traccia dell'endomorfismo di moltiplicazione $a\colon L \to L$, mentre se $a_1,...,a_n \in L$ definiamo il discriminante $disc(a_1,...,a_n) = \det(Tr(a_i a_j))$.
Provare che:
i) $Tr(a) = \sum \sigma_i(a)$. (Sugg. Sia $b \in L$ tale che $\sigma_i(b)$ sia una base di L su K e calcolare $Tr(\sigma_i(b))$.)
ii) $disc(a_1,...,a_n) = \det(\sigma_i(a_j))^2$.
iii) $disc(1,a,...,a^{n-1})$ è uguale al discriminante del polinomio caratteristico di $a\colon L \to L$.

ESERCIZIO 34: Esiste una semplice dimostrazione alternativa di 3.4 che utilizza il lemma di Nakayama (cf. [Reid] esercizio II.3.15). Per dimostrare che $(a_1,...,a_{n-1}) \in V(J^c)$ appartiene alla proiezione di $V(J)$ basta porre, nelle notazioni di I.3.1, $A = \mathbb{K}[x_1,...,x_{n-1}]/J^c$, $M = \mathbb{K}[x_1,...,x_n]/J$, $N = 0$ e $I = (x_1 - a_1,...,x_{n-1} - a_{n-1}) \subset A$.

ESERCIZIO 35: Siano $A \subset B$ anelli Noetheriani con B finitamente generato come A-modulo. Provare:

i) Ogni $x \in B$ è radice di un polinomio monico a coefficienti in A. (Sugg. polinomio caratteristico della moltiplicazione per x).

ii) Se $I \subset A$ è un ideale proprio allora $IB \neq B$ (Sugg. Nakayama).

iii) Se $\mathbb{K}$ è un campo algebricamente chiuso, ogni morfismo $A \to \mathbb{K}$ si estende ad un morfismo $B \to \mathbb{K}$. (Sugg. usare il lemma di Zorn per ricondursi al caso A campo e $B = A[x]$ con x algebrico su A).

IV. Curve piane: nozioni base

In tutto il capitolo con il simbolo $\mathbb{K}$ indicheremo un campo **algebricamente chiuso**, denoteremo inoltre $\mathbb{P}^2 = \mathbb{P}^2_{\mathbb{K}}$ il piano proiettivo su $\mathbb{K}$.

1. Definizioni principali

In prima approssimazione possiamo definire una curva algebrica piana come il luogo dei punti di $\mathbb{P}^2$ che annullano un polinomio omogeneo nelle coordinate omogenee di $\mathbb{P}^2$. Questa definizione, sebbene semplice, non è sufficientemente precisa e presenta qualche difficoltà operativa.
Già nella teoria dei fasci di coniche proiettive si incontrano certi oggetti "le rette doppie" che insiemisticamente sono sono delle rette ma che appartengono allo spazio delle coniche di $\mathbb{P}^2$.

Definizione 1.1. Siano x_0, x_1, x_2 coordinate omogenee su $\mathbb{P}^2$, una **curva irriducibile** di grado n è un sottoinsieme $C \subset \mathbb{P}^2$ per cui esiste un polinomio irriducibile omogeneo di grado n, $F(x) = F(x_0,x_1,x_2)$ tale che

$$C = V(F) = \{[x_0,x_1,x_2] \in \mathbb{P}^2 | \, F(x_0,x_1,x_2) = 0\}$$

La definizione di curva irriducibile non dipende dal particolare sistema di coordinate omogenee. Sia infatti y_0,y_1,y_2 un altro sistema e $x_i = \sum a_{ij}y_j$ con la matrice a_{ij} invertibile, allora se $F(x_0,x_1,x_2) = G(y_0,y_1,y_2)$ vale

$$G(y_0,y_1,y_2) = 0 \Leftrightarrow [y_0,y_1,y_2] \in C,$$

inoltre il grado di F è uguale al grado di G e F è irriducibile se e solo se G è irriducibile.
Fissato un sistema di coordinate omogenee x_i, una curva irriducibile C determina a meno di costante moltiplicativa il polinomio F di cui è luogo di zeri. Infatti se $G(x_0,x_1,x_2) = 0$ per ogni $[x] \in C$ allora per il teorema degli zeri F divide G e se G è irriducibile allora $G = aF$ per qualche $a \in \mathbb{K}$.
Una curva irriducibile con molteplicità è una coppia (C,m) dove C è una curva irriducibile e $m \in \mathbb{Z}, m > 0$ è la molteplicità.

Definizione 1.2. Una **curva algebrica** C è una insieme finito di curve irriducibili con molteplicità $(C_1, m_1), ..., (C_r, m_r)$. Le curve C_i si dicono le **componenti irriducibili** della curva mentre $supp(C) = \cup C_i \subset \mathbb{P}^2$ è detto il supporto della curva. Una componente si dice **multipla** se la sua molteplicità è > 1, una curva si dice **ridotta** se non possiede componenti multiple. Se n_i è il grado di C_i definiamo il **grado** della curva come $n = n_1 m_1 + ... + n_r m_r$.
Una notazione conveniente è quella di scrivere una curva come una combinazione lineare formale $C = m_1 C_1 + m_2 C_2 + ... + m_r C_r$ dove $C_1, ..., C_r$ sono le componenti irriducibili e m_i le rispettive molteplicità. Inoltre, con un leggero abuso di notazione, se C è una curva e $p \in \mathbb{P}^2$ scriveremo $p \in C$ se $p \in supp(C)$.

ESERCIZIO 1: Data una curva algebrica C, $supp(C)$ è un sottoinsieme proprio infinito di $\mathbb{P}^2$.

Fissato un sistema di coordinate x_0, x_1, x_2 esiste una bigezione fra l'insieme delle curve algebriche di grado n ed il proiettivizzato dello spazio vettoriale dei polinomi omogenei di grado n nelle variabili x_i. Infatti dato F polinomio omogeneo di grado n esiste una decomposizione in fattori irriducibili $F = F_1^{m_1} ... F_r^{m_r}$, possiamo quindi considerare la curva le cui componenti irriducibili C_i sono i luoghi di zeri dei polinomi F_i contate con molteplicità m_i. Per l'unicità della fattorizzazione tale curva risulta ben definita. Viceversa, data una curva $C = \sum m_i C_i$, se $C_i = V(F_i)$ con F_i irriducibile si considera $F = \prod F_i^{m_i}$. Essendo F_i definita a meno di costante moltiplicativa anche F è definita a meno di costante moltiplicativa, chiameremo F **l'equazione** di C. Si noti che in tale corrispondenza biunivoca vale la relazione $supp(C) = V(F)$.

Teorema 1.3.(forma debole del teorema di Bézout) *Siano C, D due curve algebriche di gradi n, m rispettivamente, allora $V = supp(C) \cap supp(D) \neq \emptyset$, inoltre se V contiene più di nm punti allora C e D hanno una componente in comune.*

Dim. Si assuma che esistano $nm + 1$ punti distinti $p_0, ..., p_{nm} \in supp(C) \cap supp(D)$, detta $l_{ij} = p_i + p_j$ la retta passante per p_i e p_j possiamo trovare un punto $q \notin supp(C) \cup supp(D) \cup_{i \neq j} l_{ij}$ ed un sistema di coordinate omogenee x_0, x_1, x_2 tali che $q = [0, 0, 1]$.
Siano F, G le equazioni di C e D nelle coordinate x_i, si può scrivere

$$F = A_0 x_2^n + A_1 x_2^{n-1} + ... + A_n, \quad G = B_0 x_2^m + B_1 x_2^{m-1} + ..., B_m$$

dove A_i e B_i sono polinomi omogenei di grado i nelle coordinate x_0, x_1 e siccome $[0, 0, 1] \notin supp(C) \cup supp(D)$ si ha $A_0 B_0 \neq 0$. Sia dunque $R(x_0, x_1)$ il risultante di F e G calcolato rispetto alla variabile x_2, allora $R(a, b) = 0$ se e solo se i polinomi $F(a, b, x_2), G(a, b, x_2)$ hanno una radice comune $x_2 = c$, questo prova che la cardinalità di V è maggiore o uguale al numero di radici distinte di R. Sapendo che R è

omogeneo di grado nm ed è $R = 0$ se e solo se F e G hanno un fattore comune, basta dimostrare che R si annulla in almeno $nm + 1$ punti distinti di $\mathbb{P}^1$.
Sia $p_i = [a_i, b_i, c_i]$, allora i polinomi $F(a_i, b_i, x_2), G(a_i, b_i, x_2)$ hanno una radice comune $x_2 = c_i$ e quindi $R(a_i, b_i) = 0$ per ogni i; siccome $[0, 0, 1] \notin \cup l_{ij}$ ne segue che se $i \neq j$ allora $[a_i, b_i] \neq [a_j, b_j]$ e quindi $R = 0$. □

Corollario 1.4. *Due curve irriducibili distinte di gradi n, m hanno al più nm punti in comune.*

Dim. Immediata. □

Sia F l'equazione di una curva C, sia $p = [v_0, v_1, v_2] \in \mathbb{P}^2$, diremo che p è un **punto singolare** di C se

$$F(v_0, v_1, v_2) = \frac{\partial F}{\partial x_i}(v_0, v_1, v_2) = 0, \quad i = 0, 1, 2$$

Si noti che:
1) La definizione di punto singolare è una buona definizione, infatti essendo F omogeneo anche le derivate parziali sono omogenee. Inoltre se y_0, y_1, y_2 è un diverso sistema di coordinate e G è l'equazione di C nelle coordinate y_i si ha $G(y) = aF(x)$ per qualche $a \in \mathbb{K}$ e quindi

$$\frac{\partial G}{\partial y_i} = a \sum_{j=0}^{2} \frac{\partial F}{\partial x_j} \frac{\partial x_j}{\partial y_i}$$

2) Se la caratteristica del campo è 0, dalla formula di Eulero segue che un punto p è singolare per la curva di equazione F se e solo se p annulla tutte le derivate parziali di F.
3) Se C è irriducibile di grado n di equazione F allora, essendo $\mathbb{K}$ algebricamente chiuso e quindi perfetto, esiste una derivata parziale non nulla senza fattori comuni con F e quindi per Bézout debole C ha al più $n(n-1)$ punti singolari. Vedremo più avanti che questa stima può essere migliorata a $\leq \frac{1}{2}(n-1)(n-2)$.
I punti di una curva che non sono singolari si dicono **lisci**. Una curva **liscia** è una curva che non contiene punti singolari.

Proposizione 1.5. *Siano $C_1, ..., C_r$ curve algebriche e $C = C_1 + ... + C_r$.*
1) Se $p \in C_i$, $p \in C_j$, $i \neq j$ allora p è un punto singolare di C.
2) Se $p \in C_i$ e $p \notin C_j$ per ogni $j \neq i$ allora p è un punto singolare di C se e solo se è un punto singolare di C_i.
3) Una curva è ridotta se e solo se possiede un numero finito di punti singolari.

Dim. Sia F_i una equazione della curva C_i, allora $F = F_1 ... F_r$ è una equazione per C, se $p \in C_i \cap C_j$, $i \neq j$ allora $F_i(p) = F_j(p) = 0$ e per la regola di Leibnitz ogni

derivata parziale di F si annulla in p; questo prova 1). Se invece $F_i(p)=0$, $F_j(p)\neq 0$ per ogni $j\neq i$ allora sempre per Leibnitz si ha $\dfrac{\partial F}{\partial x_h}(p)=0 \Leftrightarrow \dfrac{\partial F_i}{\partial x_h}(p)=0$ per ogni $h=0,1,2$.

Siccome una curva $C=C_1+\ldots+C_r$ con le C_i irriducibili è ridotta se e solo se le C_i sono distinte, il punto 3) segue dai punti precedenti e dal fatto che ogni curva irriducibile possiede un numero finito di punti singolari. □

ESERCIZIO 2: In caratteristica 0 la curva di Fermat $x_0^n+x_1^n+x_2^n=0$ non contiene punti singolari.

ESERCIZIO 3: Sia F l'equazione di una curva irriducibile C di grado n, esistono allora almeno due derivate parziali non nulle. (Sugg. ricordarsi che il campo è perfetto).

ESERCIZIO 4: In caratteristica $\neq 2,3$ determinare per quali valori del parametro λ le seguenti curve sono singolari.

$$x_0x_2^2=x_1(x_1+x_0)(x_1+\lambda x_0)$$

$$x_0^3+x_1^3+x_2^3-3\lambda x_0x_1x_2=0$$

2. Retta tangente e molteplicità

Sia C una curva algebrica piana di grado n ed equazione $F=0$ e $L\subset\mathbb{P}^2$ una retta, se L è contenuta nel supporto di C allora L è una componente irriducibile di C.

Se invece L non è una componente irriducibile di C, allora presi due punti distinti $p=[p_0,p_1,p_2]$, $q=[q_0,q_1,q_2]$, $p,q\in L$ il polinomio $f(t_0,t_1)=F(t_0p_0+t_1q_0,t_0p_1+t_1q_1,t_0p_2+t_1q_2)$ è non nullo ed omogeneo di grado n. Esistono dunque n punti di L contati con molteplicità in cui $f=0$: chiaramente tali punti corrispondono all'intersezione della curva C con la retta L. Se $p\in L$ definiamo $\nu_p(L,C)$ la molteplicità della radice p nel polinomio f, si vede facilmente che il tutto è ben definito.

Sia $p\in L\cap C$, se $\nu_p(L,C)=1$ diremo che L è **trasversale** a C nel punto p, se invece $\nu_p(L,C)>1$ diremo che L è **tangente** a C nel punto p. Si noti che se esiste una retta trasversale ad una curva C allora C deve essere necessariamente ridotta.

Per convenzione se $p\in L\subset C$ poniamo $\nu_p(L,C)=\infty$, mentre se $p\notin C\cap L$ si pone $\nu_p(L,C)=0$.

Proposizione 2.1. *Sia C una curva di equazione F e $p=[x_0,x_1,x_2]\in C$, $q=[y_0,y_1,y_2]\neq p$, allora la retta $L=p+q$ è tangente a C in p se e solo se*

$$F_q(x_0,x_1,x_2):=\sum_{i=0}^{2}y_i\frac{\partial F}{\partial x_i}(x_0,x_1,x_2)=0$$

Dim. La retta l è tangente a C in p se e solo se $t=0$ è una radice multipla di $f(t)=F(x_0+ty_0,x_1+ty_1,x_2+ty_2)$, cioè se e solo se $f'(0)=0$ dove f' denota la derivata di f rispetto a t, basta adesso applicare la regola di derivazione della funzione composta. □

Definizione 2.2. La curva C_q di equazione $F_q=0$ si dice **polare** di q rispetto a C, naturalmente la definizione di F_q ha senso per qualsiasi $q\in\mathbb{P}^2$. Lasciamo al lettore la facile verifica che la definizione di C_q non dipende dal particolare sistema di coordinate omogenee. Naturalmente è possibile che il polinomio F_q sia identicamente nullo (e.g C unione di rette per q), in tal caso diremo che la polare C_q è indeterminata.

Corollario 2.3. *Sia C una curva ridotta di grado n ed equazione F. Allora:*

i) Se per $q\notin C$ passano infinite rette tangenti a C allora necessariamente la caratteristica di $\mathbb{K}$ è positiva.

ii) Se per $q\notin C$ passano finite rette tangenti a C il loro numero non supera $n(n-1)$.

iii) Esiste un punto $q\notin C$ per cui vale la condizione ii) precedente.

Dim. Le rette tangenti a C passanti per q sono tutte e sole quelle $q+p$ dove $F(p)=F_q(p)=0$. Dato che F_q ha grado $n-1$, in virtù del teorema di Bézout è sufficiente determinare quando F e F_q non hanno componenti in comune.

Per fare ciò prendiamo un sistema di coordinate in cui $q=[0,0,1]$, allora

$$F=A_0x_2^n+A_1x_2^{n-1}+\ldots+A_n,\quad A_0\neq 0$$

$$F_q=\frac{\partial F}{\partial x_2}$$

Se F e F_q non hanno fattori comuni, il che è vero in caratteristica 0 dato che F non ha fattori multipli, allora per Bézout F e F_q hanno al più $n(n-1)$ punti di intersezione, questo prova i punti i) e ii).

Fissiamo un sistema di coordinate in cui il punto $[0,0,1]$ non appartiene a C, in particolare ogni fattore irriducibile di F ha grado positivo rispetto a x_2. Siccome il campo $\mathbb{K}$ è perfetto e F non ha fattori multipli, i polinomi $F,\dfrac{\partial F}{\partial x_0},\dfrac{\partial F}{\partial x_1},\dfrac{\partial F}{\partial x_2}$ non hanno fattori comuni e quindi il risultante $R(a,b,c,x_0,x_1)$ rispetto a x_2 dei polinomi F, $a\dfrac{\partial F}{\partial x_0}+b\dfrac{\partial F}{\partial x_1}+c\dfrac{\partial F}{\partial x_2}$ non è nullo, in particolare esisterà $q=[a,b,c]\in\mathbb{P}^2$ tale che $R(a,b,c,x_0,x_1)\neq 0$ e quindi F,F_q non hanno fattori comuni. □

Corollario 2.4. *Sia $p\in C$, allora:*

i) Se p è singolare allora ogni retta per p è tangente a C in p.

ii) Se p è liscio allora esiste unica una retta tangente a C in p.

Dim. Conseguenza immediata di 2.1. □

Definizione 2.5. Sia C curva e $p \in \mathbb{P}^2$, si definisce la **molteplicità** $m_p(C)$ di C nel punto p come il minimo dei valori $\nu_p(L, C)$ al variare delle rette L passanti per p, si noti che $m_p(C) > 0$ se e solo se $p \in C$ e $m_p(C) > 1$ se e solo se p è un punto singolare di C.

Sia $\mathbb{A}^2 \subset \mathbb{P}^2$ il piano affine ottenuto dal piano proiettivo togliendo la retta all'infinito, una curva affine è per definizione la restrizione ad $\mathbb{A}^2$ di una curva algebrica piana C, più precisamente se $C = m_1C_1 + ... + m_rC_r$ con le C_i irriducibili si pone

$$C \cap \mathbb{A}^2 = m_1(C_1 \cap \mathbb{A}^2) + ... + m_r(C_r \cap \mathbb{A}^2).$$

Si assuma che la retta all'infinito non sia una componente irriducibile di C, se x_0, x_1, x_2 sono coordinate omogenee tali che x_0 è l'equazione della retta all'infinito e F l'equazione di C, sul piano affine $\mathbb{A}^2 = \{x_0 \neq 0\}$ vi sono le coordinate affini $y_1 = \frac{x_1}{x_0}$, $y_2 = \frac{x_2}{x_0}$ e $f(y_1, y_2) = F(1, y_1, y_2)$ è un polinomio dello stesso grado della curva C.

Esiste una corrispondenza biunivoca tra i fattori irriducibili di f e quelli di F. Infatti se $H|F$ allora x_0 non divide H e se $h(y_1, y_2) = H(1, y_1, y_2)$ allora h divide f. Viceversa se h ha grado r e divide f si ha che $H(x_0, x_1, x_2) = x_0^r h(\frac{x_1}{x_0}, \frac{x_2}{x_0})$ è un polinomio omogeneo che divide F. In particolare F è irriducibile se e solo se f è irriducibile. Chiameremo f l'equazione della curva affine $C \cap \mathbb{A}^2$.

Sia $p \in \mathbb{P}^2$ e C una curva algebrica piana di grado n e di equazione F, scegliamo un sistema di coordinate omogenee x_0, x_1, x_2 tali che $p = [1, 0, 0]$, si può scrivere l'equazione della curva affine come

$$f(y_1, y_2) = f_m(y_1, y_2) + f_{m+1}(y_1, y_2) + ... + f_n(y_1, y_2)$$

dove f_i è omogeneo di grado i e $f_m \neq 0$, allora l'intero $m \geq 0$ è uguale alla molteplicità $m_p(C)$. Infatti per definizione di molteplicità $m_p(C)$ è la minima molteplicità in $t = 0$ dei polinomi $f(ty_1, ty_2) = t^m f_m(y_1, y_2) + t^{m+1}$.. al variare di $[y_1, y_2] \in \mathbb{P}^1$. Si noti che le soluzioni di $f_m = 0$ sono esattamente le rette L per p tali che $\nu_p(L, C) > m_p(C)$, tali rette sono in numero finito e sono le componenti irriducibili di una curva di grado $m = m_p(C)$ ed equazione f_m chiamata **cono tangente** a C nel punto p.

Proposizione 2.6. *Sia $C \subset \mathbb{P}^2$ una curva ridotta di grado n e $p \in \mathbb{P}^2$ un punto di molteplicità $m \geq 0$. Se $\mathbb{K}$ ha caratteristica 0 o $> n$ esiste una retta per p che interseca $C - \{p\}$ is $n - m$ punti distinti.*

Dim. Prendiamo un sistema di coordinate in cui $p = [1, 0, 0]$, $m = m_p(C)$ allora

$$F = A_m x_0^{n-m} + A_{m+1} x_0^{n-m-1} + ... + A_n, \quad A_m \neq 0$$

Sia $\Delta(x_1, x_2)$ il discriminante di F considerato come un polinomio di grado $n - m$ in x_0, si vede facilmente che, dato che F non ha fattori multipli e la caratteristica di $\mathbb{K}$ è maggiore di $n - m$ $\Delta \neq 0$ e $\Delta(v_1, v_2) = 0$ se e solo se $f(t) = F(t, v_1, v_2) = 0$ ha una radice multipla. Dunque basta considerare una retta $x_1v_2 = x_2v_1$ per una coppia (v_1, v_2) che non annulla il discriminante. □

ESERCIZIO 5: Calcolare il grado del discriminante calcolato nella dimostrazione di 2.6. Provare inoltre che in caratteristica positiva 2.6 è generalmente falso.

Un punto di molteplicità 2 si dice un **punto doppio**. Se un punto doppio ha il cono tangente formato da due rette distinte il punto doppio si dice un **nodo**, altrimenti si dice una **cuspide**; ad esempio la curva affine di equazione $y^2 = x^2 + x^3$ ha un nodo nel punto di coordinate $(0, 0)$, mentre la curva affine $y^2 = x^n$, $n \geq 3$, possiede una cuspide in $(0, 0)$. Diremo che C ha una singolarità **ordinaria** in p se il cono tangente di C in p è ridotto; equivalentemente se x, y sono coordinate affini tali che $p = (0, 0)$ e $f = f_m + ...$, $m = m_p(C)$, è l'equazione affine di C, la singolarità è ordinaria se f_m non ha radici multiple.

Definizione 2.7. Data una curva C ed un punto liscio $p \in C$ denoteremo con $T_p(C)$ la retta tangente a C in p. Se $F(x_0, x_1, x_2)$ è l'equazione di C e $p = [v]$ l'equazione di $T_p(C)$ è $x_0F_0(v) + x_1F_1(v) + x_2F_2(v) = 0$.

Un punto liscio $p \in C$ si dice un **flesso** se $3 \leq \nu_p(C, T_p(C)) < \infty$; chiameremo inoltre $\nu_p(C, T_p(C)) - 2$ molteplicità di flesso di p.

ESERCIZIO 6: Sia $p \in C$ di grado n allora $m_p(C) \leq n$ e vale $=$ se e solo se ogni componente irriducibile di C è una retta passante per p.

ESERCIZIO 7: Si determini il numero di rette per il punto $[1, 1, 0]$ e tangenti alla curva di Fermat $x_0^n + x_1^n + x_2^n = 0$ con n non divisibile dalla caratteristica di $\mathbb{K}$.

3. Intersezione di curve piane

Nel paragrafo precedente abbiamo visto che una curva piana $C \subset \mathbb{P}^2$ interseca una retta L in esattamente n punti contati con molteplicità $\nu_p(L, C)$, sempreché L non sia contenuta in C. Inoltre, nella dimostrazione della forma debole del teorema di Bézout abbiamo costruito una bigezione fra l'insieme dei punti in comune a due curve C, D di gradi n, m senza componenti comuni e l'insieme delle radici su $\mathbb{P}^1$ di un polinomio risultante R omogeneo di grado nm. Queste considerazioni fanno ben sperare alla validità del

Teorema 3.1.(di Bézout)* *Due curve piane proiettive senza componenti comuni di gradi n, m si intersecano in nm punti contati con molteplicità.*

Naturalmente occorre definire con precisione cosa intendiamo per molteplicità di un punto di intersezione.

Le principali definizioni (tutte equivalenti) che vedremo in queste note sono:

1) Definizione per proiezione generica.
2) Definizione parametrica (si tratta della definizione data nel paragrafo precedente quando una delle due curve è una retta).
3) Definizione analitica.

La definizione per proiezione generica è la più elementare ed è motivata dalla dimostrazione di Bézout debole.

Siano dunque C, D due curve piane proiettive senza componenti comuni di gradi n, m ed equazioni F, G e $p_1, ..., p_r$, $r \leq nm$ i punti di intersezione. Per ogni coppia $i \neq j$ sia L_{ij} la retta $p_i + p_j$.

Diremo che un punto $q \in \mathbb{P}^2$ è generico se non appartiene all'unione di C, D e delle rette L_{ij}.

Fissato un punto generico q fissiamo un sistema di coordinate omogenee x_0, x_1, x_2 tali che $q = [0, 0, 1]$, si ha allora

$$F = A_0 x_2^n + A_1 x_2^{n-1} + ... + A_n, \quad G = B_0 x_2^m + B_1 x_2^{m-1} + ..., B_m$$

dove A_i e B_i sono polinomi omogenei di grado i nelle coordinate x_0, x_1 e $A_0 B_0 \neq 0$. Sia dunque $R(x_0, x_1)$ il risultante di F e G calcolato rispetto alla variabile x_2.

Sia $p_i = [a_i, b_i, c_i]$ allora i polinomi $F(a_i, b_i, x_2), G(a_i, b_i, x_2)$ hanno una radice comune $x_2 = c_i$ e quindi $R(a_i, b_i) = 0$ per ogni i, siccome $[0, 0, 1] \notin \cup L_{ij}$ ne segue che se $i \neq j$ allora $[a_i, b_i] \neq [a_j, b_j]$.

Definizione 3.2. Si definisce la molteplicità di intersezione $\nu_{p_i}(C, D)$ = molteplicità della radice $[a_i, b_i]$ in R.

Dal seguente teorema seguirà che si tratta di una buona definizione, cioè che $\nu_{p_i}(C, D)$ non dipende dalla scelta del punto generico e del sistema di coordinate omogenee. Fatto questo il teorema di Bézout è una conseguenza immediata del fatto che R è omogeneo di grado nm.

* L'enunciato del Teorema 3.1 risale a Mac-Laurin (1720), i primi accenni di dimostrazione si devono a Eulero (1748) e Cramer (1750); una trattazione più completa fu data da Bézout (1779), mentre per la prima dimostrazione rigorosa bisogna aspettare Gauss ed il teorema fondamentale dell'algebra. Spesso (e.g. [Cre]) il teorema 3.1 veniva ammesso come principio evidente.

ESERCIZIO 8: Provare che se D è una retta la definizione 3.2 è equivalente alla definizione parametrica.

Teorema 3.3.(Regola di Halphen, 1874) *La 3.2 è una buona definizione*

Dim. Vediamo per prima cosa che la molteplicità non dipende dal particolare sistema di coordinate. Sia infatti y_0, y_1, y_2 un secondo sistema di coordinate tali che $q = \{y_0 = y_1 = 0\}$, vale allora

$$\begin{cases} x_0 = ay_0 + by_1 \\ x_1 = cy_0 + dy_1 \\ x_2 = hy_0 + ky_1 + y_2 \end{cases} \qquad ad \neq bc \tag{3.4}$$

Tale cambiamento può essere visto come la composizione di una traslazione

$$\begin{cases} z_0 = y_0 \\ z_1 = y_1 \\ z_2 = hy_0 + ky_1 + y_2 \end{cases}$$

e di

$$\begin{cases} x_0 = az_0 + bz_1 \\ x_1 = cz_0 + dz_1 \\ x_2 = z_2 \end{cases} \qquad ad \neq bc$$

Dall'invarianza rispetto alle traslazioni e dalla funtorialità del risultante i precedenti cambi di coordinate non cambiano la molteplicità.

Adesso bisogna dimostrare che la molteplicità non dipende dalla scelta del punto generico q. Sia q' un altro punto generico e si prenda un sistema di coordinate omogenee x_0, x_1, x_2 tali che $q = [0, 0, 1]$, $q' = [0, 1, 0]$, $p_1 = [a, 1, 1]$ per qualche $a \in \mathbb{K}$ e

$$o = [1, 0, 0] \notin C \cup D \cup_{i \neq j} (p_i + p_j) \cup_i (q + p_i) \cup_i (q' + p_i)$$

In tale sistema di coordinate siano R_1, R_2 i risultanti di F, G pensati come polinomi in x_1, x_2 rispettivamente, per dimostrare che $\nu_{p_1}(C, D)$ è ben definita bisogna dimostrare che R_1, R_2 hanno la stessa molteplicità in $(a, 1)$.

Per fare questo introduciamo la curva di Chow $Ch(C, D) \subset (\mathbb{P}^2)^\vee$ della coppia C, D. Se $\lambda = (\lambda_1, \lambda_2) \in \mathbb{K}^2$ denotiamo con $L_\lambda \subset \mathbb{P}^2$ la retta di equazione $x_0 = \lambda_1 x_1 + \lambda_2 x_2$, si noti che le rette L_λ sono tutte e sole le rette che non passano per il punto o.

Si consideri adesso i polinomi

$$f(\lambda_1, \lambda_2, x_1, x_2) = f_\lambda(x_1, x_2) = F(\lambda_1 x_1 + \lambda_2 x_2, x_1, x_2)$$

$$g(\lambda_1, \lambda_2, x_1, x_2) = g_\lambda(x_1, x_2) G(\lambda_1 x_1 + \lambda_2 x_2, x_1, x_2)$$

e sia $R(\lambda_1, \lambda_2)$ il risultante delle forme binarie f_λ, g_λ.

Si noti che $R(\lambda_1, \lambda_2) = 0$ se e solo se L_λ contiene almeno un punto di intersezione di C e D, si definisce quindi $Ch(C, D)$ come la chiusura proiettiva della curva affine

definita dall'equazione R. Le componenti irriducibili di $Ch(C,D)$ sono tutte e sole i fasci di rette passanti per i punti di intersezione di C, D. Sia ν_1 la molteplicità del fascio di rette $\{\lambda_1+\lambda_2 = a\}$ di centro p_1 come componente di $Ch(C,D)$, dimostriamo che ν_1 coincide con le molteplicità di intersezione calcolate rispetto alle proiezioni dai punti generici q, q'.

Iniziamo con osservare che se E_j indica il fascio di rette per p_j allora, dal fatto che q, q' sono generici segue che $(a,0),(0,a) \in E_1 - \cup_{j\neq 1} E_j$ e che i polinomi $R(t,0), R(0,t)$ non sono identicamente nulli; si noti che $R(t,0), R(0,t)$ rappresentano le restrizioni di R ai fasci di rette passanti per q, q'. Dunque ν_1 è uguale alla molteplicità della radice $t = a$ nei polinomi $R(t,0), R(0,t)$.

$R(t,0)$ è il risultante delle forme

$$F(tx_1, x_1, x_2) = A_0(t,1)x_2^n + A_1(t,1)x_1x_2^{n-1} + ... + A_n(t,1)x_1^n,$$

$$G(tx_1, x_1, x_2) = B_0(t,1)x_2^m + B_1(t,1)x_1x_2^{m-1} + ... + B_m(t,1)x_1^m$$

e quindi $R(t,0) = \pm R_2(t,1)$. Allo stesso modo si prova $R(0,t) = \pm R_1(t,1)$ e per quanto visto questo conclude la dimostrazione. □

Si noti che dal teorema di Bézout segue che il grado di $Ch(C,D)$ è uguale al prodotto dei gradi di C e D.

Poniamo per convenzione $\nu_p(C,D) = \infty$ se C e D hanno una componente comune passante per p. Dalle proprietà del risultante seguono immediatamente le seguenti proprietà delle molteplicità di intersezione.

$\nu_p(C,D) \geq 0$ e vale 0 se e solo se $p \notin C \cap D$. (Positività)

$\nu_p(C,D) = \nu_p(D,C)$. (Simmetria)

$\nu_p(C, D+E) = \nu_p(D,C) + \nu_p(D,E)$. (Bilinearità)

Teorema 3.5. *Siano C, D curve senza componenti comuni e sia $p \in C \cap D$, allora vale $\nu_p(C,D) \geq m_p(C)m_p(D)$ e vale $=$ se e solo se i coni tangenti di C e D in p non hanno componenti comuni.*

Dim. Siano F, G rispettivamente le equazioni di C, D in un sistema x_0, x_1, x_2 di coordinate tali che $p = [1,0,0]$ e che $q = [0,0,1]$ sia generico e non appartenente all'unione dei coni tangenti alle curve nel punto p. Essendo q generico si ha in particolare che p è l'unico punto di intersezione di C e D sulla retta $L = \{x_1 = 0\}$. Sia $r = m_p(C) = \nu_p(L,C)$, $s = m_p(D) = \nu_p(L,D)$, passando ad un sistema di coordinate affini si ha che per definizione $\nu_p(C,D)$ è la molteplicità della radice $x = 0$ del risultante rispetto ad y dei polinomi

$$f(x,y) = F(1,x,y), \quad g(x,y) = G(1,x,y)$$

Tenendo conto delle molteplicità in p si può scrivere in modo unico

$$f = f_0x^r + f_1x^{r-1} + ... + f_ry^r + f_{r+1}y^{r+1} + ... + f_ny^n$$

$$g = g_0x^s + g_1x^{s-1} + ... + g_sy^s + g_{s+1}y^{s+1} + ... + g_my^m$$

Per opportuni $f_i, g_i \in \mathbb{K}[x]$. Si denoti $a_i = f_i(0)$, $b_i = g_i(0)$.

Il risultante $R(x)$ è allora, a meno del segno, il determinante della matrice

$$\begin{pmatrix}
f_0x^r & f_1x^{r-1} & \dots & \cdot & \cdot & \cdot & \dots & \cdot & f_n & & & \\
 & f_0x^r & \dots & \cdot & \cdot & \cdot & \dots & \cdot & \cdot & f_n & & \\
 & & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \\
 & & & f_0x^r & f_1x^{r-1} & f_2x^{r-2} & \dots & \cdot & \cdot & \cdot & \dots & f_n \\
g_0x^s & g_1x^{s-1} & \dots & \cdot & g_m & & & & & & & \\
 & g_0x^s & \dots & \cdot & \cdot & g_m & & & & & & \\
 & & \ddots & \vdots & \vdots & \vdots & \ddots & & & & & \\
 & & & g_0x^s & g_1x^{s-1} & g_2x^{s-2} & \dots & g_m & & & & \\
 & & & & g_0x^s & g_1x^{s-1} & \dots & \cdot & g_m & & & \\
 & & & & & g_0x^s & \dots & \cdot & \cdot & g_m & & \\
 & & & & & & \ddots & \vdots & \vdots & \vdots & \ddots & \\
 & & & & & & & g_0x^s & g_1x^{s-1} & g_2x^{s-2} & \dots & g_m
\end{pmatrix} \tag{3.6}$$

Per dimostrare che x^{rs} divide $R(x)$ ripetiamo nella sostanza la dimostrazione del fatto che il risultante è isobaro. Sia Δ la matrice ottenuta da (3.6) eseguendo nell'ordine le seguenti operazioni:

1) Se $1 \leq i \leq s$ moltiplicare la i-esima riga per x^{s-i+1}.

2) Se $m+1 \leq i \leq m+r$ moltiplicare la i-esima riga per $x^{m+r-i+1}$.

3) Se $1 \leq i \leq r+s$ dividere la i esima colonna per $x^{r+s-i+1}$.

Si vede facilmente che i coefficienti di Δ sono polinomi e che $R(x) = x^{rs} \det \Delta(x)$.

Rimane da dimostrare che $\Delta(0)$ è invertibile se e solo se i coni tangenti non hanno componenti comuni. La matrice $\Delta(0)$ è

$$\begin{pmatrix}
a_0 & \dots & \cdot & a_r & & & & & & & & \\
 & \ddots & \vdots & \vdots & \ddots & & & & & & & \\
 & & a_0 & \cdot & \dots & a_r & & & & & & \\
 & & & * & * & * & a_r & \dots & \cdot & a_n & & \\
 & & & & * & * & & \ddots & \vdots & \vdots & \ddots & \\
 & & & & & * & & & a_r & \cdot & \dots & a_n \\
b_0 & \dots & \cdot & b_s & & & & & & & & \\
 & \ddots & \vdots & \vdots & \ddots & & & & & & & \\
 & & b_0 & \cdot & \dots & b_s & & & & & & \\
 & & & * & * & * & b_s & \dots & \cdot & b_m & & \\
 & & & & * & * & & \ddots & \vdots & \vdots & \ddots & \\
 & & & & & * & & & b_s & \cdot & \dots & b_m
\end{pmatrix}$$

e quindi, a meno del segno, il determinante di $\Delta(0)$ è il prodotto dei determinati delle matrici

$$\Delta_1 = \begin{pmatrix} a_0 & \dots & \cdot & a_r & & \\ & \ddots & \vdots & \vdots & \ddots & \\ & & a_0 & \cdot & \dots & a_r \\ b_0 & \dots & \cdot & b_s & & \\ & \ddots & \vdots & \vdots & \ddots & \\ & & b_0 & \cdot & \dots & b_s \end{pmatrix}, \quad \Delta_2 = \begin{pmatrix} a_n & \dots & \cdot & a_r & & \\ & \ddots & \vdots & \vdots & \ddots & \\ & & a_n & \cdot & \dots & a_r \\ b_m & \dots & \cdot & b_s & & \\ & \ddots & \vdots & \vdots & \ddots & \\ & & b_m & \cdot & \dots & b_s \end{pmatrix}$$

La matrice Δ_1 è la matrice di Sylvester delle equazioni che definiscono i coni tangenti, dunque il suo determinate è nullo se e solo se i due coni hanno una componente in comune.

La matrice Δ_2 è la matrice di Sylvester dei polinomi

$$a_n y^{n-r} + \dots + a_r = y^{-r} f(0,y), \quad b_m y^{m-s} + \dots + b_s = y^{-s} g(0,y)$$

Il punto q è generico e quindi $a_n b_m \neq 0$ ed i due polinomi non hanno radici comuni diverse da $y = 0$; in zero hanno una radice comune se e solo se $a_r = b_s = 0$, ma questo significa che la retta $x = 0$ appartiene al cono tangente sia di C che D. □

Siamo adesso in grado di dimostrare alcuni interessanti corollari

Corollario 3.7. *Siano $p_1, .., p_r$ i punti di intersezione di due curve C, D senza componenti comuni di grado n, m, allora vale*

$$nm \geq \sum_{i=1}^{r} m_{p_i}(C) m_{p_i}(D)$$

Corollario 3.8. *Sia C una curva ridotta di grado n e siano $p_1, .., p_r$ i suoi punti singolari. Allora vale*

$$n(n-1) \geq \sum_{i=1}^{r} m_{p_i}(C)(m_{p_i}(C) - 1)$$

Dim. Sia F l'equazione di C, per 2.3 esiste un punto q tale che l'equazione della polare F_q è non nulla e senza componenti comuni con F. Dato che il grado di F_q è $n-1$ basta dimostrare che per ogni punto p vale $m_p(F_q) \geq m_p(F) - 1$. Prendiamo un sistema di coordinate omogenee x_i tali che $q = [0,0,1]$ e $p = [1,0,0]$, se $f(x,y) = F(1,x,y)$ allora l'equazione affine della polare è la derivata di f rispetto a y, è allora chiaro che la molteplicità diminuisce al più di 1. □

ESERCIZIO 9: Trovare i punti di intersezione delle curve di equazione $x(y^2 - xz)^2 - y^5 = 0$, $y^4 + y^3 z + x^2 z^2 = 0$.

Corollario 3.9. *Siano C, D curve piane senza componenti comuni di grado n, m rispettivamente, $p \in C$ un punto liscio, $L = T_p C \subset \mathbb{P}^2$ la retta tangente a C in p e $a = m_p(D) \geq 0$.*

Se $\nu_p(L,D) \leq \nu_p(L,C) + a - 2$ allora vale $\nu_p(L,D) = \nu_p(C,D)$.

Nota. Se $\nu_p(L,C) = 2$ (caso generico) il corollario non aggiunge nulla al teorema 3.5. Oltre all'enunciato di 3.9 è interessante anche il metodo di dimostrazione.

Dim. Sia $q \notin L$ un punto generico (nel senso di 3.2) e siano x_0, x_1, x_2 coordinate omogenee tali che $p = [0,0,1]$, $q = [0,1,0]$ ed L sia la retta di equazione $x_1 = 0$. Dette F, G le equazioni di C e D nelle coordinate x_i si ha che $\nu_p(C,D) =$ molteplicità in 0 del risultante di $f(x,y) = F(x,y,1)$ e $g(x,y) = G(x,y,1)$ calcolato rispetto alla variabile y. Siccome il punto q non appartiene a $C \cup D$, a meno di moltiplicazione per costanti possiamo supporre f, g polinomi monici in y di grado n, m rispettivamente. Abbiamo visto nel capitolo sul risultante che in tali ipotesi $R(f,g) = R(f, g + hf)$ per ogni polinomio $h \in \mathbb{K}[x,y]$. In base al teorema 3.5 possiamo quindi affermare che la molteplicità in 0 di $g + hf$ non supera $\nu_p(C,D)$ per ogni scelta di h.

Dato che C è liscia in 0 con retta tangente $y = 0$ si può scrivere $f = y + \tilde{f}(x,y)$ con $m_0(\tilde{f}) \geq 2$ e $g(x,y) = g(x,0) + y\tilde{g}(x,y)$. Si noti che $\nu_p(L,D), \nu_p(L,C)$ sono rispettivamente le molteplicità in 0 di $g(x,0)$ e $\tilde{f}(x,0)$.

Definiamo per ricorrenza dei polinomi $g_i, \tilde{g}_i$ ponendo

$$g(x,y) = g_0(x,y), \qquad g_i(x,y) = g_i(x,0) + y\tilde{g}_i(x,y), \qquad g_{i+1} = g_i - \tilde{g}_i f$$

Si noti che $g_{i+1}(x,0) = g_i(x,0) - \tilde{g}_i \tilde{f}(x,0)$ e che la molteplicità di $\tilde{g}_i$ in 0 è una funzione strettamente crescente di i. Dall'esistenza del massimo delle molteplicità di $g + hf$ si deduce che dopo un numero finito di passi la molteplicità di $\tilde{g}_i$ è maggiore o uguale a quella di $g_i(x,0)$ e quindi la retta L non appartiene al cono tangente di g_i al punto 0. Abbiamo quindi dimostrato che $\nu_p(C,D) = m_0(g_i) = m_0(g_i(x,0))$ per i sufficientemente grande.

Per finire la dimostrazione basta osservare che la molteplicità di $\tilde{g}_i$ è maggiore o uguale ad $a-1$ per ogni i e che quindi la molteplicità di $\tilde{g}_i f(x,0)$ è almeno $\nu_p(L,C) + a - 1$. Nelle ipotesi del corollario i polinomi $g_i(x,0)$ hanno quindi tutti la stessa molteplicità in 0. □

Facendo un po' di attenzione alla dimostrazione ci accorgiamo che nell'uguaglianza $\nu_p(L,D) = \nu_p(C,D)$ il termine a sinistra è definito per via parametrica (§2) mentre il termine a destra è definito per proiezione generica (3.2).

Se $C = L$ l'enunciato è quindi non vuoto e fornisce una dimostrazione dell'equivalenza delle due definizione di ν_p.

4. Sistemi lineari di curve piane

Abbiamo già osservato che le curve piane di grado n sono in corrispondenza biunivoca con il proiettivizzato dello spazio dei polinomi omogenei di grado n. Più precisamente, alla curva di equazione $\sum_{ijk} a_{ijk}x_0^i x_1^j x_2^k$ corrisponde il punto di $\mathbb{P}^N$ di coordinate omogenee $[a_{ijk}]$. Chiaramente $N+1$ è uguale al numero di monomi i tre variabili di grado n, è ben noto che $1+N=\frac{1}{2}(n+1)(n+2)$ da cui $N=\frac{1}{2}n(n+3)$. Con una notazione familiare a tutti i geometri indichiamo com $|\mathcal{O}(n)|$ lo spazio proiettivo delle curve di grado n, un sottospazio proiettivo di $|\mathcal{O}(n)|$ si dice un **sistema lineare**, lo stesso spazio $|\mathcal{O}(n)|$ è un sistema lineare detto **completo**. Se $D_1,...,D_r$ sono curve di grado n denotiamo con $<D_1,...,D_r>\subset|\mathcal{O}(n)|$ il sistema lineare da esse generato. Se V è un sistema lineare chiameremo $\dim V$ la dimensione del sistema, un sistema lineare di dimensione 1 si dice un **fascio**.

Sia $V\subset|\mathcal{O}(n)|$ un sistema lineare, un punto $p\in\mathbb{P}^2$ si dice un **punto base** di V se per ogni curva $D\in V$ vale $p\in D$, denoteremo $BS(V)$ l'insieme dei punti base di V.

Se V è un sistema lineare di dimensione r e $F_0,...,F_r$ sono le equazioni di un insieme di curve indipendenti di V, allora le curve di V sono tutte e sole quelle di equazione $\sum\lambda_i F_i$.

L'equazione di un iperpiano in $|\mathcal{O}(n)|$ si dice una **condizione lineare** sulle curve di grado n. Se $p\in\mathbb{P}^2$ la condizione $p\in D$ è una condizione lineare su $|nl|$, infatti se $p=[v_0,v_1v_2]$, una curva di equazione $\sum a_{ijk}x_0^i x_1^j x_2^k$ contiene p se e solo se vale $\sum a_{ijk}v_0^i v_1^j v_2^k=0$ che è l'equazione di un iperpiano in $|\mathcal{O}(n)|$.

Più in generale se $\mathcal{P}$ è una proprietà definita sulle curve di grado n e $V\subset|\mathcal{O}(n)|$ è un sistema lineare, diremo che $\mathcal{P}$ impone r condizioni lineari su V se l'insieme delle $D\in V$ che soddisfano $\mathcal{P}$ è un sottospazio proiettivo di codimensione r. Ad esempio la condizione di passaggio per un punto p (il termine passaggio nasce dal fatto di pensare intuitivamente un sistema lineare come una curva che si muove in $\mathbb{P}^2$ in uno spazio dei parametri che è uno spazio proiettivo) induce una condizione lineare su un sistema V se e solo se p non è un punto base di V.

ESERCIZIO 10: Trovare la dimensione del sistema lineare delle coniche passanti per 4 punti non allineati.

ESERCIZIO 11: Non tutte le condizioni lineari su $|\mathcal{O}(n)|$, $n\geq 2$, sono indotte dal passaggio per un punto.

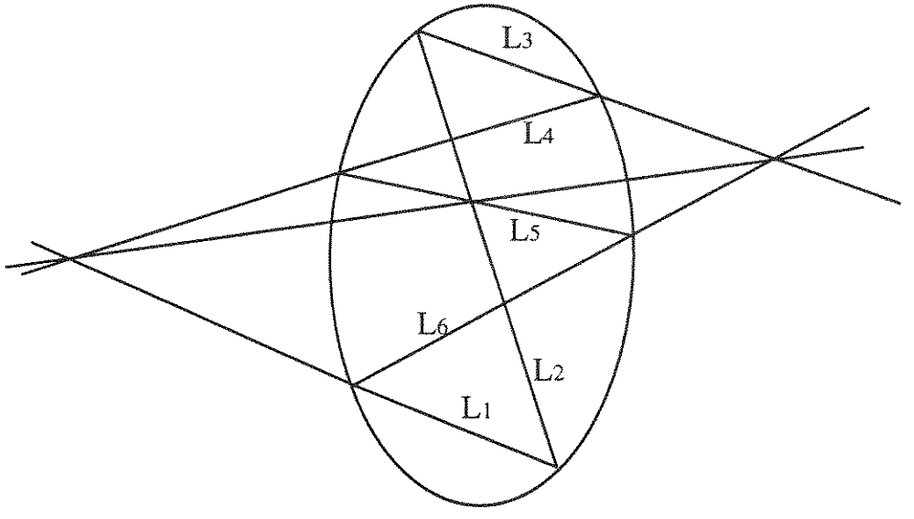
ESERCIZIO 12: Il passaggio per r punti distinti di $\mathbb{P}^2$ induce $s\leq r$ condizioni lineari su $|\mathcal{O}(n)|$. Quante condizioni lineari impongono 4 punti allineati su $|\mathcal{O}(2)|$?

Un insieme finito di punti $S\subset\mathbb{P}^2$ si dice in **posizione generica** se la condizione di passaggio per ogni sottoinsieme di cardinalità m induce m condizioni lineari sulle curve di grado n per ogni n tale che $m\leq\frac{1}{2}(n+1)(n+2)$.

Se $r\leq n$ e $p\in\mathbb{P}^2$ allora $V=\{D\in|\mathcal{O}(n)|:m_p(D)\geq r\}$ è un sistema lineare di codimensione $\frac{1}{2}r(r+1)$, infatti in un sistema di coordinate tali che $p=[1,0,0]$, una curva D di equazione affine $0=a_{00}+a_{10}x+a_{01}y+...+a_{ij}x^iy^j+..$ allora $m_p(D)\geq r$ se e solo se $a_{ij}=0$ per ogni $i+j<r$.

Teorema 4.1.(Teorema di Gergonne, 1827) *Siano C,D due curve piane di grado n che si intersecano in esattamente n^2 punti distinti. Se nm di questi punti appartengono ad una curva E di grado $m\leq n$ allora i restanti $n(n-m)$ punti appartengono ad una curva H di grado $n-m$.*

Dim. Siano $p_1,...,p_{n^2}$ i punti di intersezione di C e D, dal teorema di Bézout segue che necessariamente C,D,E sono curve ridotte e p_i è un punto liscio per C,D,E. Siano C_t, $t\in\mathbb{P}^1$ le curve del fascio V generato da C e D, si noti che $C\cap D=BS(V)$. Sia $E=E_1+...+E_r$ la decomposizione in componenti irriducibili e sia m_i il grado di E_i. Sia per ogni i, $q_i\in E_i-BS(V)$ un punto fissato, esiste allora un unico $t_i\in\mathbb{P}^1$ tale che $q_i\in C_{t_i}$, siccome $E_i\cap C\cap D$ deve necessariamente contenere nm_i punti, $E_i\cap C_{t_i}$ contiene almeno nm_i+1 punti e quindi E_i è una componente di C_{t_i}. Si noti che se $q=q_i=q_j\in E_i\cap E_j$, $i\neq j$, allora q è un punto singolare di E e quindi non appartiene ai punti base di V, ragionando come sopra ne segue che $t_i=t_j=t$ per ogni i,j. Dunque E è contenuta in una curva C_t del fascio, basta quindi prendere $H=C_t-E$. □



Corollario 4.2.(Teorema di Pascal, 1640) *Le coppie di lati opposti di un esagono inscritto in una conica ridotta si intersecano in punti allineati.*

Dim. (Plücher, 1828) Siano $L_1,L_2,..,L_6$ i lati successivi dell'esagono inscritto nella conica E. Basta osservare che le due cubiche $C=L_1+L_3+L_5$, $D=L_2+L_4+L_6$

si intersecano in 9 punti e 6 di questi appartengono a E. □

Un'altra elegantissima dimostrazione di 4.2 sarà proposta come esercizio nel capitolo VI, altre dimostrazioni del teorema di Pascal (1640) sono riportate in [Sev] §11. L'argomento originale di Pascal era quello di ricondursi ad un cerchio mediante una affinità e poi usare le proprietà metriche della geometria euclidea.

Lo studio dei sistemi lineari e delle condizioni lineari è un ottimo strumento per stabilire l'esistenza di curve con date caratteristiche.

Ad esempio si consideri k punti $p_1,..,p_k \in \mathbb{P}^2$ e $r_1,...,r_k$ interi positivi. Se $n(n+3) \geq \sum r_i(r_i+1)$ allora esiste una curva C di grado n tale che $m_{p_i}(C) \geq r_i$, infatti la dimensione di $|\mathcal{O}(n)|$ è $\frac{1}{2}n(n+3)$ mentre le condizioni $m_{p_i}(C) \geq r_i$ inducono al più $\frac{1}{2}\sum r_i(r_i+1)$ condizioni lineari.

Teorema 4.3. *Sia C curva* **irriducibile** *di grado n e siano $p_1,...,p_k$ i punti singolari di C, se r_i è la molteplicità di p_i vale*

$$(n-1)(n-2) \geq \sum r_i(r_i-1).$$

Dim. Abbiamo già dimostrato che $n(n-1) \geq \sum r_i(r_i-1)$, dato che $(n-1)(n+2) \geq n(n-1)$ si ha che

$$h = \frac{1}{2}((n-1)(n+2) - \sum r_i(r_i-1)) \geq 0,$$

scelti $q_1,...,q_h$ punti non singolari di C, per quanto osservato precedentemente esiste una curva D di grado $n-1$ passante per $q_1,...,q_h$ e tale che $m_{p_i}(D) \geq r_i - 1$ per ogni $i = 1,...,k$. Dato che C è irriducibile e distinta da D vale il teorema di Bézout

$$n(n-1) \geq \sum_{i=1}^{k} m_{p_i}(C)m_{p_i}(D) + \sum_{i=1}^{h} m_{q_i}(C)m_{q_i}(D)$$

$$\geq \sum_{i=1}^{k} r_i(r_i-1) + h = \frac{1}{2}((n-1)(n+2) + \sum_{i=1}^{k} r_i(r_i-1))$$

da cui segue tutto. □

Esistono dei casi in cui in 4.3 vale l'uguaglianza, ad esempio la curva di equazione affine $y^{n-1} = x^n$ possiede un punto di molteplicità $n-1$.

Le curve di grado $2,3,4,5,6,...,n$ si dicono rispettivamente coniche, cubiche, quartiche, quintiche, sestiche,...,n-iche

Proposizione 4.4. *Sia V un fascio di curve e p punto base di V; allora per ogni terna distinta $C,D,E \in V$ vale $\nu_p(C,D) = \nu_p(C,E) = \nu_p(D,E)$.*

Dim. Segue immediatamente dalle proprietà del risultante, in particolare la 1.3.d) del capitolo III. □

Un altra significativa applicazione dei sistemi lineari si ha nel seguente

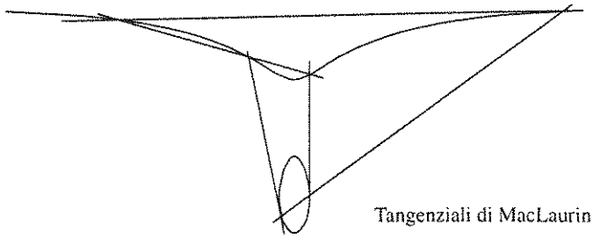
Teorema 4.5. (Dei tangenziali di MacLaurin, 1748) *Sia C una cubica irriducibile, per ogni punto nonsingolare $p \in C$ si definisce il tangenziale di p come il terzo punto di intersezione di C con la retta tangente in p.*

Se tre punti lisci di C sono allineati allora anche i loro tangenziali sono allineati.

Dim. Siano $p_1,p_2,p_3 \in C$ punti lisci allineati e sia L la retta che li contiene; dicendo questo si intende che p_1,p_2,p_3 sono i punti di intersezione di L e C contati con molteplicità. Se $p_1 = p_2$ allora p_3 è il tangenziale di p_1 e p_2 ed il teorema è banale. Possiamo quindi supporre senza traumi che la retta L interseca trasversalmente C.

Siano T_1,T_2,T_3 le rette tangenti a C nei punti p_1,p_2,p_3 rispettivamente e sia V il fascio di cubiche generato da C e $T_1+T_2+T_3$. Preso un punto $q \in L - C$ esiste unica una cubica $D \in V$ che contiene q; dato che i tangenziali appartengono ai punti base del fascio appartengono anche a D e se proviamo che $D = 2L+R$ allora saranno contenuti nella retta R.

La retta L interseca D in almeno quattro punti distinti, p_1,p_2,p_3,q e per Bézout si ha $D = L+Q$ con Q conica. Dato che per ogni i vale $\nu_{p_i}(C,D) = \nu_{p_i}(C,T_1+T_2+T_3) \geq 2$ e $\nu_{p_i}(C,L) = 1$ i punti p_i devono necessariamente appartenere a Q che deve quindi contenere L come componente. □



Tangenziali di MacLaurin

ESERCIZIO 13: Se k punti di $\mathbb{P}^2$ inducono k condizioni lineari sulle curve di grado n allora inducono k condizioni lineari su $|\mathcal{O}(m)|$ per ogni $m \geq n$.

ESERCIZIO 14: (Principio di Lamé, 1818)

Siano C,D curve di grado n che si intersecano in n^2 punti distinti $p_1,...,p_{n^2}$. Ogni curva di grado n passante per $p_1,...,p_{n^2}$ appartiene al fascio generato da C,D.

ESERCIZIO 15: Provare che $n+1$ punti distinti di $\mathbb{P}^2$ inducono condizioni indipendenti sul sistema lineare delle curve di grado n. Si deduca quindi per induzione su n che la

dimensione di $|\mathcal{O}(n)|$ è $\frac{1}{2}n(n+3)$.

5. Esercizi complementari

ESERCIZIO 16: Siano $C_1,...,C_r$ curve senza componenti comuni di gradi $n_1 \geq n_2 \geq ... \geq n_r$. Allora i supporti di $C_1,...,C_r$ hanno al più $n_1 n_r$ punti in comune.

ESERCIZIO 17: Provare che in caratteristica p esistono curve irriducibili C e punti esterni q tali che ogni retta passante per q è tangente a p.

ESERCIZIO 18: (*) Sia data una curva irriducibile C con al più singolarità ordinarie ed un punto $q \in \mathbb{P}^2$ tale che la polare C_q è indeterminata, o equivalentemente tale che tutte le rette tangenti a C nei suoi punti lisci passano per q (una curva siffatta si dice *strana*). Assumendo che $m_q(C) \leq 1$ si provi che C o è una retta oppure una conica in caratteristica 2 (il risultato è vero anche senza l'ipotesi $m_q(C) \leq 1$ ma la dimostrazione sembrerebbe richiedere strumenti non ancora visti).
(Sugg. Trattare separatamente i casi $q \in C$ e $q \notin C$. Nel primo caso si prendano coordinate affini x,y tali che $q=(0,0)$ e detta f l'equazione affine di C si ha che f divide $xf_x + yf_y$. Nel secondo caso siano x,y,z coordinate omogenee tali che $q=[0,0,1]$ e detti n,F il grado e l'equazione di C si provi che la caratteristica di $\mathbb{K}$ divide n e che F_x, F_y hanno un fattore comune di grado $n-2$.)

ESERCIZIO 19: Sia C curva ridotta, $p \in C$ liscio, $char\mathbb{K}=0$, allora esistono al più $n(n-1)-1$ rette tangenti a C passanti per p (Sugg. calcolare il grado del risultante di F, F_q quando $A_0 = 0$).

ESERCIZIO 20: (**?) Data una curva C di grado n, una retta l si dice una tangente semplice a C se $l \cap C$ contiene esattamente $n-1$ punti o in altri termini 1 punto di molteplicità 2 e $n-2$ punti di molteplicità 1. Provare che se $\mathbb{K}$ ha caratteristica 0 e C è liscia esistono al più un numero finito di rette che non sono ne trasversali ne tangenti semplici a C.

ESERCIZIO 21: Se C è una unione di rette allora vale il segno uguale in 3.8.

ESERCIZIO 22: In caratteristica 0 per la polare generica C_q vale $m_p(C_q) = m_p(C) - 1$.

ESERCIZIO 23: (*) Sia $p \in C \cap D$ e sia t il numero (contato con molteplicità) delle componenti comuni ai coni tangenti a C e D nel punto p, provare che $\nu_p(C,D) \geq m_p(C)m_p(D) + t$ (Sugg. nella dimostrazione di 3.5 valutare il rango della matrice $\Delta(0)$ ed utilizzare l'esercizio 14 del capitolo I).

ESERCIZIO 24: Per ogni n si determini il massimo intero $k = k(n)$ tale che presi comunque k punti distinti $p_1,...,p_k$, il passaggio per $p_1,..,p_k$ impone esattamente k condizioni lineari (esempio $k(2)=3$).

ESERCIZIO 25: Siano a,b,c tre punti distinti di una conica irriducibile e siano A,B,C le rispettive rette polari. Dimostrare che i punti $p = A \cap (b+c)$, $q = B \cap (a+c)$, $q = C \cap (a+b)$ sono allineati.

ESERCIZIO 26: Sia L retta, $p \in L$; C,D curve di grado n senza componenti comuni. Provare che:

i) Esiste al più una curva $C' \in < C,D >$ contenente L.

ii) Per ogni $C' \in < C,D >$ vale $\nu_p(L,C') \geq \min(\nu_p(L,C), \nu_p(L,D))$ e vale $=$ eccetto per un numero finito di C'.

si dica se i punti i) e ii) continuano a valere se si considera una curva irriducibile E al posto della retta L?

ESERCIZIO 27: Costruire un sistema lineare di quartiche di dimensione 3 con esattamente 12 punti base.

ESERCIZIO 28: Trovare una quartica irriducibile con tre nodi.

ESERCIZIO 29: Dati 4 punti distinti $p_1,...,p_4$, determinare tutte le quartiche che hanno punti doppi in p_i per ogni i. (per 4.3 tali quartiche non possono essere irriducibili).

ESERCIZIO 30: Sia $char\mathbb{K} \neq 2,3$. Una cubica irriducibile possiede al più un punto singolare, provare che ogni cubica irriducibile singolare si può scrivere in un opportuno sistema di coordinate affini come $y^2 = x^3$ oppure $y^2 = x^3 + x^2$.

ESERCIZIO 31: Sia $char\mathbb{K} \neq 2,3$, $f(x,y)$ omogeneo di terzo grado. Mostrare che esistono $\alpha, \beta \in \mathbb{K}$ tali che $f(x,y) + \alpha(x^3 + xy^2) + \beta(x^2y + y^3)$ possiede una radice tripla.

ESERCIZIO 32: Siano $f_0, f_1 \in \mathbb{K}[x]$ senza radici comuni, se $\frac{df_0}{dx} \neq 0$, i polinomi $f_t = (1-t)f_0 + tf_1$ non possiedono radici multiple per quasi tutti i t (cioè eccetto un numero finito).

ESERCIZIO 33: Siano $f_0, f_1, f_2 \in \mathbb{K}[x_0, x_1]$ omogenei di grado n senza fattori comuni. Si può definire una applicazione $\phi: \mathbb{P}^1 \to \mathbb{P}^2$, $\phi(x_0,x_1) = (f_0(x_0,x_1), f_1(x_0,x_1), f_2(x_0,x_1))$. Provare che l'immagine di ϕ è una curva irriducibile C; se inoltre esiste $c \in C$ tale che $\phi^{-1}(c)$ contiene un solo punto (contato con molteplicità) allora C ha grado n. (Sugg. il punto $[v_0,v_1,v_2]$ appartiene all'immagine di ϕ se e solo se le forme binarie $v_i f_j - v_j f_i$ hanno una radice comune).

ESERCIZIO 34: Precisare il concetto di molteplicità usato nell'esercizio precedente.

ESERCIZIO 35: Siano C,D,C' curve di grado n tali che C' sia irriducibile, C,D senza componenti comuni e per ogni $p \in C \cap D$ vale $\nu_p(C,D) = \nu_p(C',D) = \nu_p(C',C)$ allora $C' \in < C,D >$. Mostrare che questa ultima conclusione è in generale falsa se C' ha delle componenti multiple.

ESERCIZIO 36: (Teorema di Jacobi, 1836)

Siano $p_1,...,p_{nm}$ punti distinti di interserzione di una curva di grado n e di una curva irriducibile di grado $m \leq n$ e sia $p = \frac{1}{2}(m-1)(m-2)$. Si provi che i punti p_i inducono $mn - p$ condizioni lineari indipendenti sullo spazio delle curve di grado n

Nota. I teoremi di Gergonne, Jacobi ed il principio di Lamé sono casi particolari dell'importantissimo *Teorema AF + BG di Max Noether (1872)* che affronteremo e dimostreremo nel prossimo capitolo.

Nota. (cf. [E-C]) Ci può sembrare strano ma, mentre la teoria delle curve algebriche piane è stata uno dei temi centrali della matematica del XVIII secolo, lo sviluppo dell'algebra lineare e degli spazi a più dimensioni nasce invece all'inizio del secolo XIX. Si capisce quindi come nel 1750, Cramer ritenesse un paradosso il fatto che $\frac{1}{2}n(n+3)$ punti contenuti nell'intersezione di due curve non determinano univocamente una curva di grado n passante per essi. (Oltre a Cramer, lo stesso fatto mise in crisi pure Mac-Laurin ed Eulero).

ESERCIZIO 37: Sia dato un quadrilatero in $\mathbb{P}^2$ di vertici a,b,c,d e siano e,f,g i punti di intersezione delle diagonali. Due cubiche passanti per a,b,c,d,e,f,g e aventi un contatto multiplo in e hanno il nono punto di intersezione sulla retta $f+g$.

ESERCIZIO 38: Siano C e D curve di grado n tali che $Sing(C) \cap D = \emptyset$. Se E è una curva di grado n tale che $\nu_p(C,D) = \nu_p(C,E)$ per ogni $p \in C$ allora C è ridotta e appartiene al fascio di curve generato da E e D.

Provare inoltre che tale risultato è generalmente falso se D contiene un punto singolare di C.

ESERCIZIO 39: Sia $f \in \mathbb{C}[x,y,z]$ irriducibile ed omogeneo di grado n e sia

$$V_{\mathbb{R}}(f) = \{[x,y,z] \in \mathbb{P}^2_{\mathbb{R}} | \, f(x,y,z) = 0\}$$

Vale allora una delle seguenti possibilità:

i) Esiste una costante non nulla $a \in \mathbb{C} - \{0\}$ tale che $af \in \mathbb{R}[x,y,z]$.

ii) $V_{\mathbb{R}}(f)$ contiene al più n^2 punti.

ESERCIZIO 40: Sia F un fascio di curve di grado n e sia L una retta che non interseca il luogo base di F. Provare che se il campo $\mathbb{K}$ ha caratteristica 0 allora vi sono al più $2n-2$ curve del fascio che sono tangenti a L. Mostrare con un esempio che lo stesso risultato è falso senza ipotesi sulla caratteristica di $\mathbb{K}$.

ESERCIZIO 41: Sia C una curva affine di equazione $f(x,y) = 0$ avente una cuspide in $o = (0,0)$. Sia inoltre L l'unica componente del cono tangente a C in o. Se $char\mathbb{K} \neq 2$ le seguenti condizioni sono equivalenti:

1) $\nu_o(C,L) = 3$.

2) A meno di un cambio lineare di coordinate si ha $f = y^2 + x^3 +$ termini di grado ≥ 4.

Una cuspide con tali caratteristiche si dice **cuspide semplice**.

ESERCIZIO 42: Si disegni (approssimativamente) la parte affine reale delle curve di equazioni: $y^2 + x^3(x^2-1)^2(x-2)$, $y^2 = x^2(x-1)$, $y^2 = x^2(x^2-2x-3)$.

ESERCIZIO 43: Sia L una retta in $\mathbb{P}^2$, $u(x,y,z)$ omogeneo di grado $2n-2$ e $[x_i,y_i,z_i] \in \mathbb{P}^2$, $i = 0,...,2n$, i punti di intersezione contati con molteplicità di L con la curva di equazione $x^{2n+1} + y^{2n+1} + z^{2n+1} = xyzu$.

Provare che $x_0x_1...x_{2n} + y_0...y_{2n} + z_0...z_{2n} = 0$.

ESERCIZIO 44: Determinare e descrivere i punti singolari (su $\mathbb{C}$) delle curve di equazioni $y^3(4z-y)^3 - 4x^4(x+3z)^2 = 0$, $(8y-x-z)^3 = 216xyz$, $(x^2-z^2)^2y = (y^2-z^2)^2x$.

ESERCIZIO 45: Siano $p_1,...,p_8 \in \mathbb{P}^2$ punti in posizione generica e S una sestica con 8 punti doppi in $p_1,...,p_8$. Provare che l'equazione di S è $aU^2 + bUV + cV^2 = CQ$ con U,V equazioni di cubiche passanti per $p_1,...,p_8$ e C equazione di una conica passante per $p_1,...,p_5$.

ESERCIZIO 46: Caratteristica $\neq 2,3$. Siano $F(x_0,x_1,x_2), G(x_0,x_1,x_2)$ omogenei di gradi 2,3 rispettivamente. Studiare le singolarità della sestica di equazione $F^3 - G^2 = 0$.

ESERCIZIO 47: Caratteristica $\neq 2,3$. Trovare le tangenti dal punto $[1,1,1]$ alle cubiche di equazione $(x^2+y^2)z = 2x^3$, $x^3 + y^3 = 2z^3$

ESERCIZIO 48: Caratteristica $\neq 2$. Provare che esistono quartiche irriducibili con tre cuspidi. (Sugg.: Si determini il sistema lineare delle quartiche aventi punti singolari in $[1,0,0]$, $[0,1,0]$ e $[0,0,1]$.

ESERCIZIO 49: Sia Q una quartica irriducibile con tre cuspidi in p_1,p_2,p_3. Provare che le componenti dei coni tangenti a Q in p_1,p_2,p_3 sono rette concorrenti.

ESERCIZIO 50: (Trucco di Berzolari)

Sia C una curva piana ridotta di grado n e siano $L_1,...,L_n$ rette tre a tre non concorrenti e tali che C interseca $L_1 + L_2 + .. + L_n$ in n^2 punti distinti. Si costruisca un sottoinsieme $S \subset C$ prendendo gli n punti di intersezione di C con L_1, r punti di $L_r \cap C$ per ogni $r = 2,...,n$ ed un punto $p \in C$ esterno alle rette L_i. Provare che S ha cardinalità $\frac{1}{2}n(n+3)$ e che C è l'unica curva di grado n che lo contiene.

ESERCIZIO 51: Sia $F \in \mathbb{C}[x_0,x_1,x_2]$ omogeneo di grado 2 e sia $C \subset \mathbb{C}^2$ la curva affine di equazione $f(x,y) = F(x,y,1)$. Provare che le seguenti condizioni sono equivalenti:

i) $C \cap \mathbb{R}^2$ è un cerchio.

ii) $F(1,i,0) = F(1,-i,0) = 0$ e $C \cap \mathbb{R}^2$ contiene almeno tre punti non allineati.

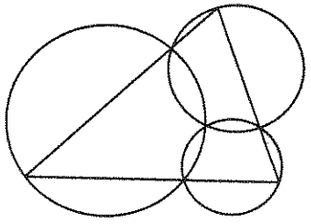
I due punti all'infinito $[1,\pm i,0]$ si dicono *punti ciclici*.

ESERCIZIO 52: (Teorema di Miquel, 1838).

Siano A_{11}, A_{22} e A_{33} i vertici di un triangolo in $\mathbb{R}^2$ e per ogni coppia (i,j) sia $A_{ij} = A_{ji}$ un punto interno al lato di estremi A_{ii}, A_{jj}.

Detto $C_i \subset \mathbb{R}^2$ il cerchio passante per i tre punti A_{i1}, A_{i2}, A_{i3} si ha che $C_1 \cap C_2 \cap C_3 \neq \emptyset$. (Sugg. Detta L_i la retta contenente il lato del triangolo opposto ad A_{ii} si consideri le curve $B_i = C_i + L_i$. Per continuità si può assumere che esista una coppia i, j tale che B_i interseca B_j in 9 punti distinti di $\mathbb{P}^2_{\mathbb{C}}$. Usare quindi il teorema di Gergonne e l'esercizio 51.)

Teorema di Miquel



ESERCIZIO 53: Sia C una curva di grado n di equazione F; $char\mathbb{K} = 0$ oppure $char\mathbb{K} > n$. La polare C_q è indeterminata se e solo se C è unione di rette passanti per q.

ESERCIZIO 54: $(*)$ Un sistema lineare bidimensionale V di curve piane si dice una *rete di Laguerre* se esiste un isomorfismo proiettivo $\phi: \mathbb{P}^2 \to V$ tale che $p \in \phi(p)$ per ogni $p \in \mathbb{P}^2$. Dati 7 punti di $\mathbb{P}^2$ in posizione generica (i.e. nessuna terna allineata e nessuna sestupla in una conica) provare che le cubiche passanti per i sette punti formano una rete di Laguerre. (Sugg. Siano C_1, C_2 cubiche generiche per i 7 punti di equazione F_1, F_2 e siano a, b i rimanenti punti di intersezione; provare che la retta $L = a + b$ non contiene nessuno dei sette punti base. Esistono coordinate omogenee x_0, x_1, x_2 tali che $L = \{x_0 = 0\}$ e $x_1F_1 + x_2F_2$ è nulla su L.)

ESERCIZIO 55: (Teorema di Carnot, 1803)

Sia $C \subset \mathbb{P}^2$ una curva piana di grado m e siano $a_1, .., a_n \in \mathbb{P}^2 - C$. Per ogni $i = 1, .., n$ siano $b_{i1}, .., b_{im}$ i punti di intersezione (contati con molteplicità) di C con la retta $\overline{a_i a_{i+1}}$. Provare che

$$\prod_{j=1}^{m} (a_1 .... a_n b_{1j} ... b_{nj}) = 1$$

(Sugg. Prendere un sistema di coordinate affini x, y tali che la retta all'infinito non contiene nessuno dei punti a_i, b_{ij}, detta f l'equazione affine di C si provi che $\prod_{j=1}^{m} (a_i a_{i+1} b_{ij}) = \frac{f(a_i)}{f(a_{i+1})}$.)

ESERCIZIO 56: Dedurre il teorema dei tangenziali di MacLaurin dal teorema di Carnot e dal teorema di Menelao.

ESERCIZIO 57: (Trasformata di Tschirnhausen, 1861)

In caratteristica 0, mediante la risoluzione di alcune equazioni di secondo grado è possibile ricondurre la soluzione di una equazione algebrica $f(x) = x^n + a_1x^{n-1} + ... + a_n = 0$ alla soluzione di una equazione $g(y) = y^n + b_3y^{n-3} + ... + b_n$. (Sugg. si consideri il polinomio $h = y - rx^2 - sx - t$ e sia $g(y) = \sum b_i y^{n-i}$ il risultante dell'eliminazione di x da f e h. Provare che b_i è un polinomio omogeneo di grado i in r, s, t).

ESERCIZIO 58: Utilizzare la trasformata di Tschirnhausen per ricondurre la soluzione dell'equazione di quarto grado alla soluzione di una equazione di terzo grado ed una equazione biquadratica $y^4 + by^2 + c = 0$.

ESERCIZIO 59: Sia $S \subset \mathbb{P}^2$ un sottoinsieme finito di $n + 1$ punti, $n > 0$. Provare che S è contenuto in una curva irriducibile di grado $\leq n$. Trovare inoltre un opportuno S che non è contenuto in nessuna curva irriducibile di grado $< n$. (Sugg. si può supporre $S \subset \mathbb{A}^2$ e $p_i = (x_i, y_i)$ con le ascisse x_i distinte. Si consideri una curva affine di equazione $y - \sum a_i x^i$)

ESERCIZIO 60: Trovare due polinomi $f, g \in \mathbb{K}[x, y]$ monici rispetto a y e senza fattori comuni tali che il risultante di $f - u, g - v$ abbia un fattore multiplo in $\mathbb{K}[x, u, v]$.

V. Curve piane: argomenti scelti

1. Le coniche

In questo paragrafo assumeremo, salvo avviso contrario, che $\mathbb{K}$ sia un campo algebricamente chiuso di caratteristica diversa da 2.

Una conica C è una curva algebrica piana di grado 2. Due coniche si dicono proiettivamente equivalenti se esiste una proiettività di $\mathbb{P}^2$ che trasforma l'una nell'altra.

Una conica non irriducibile è unione di due rette che possono essere distinte o coincidenti.

Data una conica C di equazione $F(x_0, x_1, x_2) = 0$ chiameremo **rango** di C il rango della matrice Hessiana

$$H = \begin{pmatrix} F_{00} & F_{01} & F_{02} \\ F_{10} & F_{11} & F_{12} \\ F_{20} & F_{21} & F_{22} \end{pmatrix} \in M(3,3,\mathbb{K}), \qquad F_{ij} = \frac{\partial^2 F}{\partial x_i \partial x_j}$$

Il rango di una conica non dipende dalla scelta del sistema di coordinate omogenee e determina completamente la classe di equivalenza proiettiva

Teorema 1.1. *Due coniche sono proiettivamente equivalenti se e solo se hanno lo stesso rango. In particolare ogni conica è proiettivamente equivalente ad una delle seguenti:*

i) $x_0^2 = 0$, *retta doppia.*

ii) $x_0 x_1 = 0$, *rette incidenti.*

iii) $x_0 x_2 = x_1^2$, *conica liscia.*

Dim. Si consideri un punto $p = [v_0, v_1, v_2] = [v] \in \mathbb{P}^2$; il punto p è un punto singolare di C se e solo se $Hv = (F_0(v), F_1(v), F_2(v)) = 0$.

Se il rango di H è 1 allora esiste una retta L composta di punti singolari di C e quindi deve necessariamente essere $C = 2L$.

Se il rango è 2 esiste un unico punto singolare $p = [v]$, proviamo che C è unione di rette passanti per p. Se $q = [y] \in C$ si ha per ogni $a, b \in \mathbb{K}$

$$2F(av + by) = (av + by)^t H(av + by) = y^t Hy = 0$$

Infine se il rango è 3 la conica è liscia, siano p, q, r punti distinti di C, T_p, T_q le rette tangenti a C nei punti p e q rispettivamente e o il punto di intersezione di T_p e T_q. La quaterna p, q, r, o è un sistema di riferimenti di $\mathbb{P}^2$, esiste quindi un unico sistema di coordinate omogenee x_0, x_1, x_2 tali che

$$p = [1,0,0], \qquad q = [0,0,1], \qquad r = [1,1,1], \qquad o = [0,1,0]$$

Sia F l'equazione di C in tale sistema di coordinate, dalla condizione $p, q \in C$ si deduce che $F_{00} = F_{22} = 0$.

Dalla condizione che le equazioni di T_p e T_q sono rispettivamente $x_2 = 0$, $x_0 = 0$ si deduce che $F_{01} = F_{12} = 0$ e si ha $F = ax_0x_2 - bx_1^2$. La condizione di passaggio da r impone infine che $a = b$. □

La dimostrazione appena terminata è costruttiva e fornisce un metodo effettivo per il calcolo della proiettività che trasforma una conica nella sua forma canonica. Tale calcolo richiede la soluzione di una equazione di secondo grado ed alcuni sistemi di equazioni lineari.

Nella precedente dimostrazione la scelta dei punti p, q, r è arbitraria, abbiamo dimostrato quindi il

Corollario 1.2. *Data una conica irriducibile C e tre punti distinti $p, q, r \in C$ esiste un sistema di coordinate omogenee tali che $p = [1,0,0]$, $q = [0,0,1]$, $r = [1,1,1]$ e l'equazione di C è $x_0x_2 = x_1^2$.*

ESERCIZIO 1: Provare che il corollario 1.2 è vero anche in caratteristica 2.

ESERCIZIO 2: Trovare le componenti irriducibili della conica di equazione

$$3x_0^2 + 5x_0x_1 + 2x_0x_2 + 2x_1^2 + x_1x_2 - x_2^2 = 0$$

ESERCIZIO 3: Sia V un fascio di coniche generato da due rette doppie. Provare che ogni conica del fascio è singolare.

Si consideri adesso l'applicazione $v\colon \mathbb{P}^1 \to \mathbb{P}^2$ descritta in coordinate omogenee da $v(t_0, t_1) = (t_0^2, t_0t_1, t_1^2)$. Si vede facilmente che v è iniettiva ed ha come immagine la conica di equazione $x_0x_2 = x_1^2$.

Corollario 1.3. *Sia $C \subset \mathbb{P}^2$ una conica liscia. Esiste allora una base h_0, h_1, h_2 dello spazio vettoriale dei polinomi omogenei di grado 2 nelle variabili t_0, t_1 tale che l'applicazione $h\colon \mathbb{P}^1 \to \mathbb{P}^2$, definita in coordinate omogenee da*

$$h(t_0, t_1) = (h_0(t_0, t_1), h_1(t_0, t_1), h_2(t_0, t_1))$$

induce una bigezione tra $\mathbb{P}^1$ e C. Inoltre h è unica a meno di proiettività di $\mathbb{P}^1$.

Dim. Dato che t_0^2, t_0t_1, t_1^2 formano una base dello spazio vettoriale dei polinomi omogenei di grado 2 in t_0, t_1, dal corollario 1.2 segue l'esistenza di un tale morfismo h. Per dimostrare l'unicità si può assumere che C sia la conica di equazione $x_0x_2 = x_1^2$. A meno di comporre h con una proiettività di $\mathbb{P}^1$ si può assumere che $h(1,0) = [1,0,0]$, $h(0,1) = [0,0,1]$, $h(1,1) = [1,1,1]$. Si deve quindi avere $h_0 = t_0f$, $h_1 = t_0t_1a$, $h_2 = t_1g$ con a costante e f, g polinomi omogenei di grado 1 tali che $f(1,0) \neq 0$, $g(0,1) \neq 0$, $f(1,1) = g(1,1) = a$ e $gf = a^2t_0t_1$. □

Il corollario 1.3 permette di definire su C una struttura di retta proiettiva, in particolare è ben definito il birapporto di una quaterna ordinata di punti su C. Su tale struttura si basa il ben noto teorema di Steiner, infatti dato un punto $[a, b] \in \mathbb{P}^1$, la retta di $\mathbb{P}^2$ di equazione $bx_1 - ax_2$ interseca la conica $x_0x_2 = x_1^2$ nei punti $p = [1,0,0]$ e $v([a,b])$. L'applicazione $[a,b] \to ax_1 - bx_2$ è una proiettività tra $\mathbb{P}^1$ ed il fascio di rette passanti per p; similmente l'applicazione $[a,b] \to ax_1 - bx_0$ è una proiettività tra $\mathbb{P}^1$ ed il fascio di rette passanti per il punto $q = [0,0,1]$. Da quanto detto segue dunque il

Teorema 1.4.(Steiner, 1832) *Sia C una conica liscia, $p, q \in C$, F_p, F_q i fasci di rette passanti per p e q rispettivamente. L'applicazione $F_p \to F_q$ definita da $F_p \ni L \to q + s$, dove s è il punto di intersezione di L con C diverso da p, è una proiettività.*

È facile dimostrare che ogni fascio di coniche contiene almeno una conica singolare. Infatti siano C_1, C_2 coniche di equazioni F_1, F_2 e matrici Hessiane H_1, H_2 rispettivamente. Se C_2 è singolare abbiamo finito. Altrimenti si ha che la conica di equazione $F_1 - tF_2$ è singolare se e solo se $p(t) = \det(H_1 - tH_2) = 0$; Il polinomio $p(t)$ ha grado 3 e quindi ammette radici.

Se vogliamo determinare i punti di intersezione di due coniche C_1, C_2 si può procedere in almeno tre modi distinti.

1) Prendere un sistema di coordinate omogenee in cui il punto $[0,0,1]$ non appartiene all'unione $C_1 \cup C_2$, calcolare il risultante rispetto a x_2 delle equazioni di C_1 e C_2 e determinarne le radici.

2) Se C_2 è singolare se ne determina le componenti irriducibili e quindi l'intersezione di queste con C_1. Se C_2 è liscia, $h\colon \mathbb{P}^1 \to C_2$ è una proiettività (cf. Corollario 1.3)

e F_1 è un'equazione per C_1, i punti di intersezione sono in bigezione naturale con le radici del polinomio omogeneo in due variabili $F(h(t_0,t_1))$.

3) Determinare una conica singolare C_0 appartenente al fascio generato da C_1 e C_2 e quindi ricondursi al caso particolare del punto 2) ricordandosi che se $C_0 \neq C_2$ allora $C_1 \cap C_2 = C_0 \cap C_2$.

I metodi 1) e 2) richiedono in generale la soluzione di una equazione di quarto grado mentre il metodo 3) richiede solamente la soluzione di una equazione di terzo grado e di tre equazioni di secondo grado.

Esempio 1.5. Il generico polinomio monico di quarto grado

$$R(x) = x^4 + ax^3 + bx^2 + cx + d$$

può essere visto come il risultante dell'eliminazione di y dai polinomi

$$f_1(x,y) = y^2 + axy + by + cx + d, \qquad f_2(x,y) = y - x^2$$

e quindi le radici di R corrispondono alle intersezioni delle coniche affini di equazioni $f_1 = 0$ e $f_2 = 0$. Le matrici Hessiane di f_1 e f_2 (o più precisamente dei loro omogeneizzati) sono rispettivamente

$$H_1 = \begin{pmatrix} 0 & a & c \\ a & 2 & b \\ c & b & 2d \end{pmatrix}, \qquad H_2 = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

e quindi

$$p(t) = \det(H_1 - tH_2) = \begin{vmatrix} 2t & a & c \\ a & 2 & b-t \\ c & b-t & 2d \end{vmatrix}$$

Se avete già letto il capitolo II troverete interessante assumere la caratteristica di $\mathbb{K}$ diversa da $2,3$, porre $a_0 = 1$, $4a_1 = a$, $6a_2 = b$, $4a_3 = c$, $a_4 = d$ ed eseguire la "misteriosa" sostituzione $t = 4(s + a_2)$.

Un semplice conto che omettiamo ci dà

$$q(s) = -\frac{p(4(s+a_2))}{32} = 4s^3 - g_2 s - g_3$$

dove $g_2 = a_0a_4 - 4a_1a_3 + 3a_2^2$ e $g_3 = a_0a_2a_4 - a_0a_3^2 + 2a_1a_2a_3 - a_2^3 - a_1^2a_4$.

Il polinomio $q(s)$ viene talvolta detto *risolvente* di $R(x)$ e come abbiamo visto la quaterna delle radici di R è proiettivamente equivalente alla quaterna formata dalle radici di q più il punto all'infinito.

ESERCIZIO 4: Calcolare i punti di intersezione delle coniche di equazioni

$$x_0^2 + x_1^2 + x_2^2 = 0, \qquad x_1^2 + x_2^2 - x_0x_1 - x_0x_2 = 0$$

ESERCIZIO 5: Scrivere l'equazione della conica affine passante per i punti $(0,0)$, $(1,0)$, $(0,1)$ e tangente alla retta $x+y=4$ nel punto $(2,2)$.

Dato che lo spazio delle coniche ha dimensione 5, per cinque punti distinti di $\mathbb{P}^2$ passa almeno una conica; inoltre tale conica è unica se i punti sono presi in posizione generica. Più precisamente vale la

Proposizione 1.6. *Se per cinque punti distinti di $\mathbb{P}^2$ passano due coniche distinte allora quattro di essi sono allineati.*

Dim. Per Bézout le due coniche devono avere una retta L in comune e le due coniche possono avere al più un punto di intersezione al di fuori di L. □

Si noti che il teorema di Steiner può essere interpretato come una condizione necessaria e sufficiente sulle sestuple di punti distinti affinché siano contenute in una conica. Se C è una conica liscia di equazione $F(x_0,x_1,x_2) = 0$ e $p = [y_0,y_1,y_2]$, la curva polare di p rispetto a C è la retta C_p di equazione $F_p(x) = y^t H x = 0$ dove H indica la matrice Hessiana di F. Dato che C è liscia la matrice H è invertibile e quindi l'applicazione $p \to C_p$ definisce una proiettività $\mathbb{P}^2 \to (\mathbb{P}^2)^\vee$.

Lemma 1.7. *Nelle notazioni precedenti $p \in C_q$ se e solo se $q \in C_p$.*

Dim. La matrice Hessiana è simmetrica. □

Esempio 1.8. Sia $L \subset \mathbb{P}^2$ retta, $p,q \in L$ punti distinti, $r = C_p \cap C_q$. Si ha $p,q \in C_r$ e quindi $L = C_r$.

Teorema 1.9. *C conica liscia. Se $p \in C$ allora C_p è la retta tangente a C nel punto p. Se $p \notin C$ allora C_p interseca C in due punti distinti e per p passano esattamente due rette distinte tangenti a C.*

Dim. Se $p \in C$ e $q \in C_p$, $q \neq p$ allora $p \in C_q$ e quindi $p+q = C_p$ è tangente a C in p.

Se $p \in \mathbb{P}^2$ e C_p è tangente a C nel punto $q \in C$ allora per il punto precedente $C_p = C_q$ e $p = q$. Per Eulero se $p \notin C$ allora $p \notin C_p$ e quindi i punti di intersezione di C_p con C non sono allineati con p. □

Quanto dimostrato mostra in particolare che, data una conica liscia $C \subset \mathbb{P}^2$, l'insieme delle sue rette tangenti $C^\vee = \{C_p \in (\mathbb{P}^2)^\vee \mid p \in C\}$ è una conica detta **conica duale** di C. Si ha inoltre $C^{\vee\vee} = C$.

ESERCIZIO 6: Sia $\mathbb{P}^5$ lo spazio di tutte le coniche e sia $v\colon (\mathbb{P}^2)^\vee \to \mathbb{P}^5$ data da $v(L) = 2L$. L'immagine V di v è detta superficie di Veronese. Dati $p,q \in V$ la retta $p+q$ è contenuta nel luogo delle coniche singolari.

ESERCIZIO 7: Provare che le coniche tangenti ad una retta data sono una quadrica non degenere di $|\mathcal{O}(2)|$.

2. Corrispondenze e poligoni di Poncelet

In questa sezione daremo una dimostrazione del celebre teorema dei poligoni di Poncelet; le idee principali di questa dimostrazione sono state indicate da Cayley nel 1871 ([Cay], [E-C] Libro II p. 164, [An]) e riposano sulla teoria delle corrispondenze su $\mathbb{P}^1$.

Definizione 2.1. Sia $F(x_0,x_1,y_0,y_1)$ un polinomio biomogeneo irriducibile di bigrado (a,b). L'insieme dei punti

$$C = V(F) = \{([x_0,x_1],[y_0,y_1]) \in \mathbb{P}^1 \times \mathbb{P}^1 | \, F(x_0,x_1,y_0,y_1) = 0\}$$

si dice una **corrispondenza irriducibile** di tipo (a,b).

Per il teorema degli zeri di Hilbert la corrispondenza C determina la sua equazione F a meno di una costante moltiplicativa.

Ad esempio la diagonale

$$\Delta = \{([x_0,x_1],[y_0,y_1]) \in \mathbb{P}^1 \times \mathbb{P}^1 | \, x_0y_1 - x_1y_0 = 0\}$$

è una corrispondenza irriducibile di tipo $(1,1)$.

Più in generale se $f(x_0,x_1)$, $g(x_0,x_1)$ sono polinomi omogenei di grado n senza fattori comuni l'insieme

$$\Gamma = \{([x_0,x_1],[y_0,y_1]) \in \mathbb{P}^1 \times \mathbb{P}^1 | \, y_0g(x_0,x_1) - y_1f(x_0,x_1) = 0\}$$

è una corrispondenza irriducibile di tipo $(n,1)$. Si noti che Γ è il grafico dell'applicazione $\gamma\colon \mathbb{P}^1 \to \mathbb{P}^1$ data in coordinate omogenee da $\gamma(x_0,x_1) = (f(x_0,x_1), g(x_0,x_1))$.

Definizione 2.2. Una **corrispondenza** è una combinazione lineare formale finita di corrispondenze irriducibili a coefficienti interi positivi. In simboli una corrispondenza è $C = m_1C_1 + ... + m_kC_k$ con $m_i > 0$ e C_i corrispondenza irriducibile.

Ragionando come per le curve piane si dimostra che esiste una bigezione naturale tra l'insieme delle corrispondenze di tipo (a,b) ed il proiettivizzato dello spazio dei polinomi biomogenei di bigrado (a,b).

Se C è una corrispondenza di equazione $F(x,y) = 0$ si definisce la sua **inversa** C^{-1} come la corrispondenza di equazione $F(y,x) = 0$. Il nome di corrispondenza inversa è motivato esclusivamente da ragioni storiche (cf. [G-H] p. 283); sarebbe infatti molto più sensato chiamarla trasposta. Si osservi ad esempio che $(C_1+C_2)^{-1} = C_1^{-1}+C_2^{-1}$. Il nome di corrispondenza inversa è inoltre in aperta contraddizione con la seguente (ugualmente storica)

Definizione 2.3. Una corrispondenza C si dice **simmetrica** se $C = C^{-1}$.

Si noti che se C ha tipo (a,b) allora C^{-1} ha tipo (b,a) e che la corrispondenza di equazione F è simmetrica se e solo se $F(x,y) = \delta F(y,x)$, $\delta^2 = 1$.

Definizione 2.4. I **punti fissi** di una corrispondenza C sono i punti di intersezione di C con la diagonale Δ.

Se F è l'equazione di C le radici del polinomio $f(x_0,x_1) = F(x_0,x_1,x_0,x_1)$ sono in bigezione con i punti fissi; si ha dunque il

Lemma 2.5.(Principio di Chasles) *Sia C una corrispondenza di tipo (a,b). Se la diagonale Δ non è una componente di C allora C contiene $a+b$ punti fissi contati con molteplicità.*

ESERCIZIO 8: Sia C una corrispondenza simmetrica non contenente la diagonale Δ. Il punto (p,p) è un punto fisso multiplo se e solo se la retta $\{p\} \times \mathbb{P}^1$ è tangente a C nel punto (p,p). (Sugg. Se F è l'equazione di C provare che $F(x,y) = F(y,x)$.)

Se la caratteristica del campo $\mathbb{K}$ è 0 o sufficientemente alta è facile calcolare il numero di punti p tali che la retta $\{p\} \times \mathbb{P}^1$ è tangente ad una data corrispondenza C di tipo (a,b). Sia infatti $F(x_0,x_1,y_0,y_1)$ l'equazione di C, se pensiamo F come una forma binaria di grado b a coefficienti in $\mathbb{K}[x_0,x_1]$ allora i punti p cercati sono le radici del discriminante $\Delta(x_0,x_1)$ di F. Siccome il discriminante di una forma di grado b è omogeneo di grado $2b-2$ nei coefficienti della forma ne segue che $\Delta(x_0,x_1)$ è omogeneo di grado $2a(b-1)$ nelle variabili x_0,x_1. Abbiamo quindi il

Lemma 2.6. *Sia C una corrispondenza di tipo (a,b) senza componenti multiple. Se la caratteristica di $\mathbb{K}$ è 0 oppure $> b$ esistono $2a(b-1)$ punti $p \in \mathbb{P}^1$ contati con molteplicità tali che la retta $\{p\} \times \mathbb{P}^1$ è tangente a C.*

Classicamente una corrispondenza C di tipo (a,b) veniva interpretata come una applicazione "algebrica" di grado a definita su $\mathbb{P}^1$ a valori nello spazio proiettivo delle b-uple non ordinate di punti di $\mathbb{P}^1$. Più precisamente al punto $p \in \mathbb{P}^1$ si associava la b-upla $C_p = C \cap (\{p\} \times \mathbb{P}^1)$. Si aveva quindi in particolare che:

$p \in C_p$ se e solo se p è un punto fisso.

$p \in C_q$ se e solo se $q \in C_p^{-1}$.

Se C e D sono due corrispondenze viene spontaneo definire la loro composizione $D \circ C$ in modo tale che per ogni punto $p \in \mathbb{P}^1$ si abbia

$$D \circ C_p = \cup_{q \in C_p} D_q$$

In termini moderni e rigorosi si definisce la composizione mediante l'uso del risultante. Se il polinomio F di bigrado (a,b) è l'equazione di C ed il polinomio G di bigrado (m,n) è l'equazione di D si definisce $D \circ C$ come la corrispondenza di equazione

$$H(x_0,x_1,y_0,y_1) = R_{b,m}(F(x_0,x_1,z_0,z_1), G(z_0,z_1,y_0,y_1))$$

dove il risultante è fatto considerando F e G come forme binarie nelle variabili z_0, z_1. Tale definizione è perfettamente compatibile con la descrizione intuitiva di corrispondenza composta, infatti se $p = [u_0, u_1]$ è un punto fissato tale che $\{p\} \times \mathbb{P}^1$ non è una componente di C si ha, a meno di costanti moltiplicative

$$H(u_0, u_1, y_0, y_1) = \prod_{i=1}^{b} G(\alpha_i, \beta_i, y_0, y_1)$$

dove $[\alpha_i, \beta_i] \in \mathbb{P}^1$, $i = 1, ..., b$ sono tutte e sole le radici della forma $F(u_0, u_1, z_0, z_1)$. Dalle proprietà basilari del risultante segue immediatamente che:

1) Se C ha tipo (a, b) e D ha tipo (m, n) allora $D \circ C$ ha tipo (am, bn).
2) $(D \circ C)^{-1} = C^{-1} \circ D^{-1}$ e quindi $C^{-1} \circ C$ è simmetrica.
3) $D \circ (C_1 + C_2) = D \circ C_1 + D \circ C_2$, $(D_1 + D_2) \circ C = D_1 \circ C + D_2 \circ C$.

ESERCIZIO 9: Siano C, D corrispondenze irriducibili. Se per infiniti punti $p \in \mathbb{P}^1$ vale $C_p \subset D_p$ allora $C = D$.

ESERCIZIO 10: (Teorema di Bézout per le corrispondenze).

Due corrispondenze senza componenti comuni di tipo (a, b) e (m, n) si intersecano in $an + bm$ punti contati con molteplicità.

Si consideri adesso due coniche liscie $Q_1, Q_2 \subset \mathbb{P}^2$ e identifichiamo Q_1 con $\mathbb{P}^1$ tramite una proiettività fissata. Si assuma inoltre la caratteristica del campo diversa da 2. Vogliamo mostrare che esiste unica una corrispondenza $B \subset Q_1 \times Q_1$ simmetrica di tipo $(2, 2)$ tale che $(p, q) \in B$ se e solo se la retta $L \subset \mathbb{P}^2$ tale che $L \cap Q_1 = \{p, q\}$ è tangente a Q_2.

Per mostrare ciò fissiamo un sistema di coordinate omogenee su $\mathbb{P}^2$, sia H la matrice Hessiana di Q_2 e $f = (f_0, f_1, f_2) \colon \mathbb{P}^1 \to Q_1$ una proiettività fissata; i polinomi $f_i \in \mathbb{K}[t_0, t_1]$ sono omogenei di grado 2.

Fissato un punto $p = [u] \in \mathbb{P}^2$, $u = (u_0, u_1, u_2)$ la conica S_p di equazione

$$({}^t uHx)^2 - ({}^t uHu)({}^t xHx) = 0$$

è l'unione delle due rette (possibilmente coincidenti) passanti per p e tangenti a Q_2. In particolare se $p \in Q_1$ si ha:

i) $\nu_p(S_p, Q_1) = 4$ se $p \in Q_2$ e $T_pQ_1 = T_pQ_2$.
ii) $\nu_p(S_p, Q_1) = 3$ se $p \notin Q_2$ e T_pQ_1 è tangente a Q_2 in un punto $q \neq p$.
iii) $\nu_p(S_p, Q_1) = 2$ in tutti gli altri casi, cioè se T_pQ_1 non è tangente a Q_2.

Dunque se $S \subset Q_1 \times Q_1$ è la corrispondenza di tipo $(4, 4)$ di equazione

$$({}^t f(x_0, x_1) H f(y_0, y_1))^2 - ({}^t f(x_0, x_1) H f(x_0, x_1))({}^t f(y_0, y_1) H f(y_0, y_1)) = 0$$

si ha che $S = B + 2\Delta$ dove B è la corrispondenza cercata.

ESERCIZIO 11: Nelle notazioni precedenti sia $B^n \subset Q_1 \times Q_1$ la composizione di B con se stessa n volte. Provare che $(p, q) \in B^n$ se e solo se esiste una successione $p = p_0, p_1, ..., p_n = q \in Q_1$ tale che per ogni i la retta $p_{i-1} + p_i$ è tangente a Q_2.

Fissato un intero $n > 0$ ed un punto $p \in Q_1$ possiamo costruire due punti $p_1^{(n)}, p_2^{(n)} \in Q_1$ nel modo seguente.

Siano L_1, L_2 le rette per p tangenti a Q_2. Si definisce p_1' come il secondo punto di intersezione di L_1 con Q_1 e L_1' come la seconda retta per p_1' tangente a Q_2. Si definisce poi p_1'' come il secondo punto di intersezione di L_1'; proseguendo per n passi si arriva a definire $p_1^{(n)}$. Ripetendo la stessa procedura partendo da L_2 si definisce $p_2^{(n)}$.

Si vede facilmente che l'applicazione $p \to \{p_1^{(n)}, p_2^{(n)}\}$ è indotta da una corrispondenza simmetrica $B^{(n)}$ di tipo $(2, 2)$, basta infatti definire per ricorrenza $B^{(0)} = 2\Delta$, $B^{(1)} = B$ e per ogni $n \geq 2$ $B^{(n)} = B \circ B^{(n-1)} - B^{(n-2)}$.

Si possono verificare due casi. Nel primo la diagonale Δ è una componente di $B^{(n)}$ e quindi ogni punto di Q_1 è vertice di un poligono chiuso di n lati inscritto a Q_1 e circoscritto a Q_2. Nel secondo caso la diagonale non è una componente di $B^{(n)}$ e quindi esistono $4 = 2 + 2$ punti fissi di $B^{(n)}$ contati con molteplicità.

Siamo adesso in grado di dimostrare il ben noto

Teorema 2.7.(dei poligoni di Poncelet, 1822) *Siano $Q_1, Q_2 \subset \mathbb{P}^2$ due coniche liscie definite su di un campo algebricamente chiuso di caratteristica $\neq 2$ e $n \geq 3$ un intero. Per ogni punto $p \in Q_1$ si consideri la seguente proprietà:*

(P) Esiste una n-upla ordinata di punti distinti $p_1, p_2, ..., p_n \in Q_1$ tali che $p = p_1$ e le rette $p_n + p_1$, $p_i + p_{i+1}$ sono tangenti a Q_2 per ogni $i = 1, ..., n-1$.

Se la proprietà (P) è vera per un punto allora è vera per tutti i punti di Q_1 eccetto un insieme finito.

Dim. Si assuma vera la (P) per un punto p e siano $p = p_1, ..., p_n$ i vertici dell'n-gono relativo; si osserva innanzitutto che la (P) è soddisfatta da $p_1, ..., p_n$.

Siccome $p_1, ..., p_n$ sono tutti distinti si ha che per ogni $i = 1, .., n-1$ la corrispondenza $B^{(i)}$ non contiene la diagonale e quindi esistono al più finiti n-goni inscritti a Q_1, circoscritti a Q_2 aventi almeno un vertice punto fisso per $B^{(i)}$ per qualche $i = 1, ..., n-1$; Sia $R \subset Q_1$ l'unione dei vertici di tali n-goni.

Dalle definizioni segue subito che un punto p ha la proprietà (P) se e solo se è un punto fisso di $B^{(n)}$ e non appartiene a R. Basta quindi dimostrare che $B^{(n)}$ contiene la diagonale.

Distinguiamo tre casi:

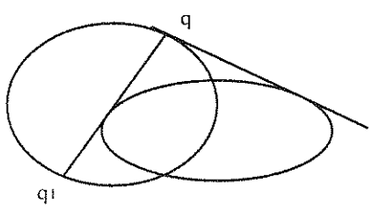
1) $n \geq 5$: la corrispondenza $B^{(n)}$ ha almeno n punti fissi e quindi deve contenere la diagonale.

2) $n = 4$: basta dimostrare che esiste un punto fisso di $B^{(4)}$ distinto da $p_1, .., p_4$. Sia $q \in Q_1 \cap Q_2$, $q_1 \in Q_1$ il secondo punto di intersezione di Q_1 con T_qQ_2, L la seconda retta per q_1 tangente a Q_2 e q_2 il secondo punto di intersezione di Q_1 con L. Lasciamo al lettore la semplice verifica che q_3 è un punto fisso di $B^{(4)}$ distinto dai punti p_i.

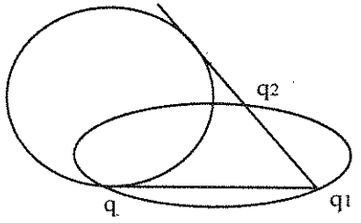
3) $n = 3$: Occorre trovare due ulteriori punti fissi di $B^{(3)}$. Distinguiamo due sottocasi:

3.1) Esiste un punto di contatto multiplo tra Q_1 e Q_2, cioè esiste $q \in Q_1 \cap Q_2$ tale che $T_qQ_1 = T_qQ_2$. Lasciamo per esercizio al lettore provare che p è un punto fisso di molteplicità ≥ 2 per ogni corrispondenza $B^{(i)}$, $i \geq 1$.

3.2) Q_1 e Q_2 si intersecano trasversalmente. Dalla teoria della polarità segue che anche le coniche duali si intersecano trasversalmente e quindi esistono esattamente quattro rette distinte $L_1, .., L_4$ che sono contemporaneamente tangenti a Q_1 e Q_2. Per ogni i sia q_i il punto di intersezione di L_i con Q_1, L_i' la seconda retta per q_i tangente a Q_2 e s_i il secondo punto di intersezione di L_i' con Q_1. I punti $s_1, ..., s_4$ sono punti fissi di $B^{(3)}$ e non possono essere tutti coincidenti. Concludiamo la dimostrazione osservando che se $p \in R$ l'n-gono di Poncelet costruito a partire da p è ancora chiuso ma può avere lati e vertici ripetuti. □

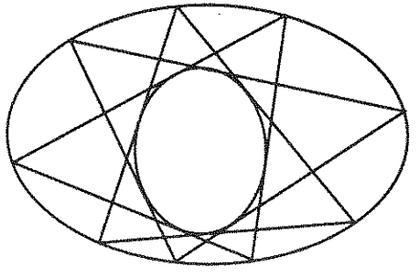


Punti fissi di $B^{(3)}$



Punti fissi di $B^{(4)}$

Triangoli di Poncelet



Per una dimostrazione (non banale) di 2.7 che utilizza i metodi classici della geometria proiettiva rimandiamo a [Sev. p. 226]. Si noti come nel caso $n = 3$ il teorema dei triangoli di Poncelet segue facilmente dal teorema di Brianchon (vedi esercizi), (cf. [E-C] libro III, p. 69.)

Esempio 2.8. (Le corrispondenze associate ad una curva piana).

Siano a, b punti distinti di $\mathbb{P}^2$, $L = a + b$ la retta passante per essi e F_a, F_b i fasci di rette passanti per a e b rispettivamente.

Per ogni curva $C \subset \mathbb{P}^2$ di grado n si può associare in modo naturale una corrispondenza $C_{a,b} \subset F_a \times F_b$ di tipo (n, n) nel modo seguente:

a) Dal punto di vista sintetico una coppia $(L_1, L_2) \in F_a \times F_b$ appartiene a $C_{a,b}$ se e solo se $C \cap L_1 \cap L_2 \neq \emptyset$.

b) Dal punto di vista algebrico, se x_0, x_1, x_2 è un sistema di coordinate omogenee tali che $a = [1, 0, 0]$, $b = [0, 1, 0]$ ed L è la retta all'infinito il punto di intersezione di una generica coppia di rette $L_1 \in F_a$, $L_2 \in F_b$ si ottiene risolvendo il sistema lineare omogeneo

$$\begin{cases} u_0x_1 - u_1x_2 = 0 \\ v_0x_0 - v_1x_2 = 0 \end{cases}$$

che se $(u_0, v_0) \neq (0, 0)$ ha come soluzione

$$(x_0, x_1, x_2) = (u_0v_1, v_0u_1, u_0v_0)$$

e quindi $C_{a,b}$ è la corrispondenza di equazione

$$G(u_0, u_1, v_0, v_1) = F(u_0v_1, v_0u_1, u_0v_0)$$

Si noti che se se $a \in C$ (risp. $b \in C$) allora $F_a \times \{L\}$ (risp. $\{L\} \times F_b$) è una componente di $C_{a,b}$ e che $C_{a,b}^{-1} = C_{b,a}$.

L'equazione affine di $C_{a,b}$ nell'aperto affine $(F_a - \{L\}) \times (F_a - \{L\}) = \{u_0v_0 \neq 0\}$ è

$$g(x, y) = G(1, x, 1, y) = F(y, x, 1)$$

e quindi le curve affini $C_{a,b} - (F_a \times \{L\} \cup \{L\} \times F_b)$ e $C - \{L\}$ sono isomorfe. È quindi possibile ricostruire C conoscendo $C_{a,b}$. Infatti se $C_{a,b}$ ha tipo (n, n) basta aggiungere un certo numero di volte la retta L alla curva di equazione affine $G(1, x, 1, y) = F(y, x, 1)$ in modo da ottenere una curva C di grado n.

ESERCIZIO 12: Nelle notazioni precedenti si provi:

1) se $a \in C$ è un punto di molteplicità m allora $F_a \times \{L\}$ è una componente di molteplicità m in $C_{a,b}$.

2) $\{L, L\}$ è un punto di molteplicità $\geq n$ di $C_{a,b}$ e vale $=$ se e solo se L non è una componente di C.

3) Se L non è una componente di C esiste una bigezione naturale fra $L \cap C$ e le componenti del cono tangente a $C_{a,b}$ nel punto (L, L).

4) Se C è una cubica liscia e $a, b \in C$ allora $C_{a,b} - (F_a \times \{L\} \cup \{L\} \times F_b)$ è una corrispondenza liscia di tipo $(2, 2)$.

3. Il Teorema di Salmon e la configurazione dei flessi di una cubica piana.

Nel seguito supporremo $C \subset \mathbb{P}^2$ una **cubica liscia** fissata su di un campo algebricamente chiuso $\mathbb{K}$ di caratteristica diversa da 2 e 3.

Se $p, q \in C$ indicheremo con $\overline{pq}$ la retta passante per p e q quando $p \neq q$ e la retta tangente a C in p quando $p = q$.

Lemma 3.1. *I flessi di una cubica liscia C sono semplici, hanno cioè molteplicità 1.*

Dim. Se fosse $\nu_p(C, T_pC) > 3$ la retta T_pC sarebbe una componente di C. □

Per ogni $p \in \mathbb{P}^2$ denotiamo con C_p la conica polare di C rispetto al punto p.

Proposizione 3.2. *Sia p un punto di C:*

a) Se $q \neq p$, $q \in C \cap C_p$, allora $\nu_q(C, C_p) = 1$.

b) La polare C_p è liscia in p e vale $\nu_p(C, C_p) = \nu_p(C, \overline{pp})$.

c) Il punto p è un flesso se e solo se C_p è singolare.

Dim. Si osserva innanzitutto che C_p è liscio in p con retta tangente uguale a $\overline{pp}$. Sia F l'equazione di C in un sistema di coordinate omogenee fissato e siano $p = [u]$, $q = [v]$, $u, v \in \mathbb{K}^3 - 0$. Il polinomio $f(t) = F(v + tu)$ è non nullo ed ha grado ≤ 2 perché $F(u) = 0$, la sua derivata rispetto a t è $f'(t) = F_u(v + tu)$. Vediamo che cosa succede al variare di q.

Se $q \notin \overline{pp}$ allora il grado di f è esattamente 2, il grado di f' è 1 e quindi la retta $\overline{pq}$ è trasversa a C_p.

Se $q \neq p$ e $q \in C \cap C_p$ allora f ha $t = 0$ come radice di molteplicità 2. Deve quindi essere $f(t) = at^2$, derivando rispetto a t si ha $2at = f'(t) = F_u(u + tv)$; questo prova che la retta tangente a C in q è trasversa a C_p e quindi il punto a).

Si fissi adesso $q \in \overline{pp}$; sono possibili due casi: se p è un flesso allora f è costante, $f' = 0$ e $\overline{pp}$ è una componente di C_p. La restante componente di C_p non può contenere il punto p e quindi in questo caso $\nu_p(C, C_p) = \nu_p(C, \overline{pp}) = 3$.

Se invece p non è un flesso allora $\overline{pp}$ non è una componente di C_p pur essendone tangente in un suo punto liscio, questo implica che C_p è liscia e prova il punto c). Per il calcolo di $\nu_p(C, C_p)$ prendiamo un sistema di coordinate omogenee x_0, x_1, x_2 tali che $p = [1, 0, 0]$ e $\overline{pp}$ è la retta di equazione $x_2 = 0$. In tali coordinate le equazioni di C e C_p sono rispettivamente

$$F = x_2x_0^2 + 2B(x_1, x_2)x_0 + C(x_1, x_2), \qquad \frac{1}{2}F_p = x_2x_0 + B(x_1, x_2)$$

che nelle coordinate affini $x = x_1/x_0$, $y = x_2/x_0$ diventano

$$f = y + 2B(x, y) + C(x, y), \qquad g = y + B(x, y)$$

La condizione che p non sia un flesso equivale a dire che y non divide il polinomio omogeneo $B(x, y)$ e quindi che la retta $y = 0$ non è una componente del cono tangente di $f - g = B(x, y) + C(x, y)$. Dal teorema IV.3.5 del capitolo IV segue dunque che f e g hanno molteplicità di intersezione 2 in p. □

L'apparentemente innocua proposizione 3.2 permette di dimostrare facilmente due interessanti corollari:

Corollario 3.3. *La cubica liscia C contiene esattamente 9 flessi distinti. Ogni retta passante per due flessi ne contiene un terzo.*

Dim. Dimostriamo solo la prima asserzione: la seconda è un caso particolare del teorema dei tangenziali di Mac-Laurin.

Definiamo $H \subset \mathbb{P}^2$ come l'insieme dei punti p tali che C_p è singolare, per Bézout basterà dimostrare che H è una cubica che interseca trasversalmente C.

In un sistema di coordinate omogenee x_0, x_1, x_2, detta $F = 0$ l'equazione di C e H_i la matrice Hessiana della conica $\dfrac{\partial F}{\partial x_i}$ allora H non è altro che la curva di equazione $\det(x_0H_0 + x_1H_1 + x_2H_2) = 0$ che ha evidentemente grado 3.

Sia ora $p \in C \cap H$ un flesso di C e prendiamo un sistema di coordinate omogenee tali che $p = [1, 0, 0]$ e C_p è la conica di equazione $x_0x_2 = 0$; la retta L di equazione $x_2 = 0$ è la retta tangente a C in p e quindi $\nu_p(C, H) = 1$ se e solo se $\nu_p(L, H) = 1$, cioè se e solo se $t = 0$ è una radice semplice di $\det(H_0 + tH_1) = 0$.

Si noti adesso che il punto $q = [0, 1, 0]$ non appartiene a C e per la formula di Eulero q non appartiene nemmeno a C_q, questo prova che se $H_1 = (a_{ij})_{i,j=0,1,2}$ allora $a_{11} \neq 0$ e tenendo presente che

$$H_0 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

si ha che $\det(H_0 + tH_1) = -a_{11}t + t^2(...)$. □

Corollario 3.4. *Dato $p \in C$ siano $\{p, p, q_1, q_2, q_3, q_4\}$ i punti di $C \cap C_p$ contati con molteplicità. Allora le quattro rette $L_i = \overline{pq_i}$ sono distinte.*

Dim. Dalla proposizione segue che i punti $q_1, ..., q_4$ sono distinti e quindi se $L_i = L_j$ avremo una retta tangente a C nei punti q_i e q_j in contraddizione con il teorema di Bézout. □

Definizione 3.5. Se $p \in C$ e F_p è il fascio delle rette passanti per p chiameremo la quaterna $\{L_1, L_2, L_3, L_4\} \subset F_p$ definita nel corollario 3.4 **quaterna di Salmon** della coppia (C, p).

È molto facile descrivere algebricamente la forma binaria di quarto grado le cui soluzioni formano la quaterna di Salmon di (C,p). Siano infatti x_0,x_1,x_2 coordinate omogenee tali che $p=[1,0,0]$ e interpretiamo la retta parametrica $t\to[t,a,b]$ di F_p come il punto di coordinate omogenee $[a,b]$.

Se $F(x_0,x_1,x_2)=A(x_1,x_2)x_0^2+2B(x_1,x_2)x_0+C(x_1,x_2)$ è l'equazione di C, la retta $[a,b]\in F_p$ appartiene alla quaterna di Salmon se e solo se $f(t)=F(t,a,b)$ è costante oppure ha una radice doppia, ne segue che le rette L_i sono in bigezione con le radici del discriminante B^2-AC.

Teorema 3.6. (Salmon, 1851) *Per ogni coppia di punti $p,q\in C$ esiste una proiettività di fasci $\phi\colon F_p\to F_q$ che trasforma l'una nell'altra le quaterne di Salmon delle coppie (C,p), (C,q).*

Dim. La dimostrazione che daremo risale a Cremona (1861); non si tratta della dimostrazione più semplice possibile ma ha il vantaggio di fornire una costruzione esplicita di ϕ.

Sia $L=\overline{pq}$, a meno di scambiare p e q possiamo supporre che L non sia tangente a C nel punto p. Sia r il terzo punto di intersezione di L con C, e s un punto tale che $\overline{ss}\cap C=\{s,s,r\}$ e denotiamo $M=\overline{ps}$. Si noti che avendo supposto $L\neq\overline{pp}$ si ha che $r\neq p$ e di conseguenza $M\neq\overline{ss}$.

Dati due punti $a,b\in C$ e detta $L=\overline{ab}$ si definisce $\hat C_{a,b}=C_{a,b}-\{\overline{ab}\}\times F_b-F_a\times\{\overline{ab}\}$ dove $C_{a,b}$ è la corrispondenza di tipo $(3,3)$ definita precedentemente. Si consideri la corrispondenza di tipo $(4,4)$, composizione delle due corrispondenze di tipo $(2,2)$

$$\hat C_{s,q}\circ\hat C_{p,s}\subset F_p\times F_q$$

È chiaro che tale corrispondenza contiene come componente la corrispondenza $\hat C_{p,q}$, si definisce quindi

$$B=\hat C_{s,q}\circ\hat C_{p,s}-\hat C_{p,q}\subset F_p\times F_q$$

In termini sintetici per $N\in F_p$ siano p,p_1,p_2 i punti di intersezione di N con C, sia poi q_i il terzo punto di intersezione di C con la retta passante per s,p_i e N_i la retta di F_q passante per q_i. Allora vale $B_N=\{N_1,N_2\}$.

Se L_i appartiene alla quaterna si Salmon di (C,p) segue dal teorema dei tangenziali di Mac-Laurin che $B_{L_i}=\{V,V\}$ dove V appartiene alla quaterna di Salmon di (C,q). Inoltre $B_M=\{L,L\}$ e quindi esistono almeno cinque rette verticali distinte tangenti a B, per il lemma 2.6 segue che esiste una corrispondenza ϕ di tipo $(1,1)$ tale che $B=2\phi$ e ϕ è esattamente la proiettività cercata. □

ESERCIZIO 13: Sia $\phi\colon F_p\to F_q$ la proiettività costruita nella dimostrazione di 3.6 e sia Q la conica proiettivamente generata da ϕ. Determinare le tangenti a Q nei punti p,q e la polare di s rispetto a Q.

Se C e D sono due cubiche liscie proiettivamente equivalenti allora per ogni $p\in C$, $q\in D$ le quaterne di Salmon delle coppie (C,p), (D,q) sono a loro volta proiettivamente equivalenti. Viceversa si ha il

Teorema 3.7. *Siano $C,D\subset\mathbb{P}^2$ cubiche liscie, $p\in C$, $q\in D$. Allora C e D sono proiettivamente equivalenti se e solo se le quaterne di Salmon dele coppie (C,p), (D,q) sono proiettivamente equivalenti.*

Dim. Si assuma le quaterne di Salmon proiettivamente equivalenti, per 3.3 e 3.6 non è restrittivo supporre p e q punti di flesso di C e D rispettivamente. Sia $\phi\colon F_p\to F_q$ la proiettività che trasforma l'una nell'altra le quaterne di Salmon di C e D, a meno di un'azione del gruppo trirettangolo sulle quaterne possiamo supporre che ϕ trasforma la retta tangente a C in p nella retta tangente a D in q.

Agendo su D con una opportuna proiettività di $\mathbb{P}^2$ possiamo senz'altro assumere che $p=q$ e che le due quaterne di Salmon coincidano, in particolare C e D avranno la stessa retta tangente L in p.

Agendo ancora su D con una proiettività che lascia fissa ogni retta del fascio F_p si può assumere che $C_p=D_p=L+M$.

Prendiamo adesso un sistema di coordinate omogenee tali che $p=[0,0,1]$, $L=\{x_0=0\}$, $M=\{x_2=0\}$, un facile conto mostra che nelle coordinate affini $x=x_1/x_0$, $y=x_2/x_0$ le equazioni di C e D sono rispettivamente

$$y^2=c(x),\qquad y^2=d(x)$$

con c e d polinomi di grado 3. Se α è una radice di c la retta $x=\alpha$ appartiene alla quaterna di Salmon di (C,p) e quindi i polinomi c e d hanno le stesse radici e differiscono per una costante moltiplicativa a^2. La trasformazione affine $y\to ay$ trasforma infine C in D.

La dimostrazione di 3.7 mostra inoltre che ogni cubica liscia è proiettivamente equivalente ad una cubica di equazione affine

$$y^2=4x^3-g_2x-g_3 \tag{3.8}$$

Una cubica di equazione 3.8 viene talvolta detta in **forma normale di Weierstrass**. Se C è in forma di Weierstrass l'invariante j associato alle quaterne di Salmon di C si calcola facilmente tramite la formula

$$j=1728\frac{g_2^3}{g_2^3-27g_3^2}$$

4. La legge di gruppo su di una cubica liscia

In questa sezione denoteremo con $\mathbb{K}$ un campo algebricamente chiuso di caratteristica arbitraria. Se C è una curva piana e $p \in \mathbb{P}^2$ denoteremo come al solito con C_p la curva polare di p rispetto a C.

Date tre curve $C, D, E \subset \mathbb{P}^2$ si può considerare l'insieme

$$Z = \{(p,q) \in \mathbb{P}^2 \times \mathbb{P}^2 \,|\, p \in C_q \cap D_q \cap E_q\}$$

e con $J(C,D,E) \subset \mathbb{P}^2$, $S(C,D,E) \subset \mathbb{P}^2$ le proiezioni di Z sul primo e secondo fattore rispettivamente. Si può dimostrare che "in generale" J e S sono curve piane, tra poco calcoleremo esattamente l'equazione di J.

Definizione 4.1.(Cremona) Le curve $J(C,D,E)$ e $S(C,D,E)$ si dicono rispettivamente **Jacobiana*** e **Steineriana** della terna C, D, E.

Se $J(C,D,E) = \mathbb{P}^2$ diremo che la Jacobiana della terna è indeterminata; similmente per la Steineriana.

Seguirà a posteriori che la Jacobiana è molto più interessante della Steineriana, nonché più facile da studiare, per questo motivo ci occuperemo in queste note solamente delle Jacobiane. Un altra curva storicamente associata alla terna C, D, E è la *Cayleyana* definita come l'inviluppo delle rette $p+q$ al variare di $(p,q) \in Z$.

Lemma 4.2. *Siano C, D, E curve piane di grado n, m, l rispettivamente. Se la Jacobiana $J(C,D,E)$ non è indeterminata allora è una curva piana di grado $n+m+l-3$.*

Dim. Siano F, G, H le equazioni di C, D, E in un sistema di coordinate omogenee fissato x_0, x_1, x_2; denotiamo con F_i, G_i, H_i le derivate parziali di F, G, H rispetto alla variabile x_i, $i = 0, 1, 2$.

La coppia $([u],[v])$ appartiene a Z se e solo se vale

$$\begin{cases} v_0F_0(u) + v_1F_1(u) + v_2F_2(u) = 0 \\ v_0G_0(u) + v_1G_1(u) + v_2G_2(u) = 0 \\ v_0H_0(u) + v_1H_1(u) + v_2H_2(u) = 0 \end{cases}$$

e quindi $J(C,D,E)$ è l'insieme dei punti $p = [u]$ tali che il precedente sistema lineare nelle incognite v_i possiede una soluzione non banale. È quindi evidente che l'equazione di $J(C,D,E)$ è

$$\det \begin{pmatrix} F_0 & G_0 & H_0 \\ F_1 & G_1 & H_1 \\ F_2 & G_2 & H_2 \end{pmatrix} = 0$$

* Non bisogna assolutamente confondere la curva Jacobiana di una terna con la varietà Jacobiana di una curva, [G-H, p.333]

□

È chiaro che se C, D, E hanno lo stesso grado allora $J(C,D,E)$ dipende solo dal sistema lineare generato dalle tre curve.

ESERCIZIO 14: Nelle notazioni di 4.2 se la caratteristica di $\mathbb{K}$ divide n, m, l allora la Jacobiana è indeterminata.

ESERCIZIO 15: (*) (La Hessiana)

(caratteristica 0). Sia C una curva piana irriducibile di grado $n \geq 2$ e di equazione $F(x_0, x_1, x_2) = 0$. La **Hessiana** di C è la curva di grado $3(n-2)$ e di equazione

$$\det \begin{pmatrix} F_{00} & F_{01} & F_{02} \\ F_{10} & F_{11} & F_{12} \\ F_{20} & F_{21} & F_{22} \end{pmatrix} = 0$$

Provare che H non è indeterminata e non contiene C come componente. Se $p \in C$ è un punto liscio e L è la retta tangente a C in p si provi che $\nu_p(C,L) = \nu_p(C,H) + 2$ e si deduca che una curva liscia di grado n possiede $3n(n-2)$ flessi contati con molteplicità. (Sugg. Mostrare che $\nu_p(C,L) > 2$ se e solo se $p \in H$ e poi usare IV.3.9. Vedi anche [Wa]).

Lemma 4.3. *Sia C curva piana, $p \in C$ un punto liscio, a, m interi positivi. Allora l'insieme delle curve D di grado m tali che $\nu_p(C,D) \geq a$ è un sistema lineare di codimensione $\leq a$ nello spazio $|\mathcal{O}(m)|$.*

Dim. basta mostrare che se $V \subset |\mathcal{O}(m)|$ è un sistema lineare e a è il minimo valore di $\nu_p(C,D)$ al variare di $D \in V$ allora $W = \{D \in V \,|\, \nu_p(C,D) > a\}$ è un iperpiano in V.

Siano x, y coordinate affini tali che $p = (0,0)$ e la retta $y = 0$ è tangente a C in p. Sia r la dimensione di V, f l'equazione affine di C e $g_0, ..., g_r$ le equazioni affini di un sistema di generatori di V tali che $\nu_p(f, g_0) = a$.

Esistono costanti $\alpha_1, ..., \alpha_r \in \mathbb{K}$ tali che $\nu_p(f, g_i - \alpha_i g_0) > a$: infatti per ogni $i = 0, ..., r$ esiste un polinomio h_i tale che $g_i = \beta_i x^a + o(a)$ con $\beta_0 \neq 0$ e basta prendere $\alpha_i = \beta_i \beta_0^{-1}$. □

Vogliamo adesso studiare la molteplicità di intersezione $\nu_p(C,J)$, $J = J(C,D,E)$ nelle seguenti ipotesi:

i) C curva di grado n e $p \in C$ punto liscio.

ii) D, E hanno lo stesso grado m non divisibile per la caratteristica di $\mathbb{K}$ e generano un fascio V.

iii) $\nu_p(C,D) < \infty$.

Per il lemma 4.3 possiamo assumere senza perdita di generalità che $d = \nu_p(C,D) < \nu_p(C,E) = e \leq \infty$ ed E è l'unica curva di V ad avere molteplicità maggiore di d.

Definizione 4.4. Diremo che $p \in C$ è un **punto di ramificazione** per il fascio V se $e \geq d+2$.

Lemma 4.5. *Nelle notazioni precedenti vale $\nu_p(C,J) \geq d+e-1$ e vale $=$ se e solo se $e=\infty$ oppure se $e<\infty$ e la caratteristica di $\mathbb{K}$ non divide $e-d$. In particolare $\nu_p(C,J) \geq 2d+1$ se e solo se p è un punto di ramificazione per il fascio V.*

Dim. Siano F,G,H le equazioni di C,D,E in un sistema di coordinate omogenee x_0,x_1,x_2 tali che $p=[1,0,0]$ e $x_2=0$ è la retta tangente a C in p. Per la formula di Eulero vale

$$x_0F_0-(n-m)F = mF-x_1F_1-x_2F_2$$

$$x_0G_0 = mG-x_1G_1-x_2G_2, \qquad x_0H_0 = mH-x_1H_1-x_2H_2$$

e quindi vale

$$mx_0\begin{vmatrix} F_0 & G_0 & H_0 \\ F_1 & G_1 & H_1 \\ F_2 & G_2 & H_2 \end{vmatrix} \equiv \begin{vmatrix} F & G & H \\ F_1 & G_1 & H_1 \\ F_2 & G_2 & H_2 \end{vmatrix} \qquad mod(F)$$

Passando alle coordinate affini $x=\dfrac{x_1}{x_0}$, $y=\dfrac{x_2}{x_0}$ si ha quindi che $\nu_p(C,J)=\nu_p(f,\phi)$ ove f,g,h sono le equazioni affini di C,D,E e

$$\phi = \begin{vmatrix} f & g & h \\ f_x & g_x & h_x \\ f_y & g_y & h_y \end{vmatrix}$$

Aggiungendo a g ed h elementi dell'ideale principale $(f)\subset\mathbb{K}[x,y]$ otteniamo un nuovo ϕ che è congruo al precedente modulo f. Tenendo presente che $f=y+o(1)$, non è restrittivo supporre $g=x^d+o(d)$ e, se $e<\infty$, $h=x^e+o(e)$.

Un semplice conto mostra che $\phi=(e-d)x^{d+e-1}+o(d+e-1)$ che prova il teorema nel caso $e<\infty$.

Se invece $e=\infty$ allora f e h hanno un fattore comune f_1 tale che $f_1(0,0)=0$ e lo sviluppo del determinante mostra che $\phi\in(f_1)$ e quindi $\nu_p(f,\phi)=\infty$. □

Il lemma 4.5 ci permette di dimostrare il seguente importante risultato

Teorema 4.6. *Sia C una curva liscia di grado $n\geq 3$ e siano D,E curve di grado m che non contengono C come componente.*

Siano $p_1,\dots,p_{nm}$ i punti di intersezione di C e D contati con molteplicità. Se $E\cap C$ contiene $nm-1$ punti di $C\cap D$ allora:

i) $D=E$ oppure.

ii) $D\neq E$, $m\geq n$ ed esiste una curva del fascio generato da D,E che contiene C come componente.

In entrambi i casi D ed E hanno la stessa intersezione con C.

Dim. Assumiamo che $D\neq E$ e proviamo che vale l'opzione ii). Non è restrittivo supporre che la caratteristica di $\mathbb{K}$ non divida m, altrimenti basta considerare al posto di D,E le curve $D+L,E+L$ dove L è una retta generica.

Proviamo per prima cosa che $\nu_p(C,D)=\nu_p(C,E)$ per ogni punto $p\in C$. Se così non fosse, detto $\{p_1,\dots,p_r\}=C\cap D$ si avrebbe a meno di permutazioni degli indici

$$\begin{cases} \nu_{p_i}(C,E)\geq\nu_{p_i}(C,D) & \text{per } i=1,\dots,r-1. \\ \nu_{p_r}(C,E)=\nu_{p_r}(C,D)-1 & . \end{cases}$$

Per il teorema di Bézout e per il lemma 4.3 si ha che C non contiene punti di ramificazione per il fascio V generato da D,E ed in particolare la Jacobiana J della terna C,D,E non è indeterminata e non contiene C come componente.

Ora il grado di J è $2m+(n-3)\geq 2m$ e per Bézout

$$\sum_p \nu_p(C,J)\geq 2nm > \sum_p 2\min(\nu_p(C,D),\nu_p(C,E))$$

Quindi esiste un punto $p\in C$ tale che $\nu_p(C,J)>2\min(\nu_p(C,D),\nu_p(C,E))$ e per 4.5 p è un punto di ramificazione per V.

Abbiamo dunque stabilito che $\nu_p(C,D)=\nu_p(C,E)$ per ogni $p\in C$; preso $q\in C-D$ allora l'unica curva di V che contiene q deve contenere C come componente. □

Una delle applicazioni più piacevoli del teorema 4.6 è senza dubbio la verifica della struttura di gruppo sulle cubiche liscie.

Sia $C\subset\mathbb{P}^2$ una cubica liscia e sia $o\in C$ un punto fissato. Per semplicità di notazione se $a\in C$ denotiamo con $\hat{a}\in C$ il terzo punto di intersezione di C con la retta $\overline{oa}$; si osservi che $\hat{o}$ coincide con il tangenziale di o.

Definiamo una applicazione simmetrica "di somma" $C\times C\xrightarrow{+}C$ nel modo seguente: Presi due punti $a,b\in C$ sia r il terzo punto di intersezione di C con la retta $\overline{ab}$, si definisce $a+b=\hat{r}$. L'applicazione è simmetrica nel senso che $a+b=b+a$.

Teorema 4.7. *L'applicazione $+$ precedentemente definita induce su C una struttura di gruppo abeliano con elemento neutro o.*

Dim. Verifichiamo che gli assiomi di gruppo sono soddisfatti.

1) Elemento neutro. Per definizione si ha $o+a=a+o=\hat{\hat{a}}=a$.

2) Esistenza dell'inverso. Per ogni $a\in C$ definiamo $-a$ come il terzo punto di intersezione di C con la retta $\overline{a\hat{o}}$. Allora $(-a)+a=a+(-a)=\hat{\hat{o}}=o$.

3) Associatività. Siano $a,b,c\in C$, definiamo $d=a+b$, $e=b+c$, $f=d+c$, $g=a+e$; bisogna dimostrare che $f=g$ o equivalentemente che $\hat{f}=\hat{g}$.

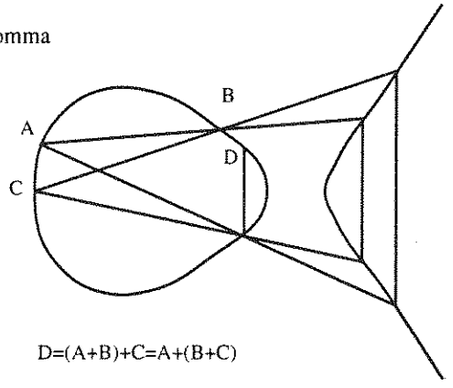
Consideriamo l'esagono inscritto a C di vertici a,b,c,d,o,e, i suoi lati sono le rette $L_1=\overline{ab}$, $L_2=\overline{bc}$, $L_3=\overline{cd}$, $L_4=\overline{do}$, $L_5=\overline{oe}$, $L_6=\overline{ea}$ e analizziamo le intersezioni di C con le due cubiche formate rispettivamente dai lati pari e dispari dell'esagono.

$$C\cap(L_1+L_3+L_5)=\{a,b,\hat{d},c,d,\hat{f},o,e,\hat{e}\}$$

$$C \cap (L_2 + L_4 + L_6) = \{b, c, \hat{e}, d, o, \hat{d}, e, a, \hat{g}\}$$

Le due intersezioni hanno otto dei nove punti in comune e per 4.6 devono coincidere e quindi $\hat{f} = \hat{g}$. □

Associatività della somma



ESERCIZIO 16: La somma di tre punti allineati è sempre uguale a $\hat{o}$.

In realtà continua ad essere vero il fatto che la somma dei $3m$ punti di intersezione di C con una qualsiasi curva D di grado m è indipendente da D. Per dimostrare questo fatto abbiamo però bisogno di dare una diversa caratterizzazione della struttura di gruppo su C.

Più in generale sia $C \subset \mathbb{P}^2$ una curva liscia di grado n, definiamo il **gruppo dei divisori** su C come il gruppo $Div(C)$ di tutte le applicazioni $\phi: C \to \mathbb{Z}$ che sono nulle quasi ovunque, cioè tali che $\phi(p) \neq 0$ per al più un numero finito di punti $p \in C$. È spesso utile rappresentare un divisore ϕ tramite la combinazione lineare formale finita $\sum_p \phi(p)(p)$; è chiaro che i divisori (p) al variare di $p \in C$ formano una base canonica dello $\mathbb{Z}$-modulo libero $Div(C)$.

Un divisore $\sum n_i(p_i)$ si dice **effettivo** se $n_i \geq 0$ per ogni i; denotiamo con 0 il divisore nullo, elemento neutro di $Div(C)$.

Se $D \subset \mathbb{P}^2$ è una curva che non contiene C si definisce un divisore effettivo $D_{|C} \in Div(C)$ ponendo

$$D_{|C} = \sum \nu_p(C, D)(p).$$

I divisori su C della forma $D_{|C}$ sono talvolta detti **divisori aggiunti**.

Notiamo incidentalmente che nella dimostrazione di 4.6 si è provato che se $D_{|C} = E_{|C}$ allora o $E = D$ oppure esiste una curva nel fascio generato da D, E che contiene C come componente. Il **grado** di un divisore $\phi = \sum n_i(p_i)$ è per definizione la somma $\deg(\phi) = \sum n_i \in \mathbb{Z}$. Per Bézout $\deg(D_{|C}) = \deg(C)\deg(D)$.

I divisori di grado 0 formano un sottogruppo $Div^0(C) \subset Div(C)$.

Definizione 4.8. Due divisori $\phi, \psi \in Div(C)$ si dicono **linearmente equivalenti** se esistono due curve piane D, E dello stesso grado che non contengono C come componente tali che $\phi + D_{|C} = \psi + E_{|C}$. Lasciamo per esercizio al lettore la facile verifica che l'equivalenza lineare è una relazione di equivalenza che denoteremo con il simbolo $\sim$.

È inoltre immediato osservare che divisori linearmente equivalenti hanno lo stesso grado e che la relazione $\sim$ commuta con l'operazione di somma di divisori.

Teorema 4.9. *Sia $C \subset \mathbb{P}^2$ curva liscia di grado $n \geq 3$, $p, q \in C$. Allora vale $(p) \sim (q)$ se e solo se $p = q$.*

Dim. Siano D, E curve di grado m tali che $(p) + D_{|C} = (q) + E_{|C}$, allora le intersezioni di D, E con C hanno almeno $nm - 1$ punti in comune e per il teorema 4.6 si ha $D_{|C} = E_{|C}$ da cui $(p) = (q)$. □

Definizione 4.10. Il **gruppo di Picard** $Pic(C)$ è il quoziente di $Div(C)$ per la relazione di equivalenza lineare. La **varietà di Picard** $Pic^0(C) \subset Pic(C)$ è il sottogruppo delle classi di equivalenza lineare di divisori di grado 0.

ESERCIZIO 17: Se C ha grado ≤ 2 allora $Pic^0(C) = 0$ e la funzione grado induce un isomorfismo tra $Pic(C)$ e $\mathbb{Z}$.

Teorema 4.11. *Sia C curva liscia di grado $n \geq 3$ e $o \in C$ un punto fissato. La mappa $\mu: C \to Pic^0(C)$, $\mu(p) = (p) - (o)$, è iniettiva. Se $n = 3$ allora μ è un isomorfismo di gruppi (rispetto alla struttura di gruppo su C precedentemente definita).*

Dim. L'iniettività di μ non è altro che una riformulazione del teorema 4.9. Se C è una cubica occorre provare che:

i) $\mu(a + b) = \mu(a) + \mu(b)$.

ii) L'immagine di μ contiene un insieme di generatori di $Pic^0(C)$.

Per i) basta osservare che se $c = a + b$ allora esistono due rette L, N tali che $L_{|C} = (a) + (b) + (\hat{c})$, $N_{|C} = (o) + (c) + (\hat{c})$ e quindi

$$(a) - (o) + (b) - (o) + N_{|C} = (c) - (o) + L_{|C} \quad \Rightarrow \quad (a) + (b) - 2(o) \sim (c) - (o)$$

Per ii) basta osservare che ogni divisore di grado 0 si può scrivere come combinazione lineare a coefficienti interi di divisori del tipo $(p) - (o)$, $p \in C$. □

5. Il teorema del resto

Iniziamo questa sezione dimostrando una versione debole (ma non troppo) del teorema $AF + BG$ di Max Noether. La versione completa sarà proposta come esercizio nel capitolo VII.

Teorema 5.1.(Noether, 1872) *Siano $C, D, E \subset \mathbb{P}^2$ curve piane di grado $n, m, l > 0$ ed equazione F, G, H rispettivamente tali che C e D siano senza componenti comuni e D non contenga punti singolari di C.*
Allora vale $\nu_p(C,E) \geq \nu_p(C,D)$ per ogni $p \in C$ se e solo se $H = AF + BG$ per opportuni polinomi omogenei A, B.

Dim. Se vale $H = AF + BG$ è chiaro che vale la relazione sulle molteplicità di intersezione. Viceversa si assuma che $\nu_p(C,E) \geq \nu_p(C,D)$ per ogni $p \in C$; si noti che necessariamente C è una curva ridotta.
Al fine di alleggerire la dimostrazione identificheremo liberamente una curva piana con la sua equazione, in particolare se P, Q sono polinomi omogenei e $q \in \mathbb{P}^2$ denoteremo con $\nu_p(P,Q)$ la molteplicità di intersezione in q delle curve di equazione P e Q.
Daremo due distinte dimostrazioni del teorema; la prima, di natura più algebrica, è presa da [Wa] mentre la seconda, più geometrica, è presa da [E-C].
Prima dimostrazione: Proviamo dapprima il teorema in alcuni casi particolari.
a) Esiste un punto $q \notin C$ tale che $m_q(E) > l - n$ e $D = \sum a_i L_i$ con L_i retta passante per q e trasversale a C. In questo caso G divide H, cioè per ogni i la retta L_i è una componente di E di molteplicità almeno a_i; sia infatti $E = b_1 L_1 + E_1$ con $b_1 < a_1$ e proviamo che L_1 è una componente di E_1. Siano $p_1, ..., p_n$ i punti di intersezione di C con L_1, vale $\nu_{p_i}(C,E) \geq \nu_{p_i}(C,D) = a_1$ e quindi, essendo $b_1 < a_1$, i punti $p_1, ..., p_n$ appartengono anche alla curva E_1. Inoltre $m_q(E_1) > l - n - b_1$ e quindi $\nu_q(E_1, L_1) + \sum_i \nu_{p_i}(L_1, E_1) > l - b_1 = \deg(b_1)$ e per Bézout L_1 è una componente di E_1.
b) La curva D è come al punto a) e la curva E qualsiasi. Fissiamo un sistema di coordinate omogenee tali che $q = [0,0,1]$; dato che $q \notin C$ il polinomio F è, a meno di scalari, monico rispetto alla variabile x_2 e quindi esistono unici Q, T tali che $H = QF + T$ con T di grado $< n$ rispetto alla variabile x_2, e quindi $m_q(T) > l - n$. Possiamo tranquillamente scambiare H con T e ricondurci al punto a).
In generale siano $p_1, .., p_r$ i punti di intersezione di C e D, siccome i punti p_i sono lisci per C, per ogni punto p_i passano finite rette contenenti un p_j, $i \neq j$ e tangenti a C. Sia $q \in \mathbb{P}^2$ un punto non appartenente all'unione di C, D e delle rette sopra descritte. Fissato un sistema di coordinate omogenee tali che $q = [0,0,1]$ sia $R(x_0, x_1) = QF + UG$ il risultante di F e G rispetto alla variabile x_2, data la scelta di q, la curva R soddisfa le stesse condizioni della curva G nel precedente caso particolare b), in particolare R e F non hanno fattori comuni.

Dato che $\nu_p(F, UH) \geq \nu_p(F, UG) = \nu_p(F, R)$ per ogni $p \in C$ ci siamo ricondotti al punto b) e quindi $UH = AF + BR = (A + BQ)F + UBG$; notiamo infine che F e U non hanno fattori comuni e quindi U divide $A + BQ$ ed il teorema è dimostrato.
Seconda dimostrazione. Dividiamo la dimostrazione in due passi, nel primo proviamo il teorema quando $l \geq nm$ e nel secondo proviamo che, se il teorema vale per i gradi (n, m, l) allora vale anche per i gradi $(n, m, l-1)$.
Sia dunque $l \geq nm$ e sia V il sistema lineare delle curve E di grado l tali $\nu_p(C,E) \geq \nu_p(C,D)$ per ogni $p \in C$. Proviamo che la codimensione di V è esattamente nm e quindi che la dimensione di V è $\frac{1}{2}l(l+3) - nm$. Siano $p_1, ..., p_{nm}$ i punti di intersezione di C e D contati con molteplicità e per ogni i sia L_i una retta generica passante per p_i. Detta L una retta tale che $L \cap C \cap D = \emptyset$ si ha che per ogni $j < nm$ la curva di grado l $L_1 + ... + L_j + (l-j)L$ passa per $p_1, ..., p_j$ ma non per i rimanenti, questo prova che le nm condizioni di passaggio per i punti p_i inducono condizioni lineari indipendenti sulle curve di grado $l \geq nm$.
Sia ora $V' \subset V$ il sistema lineare delle curve $H = AF + BG$ al variare di A, B nello spazio dei polinomi di grado $l - n$ e $l - m$ rispettivamente. Chiaramente $V' = \mathbb{P}(W_F + W_G)$ dove W_F (resp. W_G) è lo spazio vettoriale dei polinomi di grado l divisibili per F (resp G).
Vale quindi $(W_F \cap W_G) = W_{FG}$ e

$$\dim W_F = \binom{l-n+2}{2}, \quad \dim W_G = \binom{l-m+2}{2}, \quad \dim W_{FG} = \binom{l-n-m+2}{2}$$

Una semplice addizione che omettiamo mostra che V' e V hanno la stessa dimensione e questo prova il primo passo.
Proviamo adesso il teorema assumendolo vero per la terna di gradi $n, m, l+1$. Sia L l'equazione di una retta non passante per i punti di intersezione di C, D trasversa a C, per induzione esistono $\tilde{A}, \tilde{B}$ tali che $HL = \tilde{A}F + \tilde{B}G$. Dato che $\nu_p(F, \tilde{B}) \geq \nu_p(F, L)$ per ogni $p \in C$, se il grado di $\tilde{B}$ è minore di n allora L divide $\tilde{B}$ mentre se il grado di $\tilde{B}$ è maggiore o uguale a n per il primo passo si ha $\tilde{B} = UF + BL$. Sostituendo nell'espressione di HL e tenendo presente che L non divide F si arriva alla conclusione cercata. □

Teorema 5.2.(Teorema del resto di Brill e Noether, 1873) *Siano ϕ, ψ, η divisori effettivi su una curva liscia C con ϕ e ψ linearmente equivalenti. Allora $\phi + \eta$ è aggiunto se e solo se $\psi + \eta$ è aggiunto*

Dim. L'enunciato è simmetrico in ϕ e ψ, assumiamo che $\phi + \eta$ sia aggiunto. Per definizione di equivalenza lineare esistono divisori aggiunti ξ, ζ tali che

$$\phi + \eta + \xi = \psi + \eta + \zeta$$

e quindi $\psi+\eta=\phi+\eta+\xi-\zeta$ è la differenza di due divisori aggiunti, diciamo $\psi+\eta=E_{|C}-D_{|C}$.
In termini di intersezione $\nu_p(C,E)\geq\nu_p(C,D)$ e per il teorema di Noether segue che $\psi+\eta$ è aggiunto. □

Corollario 5.3. *Siano ϕ,ψ divisori effettivi linearmente equivalenti. ψ è aggiunto se e solo se ϕ è aggiunto.*

Dim. basta mettere $\eta=0$ in 5.2. □

Nel paragrafo 4 abbiamo introdotto il gruppo di Picard di una curva piana liscia e definito una applicazione $\mu: C\to Pic^0(C)$.
Più in generale per ogni $s>0$ possiamo definire una applicazione

$$\mu_s: C^s\to Pic^0(C),\qquad \mu_s(p_1,...,p_s)=(p_1)+...+(p_s)-s(o)$$

Definizione 5.4. (Weierstrass) Si dice **genere** della curva C il più piccolo intero positivo g tale che $\mu_g: C^g\to Pic^0(C)$ è surgettiva. *

Naturalmente la definizione precedente ha senso solamente dopo aver provato che μ_s è surgettiva per $s>>0$. Abbiamo già osservato che se C è una retta o una conica liscia allora $Pic^0(C)=0$ e quindi il genere di C è uguale a 0. Per le curve piane di grado ≥ 3 vale il seguente

Teorema 5.5. *Il genere di una curva liscia di grado $n\geq 3$ è uguale a*

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

Dim. la dimostrazione è divisa in due passi, nel primo si prova che μ_g è surgettiva, nel secondo che μ_{g-1} non è surgettiva.
Sia C curva liscia fissata di grado $n\geq 3$. Per ogni $m>0$ fissato sia $P_m\subset Div(C)$ l'insieme dei divisori aggiunti di grado nm. Esiste una struttura naturale di spazio proiettivo su P_m. Infatti detto $S_d\subset\mathbb{K}[x_0,x_1,x_2]$ il sottospazio vettoriale dei polinomi omogenei di grado d e $F\in S_n$ l'equazione di C esiste una bigezione naturale $\alpha:\mathbb{P}(S_m/FS_{m-n})\to P_m$. Per ogni $G\in S_m-FS_{m-n}$ si pone $\alpha([G])=D_{|C}$ dove D

* È sicuramente più nota al grande pubblico la definizione di Riemann del genere g di una curva piana liscia complessa come $g=$"numero di manici"$=1-\frac{e}{2}$ con e caratteristica di Eulero. Le due definizioni sono apparentemente indipendenti (non a caso Riemann chiamava il suo invariante *Klassenzahl* e Weierstrass *Rang*) e rimandiamo all'esercizio 22 per una dimostrazione della loro equivalenza. Il nome *genere* è stato introdotto, probabilmente seguendo Linneo, da Clebsch

è la curva di equazione G. In base al teorema 5.1 l'applicazione α è ben definita e bigettiva.
Se $m\geq n$ la dimensione di P_n si calcola facilmente ed è uguale a

$$\frac{1}{2}m(m+3)-\frac{1}{2}(m-n)(m-n+3)-1=mn-g$$

Da questo semplice conto di dimensioni si ha che per ogni $m\geq n$:
1) Dato comunque un divisore effettivo ϕ su C di grado $nm-g$ esiste una curva D di grado m tale che $D_{|C}\geq\phi$.
2) Dato un punto $o\in C$ esistono $nm-g$ punti p_i su C tali che ogni curva D di grado m che contiene $o,p_1,...,p_{nm-g}$ contiene anche C come componente. Basta infatti prendere p_i che inducono condizioni indipendenti sull'iperpiano di P_m formato dai divisori che contengono o.
Quello che dobbiamo dimostrare è che ogni divisore di grado 0 è linearmente equivalente ad un divisore del tipo $\phi-g(o)$ con ϕ divisore effettivo di grado g. Sia $\psi=\psi_0-\psi_\infty$ con ψ_0, ψ_∞ divisori effettivi dello stesso grado. Esiste allora una curva D di grado m sufficientemente elevato tale che $D_{|C}=\psi_0+g(o)+\eta$ con η divisore effettivo, per il punto 1) esiste una curva E di grado m tale che $E_{|C}=\eta+\psi_\infty+\phi$ con ϕ divisore effettivo di grado g. Dato che $\psi+E_{|C}=\phi-g(o)+D_{|C}$ si ha che $\psi\sim\phi-g(o)$.
Proviamo adesso che μ_{g-1} non è surgettiva. Sia $m\geq n$ un intero fissato e siano $p_1,...,p_{nm-g}\in C$ punti distinti come al punto 2), esiste allora un divisore effettivo ϕ di grado g tale che $\phi+\sum(p_i)\in P_m$. Proviamo che $\phi-g(o)$ non appartiene all'immagine di μ_{g-1}; infatti se cosi non fosse avremo un divisore effettivo ψ di grado $g-1$ tale che $\phi-g(o)\sim\psi-(g-1)(o)$ da cui $\psi+(o)+\sum(p_i)\sim\phi+\sum(p_i)=D_{|C}$ e per 5.3 esisterebbe una curva E tale che $E_{|C}=\psi+(o)+\sum(p_i)$ in aperta e dichiarata contraddizione con la scelta dei punti p_i. □

ESERCIZIO 18: Provare che il teorema del resto implica il teorema di Noether nel caso di C curva liscia.

ESERCIZIO 19: I tangenziali dei $3m$ punti di intersezione di una curva di grado m con una cubica liscia C appartengono ad una curva di grado m.

ESERCIZIO 20: (Caratteristica 0). Sia C curva irriducibile di grado $n\geq 2$, $p\in\mathbb{P}^2$, $q\in C\cap C_p$ punto liscio di C distinto da q. Sia L la retta tangente a C in q, provare che $\nu_q(C,C_p)=\nu_q(L,C_p)=\nu_q(L,C)-1$.

ESERCIZIO 21: (Caratteristica 0). Sia C curva liscia di grado n, $p\notin C$ e $L_1,...,L_r$ le rette passanti per p tangenti a C. Sia a_i la molteplicità di L_i come componente della curva risultante di C,C_p di centro p. Per la formula della classe $\sum a_i=n(n-1)$.

Provare che L_i interseca C in esattamente $n-a_i$ punti distinti e che quindi $L_1+\ldots+L_r$ interseca C in esattamente $n(r-n+1)$ punti distinti.

ESERCIZIO 22: (In questo esercizio sono richieste nozioni di topologia algebrica e di teoria dei rivestimenti).

Se $\mathbb{K}=\mathbb{C}$ usare l'esercizio precedente per dimostrare che la caratteristica di Eulero-Poincaré topologica e di una curva liscia C di grado n è uguale a $3n-n^2=2-2g(C)$.

(Sugg. Se $A\subset C$ è un insieme finito di a punti si ha $e(C-A)=e(C)-a$, si consideri la restrizione a C della proiezione di centro $p\notin C$ su di una retta $\mathbb{P}^1\subset\mathbb{P}^2-\{p\}$.)

6. Esercizi complementari

ESERCIZIO 23: (*) (Variante al teorema di Steiner, 1832)

Data una conica liscia C, un triangolo $T=\{p_1,p_2,p_3\}$ si dice autoconiugato rispetto a C se $C_{p_i}=p_j+p_k$, $\{i,j,k\}=\{1,2,3\}$. Dati sei punti distinti $p_1,p_2,p_3,q_1,q_2,q_3\in\mathbb{P}^2$, tre a tre non allineati, se ne faccia due triangoli $P=\{p_1,p_2,p_3\}$, $Q=\{q_1,q_2,q_3\}$.

Provare che le seguenti condizioni sono equivalenti:

i) P e Q sono autoconiugati rispetto ad una conica liscia.

ii) P e Q sono inscritti in una conica liscia.

iii) P e Q sono circoscritti ad una conica liscia.

Nota: L'equivalenza fra ii) e iii) è conosciuta con il nome di teorema di Brianchon (1817).

(Sugg. Per dualità basta dimostrare che i) è equivalente a ii).

Se vale i), si consideri le intersezioni dei fasci di rette di centro p_1,q_1 con la retta p_2+p_3 e si provi l'uguaglianza dei birapporti delle quaterne ordinate $(p_1+p_2,p_1+p_3,p_1+q_2,p_1+q_3)$, $(p_1+p_3,p_1+p_2,p_1+q_3,p_1+q_2)$ e $(q_1+p_2,q_1+q_3,q_1+q_2,q_1+q_3)$.

Viceversa se vale ii) si provi che esiste una conica liscia C tale che $C_{p_i}=p_j+p_k$ e $C_{q_1}=q_2+q_3$. Si provi quindi che $C_{q_2}=q_1+q_3$ usando l'unicità della conica passante per p_1,p_2,p_3,q_1,q_2.)

ESERCIZIO 24: Sia $S^1\subset\mathbb{C}$ l'insieme di vettori di norma 1. Dati quattro punti di S^1 possiamo definire due tipi di birapporto:

1) Il birapporto complesso - pensando S^1 come un sottoinsieme di $\mathbb{P}^1_{\mathbb{C}}$.

2) Il birapporto di Steiner - pensando S^1 come una conica liscia di $\mathbb{P}^2_{\mathbb{R}}$.

Provare che i due birapporti coincidono.

ESERCIZIO 25: Caratteristica $\neq 2$. Sia $C\subset\mathbb{P}^2$ una conica liscia e $p\notin C$. Si consideri l'applicazione $\phi_p\colon C\to C$ che manda il punto q nel rimanente punto di intersezione di C con la retta $\overline{pq}$. Provare che ϕ è una proiettività. (Sugg. Considerare coordinate omogenee tali che $p=[1,0,0]$ e la polare C_p è la retta $x_0=0$).

ESERCIZIO 26: (Punto di Frégier, 1816)

Sia $C\subset\mathbb{R}^2$ un'ellisse e $p\in C$ un punto fissato. Provare che tutte le corde di C che vedono un angolo retto in p passano per uno stesso punto q sulla normale a C in p e interno alla conica. (Sugg. Sia q il punto di intersezione di due tali corde e sia ϕ_p l'involuzione definita all'esercizio precedente. Provare che ϕ_q induce sul fascio delle rette per p l'involuzione degli angoli retti).

ESERCIZIO 27: (Problema di Staudt, 1831)

Date due coniche liscie distinte determinare il luogo dei punti p tali che le quattro rette del fascio per p, tangenti alle coniche date, formano una quaterna armonica.

ESERCIZIO 28: Sia C una corrispondenza simmetrica di tipo (a,a). Allora $C^2=C\circ C$ contiene Δ con molteplicità $\geq a$.

ESERCIZIO 29: Sia $C(r,d)=\{(x,y)\in\mathbb{R}^2|(x-d)^2+y^2=r^2\}$. Descrivere le coppie (d,r) per le quali esiste un triangolo inscritto a $C(1,0)$ e circoscritto a $C(r,d)$.

ESERCIZIO 30: (Dimostrazione di Dandelin (1826) del teorema di Pascal)

Premettiamo alcune semplici osservazioni:

a) dato un piano $\Pi\subset\mathbb{P}^3$ e tre punti distinti $p,q,r\in\mathbb{P}^3-\Pi$, i punti di intersezione di Π con i lati del triangolo di vertici p,q,r sono allineati.

b) Siano $\mathbb{P}^1,\mathbb{P}^1$ e $\mathbb{P}^3$ spazi proiettivi dotati dei sistemi di coordinate omogenee x_0,x_1, y_0,y_1, $u_{00},u_{01},u_{10},u_{11}$ e si consideri la mappa di Segre

$$s\colon\mathbb{P}^1\times\mathbb{P}^1\to\mathbb{P}^3,\qquad s([x_0,x_1],[y_0,y_1])=[x_0y_0,x_0y_1,x_1y_0,x_1y_1]$$

Si osserva che s induce una bigezione tra $\mathbb{P}^1\times\mathbb{P}^1$ e la quadrica Q di equazione $u_{00}u_{11}=u_{10}u_{01}$ e tra la diagonale Δ e la conica liscia C intersezione di Q con il piano $H=\{u_{10}-u_{01}=0\}$.

c) Sostituendo x_iy_j al posto di u_{ij} nell'equazione di un piano di $\mathbb{P}^3$ si ottiene l'equazione di una corrispondenza di tipo $(1,1)$ su $\mathbb{P}^1\times\mathbb{P}^1$ ed esiste una bigezione naturale tra $(\mathbb{P}^3)^\vee$ e lo spazio di tutte le corrispondenze di tipo $(1,1)$.

Siano $p_1,\ldots,p_6$ punti distinti sulla conica C e poniamo $s^{-1}(p_i)=(q_i,q_i)$, $q_1,\ldots,q_6\in\mathbb{P}^1$, $a=s(q_1,q_4)$, $b=s(q_3,q_6)$, $c=s(q_5,q_2)$. Provare che

$$\begin{cases}a+b\cap H=(p_3+p_4)\cap(p_6+p_1)\\ a+c\cap H=(p_4+p_5)\cap(p_1+p_2)\\ b+c\cap H=(p_2+p_3)\cap(p_5+p_6)\end{cases}$$

(Sugg. Ragionare in termini di corrispondenze per provare che c appartiene al piano $a+p_1+p_2$ e che a appartiene al piano $c+p_4+p_5$.)

ESERCIZIO 31: (Regola di Zeuthen, 1873)

Sia p un punto di intersezione di due curve C, D senza componenti comuni e siano a, b punti di $\mathbb{P}^2$ in posizione generica. Sia L la retta $a+p$, provare che $\nu_p(C,D)$ è uguale alla molteplicità di L come punto fisso della corrispondenza $D_{b,a} \circ C_{a,b}$ (notazioni come in 2.8).

Se C e D hanno rispettivamente gradi n e m provare che la retta $a+b$ è un punto fisso di molteplicità nm e si deduca il teorema di Bézout dal principio di Chasles.

ESERCIZIO 32: Trovare l'errore nella dimostrazione del seguente:

Sofisma: Esiste una corrispondenza $\emptyset \neq C \subset \mathbb{P}^1 \times \mathbb{P}^1$ che non interseca la diagonale.

Dim. Siano $p_1, p_2 \in \mathbb{P}^1$ punti distinti e sia C l'insieme delle coppie $(p_3, p_4) \in \mathbb{P}^1 \times \mathbb{P}^1$ tali che $(p_1 p_2 p_3 p_4) = -1$ (quaterna armonica). C è chiaramente nonvuoto ed è definito da una equazione algebrica, dunque C è una corrispondenza. Dato che il birapporto di quattro punti due dei quali coincidenti non può essere -1 la dimostrazione è conclusa.

ESERCIZIO 33: (Steiner, 1846)

Un punto $p \in C$ si dice *sestatico* se esiste una conica ridotta Q tale che $\nu_p(C,Q) = 6$. Provare che se p è un flesso e $C \cap C_p = \{p, p, p, q_1, q_2, q_3\}$ allora i punti q_i sono sestatici. Viceversa ogni punto sestatico si ottiene in questo modo e quindi C ha esattamente 27 punti sestatici distinti.

(Sugg. Se q è sestatico e Q è una conica tale che $\nu_q(C,Q) = 6$ provare che Q è liscia in q e considerare il sistema lineare generato da C e da $3\,\overline{qq}$.)

ESERCIZIO 34: Nelle notazioni della dimostrazione di 3.6 se $s = r$ è un punto di flesso e $C_r = \overline{rr} + L$ allora ϕ è indotta dalla proiezione di centro $L \in (\mathbb{P}^2)^\vee$.

ESERCIZIO 35: $(*)$ (Forme canoniche dell'equazione cubica)

Nei seguenti punti C denota una cubica piana liscia su un campo algebricamente chiuso di caratteristica $\neq 2, 3$.

i) Siano p, q, r tre flessi distinti e allineati di C; provare che $T_pC \cap T_qC \cap T_rC = \emptyset$.

ii) In un opportuno sistema di coordinate affini l'equazione di C assume la forma canonica di Deuring

$$y^2 + y + \delta xy = x^3$$

(Sugg. Siano $p = [0,0,1]$, $q = [1,0,0]$ due flessi e $[0,1,0] = T_pC \cap T_qC$).

iii) In un opportuno sistema di coordinate omogenee l'equazione di C assume la forma

$$(x_0 + x_1 + x_2)^3 + l x_0 x_1 x_2 = 0$$

(Sugg. Sia L retta, $p_0, p_1, p_2 \in C \cap L$ flessi allineati e $T_{p_i}C = \{x_i = 0\}$, $L = \{x_0 + x_1 + x_2\}$.)

iv) In opportuni sistemi di coordinate omogenee l'equazione di C assume le forme

$$x_0^3 + x_1^3 + x_2^3 + m x_0 x_1 x_2 = 0$$

$$(x_0^2 + x_1^2 + x_2^2)(x_0 + x_1 + x_2) - (x_0^3 + x_1^3 + x_2^3) + n x_0 x_1 x_2 = 0$$

$$x_0^3 + x_1^3 + x_2^3 = h(x_0 + x_1 + x_2)^3$$

(Sugg. Considerare il generico cambio di coordinate omogenee che commuta con l'azione del gruppo simmetrico Σ_3; tali cambi di coordinate sono rappresentati da una matrice

$$\begin{pmatrix} \alpha & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{pmatrix}$$

Sostituire in iii) e risolvere in α.)

ESERCIZIO 36: Caratteristica $\neq 2, 3$. Ogni cubica liscia è l'hessiana di un'altra cubica liscia.

ESERCIZIO 37: $(*)$ Sia C cubica liscia fissata e G il gruppo delle proiettività ϕ di $\mathbb{P}^2$ tali che $\phi(C) = C$. Provare:

1) G è finito (se $\phi(C) = C$ allora ϕ manda flessi in flessi).
2) G agisce transitivamente sull'insieme dei nove flessi di C.
3) Fissato un flesso $p \in C$ sia $G_p \subset G$ lo stabilizzatore di p e $H_p \subset G_p$ lo stabilizzatore della quaterna di Salmon di (C,p). Provare che $H_p = \mathbb{Z}/2\mathbb{Z}$.
4) Provare che la cardinalità di G è uguale a:
   54 se la quaterna di Salmon è equianarmonica.
   36 se la quaterna di Salmon è armonica.
   18 in tutti gli altri casi.
5) Se $|G| = 18$ allora ogni elemento di G è prodotto di al più due involuzioni.
6) Esiste una bigezione tra l'insieme dei flessi ed il gruppo $T = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ tale che tre flessi risultano allineati se e solo se la somma dei corrispondenti elementi di T è uguale a 0.
7) Esiste un sottogruppo normale di G isomorfo a T.
8) Esplicitare G in un sistema di coordinate omogenee nelle quali C ha equazione $x^3 + y^3 + z^3 + mxyz = 0$.
9) L'inclusione $G \to PGL(3,\mathbb{K})$ non si solleva ad una inclusione $G \to GL(3,\mathbb{K})$.

ESERCIZIO 38: (caratteristica $\neq 2, 3$) Sia $F(x_0, x_1, x_2)$ l'equazione di una cubica liscia e sia $S \subset \mathbb{P}^3$ l'insieme dei punti $[x_0, .., x_3]$ tali che $x_3^3 = F(x_0, x_1, x_2)$.

Provare che S contiene esattamente 27 rette distinte e che ogni retta ne interseca altre 10 (Sugg.: $27 = 9 \times 3$).

ESERCIZIO 39: Sia $\mathbb{K}$ algebricamente chiuso di caratteristica 3, C la curva piana di equazione $x^3y + y^3z + z^3x = 0$. Provare che C è liscia e che ogni punto di C è un punto di flesso.

ESERCIZIO 40: (Steiner, 1853) C cubica liscia, se per un punto $p \in \mathbb{P}^2$ la conica polare C_p ha un punto singolare in q allora C_q ha un punto singolare in p.

ESERCIZIO 41: (Le Poloconiche)

Sia C una cubica liscia e L una retta. Per ogni $p \in L$ sia $C_{pp} = (C_p)_p$ la polare doppia di p rispetto a C. Provare che le rette C_p, $p \in L$, sono tutte tangenti ad una conica Q detta *Poloconica* di L.

ESERCIZIO 42: Due cubiche liscie si dicono *sizigetiche* se hanno in comune i nove flessi. Provare che in ogni fascio generato da due cubiche sizigetiche vi sono quattro cubiche ognuna delle quali è unione di tre rette.

ESERCIZIO 43: Provare:

i) Nelle notazioni di 4.2, se esiste $\psi \in \mathbb{K}[w_0, w_1, w_2]$ tale che $\psi(F, G, H) = 0$ allora $J(C, D, E)$ è indeterminata.

ii) (**?) In caratteristica 0 vale anche il viceversa del punto i).

(Suggerimento per gli esperti: F, G, H definiscono un'applicazione razionale da $\mathbb{P}^2$ in uno spazio proiettivo pesato).

ESERCIZIO 44: (**?) Nelle notazioni di 4.2 se la Steineriana non è indeterminata allora è una curva piana di grado $(n-1)(m-1)+(m-1)(l-1)+(l-1)(n-1)$.

ESERCIZIO 45: (**?) Se $S(C, D, E)$ è determinata e $J(C, D, E)$ è indeterminata esistono infiniti punti q tali che C_q, D_q, E_q hanno una componente comune.

ESERCIZIO 46: Sia B la corrispondenza costruita nella dimostrazione del teorema di Salmon. Usare la legge di gruppo della cubica per provare che $B = 2\phi$.

ESERCIZIO 47: Data una cubica C ed una retta L, la retta L' che contiene i tangenziali dei punti di intersezione di C con L si dice *retta satellite* di L.

Sia L una retta che interseca C in tre punti distinti nessuno dei quali flesso. Provare che L è satellite di 16 rette distinte concorrenti a gruppi di 4 in 12 punti. Ognuna delle 16 rette contiene esattamente 3 dei suddetti punti.

ESERCIZIO 48: Sia $E \subset \mathbb{R}^2$ insieme finito tale che per ogni coppia di punti di E la retta passante per essi contiene almeno un altro punto di E. Provare che i punti di E sono allineati. Dedurre che una cubica affine liscia $C \subset \mathbb{C}^2$ di equazione $f \in \mathbb{R}[x, y]$ possiede al più tre flessi a coordinate reali. (Sugg. Sia S l'insieme delle rette che contengono almeno due punti di E e sia $A = \{(L, p) \in S \times E \,|\, p \notin L\}$. Se per assurdo $A \neq \emptyset$ si prenda un elemento (L_0, p_0) tale che la distanza tra p_0 e L_0 sia minima.)

ESERCIZIO 49: (Teorema di Riemann)

Sia C una curva piana liscia di grado n e di genere g. Dato un divisore effettivo ϕ su C sia η effettivo tale che $\phi + \eta$ sia aggiunto di grado d. L'insieme $|\phi|$ dei divisori effettivi linearmente equivalenti a ϕ è in bigezione naturale con l'insieme dei divisori aggiunti di

grado d maggiori o uguali a η ed è quindi uno spazio proiettivo di dimensione finita $l(\phi)$. Provare che $l(\phi)$ non dipende dalla scelta di η e che vale

$$\deg \phi - g \leq l(\phi) \leq \deg \phi$$

(Sugg. Se ξ è un divisore effettivo provare che l'insieme dei divisori effettivi linearmente equivalenti a ϕ che contengono ξ è un sottospazio proiettivo di $|\phi|$).

ESERCIZIO 50: (Teorema di Cayley, 1843). Siano $p_1, ..., p_{nm}$ punti distinti di intersezione di due curve irriducibili di grado n, m. Se $0 < p \leq \min(n, m)$ allora $p_1, ..., p_{nm}$ inducono

$$mn - \frac{(p-1)(p-2)}{2}$$

condizioni lineari sulle curve di grado $n + m - p$.

Nota. La dimostrazione del risultato del precedente esercizio richiede il teorema $AF + BG$ datato 1872. Non ho visto l'articolo originale di Cayley ma la dimostrazione presentata in [Cre] non è corretta. Il teorema di Cayley è stato generalizzato da Bacharach nel 1886 (vedi esercizio seguente per una versione debole)

ESERCIZIO 51: (Teorema di Cayley-Bacharach, 1886)

Ecco una interessante applicazione del teorema del resto di Brill e Noether.

Siano C, D curve piane liscie di grado n, m che si intersecano trasversalmente e sia $0 \leq l < \min(n, m)$ un intero. Per Bézout non esiste nessuna curva di grado l contenente $C \cap D$ ed è quindi possibile trovare un sottoinsieme $A \subset C \cap D$ di cardinalità $\frac{1}{2}(l+1)(l+2) = \frac{1}{2}l(l+3)+1$ che non è contenuto in nessuna curva di grado l; sia $B \subset C \cap D$ il complementare di A. Dimostrare che ogni curva di grado $n + m - l - 3$ che contiene B contiene anche A. (Sugg. Si assuma $n \geq m$ per fissare le idee, sia H una curva fissata di grado $n+m-l-3$ che contiene B e sia $p \in A$; bisogna dimostrare che $p \in H$. Si prenda L una retta generica per p e sia E l'unica curva di grado l contenente $A - p$. Possiamo scrivere $H_{|D} = B + \eta$, $(E + L)_{|D} = B + \mu$ con η, μ divisori effettivi su D. Per il teorema del resto esiste una curva F di grado $m-2$ tale che $F_{|D} = \mu + \eta$. Provare che L è una componente di F e quindi che $p \in \eta$)

ESERCIZIO 52: Forse il modo più semplice per dimostrare che le quaterne di Salmon di una cubica liscia C sono proiettivamente equivalenti è quello di usare la forza bruta e dimostrare che l'invariante j è lo stesso.

Per facilitare il conto, se $p, q \in C$, non è restrittivo supporre $\overline{pq}$ trasversa a C, si può quindi prendere un sistema di coordinate omogenee tali che $p = [1, 0, 0]$, $q = [0, 1, 0]$, $T_pC \cap T_qC = [0, 0, 1]$ e C è definita dall'equazione $x_2^3 + x_2^2(x_0 + x_1) + x_0x_1(ax_0 + bx_1 + cx_2) = 0$.

ESERCIZIO 53: Per ogni $a \in \mathbb{C}$ sia $C_a \subset \mathbb{C}^2$ la conica affine di equazione

$$(ia - 1)(x^2 + y^2 + 1) + 2(a - i)xy, \qquad i = \sqrt{-1}$$

Determinare i valori di a peri quali C_a contiene infiniti punti a coordinate reali. (Sugg. per una soluzione elegante dell'esercizio suggeriamo l'uso dei ben noti isomorfismi conformi tra il disco unitario di $\mathbb{C}$ ed il semipiano superiore.)

ESERCIZIO 54: (*) La definizione originale di Weierstrass del genere di una curva liscia è leggermente diversa, ma sostalmente equivalente, dalla 5.4 (cf. [E-C] Libro V, p. 141-148). Egli infatti definiva il genere di C come il più piccolo intero p tale che per ogni divisore effettivo ϕ di grado $p+1$ l'insieme $|\phi|$ dei divisori effettivi linearmente equivalenti a ϕ è uno spazio proiettivo di dimensione $l(\phi) > 0$. Provare l'equivalenza tra la 5.4 e la definizione di Weierstrass. (Sugg. Utilizzare il teorema di Riemann (esercizio 49) per dimostrare che la definizione di Weierstrass ha senso dopodiché, per p definito come sopra, provare la disuguaglianza di Riemann $l(\phi) \geq \deg \phi - p$).

ESERCIZIO 55: Siano $C, D \subset \mathbb{R}^2$ due cerchi che si intersecano in due punti distinti p, q. Siano $c \in C$ e $d \in D$ e per ogni retta L passante per c sia $l \in C$ il secondo punto di itersezione di C e L, l' il secondo punto di intersezione di D e $\overline{pl}$ e l'' il punto di itersezione di L e $\overline{dl'}$. Provare che, al variare della retta L il luogo E dei punti l'' è il cerchio passante per c, d, q. (Sugg. utilizzare la generazione proiettiva delle coniche per dimostrare che E è una conica passante per c, d e per i punti di intersezione di C, D diversi da p. Si noti che questo risultato è sostanzialmente equivalente al teorema di Miquel)

ESERCIZIO 56: ($char\mathbb{K} \neq 2, 3$), C cubica liscia $p, q \in C$. Provare che esistono 4 coniche tritangenti a C in p, q ed in un terzo punto r.

VI. Aspetti algebrici delle serie di potenze

1. Il lemma di Hensel

Sia $\mathbb{K}$ un campo, una norma su $\mathbb{K}$ è una applicazione $|\ |: \mathbb{K} \to \mathbb{R}$ che soddisfa le seguenti proprietà:

1) $|a| \geq 0$ per ogni $a \in \mathbb{K}$.
2) $|a| = 0$ se e solo se $a = 0$.
3) $|a + b| \leq |a| + |b|$ per ogni $a, b \in \mathbb{K}$ (disuguaglianza triangolare).
4) $|ab| = |a||b|$ per ogni $a, b \in \mathbb{K}$.

Si noti che $|1| = |-1| = 1$. Ogni norma induce una metrica $d(a, b) = |a - b|$, il campo normato $(\mathbb{K}, |\ |)$ si dice completo o di Banach se è uno spazio metrico completo per la metrica indotta dalla norma.

Esempio 1.1. Se $\mathbb{K}$ è un sottocampo di $\mathbb{C}$ allora il valore assoluto usuale induce una norma su $\mathbb{K}$. Tale norma viene spesso indicata con $|\ |_\infty$.

Esempio 1.2. Sia $\mathbb{K}$ un campo qualsiasi, la funzione $|0| = 0$, $|a| = 1$ per ogni $a \neq 0$ è una norma che induce la topologia discreta.

Esempio 1.3. Sia $\mathbb{K} = \mathbb{Q}$ e $p \in \mathbb{Z}$ un numero primo, la norma p-adica $|\ |_p: \mathbb{Q} \to \mathbb{R}$ si definisce nel modo seguente: se $a = p^r \frac{b}{c}$ con $b, c, r \in \mathbb{Z}$ e b, c non divisibili per p si pone $|a|_p = p^{-r}$, si dimostra facilmente che si tratta di una norma.

Sia n un intero positivo fissato, un multiindice $I = (i_1, ..., i_n)$ è un elemento di $\mathbb{N}^n$; il grado di I è $|I| = i_1 + ... + i_n$.
Un **multiraggio** $r = (r_1, ..., r_n)$ è un elemento di $(0, +\infty)^n$. Se $r = (r_1, ..., r_n)$ è un multiraggio e $I = (i_1, ..., i_n)$ un multiindice si pone $r^I = r_1^{i_1} r_2^{i_2} \dots r_n^{i_n}$.
Una **serie formale** a coefficienti in $\mathbb{K}$ nelle indeterminate $x_1, ..., x_n$ è una espressione del tipo

$$\phi = \sum_I a_I x^I \qquad a_I \in \mathbb{K}, \quad I \in \mathbb{N}^n$$

dove si è posto $x^I = x_1^{i_1}x_2^{i_2}...x_n^{i_n}$, chiaramente un polinomio può essere pensato come una serie formale in cui $a_I \neq 0$ per al più un numero finito di multiindici.

La **molteplicità** di una serie formale $\sum a_I x^I$ è il più piccolo intero $m \geq 0$ tale che $a_I \neq 0$ per qualche multiindice I di grado m.

Con le ben note regole di somma e di prodotto di Cauchy le serie formali formano un anello commutativo

$$\mathbb{K}[[x_1, ..., x_n]]$$

Sia ora $|\ |$ una norma fissata su $\mathbb{K}$, una serie formale $\phi = \sum a_I x^I$ si dice **convergente** se esiste un multiraggio r tale che

$$\|\phi\|_r := \sum_I |a_I| r^I < \infty$$

Se $\mathbb{K} = \mathbb{R}, \mathbb{C}$ questa definizione coincide con la classica nozione di serie totalmente convergente; se $|\ |$ è la norma dell'esempio 1.2 ogni serie formale è convergente.

ESERCIZIO 1: Sia $s > 0$ fissato, una serie $\sum a_I x^I$ è convergente se e solo se esiste un numero reale positivo R tale che $|a_I||I|^s \leq R^{|I|}$ per ogni multiindice I.

ESERCIZIO 2: Sia $\phi \in \mathbb{K}\{x_1, ..., x_n\}$ di molteplicità m, r un multiraggio e $a \in]0, 1]$. Provare che $\|\phi\|_{ar} \leq a^m \|\phi\|_r$.

ESERCIZIO 3: Se $(\mathbb{K}, |\ |)$ è un campo completo e $\phi \in \mathbb{K}\{x_1, ..., x_n\}$ allora ϕ definisce una funzione continua su un intorno di 0 in $\mathbb{K}^n$.

Si faccia attenzione al fatto che, se il campo non è completo, una serie convergente non definisce in generale una funzione in un intorno di 0.

Denotiamo $\mathbb{K}\{x_1, ..., x_n\} \subset \mathbb{K}[[x_1, ..., x_n]]$ il sottoanello delle serie convergenti. La dimostrazione che $\mathbb{K}\{x_1, ..., x_n\}$ è un sottoanello segue immediatamente dal seguente

Lemma 1.4. *Siano $\phi, \psi \in \mathbb{K}\{x_1, ..., x_n\}$ e sia r un multiraggio tale che $\|\phi\|_r < \infty$, $\|\psi\|_r < \infty$, allora*

1) $\|\phi + \psi\|_r \leq \|\phi\|_r + \|\psi\|_r$

2) $\|\phi\psi\|_r \leq \|\phi\|_r \|\psi\|_r$

Dim. 1) è immediato. Se ψ è un monomio è ovvio che $\|\phi\psi\|_r = \|\phi\|_r \|\psi\|_r$ e quindi se ψ è un polinomio il punto 2) segue immediatamente da 1). Dunque se $\psi = \sum a_I x^I$, per ogni $s > 0$ si ha $\|\phi(\sum_{|I|<s} a_I x^I)\|_r \leq \|\phi\|_r \|\psi\|_r$ e passando al limite per $s \to \infty$ si ottiene la tesi. □

L'applicazione $\phi = \sum a_I x^I \to \phi(0) = a_0$ definisce un morfismo surgettivo di anelli $\mathbb{K}\{x_1, ..., x_n\} \to \mathbb{K}$, sia $\mathbf{m}$ il suo nucleo.

Lemma 1.5. $\mathbf{m}$ *è l'unico ideale massimale di $\mathbb{K}\{x_1, ..., x_n\}$ (che è quindi un anello locale).*

Dim. Sia $\phi \in \mathbf{m}$, dobbiamo dimostrare che $1 - \phi$ è invertibile.

La serie formale $\psi = \sum_{i=0}^{\infty} \phi^i$ è l'inverso di $1 - \phi$ in $\mathbb{K}[[x_1, ..., x_n]]$, rimane da vedere che ψ è convergente.

Sia R un multiraggio tale che $\|\phi\|_R < \infty$, siccome $\phi(0) = 0$, per ogni scalare positivo $\delta \leq 1$ si ha $\|\phi\|_{\delta R} \leq \delta \|\phi\|_R$ e quindi per δ sufficientemente piccolo $r = \delta R$ soddisfa la condizione $\|\phi\|_r < 1$ e per il lemma precedente $\|\psi\|_r < \infty$. □

Corollario 1.6. $\mathbb{K}\{t\}$ *è un anello ad ideali principali, più precisamente ogni ideale non banale è generato da t^n per qualche $n \geq 0$.*

Dim. Sia $I \neq 0$ un ideale e sia $f \in I$ di molteplicità minima m, siccome t^m divide ogni $g \in I$ basta dimostrare che $t^m \in I$.

Si può scrivere $f = t^m \phi$ con $\phi(0) \neq 0$, un tale ϕ è invertibile e quindi $t^m = f\phi^{-1} \in I$.

□

Definizione 1.7. Una serie $p(x, t) \in \mathbb{K}\{x_1, ..., x_n, t\}$ si dice uno **pseudopolinomio** [1] di grado N in t se è

$$p(x, t) = t^N + \sum_{i=1}^{N} \phi_i(x) t^{N-i}, \qquad \phi_i \in \mathbb{K}\{x_1, ..., x_n\}$$

Teorema 1.8.(Lemma di Hensel) *Sia $p(x, t) \in \mathbb{K}\{x_1, ..., x_n\}[t]$ uno pseudopolinomio di grado N in t e sia $p_0(t) = p(0, t) \in \mathbb{K}[t]$. Siano $h_0, k_0 \in \mathbb{K}[t]$ due polinomi monici senza fattori comuni tali che $p_0 = h_0 k_0$ e di gradi rispettivi $a, b = N - a$.*

Esistono allora unici due pseudopolinomi $h, k \in \mathbb{K}\{x_1, ..., x_n\}[t]$ di gradi rispettivi a, b in t tali che $hk = p$ e $h_0(t) = h(0, t)$, $k_0(t) = k(0, t)$.

Premettiamo alla dimostrazione alcuni risultati preliminari. Dato $q = \sum a_i t^i \in \mathbb{K}[t]$ si pone $|q| = \|q\|_1 = \sum |a_i|$, vale allora il seguente

Lemma 1.9. *Siano h_0, k_0 come sopra: per ogni polinomio $q \in \mathbb{K}[t]$ di grado $< N$ esistono unici due polinomi q_1, q_2 di grado $< b, < a$ rispettivamente tali che $h_0 q_1 + k_0 q_2 = q$.*

Esiste inoltre una costante $C > 0$ indipendente da q tale che $|q_1| + |q_2| \leq C|q|$.

[1] I matematici sono grandi abusatori dei prefissi quasi- e pseudo-. In sintonia con il linguaggio comune il termine pseudo-x viene usato per indicare oggetti che non sono x ma che si comportano come se lo fossero, mentre con quasi-x si intende un oggetto che possiede una parte delle proprietà che definiscono x. Esempio: polinomio quasiomogeneo, curva pseudoolomorfa, varietà quasicomplessa, fascio quasicoerente, etc.

Dim. Siccome h_0 e k_0 sono relativamente primi, esistono polinomi l, m tali che $h_0 l + k_0 m = 1$ e quindi

$$h_0(lq) + k_0(mq) = q$$

ed è chiaro che esiste una costante C_1 (dipendente solo da l, m) tale che $|lq| + |mq| \leq C_1|q|$.
Per ogni polinomio r vale ancora

$$h_0(lq - rk_0) + k_0(mq + rh_0) = q$$

e quindi $h_0 q_1 + k_0 q_2 = q$ dove q_1 è il resto della divisione di lq per il polinomio monico k_0. Dall'algoritmo della divisione euclidea tra polinomi segue facilmente che esiste una costante C_2 dipendente solo da k_0 tale che $|q_1| \leq C_2|lq|$.
Siccome q ha grado $< N$ il polinomio q_2 è necessariamente il resto della divisione di mq per h_0 ed esiste una costante C_3 tale che $|q_2| \leq C_3|mq|$. Basta allora prendere $C = C_1(C_2 + C_3)$. □

Lemma 1.10. *Esiste una costante $B > 0$ dipendente da n tale che per ogni multiindice $I \neq 0$, $I \in \mathbb{N}^n$, $n > 0$ vale*

$$\sum_{0<J<I} \frac{1}{(|J||I-J|)^{n+1}} \leq \frac{B}{|I|^{n+1}}$$

Dim. Sia d la parte intera di $\frac{1}{2}|I|$, per simmetria

$$\sum_{0<J<I} \frac{1}{(|J||I-J|)^{n+1}} \leq 2 \sum_{0<|J|\leq d} \frac{1}{(|J||I-J|)^{n+1}}$$

Dato che esistono al più s^{n-1} multiindici J con $|J| = s$ si ha

$$\sum_{0<|J|\leq d} \frac{1}{(|J||I-J|)^{n+1}} \leq \sum_{s=1}^{d} \frac{s^{n-1}}{s^{n+1}d^{n+1}} = \sum_{s=1}^{d} \frac{1}{s^2 d^{n+1}} \leq \frac{\pi^2}{6d^{n+1}}$$

□

Dimostrazione di 1.8: Scriviamo $p = \sum_I p_I(t)x^I$, si noti che $p_I(t)$ è un polinomio di grado $< N$ per ogni $I \neq 0$. Siccome p è convergente esiste un multiraggio $r = (r_1, ..., r_n)$ tale che per ogni $I \neq 0$ $|p_I| \leq r^I$.
Cerchiamo h e k del tipo

$$h = \sum_I h_I(t)x^I \qquad k = \sum_I k_I(t)x^I$$

dove h_I, k_I sono polinomi di grado $< a$, $< b$ rispettivamente per ogni $I \neq 0$.
h e k sono soluzioni formali di $hk = p$ se e solo se per ogni $I \neq 0$

$$h_0 k_I + k_0 h_I = p_I - \sum_{J<I} h_J k_{I-J}$$

Usando il lemma 1.9 e induzione sul grado di I si vede che tali h_I, k_I esistono unici, rimane da dimostrare la convergenza di h e k.
Siano B, C le costanti introdotte in 1.9 e 1.10 e $A > 0$ tale che $2ABC < 1$; esiste un numero reale positivo R sufficientemente grande tale che per ogni $I \neq 0$ vale $2C|I|^{n+1}|p_I| \leq AR^{|I|}$.
Dimostriamo per induzione su $|I|$ che $|h_I| + |k_I| \leq AR^{|I|}|I|^{-n-1}$.

$$|h_I| + |k_I| \leq C(|p_I| + \sum_J |h_J||k_{I-J}|) \leq C(\frac{AR^{|I|}}{2C|I|^{n+1}} + \frac{A^2BR^{|I|}}{|I|^{n+1}}) \leq AR^{|I|}|I|^{-n-1}$$

Questa stima sulla norma chiaramente implica la convergenza di h e k. □

Corollario 1.11. *Sia $p(x,t) \in \mathbb{K}\{x_1, ..., x_n\}[t]$,*

$$p(x,t) = t^N + \sum_{i=1}^{N} \phi_i(x)t^{N-i} \quad \phi_i \in \mathbb{K}\{x_1, ..., x_n\}$$

Se $\phi_N(0) = 0$, $\phi_{N-1}(0) \neq 0$ esiste unica una serie convergente $\psi \in \mathbb{K}\{x_1, ..., x_n\}$ tale che $\psi(0) = 0$ e $p(x, \psi(x)) = 0$.

Dim. Per il lemma di Hensel esiste una serie convergente ψ ed uno pseudopolinomio p_1 tale che $p = (t - \psi)p_1$ con $p_1(0) = \phi_{N-1}(0) \neq 0$, in particolare per ogni $\psi_1 \in \mathbb{K}\{x_1, ..., x_n\}$ tale che $\psi_1(0) = 0$ si ha $p_1(x, \psi_1(x)) \neq 0$ e quindi se $p(x, \psi_1(x)) = 0$ deve necessariamente essere $\psi_1 = \psi$. □

2. Il teorema fondamentale dell'algebra ed il teorema di Newton-Puiseux.

In questa sezione daremo una dimostrazione del fatto che $\mathbb{C}$ è un campo algebricamente chiuso che utilizza i concetti introdotti nel §1. Tale dimostrazione, sebbene più complicata di quelle tradizionali, ha il pregio di gettare luce sulla geometria dei polinomi complessi. Inoltre, con lievi modifiche (vedi esercizi), la stessa dimostrazione può essere utilizzata per dimostrare che un campo completo $(\mathbb{K}, |\ |)$ è algebricamente chiuso se $\mathbb{K} - \{0\}$ è connesso.

Teorema 2.1.(Teorema fondamentale dell'algebra) *Ogni polinomio $p \in \mathbb{C}[t]$ di grado positivo è un prodotto di polinomi di grado 1.*

Dim. Si può chiaramente supporre p monico di grado $n \geq 2$

$$p(t) = t^n + a_1 t^{n-1} + ... + a_n$$

Inoltre, a meno di effettuare sostituzione $t \to t - \frac{a_1}{n}$, si può assumere $a_1 = 0$.
Per induzione su n si può assumere il teorema vero per ogni polinomio di grado $< n$.
Dato un vettore $a = (a_2, ..., a_n) \in \mathbb{C}^{n-1}$ si pone $p_a(t) = t^n + a_2 t^{n-2} + ... + a_n$. Si consideri poi i due sottoinsiemi:
$W =$ insieme dei vettori a tali che p_a è irriducibile.
$V =$ insieme dei vettori a tali che vale $p_a = rs$ con r, s polinomi di grado positivo senza fattori comuni.
L'enunciato del teorema è quindi equivalente al fatto che $W = \emptyset$, questultimo fatto è una conseguenza dei seguenti tre lemmi:

Lemma 2.2. $V \cap W = \emptyset$, $V \cup W = \mathbb{C}^{n-1} - \{0\}$, $V \neq \emptyset$.

Lemma 2.3. *W è aperto.*

Lemma 2.4. *V è contenuto nella parte interna di $\mathbb{C}^{n-1} - W$.*

Dai tre lemmi segue $W = \emptyset$; infatti da 2.2 e 2.4 segue che V è contenuto nella sua parte interna e quindi è un aperto nonvuoto, adesso basta usare la connessione di $\mathbb{C}^{n-1} - \{0\}$.

Dimostrazione di 2.2. L'unica asserzione non banale è $V \cup W = \mathbb{C}^{n-1} - \{0\}$. Per l'ipotesi induttiva, se $a \notin V \cup W$ allora p_a deve avere una radice di molteplicità n, cioè $p_a = (t + b)^n$. Siccome $a_1 = nb = 0$ è $b = 0$ e quindi $a = 0$. □

Dimostrazione di 2.3. Siano $[t_0, t_1]$ coordinate omogenee di $\mathbb{P}^1_{\mathbb{C}}$ e si consideri il chiuso

$$H = \{(a, [t_0, t_1]) \in \mathbb{C}^{n-1} \times \mathbb{P}^1_{\mathbb{C}} \,|\, t_1^n + \sum a_i t_0^i t_1^{n-i} = 0\}$$

Se $\pi : \mathbb{C}^{n-1} \times \mathbb{P}^1_{\mathbb{C}} \to \mathbb{C}^{n-1}$ è la proiezione sul primo fattore si ha $\mathbb{C}^{n-1} - W = \pi(H)$ e siccome π è propria $\pi(H)$ è chiuso. □

Dimostrazione di 2.4. Sia $a \in V$, bisogna dimostrare che esiste un poliraggio r tale che per ogni vettore $x = (x_2, ..., x_n)$ con $|x_i| < r_i$ si ha che p_{a+x} non è irriducibile.
Sia $\phi(x, t) = p_{a+x}(t)$, siccome $\phi(0, t)$ è il prodotto di due polinomi monici relativamente primi, per il lemma di Hensel si ha $\phi(x, t) = r(x, t)s(x, t)$ con r, s pseudopolinomi in t di grado positivo, preso dunque un poliraggio r sufficientemente piccolo r ed s sono funzioni definite sul polidisco $\Delta = \{x \in \mathbb{C}^{n-1} \,||x_i| < r_i\}$ e quindi $a + \Delta \cap W = \emptyset$. □

Se si considera uno pseudopolinomio $p \in \mathbb{C}\{x\}[t]$ si osserva immediatamente che in generale non esiste nessuna fattorizzazione di p in pseudopolinomi di grado 1 in t,

basta ad esempio considerare $p = t^2 - x$. Newton ebbe per primo l'intuizione che si può sempre scrivere $p(x, t) = \prod_i (t - \phi_i(x))$ dove $\phi_i(x) = \sum a_j x^{\alpha_j}$ con gli esponenti α_j non necessariamente interi. La dimostrazione completa di questo fatto si è avuta molto più tardi ad opera di Puiseux nel 1850. Il risultato chiave è il seguente

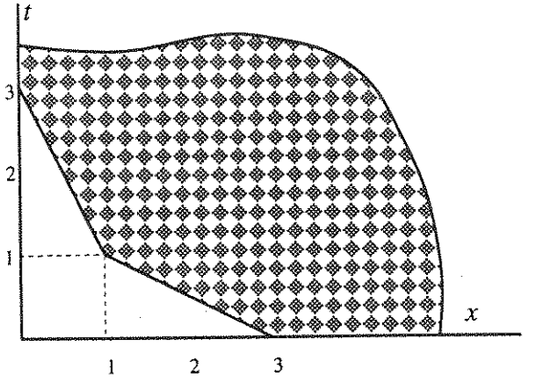
Teorema 2.5. *Sia $\mathbb{K}$ un campo algebricamente chiuso di caratteristica 0 e sia $p(x, t) = t^N + \sum \phi_i(x) t^{N-i} \in \mathbb{K}\{x\}[t]$, $N > 0$.*
Esiste allora un intero $0 < s \leq N$ tale che $p(\xi^s, t)$ è decomponibile in $\mathbb{K}\{\xi\}[t]$.

Dim. Essendo $\mathbb{K}$ di caratteristica 0 si può supporre senza perdita di generalità $\phi_1 = 0$.
Se $p = t^N$ la tesi è ovvia, altrimenti per ogni $i \geq 2$ sia α_i la molteplicità di ϕ_i (per convenzione $\alpha_i = \infty$ se $\phi_i = 0$).
Sia $j \geq 2$ fissato tale che $\frac{\alpha_j}{j} \leq \frac{\alpha_i}{i}$ per ogni i. Se $\alpha_j = 0$ allora $p(0, t)$ possiede almeno due radici distinte e per il lemma di Hensel $p(x, t)$ si decompone nel prodotto di due pseudopolinomi.
Se $\alpha_j > 0$, definiamo m il minimo comune multiplo di j e α_j, sia $s = \frac{m}{\alpha_j} \leq j$, $l = \frac{m}{j}$, vogliamo dimostrare che $p(\xi^s, t)$ è decomponibile.
Scriviamo $p(\xi^s, t) = t^N + \sum \psi_i(\xi) t^{N-i}$ dove chiaramente $\psi_i(\xi) = \phi_i(\xi)$. Per ogni i la molteplicità di ψ_i è $s\alpha_i \geq il$-ed è quindi ben definito uno pseudopolinomio

$$q(\xi, t) = p(\xi^s, \xi^l t)\xi^{-lN} = t^N + \sum \frac{\psi_i(\xi)}{\xi^{li}} t^{N-i} = t^N + \sum \eta_i(\xi) t^{N-i}$$

Siccome $\eta_j(0) \neq 0$ per il lemma di Hensel si può scrivere $q(\xi, t) = q_1(\xi, t)q_2(\xi, t)$ con q_i pseudopolinomio di grado N_i. Siano p_1, p_2 due pseudopolinomi tali che $p_i(\xi, \xi^l t) = Q_i(\xi, t)\xi^{lN_i}$, è allora chiaro che $p(\xi^s, t) = p_1(\xi, t)p_2(\xi, t)$. □

Data una serie in due variabili $f = \sum a_{ij} x^i t^j$ si definisce il **poligono di Newton** N_f di f come l'inviluppo convesso in $\mathbb{R}^2$ del sottoinsieme di $\mathbb{N}^2$ formato dalle coppie (i', j') tali che $a_{ij} \neq 0$ per qualche $i \leq i'$, $j \leq j'$.
Ad esempio il poligono di Newton di $t^3 + x^3 + tx$ è



Si noti che nella dimostrazione del teorema 2.5, gli interi s ed l sono determinati da N_p, più precisamente s è il più piccolo intero positivo tale che il bordo di N_p contiene un punto di coordinate intere $(l, N-s)$.

L'esponente s determinato dal poligono di Newton non è necessariamente il minimo indispensabile per fattorizzare p, si consideri ad esempio $p = x^4 - t^2$.

Se il campo $\mathbb{K}$ è di caratteristica positiva il teorema 2.5 non è vero in generale (vedi esercizi).

Una **serie di Puiseux** ϕ a coefficienti in $\mathbb{K}$ è una combinazione formale

$$\phi = \sum_i a_i x^{\frac{i}{C}} \qquad i \in \frac{1}{C}\mathbb{N}, a_i \in \mathbb{K}$$

dove C è un intero positivo che dipende da ϕ. Ogni serie di Puiseux possiede una forma canonica $\phi = \sum_{i=0}^{\infty} a_i x^{\frac{i}{N}}$ determinata dalla condizione aggiuntiva che esistano interi $i_1, ..., i_d$ tali che $a_{i_h} \neq 0$ per ogni h e $M.C.D.(N, i_1, ..., i_d) = 1$. L'intero N si dice **ordine di polidromia** della serie e se definiamo per ricorrenza

$$\begin{cases} i_0 = N \\ i_{s+1} = \min\{i | a_i \neq 0, MCD(i_0, ..., i_s) > MCD(i_0, ..., i_s, i)\} \end{cases}$$

gli interi $i_1, ..., i_d$ si dicono **esponenti caratteristici** di ϕ.

Una serie di Puiseux $\phi = \sum a_i x^{\frac{i}{N}}$ si dice convergente se esiste un raggio $r > 0$ tale che $\sum |a_i| r^i < \infty$. Come nel caso delle serie di potenze si prova che le serie di Puiseux convergenti formano un anello $P\{x\}$. Esiste una ovvia inclusione $\mathbb{K}\{x\} \subset P\{x\}$.

Corollario 2.6.(Newton-Puiseux) *Sia $p \in \mathbb{K}\{t\}[x]$ uno pseudopolinomio monico in t di grado N con $\mathbb{K}$ algebricamente chiuso di caratteristica 0. Esistono allora serie di Puiseux convergenti $\phi_1, ..., \phi_N \in P\{x\}$ con ordine di polidromia $\leq N$ tali che*

$$p(x,t) = \prod_{i=1}^{N} (t - \phi_i(x))$$

Dim. L'esistenza delle ϕ_i segue immediatamente da 2.5, sia s l'ordine di polidromia di ϕ_1, ció significa che si può scrivere $x = \xi^s$, $\phi_1(x) = \psi(\xi)$ con $\psi \in \mathbb{K}\{\xi\}$. Se ϵ è una radice s-upla primitiva di 1, allora le serie $\psi(\epsilon^i \xi)$ descrivono al variare di $i \in \mathbb{N}$, s radici distinte di p, dunque $s \leq N$. □

3. Il teorema di preparazione di Weierstrass

Sia r un poliraggio, $r = (r_1, ..., r_n)$, si definisce allora

$$B_r = \{f \in \mathbb{K}\{x_1, ..., x_n\} | \|f\|_r < \infty\}$$

Per 1.4 B_r è un sottoanello di $\mathbb{K}\{x_1, ..., x_n\}$ e per definizione l'unione di tutti i B_r è l'anello delle serie convergenti; con la norma $\| \ \|_r$, il $\mathbb{K}$-spazio vettoriale B_r diventa uno spazio normato.

Sia

$$\phi = \sum_{i=0}^{\infty} \phi_i(x) t^i \in \mathbb{K}\{x_1, ..., x_n, t\}$$

una serie fissata e si assuma che esista $N \geq 0$ tale che $\phi_i(0) = 0$ per ogni $i < N$ e $\phi_N(0) = 1$.

Si consideri le applicazioni (dipendenti da ϕ)

$$L: \mathbb{K}\{x_1, ..., x_n, t\} \to \mathbb{K}\{x_1, ..., x_n, t\}, \qquad L(\sum_{i \geq 0} f_i(x) t^i) = \sum_{i \geq N} f_i(x) t^{i-N}$$

$$V: \mathbb{K}\{x_1, ..., x_n, t\} \to \mathbb{K}\{x_1, ..., x_n, t\}, \qquad V(f) = L(\phi f)$$

Lemma 3.1. *Sia r un multiraggio, esiste allora $R \leq r$ tale che $V: B_R \to B_R$ è un isomorfismo.*

Dim. Scriviamo

$$\phi = t^N + t^N e(x,t) + \sum_{i=1}^{N} \phi_i(x) t^{N-i}$$

con $e(0) = \phi_i(0) = 0$. Sia $\epsilon = \frac{1}{2(N+1)}$, a meno restringere r si può supporre $\|e\|_r < \epsilon$, esiste inoltre una costante C tale che per ogni $R < r$, $R = (R_1, ..., R_n, R_t)$, vale $\|\phi_i\|_R \leq C(R_1 + ... + R_n)$.

Si noti che $\|L(t^{N-i} g)\|_R \leq R_t^{-N} \|g\|_R$, presi quindi $R_1, ..., R_n$ sufficientemente piccoli tali che $\|\phi_i\|_R \leq \epsilon R_t^N$ si ha

$$L(\phi g) - g = eg + \sum \phi_i L(t^{N-i} g)$$

$$\|V(g) - g\| = \|L(\phi g) - g\|_R \leq (N+1)\epsilon \|g\|_R = \frac{1}{2}\|g\|_R$$

Sia $\mathbf{m} \subset \mathbb{K}\{x_1, ..., x_n, t\}$ l'ideale massimale, $I = (x_1, ..., x_n)$ e $H = Id - V$, $H(g) = g - L(\phi g)$.

Se $g \in I^p \mathbf{m}^s$ allora $H(g) \in I^p \mathbf{m}^{s+1} + I^{p+1} \mathbf{m}^{s-N}$, per induzione segue che per ogni $g \in \mathbb{K}\{x_1, ..., x_n\}$, $i > 0$ vale

$$H^i(g) \in \sum_{p \geq 0} I^p \mathbf{m}^{i - p(N+1)} \subset \mathbf{m}^d$$

dove d è la parte intera di $\frac{i}{N+1}$.

Quindi per ogni g, $V^{-1}(g) = \sum_{i\geq 0} H^i(g)$ è ben definita come serie formale, essendo inoltre $\|H^i(g)\|_R \leq 2^{-i}\|g\|_R$ si ha $\|\sum_{i\geq 0} H^i(g)\|_R \leq \infty$ e quindi V è un isomorfismo su B_R. □

Teorema 3.2. (Teorema di divisione) *Siano ϕ, N definiti come sopra, per ogni $f \in \mathbb{K}\{x_1,...,x_n,t\}$ esistono unici $g \in \mathbb{K}\{x_1,...,x_n,t\}$ e $r \in \mathbb{K}\{x_1,...,x_n\}[t]$ di grado $< N$ in t tali che*

$$f = \phi g + r$$

Dim. Per il lemma 3.1 esiste g tale che $L(f) = L(\phi g)$ e quindi $r = f - \phi g$ ha grado $< N$ in t. Viceversa se $f = \phi g + r$ allora $L(f) = L(\phi g)$ e per 3.1 g è unica. □

Teorema 3.3. (Teorema di preparazione di Weierstrass) *Siano ϕ, N come sopra, esiste allora unica $e \in \mathbb{K}\{x_1,...,x_n,t\}$ invertibile tale che*

$$\phi e = t^N + \sum_{i=1}^{N} \psi_i(x) t^{N-i}, \qquad \psi_i(0) = 0.$$

Dim. Per il teorema di divisione esiste unica una serie di potenze convergente e tale che $t^N = e\phi + r$ con r polinomio in t di grado $< N$, basta quindi dimostrare che $e(0) \neq 0$, $r(0,t) = 0$.
Vale $e(0,t)\phi(0,t) = e(0)t^N + \sum_{i>N} a_i t^i$ e quindi necessariamente $r(0,t) = 0$ e $e(0) = 1$ □

Alla luce dei risultati dei paragrafi precedenti è evidente l'utilità del teorema di preparazione di Weierstrass nello studio dei luoghi di zeri delle serie convergenti.
Dimostriamo adesso che per ogni campo infinito $\mathbb{K}$ l'anello $\mathbb{K}\{x_1,...,x_n\}$ è un dominio a fattorizzazione unica, questo risultato si rivelerà di importanza fondamentale in seguito; se il campo è finito il risultato è ancora vero ma richiede una diversa dimostrazione. Premettiamo una definizione ed alcuni lemmi.

Definizione 3.4. Uno pseudopolinomio $g \in \mathbb{K}\{x_1,...,x_n\}[t]$ di grado N in t si dice **preparato in forma di Weierstrass** o più semplicemente preparato se $g(0,t) = t^N$.

Lemma 3.5. *Siano $f, g \in \mathbb{K}\{x_1,...,x_n\}[t]$ con g pseudopolinomio preparato in forma di Weierstrass. Se $f = hg$ con $h \in \mathbb{K}\{x_1,...,x_n,t\}$ allora anche $h \in \mathbb{K}\{x_1,...,x_n\}[t]$.*
Si noti che se g non è preparato il risultato è falso, si consideri ad esempio il caso $n = 0, f = t^3, g = t + t^2$.

Dim. Sia $g = t^s + \sum g_i(x)t^{s-i}$, $g_i(0) = 0$, $f = \sum_{i=0}^{r} f_i(x)t^{r-i}$ $h = \sum_i h_i(x)t^i$, bisogna dimostrare che $h_i = 0$ per ogni $i > r - s$.

Si assuma per assurdo che esista $j > r - s$ tale che $h_j \neq 0$, si può allora supporre che la molteplicità di h_j sia minima fra tutte le molteplicità di h_i, $i > r - s$. Vale l'uguaglianza $0 = h_j + \sum g_i h_{j+i}$ e siccome tutte le g_i hanno molteplicità positiva si ottiene una contraddizione. □

Lemma 3.6. *Sia $g \in \mathbb{K}\{x_1,...,x_n\}[t]$ pseudopolinomio preparato in forma di Weierstrass.*
Allora g è irriducibile in $\mathbb{K}\{x_1,...,x_n\}[t]$ se e solo se è irriducibile in $\mathbb{K}\{x_1,...,x_n,t\}$.
Come in 3.5 il risultato è falso se g non è preparato.

Dim. Assumiamo g irriducibile in $\mathbb{K}\{x_1,...,x_n,t\}$ e siano $g_1, g_2 \in \mathbb{K}\{x_1,...,x_n\}[t]$ tali che $g = g_1 g_2$. A meno di moltiplicazione per costante e scambio di indici si può supporre g_1 pseudopolinomio invertibile in $\mathbb{K}\{x_1,...,x_n,t\}$, cioè $g_1(0) = a$ con $a \in \mathbb{K} - \{0\}$. Ma essendo g preparato deve necessariamente essere $g_1(0,t) = t^s$ e quindi $s = 0$ e $g_1 = 1$.
Viceversa supponiamo g irriducibile in $\mathbb{K}\{x_1,...,x_n\}[t]$ e sia $g = h_1 h_2$ con $h_i \in \mathbb{K}\{x_1,...,x_n,t\}$. Siccome $h_1(0,t) \neq 0$ per il teorema di preparazione possiamo scrivere $h_1 = eg_1$ con e invertibile e g_1 pseudopolinomio preparato; per il lemma precedente g_1 divide g in $\mathbb{K}\{x_1,...,x_n\}[t]$ e quindi $g = g_1$, h_2 invertibile oppure $g_1 = 1$, h_1 invertibile. □

Lemma 3.7. *Sia $f \in \mathbb{K}\{x_1,...,x_n,t\}$ non nullo, esistono allora $\alpha_1,...,\alpha_n \in \mathbb{K}$ tali che $f(\alpha_1 t,...,\alpha_n t,t) \neq 0$.*

Dim. Esercizio. □

Teorema 3.8. *$\mathbb{K}\{x_1,...,x_n,t\}$ è un dominio a fattorizzazione unica.*

Dim. Induzione su n, per $n = 0$ $\mathbb{K}\{t\}$ è un dominio ad ideali principali. Sia $n > 0$ e $f \in \mathbb{K}\{x_1,...,x_n,t\}$, a meno di un possibile cambio di coordinate del tipo $t \to t$, $x_i \to x_i + \alpha_i t$ si può supporre $f(0,...,0,t) \neq 0$ e per il teorema di preparazione di Weierstrass si può supporre f uno pseudopolinomio preparato in t.
Siccome $\mathbb{K}\{x_1,...,x_n\}$ e $\mathbb{K}\{x_1,...,x_n\}[t]$ sono domini a fattorizzazione unica si ha $f = \prod f_i$ con f_i pseudopolinomi preparati irriducibili. Sia $g \in \mathbb{K}\{x_1,...,x_n,t\}$ irriducibile che divide f, allora $g(0,t) \neq 0$ e per il teorema di preparazione si può assumere g pseudopolinomio preparato e quindi $g = f_i$ per qualche i. □

Data una serie $f \in \mathbb{K}\{x,y\}$ di molteplicità m scriviamo $f = f_m + f_{m+1} + ...$ con f_i omogeneo di grado i. Vale allora il seguente

Proposizione 3.9. *Nelle notazioni precedenti sia r il numero dei fattori irriducibili distinti di f_m, allora il numero dei fattori irriducibili distinti di di f è almeno r.*

In particolare se f è irriducibile allora f_m è una potenza di un polinomio irriducibile e se f_m possiede m radici distinte in $\mathbb{P}^1$ allora f è prodotto di m serie di molteplicità 1

Dim. Dato che $\mathbb{K}\{x,y\}$ è a fattorizzazione unica basta dimostrare che se f è irriducibile allora f_m è una potenza di un polinomio irriducibile. Sia per assurdo $f_m = g_a h_b$ con g_a, h_b omogenei di grado $a, b > 0$ rispettivamente e senza fattori comuni; basta provare che esiste una decomposizione $f = gh$ con $g = g_a + g_{a+1} + \cdots$, $h = h_b + h_{b+1} + \ldots$.

A meno di un cambio lineare di coordinate e moltiplicazione per un invertibile possiamo supporre f, f_m, g_a, h_b pseudopolinomi preparati di grado m, m, a, b rispettivamente nella variabile y. Detto $\hat{f}(x,y) = \dfrac{f(x,xy)}{x^m}$ vale $\hat{f}(0,y) = \hat{f_m}(0,y) = \hat{g_a}(0,y)\hat{h_b}(0,y)$ e per il lemma di Hensel possiamo scrivere $\hat{f} = \hat{g}\hat{h}$ con $\hat{g}, \hat{h}$ polinomi monici in y di grado a, b rispettivamente; basta adesso riconsiderare $g(x,y) = x^a \hat{g}(x, \frac{y}{x})$, $h(x,y) = x^b \hat{h}(x, \frac{y}{x})$. □

Se $\mathbb{K}$ è algebricamente chiuso e $f \in \mathbb{K}\{x,y\}$, $f = f_m + f_{m+1} + \ldots$, si definisce il cono tangente di f, $C(f) \subset \mathbb{K}^2$, come la curva affine di equazione f_m. Chiaramente il supporto di $C(f)$ è unione di un numero finito di rette uguale al numero di radici distinte di f_m in $\mathbb{P}^1$. Il precedente risultato può essere allora riformulato nella seguente forma:

Proposizione 3.10. *Sia $\mathbb{K}$ algebricamente chiuso e $f \in \mathbb{K}\{x,y\}$, il numero di fattori irriducibili distinti di f non è inferiore al numero di rette distinte contenute nel cono tangente $C(f)$.*

ESERCIZIO 4: se $\mathbb{K}$ è algebricamente chiuso di caratteristica 3, allora $x^3 + t^{2s}x + t^s$ è irriducibile in $\mathbb{K}[[t]][x]$ per ogni $s > 0$.

ESERCIZIO 5: Scrivere le serie di Puiseux radici dei polinomi $x^a - t^b$, $x^2 - t^2 - t^3$, $x^3 + 3x^2t + 3xt^2 + t^4$.

ESERCIZIO 6: (*) Siano $f, g \in \mathbb{K}\{x,t\}$ senza fattori comuni, dimostrare che il $\mathbb{K}$-spazio vettoriale $\mathbb{K}\{x,t\}/(f,g)$ ha dimensione finita. (Sugg: Ridursi al caso f, g pseudopolinomi preparati e quindi mostrare che esiste $N > 0$ tale che x^N, t^N appartengono all'ideale (f,g)).

ESERCIZIO 7: Dimostrare che $\mathbb{K}\{x_1, \ldots, x_n\}$ è Noetheriano.

(Sugg. Sia $I \subset \mathbb{K}\{x_1, \ldots, x_n\}$ un ideale non banale e $f \neq 0$ un elemento di I, a meno di cambi lineari di coordinate e moltiplicazione per elementi invertibili si può supporre f pseudopolinomio preparato rispetto alla variabile x_n. Siano $g_1, \ldots, g_h$ generatori dell'ideale $J = I \cap \mathbb{K}\{x_1, \ldots, x_{n-1}\}[x_n]$, provare che $g_1, \ldots, g_h, f$ generano I.)

ESERCIZIO 8: ($\mathbb{K}$-algebre analitiche).

Una $\mathbb{K}$-algebra si dice analitica se è isomorfa ad un quoziente di un'algebra di serie di potenze convergenti. Ogni algebra analitica è un anello locale Noetheriano con campo residuo $\mathbb{K}$.

ESERCIZIO 9: Sia $\phi: \mathbb{K}\{x_1, \ldots, x_n\} \to \mathbb{K}\{y_1, \ldots y_m\}$ un morfismo di $\mathbb{K}$-algebre. Provare che per ogni $f \in \mathbb{K}\{x_1, \ldots, x_n\}$ vale $\phi(f) = f(\phi(x_1), \ldots, \phi(x_n))$. Viceversa date $g_1, \ldots, g_n \in \mathbb{K}\{y_1, \ldots, y_m\}$ serie di molteplicità positiva esiste unico un morfismo ϕ come sopra tale che $\phi(x_i) = g_i$, $i = 1, \ldots, n$. (Sugg. Detti M e N gli ideali massimali di $\mathbb{K}\{x_1, \ldots, x_n\}$ e $\mathbb{K}\{y_1, \ldots y_m\}$ rispettivamente vale $\phi(M^s) \subset N^s$ per ogni $s > 0$.)

4. Esercizi complementari

ESERCIZIO 10: In un campo finito esiste una unica norma (quella di 1.2).

ESERCIZIO 11: Sia $\mathbb{K}$ il campo delle frazioni globali di un dominio a fattorizzazione unica A e sia $f \in A$ irriducibile. Mostrare che esiste una unica norma su $\mathbb{K}$ tale che $|f| = \dfrac{1}{2}$ e $|g| = 1$ per ogni $g \in A$ non divisibile per f.

ESERCIZIO 12: Sia $\mathbb{K}$ un campo completo di caratteristica 0, se $|2| > 1$ allora $\mathbb{K}$ è connesso.

ESERCIZIO 13: Per ogni $n \in \mathbb{N}$ sia $A_n = \mathbb{K}\{t\}$ e par ogni $s \in \mathbb{N}$, $s > 0$ sia $\rho_{n,s}: A_n \to A_{ns}$ definito da $\rho_{s,n}(\phi)(t) = \phi(t^s)$. Allora $P\{t\}$ è il limite diretto del sistema $(A_n, \rho_{n,s})$.

ESERCIZIO 14: Nelle notazioni del §3 se $(\mathbb{K}, |\ |)$ è completo allora $(B_r, \|\ \|_r)$ è uno spazio di Banach per ogni multiraggio r.

ESERCIZIO 15: (*) Per ogni $r > 0$ l'anello $B_r \subset \mathbb{C}\{x\}$ non è a fattorizzazione unica. (Sugg. Mostrare che esiste una catena non stazionaria di ideali principali)

ESERCIZIO 16: (*) (Criterio valutativo di convergenza).

Sia $(\mathbb{K}, |\ |)$ un campo completo di caratteristica 0 contenente tutte le radici di 1.

Una serie $f \in \mathbb{K}[[x_1, \ldots, x_s]]$ risulta convergente se e solo se per ogni $\alpha_1, \ldots, \alpha_s \in \mathbb{K}$ la serie $f(\alpha_1 t, \ldots, \alpha_s t) \in \mathbb{K}[[t]]$ è convergente.

(Sugg. Dimostrare nell'ordine i seguenti 6 punti.

A) (Formula di Cauchy). Sia $P \in \mathbb{K}[x_1, \ldots, x_s]$ polinomio di grado $\leq n$ e sia $G \subset \mathbb{K}^*$ il sottogruppo delle radici $(n!)$-esime di 1.

Se $P = \sum a_I x^I$ allora per ogni multiindice I vale

$$a_I = \frac{1}{(n!)^s} \sum_{\epsilon \in G^s} \frac{p(\epsilon)}{\epsilon^I}$$

B) Se $P = \sum_{|I|=n} a_I x^I$ polinomio omogeneo di grado n. Sia $G \subset \mathbb{K}^*$ il gruppo delle radici n-esime di 1, allora per ogni $v \in \mathbb{K}$, $t \in \mathbb{K}^*$ vale

$$a_I = \frac{1}{t^n n^s} \sum_{\epsilon \in G^s} \frac{P(v+t\epsilon)}{\epsilon^I}$$

C) Sia $\{f_n\} \subset \mathbb{K}[x_1, ..., x_s]$ successione di polinomi, con f_n omogeneo di grado n.
Se $\{f_n\}$ è uniformemente limitata in un aperto di $\mathbb{K}^n$ allora esiste una costante $C > 0$ tale che per ogni n e per ogni coefficiente a di f_n vale $|a| \leq C^n$.
D) Sia $f = \sum f_n \in \mathbb{K}[[x_1, ..., x_s]]$ una serie non convergente. Per ogni $R > 0$ sia

$$V_R = \{\alpha \in \mathbb{K}^n | \text{ esiste } n \text{ tale che} |f_n(\alpha)| \geq R^n\}$$

Provare che V_R è un aperto denso.
E) Usare il teorema di Baire per dedurre che $\cap_R V_R \neq \emptyset$.
F) Il teorema è generalmente falso se il campo $\mathbb{K}$ non è completo. Ad esempio si provi che se $\mathbb{K}$ è numerabile allora esiste $f \in \mathbb{K}[[x,y]]$ non convergente tale che $f(at, bt)$ è un polinomio in t per ogni $a, b \in \mathbb{K}$.)

ESERCIZIO 17: (Polinomi di Hermite).
Dato un polinomio $f \in \mathbb{R}[x]$ denotiamo con $f^{(i)}$ la derivata i-esima rispetto a x. Per ogni intero positivo n e per ogni numero primo $p > n$ sia

$$F_{n,p}(x) = \sum_{i \geq 0} f_{n,p}^{(i)}(x) \in \mathbb{Q}[x]$$

dove

$$f_{n,p}(x) = \frac{x^{p-1}}{(p-1)!} \prod_{h=1}^{n} (h-x)^p$$

Si noti che $F_{n,p} - F'_{n,p} = f_{n,p}(x)$. Si provi che:

a) $F_{n,p}(0)$ è un intero non divisibile per p.

b) Per ogni $h = 1, ..., n$, $F_{n,p}(h)$ è un intero divisibile per p.

c) Sia $x \in \mathbb{R}$, allora

$$F_{n,p}(x) = \sum_{h=0}^{\infty} \sum_{j=0}^{h} \frac{x^j}{j!} f_{n,p}^{(h)}(0)$$

(Sugg. Sviluppo di Taylor).

ESERCIZIO 18: (La trascendenza di e).
La serie esponenziale è data da

$$e^x = \sum_{h \geq 0} \frac{x^h}{h!}$$

Per ogni $f = \sum a_i x^i \in \mathbb{R}[x]$ poniamo $\|f\| = \sum |a_i|$. Si provi:

a) $|f^{(i)}(0)| \leq i! \|f\|$.

b) $\|f^i\| \leq \|f\|^i$.

Siano $f_{n,p}, F_{n,p}$ i polinomi definiti nell'esercizio precedente.

c) Per ogni n fissato esiste una costante C tale che $\|f_{n,p}\| \leq \frac{C^p}{(p-1)!}$.

d) Per ogni n fissato e per ogni $h = 1, ..., n$, $\lim_{p \to \infty} F_{n,p}(h) - e^h F_{n,p}(0) = 0$. Sugg. Scrivere lo sviluppo in serie di e e usare il punto c) dell'esercizio precedente.

Dal punto d) e dall'esercizio precedente si può facilmente dedurre che e è trascendente. Sia infatti per assurdo $a_0 + a_1 e + \ldots + a_n e^n = 0$ con $a_i \in \mathbb{Z}$, si ponga $F_p = F_{n,p}$ e si consideri il limite per $p \to \infty$ di

$$\sum_{h=1}^{n} a_h (F_p(h) - e^h F_p(0)).$$

ESERCIZIO 19: Dato un campo normato $(\mathbb{K}, |\ |)$ sia $n > 0$ un intero fissato e siano $\sigma_1, ..., \sigma_n$ le funzioni simmetriche elementari definite dalla relazione

$$\prod_{i=1}^{n} (x - a_i) = \sum_{j=0}^{n} (-1)^j x^{n-j} \sigma_j(a), \qquad a = (a_1, ..., a_n)$$

Provare che:

a) Per ogni $\epsilon > 0$ (risp. $\delta > 0$) esiste un $\delta > 0$ (risp. $\epsilon > 0$) tale che

$$|\sigma_i(a)| < \delta, \quad \forall i \Rightarrow |a_i| < \epsilon$$

(Sugg. Induzione su n).

b) Per ogni $\epsilon, M > 0$ esiste $\delta > 0$ tale che per ogni $a = (a_1, ..., a_n), b = (b_1, ..., b_n) \in \mathbb{K}^n$ con $|a_1| < M$ e $|\sigma_i(a) - \sigma_i(b)| < \delta$ per ogni i si ha $|a_1 - b_j| < \epsilon$ per qualche $j = 1, ..., n$. (Sugg. sia $g(x) = \prod (x - b_i)$, $f(x) = \prod (x - a_i)$, allora $|g(a_1)| = |g(a_1) - f(a_1)| \leq \delta(M^{n-1} + ... + 1)$).

ESERCIZIO 20: Se $\mathbb{K}$ è algebricamente chiuso allora anche il suo completamento è algebricamente chiuso.

ESERCIZIO 21: Se $\mathbb{K} - \{0\}$ è connesso allora $\mathbb{K}^n - V$ è un aperto denso e connesso per ogni sottospazio vettoriale proprio $V \subset \mathbb{K}^n$.

ESERCIZIO 22: Sia $\mathbb{K}$ di caratteristica $p > 0$ e sia $f(x) = x^d + \sum a_i x^{d-i}$. Se p divide d ed esiste $a_i \neq 0$ con $p \not| i$ allora $f(x) \neq (x-a)^d$.

ESERCIZIO 23: Se un campo normato $\mathbb{K}$ è completo e $\mathbb{K} - \{0\}$ è connesso allora $\mathbb{K}$ è algebricamente chiuso. (Sugg. Ripetere la dimostrazione fatta nel caso $\mathbb{K} = \mathbb{C}$ utilizzando gli esercizi precedenti).

ESERCIZIO 24: Il completamento p-adico di $\mathbb{Q}$ possiede infinite componenti connesse.

ESERCIZIO 25: Sia $|\ |$ una norma su $\mathbb{Q}$ tale che $|p| \leq 1$ per qualche primo $p > 1$. Allora $|q| \leq 1$ per ogni numero intero. Inoltre se $|p| < 1$ e p non divide q allora $|q| = 1$. (Sugg. Scrivere q^n in base p e fare tendere $n \to \infty$).

ESERCIZIO 26: (Le algebre ombra).

Sia $\mathbb{K}$ un campo e $\mathcal{P}$ lo spazio vettoriale di tutte le applicazioni lineari $\mathbb{K}[x] \to \mathbb{K}$. esiste un isomorfismo naturale di $\mathbb{K}$-spazi vettoriali

$$\Phi: \mathcal{P} \to \mathbb{K}[[t]], \qquad \Phi(L) = \sum_n L(x^n)t^n$$

Tramite Φ lo spazio vettoriale $\mathcal{P}$ acquista una struttura di $\mathbb{K}$-algebra detta "algebra ombra" (in inglese umbral algebra) e su tale circostanza si basa il calcolo ombra (umbral calculus).

Si assuma adesso il campo $\mathbb{K}$ normato. I sottoinsiemi $B(p,r,\epsilon) \subset \mathbb{K}[x]$, $p \in \mathbb{K}[x]$, $r, \epsilon > 0$

$$B(p,r,\epsilon) = \{q \,|\, \|q-p\|_r < \epsilon\}$$

sono una base per una topologia su $\mathbb{K}[x]$.

Detto $B_\delta \subset \mathbb{K}$ la palla di centro 0 e raggio δ, un funzionale $L \in \mathcal{P}$ è continuo se e solo se per ogni $\delta > 0$ esistono ϵ, r tali che $L(B(0,r,\epsilon) \subset B_\delta$.

Tramite l'isomorfismo Φ le serie convergenti corrispondono ai funzionali continui.

ESERCIZIO 27: (**) (Anelli Henseliani).

Sia A un anello locale con ideale massimale $\mathbf{m}$ e campo residuo $\mathbb{K}$; provare che le seguenti proprietà sono equivalenti:

a) Sia $p \in A[x]$ un polinomio monico a coefficienti in A e sia $\overline{p} \in \mathbb{K}[x]$ la sua riduzione modulo $\mathbf{m}$. Se esistono $\overline{p_1}, \overline{p_2} \in \mathbb{K}[x]$ senza fattori comuni tali che $\overline{p_1}\,\overline{p_2} = \overline{p}$ allora si può sollevare $\overline{p_1}, \overline{p_2}$ a polinomi $p_1, p_2 \in A[x]$ tali che $p_1 p_2 = p$.

b) Per ogni omomorfismo di anelli $A \to B$ per cui B sia finitamente generato come A-modulo, l'applicazione naturale tra gli insiemi degli idempotenti $E(B) \to E(B/\mathbf{m}B)$ è bigettiva (per definizione di $E(B) = \{b \in B \,|\, b^2 = b\}$).

c) Per ogni morfismo di anelli $A \to B$ con B finitamente generato come A-modulo si può scrivere B come prodotto diretto di un numero finito di anelli locali.

Un anello con queste proprietà si dice *Henseliano*.

ESERCIZIO 28: $\mathbb{K}$ campo di caratteristica $p > 0$, provare che $x^p + t^s x^{p-1} + t^s = 0$ non ha radici in $\mathbb{K}[[t]]$ per ogni $s > 0$. (Sugg. si puo' chiaramente assumere $\mathbb{K}$ algebricamente chiuso, una ipotetica soluzione (x,s) deve necessariamente essere del tipo (y^p, mp); induzione su s.)

ESERCIZIO 29: Si consideri il morfismo di $\mathbb{K}$-algebre

$$\phi: \mathbb{K}\{x_1,...,x_n,t_1,...,t_m,z_1,...,z_m\} \to \mathbb{K}\{x_1,...,x_n,t_1,...,t_m\}$$

definito da $\phi(x_i) = x_i$, $\phi(t_i) = \phi(z_i) = t_i$.

i) Provare che il nucleo di ϕ è l'ideale generato da $t_1 - z_1, .., t_m - z_m$. (Sugg. eseguire il cambio lineare di coordinate $z_i \to z_i - t_i$.)

ii) Per ogni $f \in \mathbb{K}\{x_1,...,x_n,t_1,...,t_m,z_1,...,z_m\}$ sia $\hat{f}$ ottenuta da f scambiando la variabile t_i con z_i, $i = 1,..,m$. Date $f_1,...,f_s \in \mathbb{K}\{x_1,...,x_n,t_1,...,t_m,z_1,...,z_m\}$ provare l'uguaglianza degli ideali

$$(f_1,...,f_s,t_1-z_1,...,t_m-z_m) = (\hat{f}_1,...,\hat{f}_s,t_1-z_1,...,t_m-z_m)$$

. (sugg. $\phi(f) = \phi(\hat{f})$.)

ESERCIZIO 30: Siano $f \in \mathbb{K}\{x_1,...,x_n,t_1,..,t_m\}$, $g_1,...,g_m \in \mathbb{K}\{x_1,..,x_n\}$ di molteplicità positiva. Provare che l'ideale generato da $f, t_1 - g_1, .., t_m - g_m$ coincide con l'ideale generato da $f(x_1,..,x_n,g_1,...,g_m), t_1 - g_1, ..., t_m - g_m$. (Sugg. usare l'esercizio precedente).

ESERCIZIO 31: Sia $\phi: \mathbb{K}\{x_1,...,x_n,y_1,..y_m\}\mathbb{K}\{x_1,...,x_n\}$ un morfismo di $\mathbb{K}$-algebre tale che $\phi(x_i) = x_i$. Provare che il nucleo di ϕ è l'ideale generato dalle serie $y_i - \phi(y_i)$.

ESERCIZIO 32: Siano $f_1,...,f_m \in \mathbb{K}\{x_1,...,x_n\}$ di molteplicità ≥ 1, $g_1,...,g_m \in \mathbb{K}\{x_1,..,x_n,y_1,...,y_m\}$ di molteplicità ≥ 2. Provare che il morfismo

$$\alpha: \mathbb{K}\{x_1,...,x_n\} \to \frac{\mathbb{K}\{x_1,..,x_n,y_1,...,y_m\}}{(y_1 - f_1 - g_1, ..., y_m - f_m - g_m)}, \quad \alpha(x_i) = x_i$$

è un isomorfismo.(Sugg. usare i due esercizi precedenti ed il teorema di preparazione di Weierstrass).

ESERCIZIO 33: Siano $f_1,...,f_n \in \mathbb{K}\{x_1,...,x_n\}$ di molteplicità ≥ 2.

Provare che il morfismo $\phi: \mathbb{K}\{x_1,...,x_n\} \to \mathbb{K}\{x_1,...,x_n\}$ definito da $\phi(x_i) = x_i + f_i$ è un isomorfismo.

ESERCIZIO 34: Provare che ogni algebra analitica è isomorfa a $\mathbb{K}\{x_1,...,x_n\}/I$ con $I \subset (x_1,...,x_n)^2$.

ESERCIZIO 35: (Lemma di Cartan) Siano $g_1,...,g_n \in \mathbb{K}\{x_1,...,x_n\}$, $g_i = x_i + \hat{g}_i$ con $\hat{g}_i \in \mathbf{m}^2$. Sia ϕ l'isomorfismo di $\mathbb{K}\{x_1,...,x_n\}$ definito da $\phi(f)(x_1,...,x_n) = f(g_1(x),...,g_n(x))$. Provare:

i) Se il campo $\mathbb{K}$ ha caratteristica 0 e $\phi^d = Id$ per qualche $d > 0$ allora $\phi = Id$.

ii) Se la caratteristica di $\mathbb{K}$ divide d il risultato del punto ii) è generalmente falso.

ESERCIZIO 36: (*) Dato un ideale $I \subset \mathbb{K}\{x_1,...,x_n\}$ e $h \geq 0$ si definisce $J_h(I)$ come l'ideale generato dai determinanti dei minori $h \times h$ di tutte le matrici Jacobiane $(\frac{\partial f_i}{\partial x_j})$ al variare di $f_1,...,f_h \in I$. Provare:

i) la definizione dei J_h è invariante per automorfismi di $\mathbb{K}\{x_1,...,x_n\}$.

ii) Se $\mathbb{K}$ ha caratteristica 0 ed esiste h tale che $J_{n-h}(I) = (1)$, $J_{n-h+1}(I) \subset I$ allora la $\mathbb{K}$-algebra analitica $\mathbb{K}\{x_1,...,x_n\}/I$ è isomorfa a $\mathbb{K}\{y_1,...,y_h\}$.

iii) Il punto ii) è generalmente falso in caratteristica $p > 0$, è comunque vero sotto le stesse ipotesi che $\mathbb{K}\{x_1,...,x_n\}/I$ è isomorfa a $\mathbb{K}\{y_1,...,y_h\}/J$ dove J è un ideale contenuto in $\mathbb{K}\{y_1^p,...,y_h^p\}$.

ESERCIZIO 37: (**?) In caratteristica 0 se $f \in \mathbb{K}\{x_1,...,x_n\}$ è irriducibile, allora f è ancora irriducibile in $\mathbb{K}[[x_1,...,x_n]]$.

(Nota. Una dimostrazione possibile utilizza il teorema di Artin [Ar] sulla soluzione delle equazioni analitiche. Probabilmente il risultato dell'esercizio è valido in caratteristica arbitraria).

ESERCIZIO 38: (relazione di Reiss)

Caratteristica $\neq 2$. Sia $f \in \mathbb{K}\{x\}[y]$ pseudopolinomio monico di grado n tale che $f(0,y)$ abbia n radici distinte $y_1,...,y_n$. Provare che il coefficiente di x^2y^{n-1} in f è uguale a

$$\frac{1}{2}\sum_{i=1}^{n}\frac{f_{xx}f_y^2 - 2f_{xy}f_xf_y + f_{yy}f_x^2}{f_y^3}(0,y_i) = 0$$

dove come al solito si intende con f_x la derivata parziale rispetto a x etc.. (Sugg. scrivere $f = \prod(y + \phi_i(x))$, derivare le relazioni $f(x, -\phi_i(x)) = 0$ e rappresentare i singoli termini della sommatoria in funzione di $\phi_1,...,\phi_n$).

ESERCIZIO 39: Nell'esercizio precedente si assuma $\mathbb{K} = \mathbb{R}$ e f convergente in una striscia $(-\epsilon,\epsilon) \times \mathbb{R}$, descrivere i termini della sommatoria in funzione del versore tangente e della curvatura della curva piana $f = 0$ nei punti di intersezione con l'asse $x = 0$.

ESERCIZIO 40:

a) Sia $(\mathbb{K}, |\ |)$ un campo normato e $a_1,...,a_n \in \mathbb{K}$ tali che $|a_i| = 1$ per ogni $i = 1,...,n$; sia $A \subset \mathbb{K}$ il sottoanello generato dalle funzioni simmetriche elementari di $a_1,...,a_n$. Provare che se l'insieme $\{a \in A \,|\, |a| \leq n!\}$ è finito allora $a_1,...,a_n$ sono radici dell'unità. (Sugg. i polinomi $p_r(x) = \prod_i (x - a_i^r)$, $r \in \mathbb{Z}$, non sono tutti distinti.)

b) Dedurre dal punto a) che le matrici ortogonali a coefficienti interi hanno ordine finito nel gruppo $O(n)$.

VII. Le singolarità delle curve piane da un punto di vista analitico

1. Archi e parametrizzazioni

Nel seguito $\mathbb{K}$ denoterà sempre un campo normato infinito. Per ogni $f \in \mathbb{K}\{t\}$ denotiamo con $\nu(f)$ la molteplicità di f.

Definizione 1.1. Un **germe di arco analitico**, detto più semplicemente un arco, è un omomorfismo locale di $\mathbb{K}$-algebre

$$\alpha\colon \mathbb{K}\{x_1,...,x_n\} \to \mathbb{K}\{t\}$$

L'arco α è unicamente determinato dalle serie di potenze $\alpha(x_i) \in (t)$, dove $(t) \subset \mathbb{K}\{t\}$ denota l'ideale massimale, se $\alpha(x_i) = 0$ per ogni i chiameremo α arco banale. Se $f_1,...,f_n \in (t)$ si denota con $\alpha = (f_1,...,f_n)$ l'arco definito da $\alpha(x_i) = f_i$.
Un arco α si dice **primitivo** se l'immagine di α contiene un ideale non banale di $\mathbb{K}\{t\}$.

Esempio 1.2.

a) Un arco $\alpha\colon \mathbb{K}\{x\} \to \mathbb{K}\{t\}$ è primitivo se e solo se è un isomorfismo (vedi esercizi).

b) L'arco $\alpha\colon \mathbb{K}[[x,y]] \to \mathbb{K}[[t]]$ definito da $\alpha(x) = t^2$, $\alpha(y) = t^3$ è primitivo: infatti l'immagine di α contiene l'ideale (t^2).

c) Siano $\alpha\colon \mathbb{K}\{x_1,...,x_n\} \to \mathbb{K}\{t\}$, $\xi\colon \mathbb{K}\{t\} \to \mathbb{K}\{t\}$ due archi. Se $\xi \circ \alpha$ è primitivo allora ξ è un isomorfismo.

ESERCIZIO 1: Sia $M = \mathbb{K}\{x,y\}/(f)$ con $f \in \mathbb{K}\{x,y\}$. Se $\nu(f(0,y)) = n$ allora M è un $\mathbb{K}\{x\}$-modulo libero di rango n.(Sugg. Teorema di divisione).

ESERCIZIO 2: Sia $\alpha\colon \mathbb{K}\{x\} \to \mathbb{K}\{t\}$ morfismo di $\mathbb{K}$-algebre locali e sia $n = \nu(\alpha(x))$. Provare che, tramite α, $\mathbb{K}\{t\}$ è un $\mathbb{K}\{x\}$ modulo libero di rango n. In particolare α è un isomorfismo se e solo se $n = 1$.

Esiste un semplice criterio per stabilire se un arco è primitivo. Premettiamo alcuni lemmi:

Lemma 1.3. *Siano $g, f \in \mathbb{K}\{t\}$ di molteplicità positiva con $f \neq 0$ e si consideri gli archi $\alpha, \beta: \mathbb{K}\{x,y\} \to \mathbb{K}\{t\}$ definiti da $\alpha = (f,g)$ e $\beta = (f, fg)$.*
Allora α è primitivo se e solo se β è primitivo.

Dim. Siccome l'immagine di α contiene l'immagine di β se β è primitivo allora anche α è primitivo.
Viceversa essendo α primitivo esiste un intero $a > 0$ tale che $\alpha(y^a) = \alpha(xp)$ per qualche p appartenente all'ideale massimale di $\mathbb{K}\{x,y\}$ e dunque $y^a - xp$ appartiene al nucleo di α.
Se $m = \nu(f)$ e (t^N) è contenuto nell'immagine di α dimostriamo che (t^{N+am}) è contenuto nell'immagine di β.
Sia $h = f^a h_1$ con $h_1 \in (t^N)$, e sia $h_1 = \alpha(q)$, per il teorema di divisione si ha $q = q_1(y^a - xp) + r$ con r polinomio in y di grado $< a$. Siccome $\alpha(\phi(x)y^b)$ appartiene all'immagine di β se la molteplicità di ϕ è almeno b si ha che $h = \alpha(x^a q) = \alpha(x^a r)$ appartiene all'immagine di β. □

Lemma 1.4. *Sia $H \subset \mathbb{N}$ un sottoinsieme chiuso per l'operazione di addizione. Il complementare di H è un insieme finito se e solo se esistono $h_1, ..., h_k \in H$ senza fattori comuni.*

Dim. Una implicazione è ovvia. Se $h_1, ..., h_k \in H$ sono senza fattori comuni esistono interi $a_1, ..., a_k$ tali che $a_1 h_1 + ... + a_k h_k = 1$. Detto $s \geq 0$ il minimo intero tale che $sh_1...h_k + h_i a_i \geq 0$ per ogni i si ha che $h = sh_1...h_k$ e $h + 1 = \sum b_i h_i$, $b_i \geq 0$ appartengono a H e quindi $n \in H$ per ogni $n \geq h^2$. □

Teorema 1.5. *Un arco $\alpha: \mathbb{K}\{x_1, ..., x_n\} \to \mathbb{K}\{t\}$ è primitivo se e solo se esistono $g_1, ..., g_k \in \mathbb{K}\{x_1, ..., x_n\}$ tali che le molteplicità $\nu(\alpha(g_1)), ..., \nu(\alpha(g_1))$ non hanno fattori comuni.*

Dim. La condizione è chiaramente necessaria. Viceversa per il lemma precedente esistono $p, q \in \mathbb{K}\{x_1, ..., x_n\}$ tali che $\nu(\alpha(p)) = \nu(\alpha(q)) + 1$. Scriviamo $f = \alpha(q)$ e $fg = \alpha(p)$ con $g \in \mathbb{K}\{t\}$ di molteplicità 1.
Basta chiaramente provare che è primitivo l'arco $\beta: \mathbb{K}\{x,y\} \to \mathbb{K}\{t\}$ definito da $\beta(x) = f$, $\beta(y) = fg$ e questo segue dal Lemma 1.3 assieme al fatto che ogni elemento di $\mathbb{K}\{t\}$ può essere rappresentato come una serie di potenze in g. □

ESERCIZIO 3: Si consideri un arco $\alpha: \mathbb{K}\{x,y\} \to \mathbb{K}\{t\}$ definito da

$$\alpha(x) = t^n, \qquad \alpha(y) = \sum a_i t^i$$

Se la caratteristica di $\mathbb{K}$ non divide n allora α è primitivo se e solo se esistono indici $h_1, ..., h_k$ tali che $a_{h_i} \neq 0$ e $n, h_1, ..., h_k$ non hanno fattori comuni.

ESERCIZIO 4: Per un arco $\alpha: \mathbb{K}\{x_1, ..., x_n\} \to \mathbb{K}\{t\}$ le seguenti affermazioni sono equivalenti:

i) α è primitivo.

ii) Il conucleo di α è uno spazio vettoriale di dimensione finita.

iii) Detto $\mathbf{m}$ l'ideale massimale di $\mathbb{K}\{x_1, ..., x_n\}$ per ogni $s > 0$ $\alpha(\mathbf{m}^s)$ contiene un ideale non banale.

Diremo che due archi sono **equivalenti** se differiscono per un automorfismo di $\mathbb{K}\{t\}$.

Proposizione 1.6. *Sia $\alpha: \mathbb{K}\{x,y\} \to \mathbb{K}\{t\}$ un arco non banale. Allora $\ker\alpha = (f)$ con $f \in \mathbb{K}\{x,y\}$ irriducibile*

Dim. Proviamo per prima cosa che $\ker\alpha \neq 0$: se $\alpha(xy) = 0$ abbiamo finito, altrimenti per il teorema di preparazione di Weierstrass possiamo moltiplicare per degli invertibili le serie $\alpha(x) - x, \in \mathbb{K}\{t,x\}$, $\alpha(y) - y \in \mathbb{K}\{t,y\}$ e ottenere due pseudopolinomi $f(x,t) \in \mathbb{K}\{x\}[t]$, $g(y,t) \in \mathbb{K}\{y\}[t]$ preparati in t e tali che $f(\alpha(x), t) = 0$, $g(\alpha(y), t) = 0$.
Adesso basta prendere il risultante $R(f,g) \in \mathbb{K}\{x,y\} \cap (f,g)$ che chiaramente appartiene al nucleo di α.
Siccome $\ker\alpha$ è un ideale primo non banale esiste $f \in \mathbb{K}\{x,y\}$ irriducibile tale che $\alpha(f) = 0$. Sia $\alpha(g) = 0$ e proviamo che f divide g; a meno di un cambio lineare di coordinate e di moltiplicazione per invertibili non è restrittivo assumere f, g pseudopolinomi preparati in y, per VI.3.6 f è irriducibile in $\mathbb{K}\{x\}[y]$. Dato che $f(0,y) = y^m$, se fosse $\alpha(x) = 0$ si avrebbe $0 = \alpha(f) = \alpha(y)^m$ e quindi α sarebbe banale contrariamente alle ipotesi. Dunque $\alpha(x) \neq 0$ e la restrizione $\alpha: \mathbb{K}\{x\} \to \mathbb{K}\{t\}$ è iniettiva.
Sia $R \in \mathbb{K}\{x\}$ il risultante di f, g, dato che $\alpha(R) = 0$ ne segue che $R = 0$ e quindi f divide g. □

Definizione 1.7. Sia $f \in \mathbb{K}\{x,y\}$ irriducibile e $\alpha: \mathbb{K}\{x,y\} \to \mathbb{K}\{t\}$ un arco primitivo. α si dice una **parametrizzazione** di f se $\alpha(f) = 0$ e quindi (per 1.6) $\ker\alpha = (f)$.
Se il campo è algebricamente chiuso ogni serie irriducibile ammette una parametrizzazione sostanzialmente unica, più precisamente vale il

Teorema 1.8. *Sia $\mathbb{K}$ algebricamente chiuso e $f \in \mathbb{K}\{x,y\}$ irriducibile. Esiste allora un arco primitivo $\alpha: \mathbb{K}\{x,y\} \to \mathbb{K}\{t\}$ tale che $\alpha(f) = 0$. Ogni altro arco β tale che $\beta(f) = 0$ è la composizione di α e di un endomorfismo di $\mathbb{K}\{t\}$.*

Dim. Induzione sulla molteplicità d di f.

Se $d = 1$, a meno di un cambio lineare di coordinate si ha per il teorema di preparazione di Weierstrass

$$f(x,y) = (x - \phi(y))e(x,y), \qquad e(0) \neq 0$$

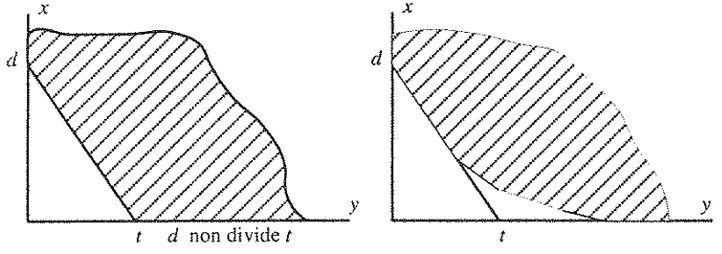
Un arco primitivo che annulla f è quindi dato da $\alpha(x) = \phi(t)$, $\alpha(y) = t$.

Se β è un altro arco primitivo che annulla f deve essere necessariamente $\beta(x) = \phi(\beta(y))$ e quindi β è la composizione di α e del morfismo $\mathbb{K}\{t\} \to \mathbb{K}\{t\}$ dato da $t \to \beta(y)$.

Si assuma adesso $d > 0$ ed il teorema vero per serie irriducibili di molteplicità minore di d. A meno di un cambio lineare di coordinate e per il teorema di preparazione possiamo assumere

$$f(x,y) = x^d + \phi_1(y)x^{d-1} + ... + \phi_d(y), \qquad \nu(\phi_i) \geq i, \qquad \phi_d \neq 0$$

Asserzione: A meno di un cambio di coordinate del tipo $x \to x - \psi(y)$, $\psi \in \mathbb{K}[y]$, $\psi(0) = 0$, $y \to y$ possiamo supporre che il poligono di Newton di f abbia una delle seguenti due forme.



Tipo irriducibile Tipo riducibile

Dim. Si osservi innanzitutto che se $r(y)$ è una serie di potenze di molteplicità sufficientemente alta il poligono di Newton di f è invariante per il cambio di coordinate $x \to x - r(y)$, $y \to y$ e quindi non è restrittivo provare l'esistenza di ψ come serie di potenze di molteplicità positiva.

Dividiamo la dimostrazione in due casi.

1) La caratteristica di $\mathbb{K}$ non divide d.

A meno di sostituire x con $x - \dfrac{\phi_1(y)}{d}$ si può supporre

$$f(x,y) = x^d + \phi_2(y)x^{d-2} + ... + \phi_d(y), \qquad \nu(\phi_i) \geq i$$

Essendo f irriducibile e $d > 1$ deve essere $\phi_d \neq 0$. Se d non divide la molteplicità di ϕ_d siamo già arrivati. Se invece $\nu(\phi_d) = ds$, essendo $\mathbb{K}$ algebricamente chiuso esiste

un cambio di coordinate del tipo $x \to x - ay^s$, $a \in \mathbb{K}$, $a \neq 0$, che rende il poligono di Newton di tipo riducibile con $t = ds$.

2) Il campo $\mathbb{K}$ ha caratteristica $p > 0$ e $p|d$.

Si consideri l'insieme E delle coppie (a,b) tali che il monomio $x^{d-a}y^b$ compare in f con coefficiente non nullo e tali che a, b, p siano senza fattori comuni. Se $E = \emptyset$ allora f sarebbe una potenza p-esima e quindi $E \neq \emptyset$. Ordiniamo E secondo l'ordinamento lessicografico; $(a,b) < (c,d)$ se e solo se $a < c$ oppure $a = c$ e $b < d$. Sia (A,B) il punto di minimo di E.

Proviamo adesso che (A,B) è invariante per cambi di coordinate del tipo $x \to x + g(y)$, $y \to y$. Infatti se $a < A$ allora $\phi_a(y)x^{d-a}$ è una potenza p-esima e quindi $\phi_a(y)(x + g(y))^{d-a}$ non contiene il monomio $x^{d-A}y^B$.

Si assuma che il poligono di Newton non sia ne di tipo irriducibile ne di tipo riducibile, allora esiste $0 < s \leq \dfrac{B}{A}$ tale che $\nu(\phi_d) = ds$. Con un cambio di coordinate di tipo $x \to x + ay^s$ si può aumentare la molteplicità di ϕ_d. Se ancora non va bene si ripete il procedimento (con un $s' > s$); la limitazione $As \leq B$ implica che il procedimento finisce dopo un numero finito di passi. □

Ritorniamo alla dimostrazione del teorema. Si assuma il poligono di Newton di tipo riducibile o irriducibile e sia $t \in \mathbb{Q}$ il punto di intersezione dell'asse delle ascisse con il prolungamento del primo segmento del poligono (vedi figura).

Detta $s \geq 1$ la parte intera di $\dfrac{t}{d}$ si può considerare lo scoppiamento di f definito da

$$\tilde{f}(x,y) = \frac{f(xy^s, y)}{y^{ds}} \in \mathbb{K}\{y\}[x]$$

La molteplicità di $\tilde{f}$ è chiaramente > 0 e $< d$, per poter applicare l'ipotesi induttiva occorre dimostrare la seguente:

Asserzione: $\tilde{f}$ è irriducibile.

Dim. Si assuma per assurdo che $\tilde{f}$ abbia un fattore irriducibile g di molteplicità strettamente minore. Essendo $g(x,0) \neq 0$ non è restrittivo supporre g pseudopolinomio preparato. Per il lemma VI.3.5 si ha $\tilde{f} = gh$ con h pseudopolinomio.

Detti a, b i gradi dei pseudopolinomi g, h rispettivamente si ha $a + b = d$ e quindi

$$f(x,y) = (y^{as}g(\frac{x}{y^s}, y))(y^{bs}h(\frac{x}{y^s}, y))$$

contraddicendo la irriducibilità di f. □

Per induzione esiste un arco primitivo $\alpha = (\alpha_1(t), \alpha_2(t))$ tale che $\tilde{f}(\alpha_1(t), \alpha_2(t)) = 0$ con $\alpha_2 \neq 0$. Chiaramente $f(\alpha_1\alpha_2^s(t), \alpha_2(t)) = 0$ e per 1.3 l'arco $(\alpha_1\alpha_2^s(t), \alpha_2(t))$ è primitivo.

Se $f(\beta_1(t),\beta_2(t))=0$ allora deve essere $\nu(\beta_1)\geq s\nu(\beta_2)$ e quindi $\gamma=\beta_1\beta_2^{-s}\in\mathbb{K}\{t\}$ e $\tilde{f}(\gamma(t),\beta_2(t))=0$. Per l'ipotesi induttiva l'arco β è la composizione di α e di un endomorfismo di $\mathbb{K}\{t\}$. □

Naturalmente in caratteristica 0 il teorema 1.8 poteva essere facilmente dimostrato utilizzando il teorema di Newton-Puiseux. La dimostrazione riportata ha tuttavia il pregio di mostrare direttamente che ogni $f\in\mathbb{K}\{x,y\}$ irriducibile si trasforma in una serie di molteplicità 1 mediante un numero finito di cambi di coordinate e scoppiamenti.

ESERCIZIO 5: (**) (Lemma degli archi selezionati)

Sia $\mathbb{K}$ un campo algebricamente chiuso, $P\subset\mathbb{K}\{x_1,\ldots,x_n\}$ un ideale primo e $h\notin P$. Provare che esiste un arco $\alpha:\mathbb{K}\{x_0,\ldots,x_n\}\to\mathbb{K}\{t\}$ tale che $\alpha(P)=0$ e $\alpha(h)\neq 0$.

(Sugg. Induzione su n, a meno di cambi lineari di coordinate esiste una base di P preparata rispetto a x_n. Usare il teorema III.1.10, le proprietà del risultante ed il teorema 1.8.)

2. Un'altra piccola dose di algebra commutativa

A) Anelli di valutazione discreta.

Definizione 2.1. Un dominio di integrità A si dice un **anello di valutazione discreta** (DVR) se esiste un elemento $t\in A-\{0\}$ detto **parametro locale** tale che ogni ideale non nullo di A è uguale a (t^s) per qualche $s\geq 0$.

L'anello $\mathbb{K}\{t\}$ è un esempio di anello di valutazione discreta.

Si osserva immediatamente che un DVR è un anello locale con ideale massimale (t), che $(t),0$ sono gli unici ideali primi e che il parametro locale è unico a meno di invertibili.

Proposizione 2.2. *Sia A un dominio locale Noetheriano con ideale massimale principale. Se A non è un campo allora è un anello di valutazione discreta.*

Dim. Si assuma che A non sia un campo e sia $t\neq 0$ un generatore dell'ideale massimale, per ogni $a\in A$ l'elemento $1-at$ è invertibile. Proviamo che $\cap_{n>0}(t^n)=0$, se così non fosse esisterebbe $a\neq 0$ ed una successione $a_n\in A$ tali che $a=t^na_n$. La catena di ideali (a_n) è stazionaria ed esiste quindi una relazione del tipo $a_{n+1}=ba_n=bta_{n+1}$ che è assurda in quanto t non è invertibile e $a_{n+1}\neq 0$.

Sia $I\subset(t)$ un ideale non nullo e sia s il più grande intero tale che $I\subset(t^s)$, dato che $(t^s)/(t^{s+1})$ ha dimensione 1 come spazio vettoriale sul campo residuo $A/(t)$ ne segue che $I+(t^{s+1})=(t^s)$ e quindi $t^s-at^{s+1}=t^s(1-at)\in I$ per qualche $a\in A$ e quindi $t^s\in I$ e $I=(t^s)$. □

Corollario 2.3. *Sia A un dominio locale Noetheriano con ideale massimale m. A è un DVR se e solo se m/m^2 ha dimensione 1 su A/m.*

Dim. A non è un campo perché $m\neq 0$, sia $t\in m$ la cui immagine in m/m^2 non è nulla. Si ha $m=(t)+m^2$ e per il lemma di Nakayama $m=(t)$. □

Per ogni DVR A con parametro locale t si definisce una valutazione

$$\nu: A\to\mathbb{N}\cup\{\infty\}$$

$$\nu(a)=sup\{s|\,a\in(t^s)\}$$

Lemma 2.4. *Sia A un DVR con valutazione ν:*

i) $\nu(a+b)\geq\min(\nu(a),\nu(b))$.

ii) $\nu(ab)=\nu(a)\nu(b)$.

iii) $\nu(a)=\infty$ *se e solo se* $a=0$, $\nu(a)=0$ *se e solo se* a *è invertibile.*

iv) a *divide* b *se e solo se* $\nu(a)\leq\nu(b)$, *in particolare* A *è un anello Euclideo con funzione grado* ν.

Dim. Lasciata per esercizio al lettore. □

In particolare valgono per tutti i DVR i risultati validi per gli anelli Euclidei. In queste note siamo interessati al teorema di classificazione delle matrici a meno di successioni di mosse elementari.

Ricordiamo che con mossa elementare su una matrice M a coefficienti in un anello A si intende una delle seguenti 6 mosse:

Mosse elementari sulle righe:

1) Permutare le righe.
2) Moltiplicare una riga per un invertibile di A.
3) Aggiungere ad una riga un multiplo di un'altra riga.

Mosse elementari sulle colonne:

1) Permutare le colonne.
2) Moltiplicare una colonna per un invertibile di A.
3) Aggiungere ad una colonna un multiplo di un'altra colonna.

Teorema 2.5. *Sia A un anello di valutazione discreta e M una matrice a coefficienti in A. È possibile trasformare M, mediante un numero finito di mosse elementari, in una matrice $N=(n_{ij})$ tale che $n_{ij}=0$ se $i\neq j$ e $n_{ii}|n_{jj}$ se $i\leq j$.*

Nota: Il teorema 2.5 è vero più in generale per matrici a coefficienti in anello ad ideali principali. Si può inoltre dimostrare (vedi esercizi) che gli elementi n_{ii} sono unici a meno di invertibili di A.

Dim. Sia $M=(m_{ij})$. A meno di permutazioni nelle righe e nelle colonne si può assumere che $\nu(m_{11})\leq\nu(m_{ij})$ per ogni i,j dove si intende con ν la valutazione associata all'anello A.

Dunque m_{11} divide m_{ij} per ogni i,j e, a meno di operazioni elementari di tipo 3), possiamo assumere che $m_{11}|m_{ij}$ per ogni i,j e che $m_{1i}=m_{i1}=0$ per ogni $i>1$. Si prosegue quindi per induzione sulle dimensioni di M. □

Corollario 2.6. *Ogni matrice invertibile a coefficienti in un anello di valutazione discreta è il prodotto di un numero finito di matrici rappresentanti mosse elementari.*

Dim. Basta applicare 2.5 ed osservare che una matrice invertibile resta invertibile anche dopo una mossa elementare. □

Corollario 2.7. *Sia M matrice $n\times m$ a coefficienti in un anello di valutazione discreta A. Esistono matrici invertibili $U_1\in GL(n,A)$, $U_2\in GL(m,A)$ tali che $U_1MU_2=(n_{ij})$ dove $n_{ij}=0$ se $i\neq j$ e $n_{ii}|n_{jj}$ se $i\leq j$.*

Dim. Basta osservare che ogni applicazione elementare sulle righe (risp. colonne) si può ottenere moltiplicando a sinistra (risp. destra) con una opportuna matrice invertibile. □

Da ora in poi considereremo per semplicità che $A=\mathbb{K}\{t\}$ lasciando le possibili generalizzazioni come esercizio. Dato un $\mathbb{K}\{t\}$-modulo M si definisce la **lunghezza** di M come

$$l(M)=\dim_{\mathbb{K}}M\in\mathbb{N}\cup\{\infty\}$$

Si noti che $\mathbb{K}\{t\}/(t^n)$ ha lunghezza n e quindi per ogni $f\in\mathbb{K}\{t\}$ si ha $l(\mathbb{K}\{t\}/(f))=\nu(f)$.

Teorema 2.8. *Sia $A=\mathbb{K}\{t\}$ e $\phi\colon A^n\to A^n$ un omomorfismo di A-moduli. Allora vale $l(\operatorname{coker}\phi)=\nu(\det\phi)$ dove con $\det\phi$ si intende il determinante della matrice che rappresenta ϕ nella base canonica di A^n.*

Dim. Le mosse elementari lasciano invariati sia $l(\operatorname{coker}\phi)$ sia $\nu(\det\phi)$, non è quindi restrittivo dimostrare il teorema nel caso in cui ϕ sia rappresentato da una matrice diagonale, $\phi=diag(a_1,....,a_n)$, $a_i\in A$. È chiaro che $\nu(\det\phi)=\nu(a_1)+...+\nu(a_n)$ e che $\operatorname{coker}\phi=A/(a_1)\oplus...\oplus A/(a_n)$, $l(\operatorname{coker}\phi)=l(A/(a_1))+...+l(A/(a_n))=\nu(a_1)+...+\nu(a_n)$. □

B) Il lemma del serpente.

Il periodo 1940-1955 è stato caratterizzato da un forte sviluppo della topologia algebrica, molte idee maturate in quel periodo hanno influenzato enormemente tutta quanta la matematica degli ultimi 50 anni. Basta citare ad esempio i concetti di Categoria e Funtore e l'utilizzo grafico delle frecce fino ad allora sconosciuto (sembra che il primo ad utilizzare una freccia per indicare un morfismo sia stato Hurewicz nel 1940: il libro di Walker [Wa], finito nel 1949, è uno degli ultimi testi a non fare uso di frecce). Tra le nuove nozioni troviamo anche quella di successione esatta.

Sia A un anello, una successione di morfismi di A-moduli

$$\ldots\longrightarrow M_n\xrightarrow{d_n}M_{n+1}\xrightarrow{d_{n+1}}M_{n+2}\longrightarrow\ldots,\quad n\in\mathbb{Z} \tag{2.9}$$

si dice un **complesso** se per ogni n vale $d_{n+1}\circ d_n=0$ o equivalentemente se $\operatorname{im}d_n\subset\ker d_{n+1}$. Si dice invece una **successione esatta** se $\operatorname{im}d_n=\ker d_{n+1}$. Una successione esatta come in (2.9) si dice limitata se $M_n=0$ ad eccezione di un numero finito di interi n, una successione esatta **corta** è una successione del tipo

$$0\longrightarrow M\longrightarrow N\longrightarrow P\longrightarrow 0$$

Un morfismo di successioni esatte corte è un diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N_1 & \longrightarrow & M_1 & \longrightarrow & P_1 & \longrightarrow & 0\\ & & \downarrow\alpha & & \downarrow\beta & & \downarrow\gamma & & \\ 0 & \longrightarrow & N_2 & \longrightarrow & M_2 & \longrightarrow & P_2 & \longrightarrow & 0 \end{array} \tag{2.10}$$

dove le righe sono successioni esatte corte. Si noti che un tale morfismo induce in modo naturale due complessi

$$0\longrightarrow\ker\alpha\longrightarrow\ker\beta\longrightarrow\ker\gamma$$

$$\operatorname{coker}\alpha\longrightarrow\operatorname{coker}\beta\longrightarrow\operatorname{coker}\gamma\longrightarrow 0$$

Un utile strumento è il seguente

Lemma 2.11.(del serpente) *Sia (2.10) un morfismo di successioni esatte corte, esiste un morfismo (di bordo) $\delta\colon\ker\gamma\to\operatorname{coker}\alpha$ tale che la successione*

$$0\longrightarrow\ker\alpha\longrightarrow\ker\beta\longrightarrow\ker\gamma\xrightarrow{\delta}\operatorname{coker}\alpha\longrightarrow\operatorname{coker}\beta\longrightarrow\operatorname{coker}\gamma\longrightarrow 0$$

è esatta.

Dim. Sia $p\in P_1$ tale che $\alpha(p)=0$, per definire $\delta(p)$ si prende $m\in M_1$ un sollevamento di p, siccome il diagramma commuta, l'immagine di $\beta(m)$ in P_2 è nulla e quindi $\beta(m)\in N_2$; poniamo $\delta(p)$ come la classe di $\beta(m)$ nel conucleo di α, lasciamo per esercizio al lettore verificare che δ è un omomorfismo ben definito e che la successione è esatta. □

ESERCIZIO 6: Sia

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & P & \longrightarrow & 0\\ & & \downarrow\alpha & & \downarrow\beta & & \downarrow\gamma & & \\ 0 & \longrightarrow & \bar{N} & \longrightarrow & \bar{M} & \longrightarrow & \bar{P} & \longrightarrow & 0 \end{array}$$

un morfismo di successioni esatte corte di spazi vettoriali di dimensione finita su $\mathbb{K}$. Provare che la traccia di β è uguale alla somma delle tracce di α e γ.

ESERCIZIO 7: Una applicazione lineare ϕ tra spazi vettoriali su un campo $\mathbb{K}$ fissato si dice di Fredholm se $\ker\phi$ e $\operatorname{coker}\phi$ hanno dimensione finita; in tal caso si definisce l'indice $i(\phi) = \dim\operatorname{coker}\phi - \dim\ker\phi$. Sia

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N_1 & \longrightarrow & M_1 & \longrightarrow & P_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & N_2 & \longrightarrow & M_2 & \longrightarrow & P_2 & \longrightarrow & 0 \end{array}$$

un morfismo di successioni esatte corte di spazi vettoriali su $\mathbb{K}$. Se α e γ sono di Fredholm allora anche β è di Fredholm e vale $i(\beta) = i(\alpha) + i(\gamma)$.

3. Aspetti analitici della molteplicità di intersezione

Da ora in poi $\mathbb{K}$ denoterà un campo algebricamente chiuso. Iniziamo con una semplice conseguenza dei risultati della precedente sezione:

Teorema 3.1. *Siano $f, g \in \mathbb{K}\{x\}[y]$ polinomi monici in y tali che $f(0,y)$ e $g(0,y)$ non abbiano radici comuni eccetto possibilmente $y = 0$.*
Sia $R = R(f,g) \in \mathbb{K}\{x\}$ il risultante di f e g, allora

$$\nu(R) = \dim_{\mathbb{K}} \mathbb{K}\{x\}/(R) = \dim_{\mathbb{K}} \mathbb{K}\{x,y\}/(f,g)$$

Dim. Per il lemma di Hensel possiamo scrivere $f = f_1 f_2$, $g = g_1 g_2$ con $f_i, g_i \in \mathbb{K}\{x\}[y]$, f_1, g_1 pseudopolinomi preparati in forma di Weierstrass, $f_2(0) \neq 0$, $g_2(0) \neq 0$. Per ipotesi i polinomi $f_2(0,y)$ e $g_2(0,y)$ non hanno radici comuni e quindi i tre risultanti $R(f_1,g_2)$, $R(f_2,g_1)$ e $R(f_2,g_2)$ sono tutti invertibili in $\mathbb{K}\{x\}$ e $\nu(R) = \nu(R(f_1,g_1))$. Essendo inoltre chiaro che $(f,g) = (f_1,g_1) \subset \mathbb{K}\{x,y\}$ si deduce che non è restrittivo dimostrare il teorema nel caso particolare di f e g pseudopolinomi preparati.
Sia $f(0,y) = y^n$, per il teorema di divisione $\mathbb{K}\{x,y\}/(f)$ è un $\mathbb{K}\{x\}$-modulo libero con base canonica $1, y, .., y^{n-1}$ e $\mathbb{K}\{x,y\}/(f,g)$ è il conucleo della moltiplicazione per g in $\mathbb{K}\{x,y\}/(f)$.
Nella base canonica la moltiplicazione per g è rappresentata dalla matrice m_{ij} i cui coefficienti soddisfano la relazione

$$y^i g = h_i f + \sum_{j=0}^{n-1} m_{ij} y^j, \qquad i = 0, ..., n-1, \qquad h_i \in \mathbb{K}\{x\}[y]$$

In base a III.1.3 il risultante di f e g è esattamente il determinante di m_{ij} e la dimostrazione si conclude usando 2.8. □

Corollario 3.2. *Siano C, D curve piane senza componenti comuni, $p \in C \cap D$ e siano x, y coordinate affini centrate in p. Se $f, g \in \mathbb{K}[x,y]$ sono le equazioni affini di C e D rispettivamente vale*

$$\nu_p(C,D) = \dim_{\mathbb{K}} \frac{\mathbb{K}\{x,y\}}{(f,g)}$$

Dim. A meno di un cambio lineare di coordinate non è restrittivo assumere che f e g soddisfano le ipotesi del teorema 3.1, basta adesso ricordarsi che per definizione di molteplicità di intersezione $\nu_p(C,D) = \nu(R)$. □

È naturale estendere la molteplicità di intersezione di due curve affini ad una applicazione

$$\nu\colon \mathbb{K}\{x,y\} \times \mathbb{K}\{x,y\} \to \mathbb{N} \cup \{\infty\}, \qquad \nu(f,g) = \dim_{\mathbb{K}} \frac{\mathbb{K}\{x,y\}}{(f,g)}$$

Dato che evidentemente ν è invariante per cambi analitici di coordinate e per moltiplicazione di f e g per elementi invertibili, ne segue che ν è univocamente determinata dai valori $\nu(f,g)$ con f, g pseudopolinomi preparati in y. In tal caso, grazie a 3.1, la molteplicità di intersezione è uguale alla molteplicità del risultante.
In particolare $\nu(f,g) = \infty$ se e solo se f e g hanno un fattore comune.

Proposizione 3.3. *ν è l'unica applicazione $\mathbb{K}\{x,y\}^2 \to \mathbb{N} \cup \{\infty\}$ che soddisfa le seguenti proprietà:*

i) $\nu(f,g) = \nu(g,f)$.
ii) *ν è invariante per cambi lineari di coordinate.*
iii) $\nu(0,f) = \infty$ *e* $\nu(f, g+fh) = \nu(f,g)$ *per ogni* $f, g, h \in \mathbb{K}\{x,y\}$.
iv) *Se e è invertibile e $f \neq 0$ allora* $\nu(e,f) = 0$.
v) $\nu(x,y) = 1$.
vi) $\nu(f,gh) = \nu(f,g) + \nu(f,h)$ *per ogni* $f, g, h \in \mathbb{K}\{x,y\}$.

Dim. Segue immediatamente dalla definizione e dal teorema 3.1 che ν soddisfa le condizioni *i),..,vi)*. Una dimostrazione alternativa di *vi)* che non utilizzi la bilinearità del risultante può essere fatta osservando che se f e gh non hanno fattori comuni allora esiste una successione esatta

$$0 \longrightarrow \frac{\mathbb{K}\{x,y\}}{(f,h)} \xrightarrow{\alpha} \frac{\mathbb{K}\{x,y\}}{(f,gh)} \xrightarrow{\beta} \frac{\mathbb{K}\{x,y\}}{(f,g)} \longrightarrow 0$$

dove β è la proiezione al quoziente e α è indotta dalla moltiplicazione per g; lasciamo per esercizio al lettore la verifica della esattezza.

Si consideri adesso una μ che soddisfa le condizioni *i),...vi)* e proviamo che $\mu(f,g)$ non dipende da μ:

Osserviamo dapprima che $\mu(f,x) = \nu(f(0,y))$ per ogni $f \in \mathbb{K}\{x,y\}$. Infatti se x divide f allora $f = xg$ e $\mu(f,x) = \mu(f - xg, x) = \mu(0,x) = \infty$. Se invece x non divide f per il teorema di preparazione $f = eh$ con e invertibile e $h = y^m + xh_1$ pseudopolinomio preparato in y; dunque $\mu(f,x) = \mu(h,x) = \mu(y^m,x) = m$.

Se $g \in \mathbb{K}\{x\}$ e $d = \nu(g)$ si può scrivere $g = x^d g_1$ con g_1 invertibile e quindi $\mu(f,g) = \nu(g(x))\nu(f(0,y))$.

In generale siano $f, g \in \mathbb{K}\{x,y\}$, a meno di un cambio lineare di coordinate e moltiplicazione per invertibili non è restrittivo supporre f e g pseudopolinomi preparati in y con $\deg f \leq \deg g$, proviamo per induzione grado di f che $\mu(f,g)$ non dipende da μ. Per il teorema di divisione scriviamo $g = fh + r$ con $r \in \mathbb{K}\{x\}[y]$; allora $\mu(f,g) = \mu(f,r)$. Se $r \in \mathbb{K}\{x\}$ abbiamo già visto che $\mu(f,r)$ non dipende da μ, altrimenti possiamo scrivere $r = sep$ con $s \in \mathbb{K}\{x\}$, e invertibile e p pseudopolinomio preparato in y di grado strettamente minore al grado di f e quindi $\mu(f,g) = \mu(f,s) + \mu(f,p)$. □

Teorema 3.4. *Sia $f \in \mathbb{K}\{x,y\}$ irriducibile e $\alpha\colon \mathbb{K}\{x,y\} \to \mathbb{K}\{t\}$ una parametrizzazione di f: allora per ogni $g \in \mathbb{K}\{x,y\}$ vale $\nu(f,g) = \nu(\alpha(g))$.*

Dim. Il risultato è evidente se f divide g, basta quindi esaminare il caso in cui f e g non hanno fattori comuni e $\alpha(g) \neq 0$.

Siano $\phi\colon \mathbb{K}\{x,y\}/(f) \to \mathbb{K}\{x,y\}/(f)$, $\psi\colon \mathbb{K}\{t\} \to \mathbb{K}\{t\}$ le moltiplicazioni per g e $\alpha(g)$ rispettivamente; ϕ e ψ sono morfismi iniettivi di $\mathbb{K}$-spazi vettoriali. Il conucleo P di α ha dimensione finita ed esiste un morfismo di successioni esatte corte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{K}\{x,y\}/(f) & \xrightarrow{\alpha} & \mathbb{K}\{t\} & \longrightarrow & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & \mathbb{K}\{x,y\}/(f) & \xrightarrow{\alpha} & \mathbb{K}\{t\} & \longrightarrow & P & \longrightarrow & 0 \end{array}$$

Per il lemma del serpente esiste una successione esatta di spazi vettoriali di dimensione finita

$$0 \longrightarrow \ker\gamma \longrightarrow \operatorname{coker}\phi \longrightarrow \operatorname{coker}\psi \longrightarrow \operatorname{coker}\gamma \longrightarrow 0$$

Dato che lo spazio vettoriale P ha dimensione finita $\dim\ker\gamma = \dim\operatorname{coker}\gamma$ e quindi $\nu(f,g) = \dim\operatorname{coker}\phi = \dim\operatorname{coker}\psi = \nu(\alpha(g))$. □

ESERCIZIO 8: Sia $\alpha = (\alpha_1, \alpha_2)$ una parametrizzazione di una serie irriducibile $f \in \mathbb{K}\{x,y\}$. Provare che la molteplicità di f è uguale al minimo delle molteplicità di α_1, α_2.

4. Esercizi complementari

ESERCIZIO 9: Sia $\mathbb{K}$ un campo di caratteristica 2, provare che l'arco $\alpha(x) = t^2 + t^3$, $\alpha(y) = t^4$ è primitivo. (Sugg. Lemma 1.3).

Nei seguenti esercizi verranno studiate alcune proprietà del poligono di Newton $N_f \subset [0,+\infty)^2$ di una serie $f \in \mathbb{K}\{x,y\}$. Per convenzione riportiamo sull'asse delle ascisse gli esponenti di y e sull'asse delle ordinate gli esponenti di x. Il campo $\mathbb{K}$ è inoltre supposto infinito.

ESERCIZIO 10: Siano $e, f \in \mathbb{K}\{x,y\}$ con $e(0) \neq 0$, allora $N_f = N_{fe}$ e quindi N_f dipende solo dall'ideale (f).

In generale chiameremo poligono di Newton qualsiasi sottoinsieme convesso $N \subset [0,+\infty)^2$ tale che $N = N_f$ per qualche f di molteplicità positiva. Dato un poligono di Newton ed un suo lato l si definisce la pendenza $0 \leq p(l) \leq \frac{\pi}{2}$ come l'angolo formato tra l e la retta verticale.

Dato un poligono di Newton N è sempre possibile ordinare i suoi lati $l_0, l_1, ..., l_k$ in modo tale che $0 = p(l_0) < p(l_1) < ... < p(l_k) = \frac{\pi}{2}$; diremo infine che il poligono N è *preparato* se l_0 e l_k sono contenuti negli assi coordinati (se $N = N_f$ la condizione equivale a $f(x,0) \neq 0$ e $f(0,y) \neq 0$).

Dato un poligono di Newton N preparato con lati $l_0, ..., l_k$ si definisce la pendenza minima e massima $min(N) = p(l_1)$, $max(N) = p(l_{k-1})$.

ESERCIZIO 11: Siano N, M poligoni di Newton preparati con $max(N) < min(M)$ si ha che

$$N + M = \{n + m \mid n \in N, m \in M\} \subset [0,+\infty)^2$$

è ancora un poligono di Newton preparato.

ESERCIZIO 12: Siano $f, g, h \in \mathbb{K}\{x,y\}$ tali che N_f, N_g siano preparati e $max(N_f) < min(N_g)$. Allora $N_h = N_f + N_g$ se e solo se $N_h = N_{fg}$.

ESERCIZIO 13: Sia $N_f = N + M$ con N, M preparati e $min(N) = max(N) = \frac{\pi}{4} < min(M)$, allora esiste $g \in \mathbb{K}\{x,y\}$ tale che $N_g = M$, $g|f$ e $M.C.D.(g, fg^{-1}) = 1$ (Sugg. Usare lo scoppiamento).

ESERCIZIO 14: Sia $N_f = N + M$ con N, M preparati e $max(N) \leq \frac{\pi}{4} < min(M)$. Allora esiste $g \in \mathbb{K}\{x,y\}$ tale che $N_g = M$, $g|f$ e $M.C.D.(g, fg^{-1}) = 1$ (Sugg. Usare il fatto che M è invariante per cambi di coordinate del tipo $x \to x$, $y \to y + \phi(x)$ per ricondursi all'esercizio precedente).

ESERCIZIO 15: Sia $\mathbb{K}$ campo infinito e $f \in \mathbb{K}\{x,y\}$. Il numero dei fattori irriducibili di f è maggiore o uguale del numero dei lati di N_f che non sono contenuti nell'unione degli assi coordinati. (Sugg. Esercizio precedente).

ESERCIZIO 16: Siano $f_1, ..., f_n \in \mathbb{K}\{x\}$ serie a molteplicità positive crescenti $0 < \nu(f_1) < ... < \nu(f_n)$.

Descrivere il poligono di Newton di $\prod_i (y - f_i(x))$. Si raccomanda di fare almeno il caso $n = 2$.

ESERCIZIO 17: (*) Sia $\mathbb{K}$ un campo di caratteristica $\neq 2$ e $f = y^2 - (x^a + y^b)^k \in \mathbb{K}\{x, y\}$, $k, a > 0$, $b > 2$. Provare che f è irriducibile se e solo se ak è dispari.

(Sugg.: Preparazione di Weierstrass e poligono di Newton).

ESERCIZIO 18: Siano $f, h \in \mathbb{K}[x_0, ..., x_n]$ con h irriducibile, $h(0) = f(0) = 0$. Se h divide f in $\mathbb{K}[[x_0, ..., x_n]]$ allora lo divide in $\mathbb{K}[x_0, ..., x_n]$.

(Sugg. Non è restrittivo assumere $\mathbb{K}$ infinito, a meno di un cambio lineare di coordinate si può supporre $h(0, ..., 0, x_n) \neq 0$; si usi quindi il lemma di Hensel, il lemma V.3.5 e le proprietà del risultante.)

Nota. L'esercizio precedente è un caso particolare del:

Principio GAGA locale. Sia $I \subset \mathbb{K}[x_0, ..., x_n]$ un ideale tale che

$$(I : f) = \{g \in \mathbb{K}[x_0, ..., x_n] | fg \in I\} \neq I \Rightarrow f(0) = 0;$$

allora vale

$$I = I\mathbb{K}\{x_0, ..., x_n\} \cap \mathbb{K}[x_0, ..., x_n].$$

La dimostrazione è troppo difficile per essere proposta come esercizio e richiede la lettura preliminare di [Mat]. GAGA è l'acronimo di Géométrie Algébrique et Géométrie Analytique, dal titolo del celebre lavoro di Serre in cui tale principio è dimostrato nel caso di $\mathbb{C}$ con la norma euclidea.

ESERCIZIO 19: Sia $\mathbb{K}$ un campo di caratteristica 0, $h, f, g \in \mathbb{K}[x, y]$ con h irriducibile, $h(0) = f(0) = 0$, $h_y(0) \neq 0$, $g(0) = 1$. Se h divide i polinomi $fg_x - gf_x$, $fg_y - gf_y$ allora h divide f.

(Sugg. Usare l'esercizio precedente.)

ESERCIZIO 20: (Teorema degli zeri di Rückert)

Sia $\mathbb{K}$ campo algebricamente chiuso, per ogni ideale $I \subset \mathbb{K}\{x_0, ..., x_n\}$ sia

$$Arc(I) = \{\phi : \mathbb{K}\{x_0, ..., x_n\} \to \mathbb{K}\{t\} | \phi(I) = 0\}.$$

Provare che $Arc(I) = Arc(J)$ se e solo se $\sqrt{I} = \sqrt{J}$ (Sugg. Lemma degli archi selezionati)

ESERCIZIO 21: Si interpreti il teorema degli zeri di Rückert nella teoria dei germi di spazi complessi.

ESERCIZIO 22: (**) (Teorema di Bertini)

$\mathbb{K}$ campo algebricamente chiuso di caratteristica 0; $D_1, D_2 \subset \mathbb{P}^2$ curve piane di grado n senza componenti comuni e sia V il fascio di curve di grado n generato da D_1, D_2.

Si provi che esiste $C \in V$ che è liscio al di fuori dei punti base di V.

(Sugg. dimostrare nell'ordine i seguenti punti:

a) quasi tutte (cioè eccetto un numero finito) le curve $C \in V$ sono ridotte.

b) sia E una curva irriducibile non contenuta in nessuna curva del fascio, provare che esiste un punto $p \in E - BS(V)$ ed una curva del fascio $C \in V$ tale che $m_p(C) = 1$ (Sugg. esercizio 15).

c) siano $F(x_0, x_1, x_2), G(x_0, x_1, x_2)$ due polinomi omogenei di grado n senza componenti comuni e siano F_i, G_i, $i = 0, 1, 2$ le derivate parziali rispetto alle variabile x_i. Provare che il luogo dei punti $p \in \mathbb{P}^2$ tali che

$$rango \begin{pmatrix} F_0(p) & F_1(p) & F_2(p) \\ G_0(p) & G_1(p) & G_2(p) \end{pmatrix} \leq 1$$

è contenuto nell'unione di un numero finito di curve del fascio V.

ESERCIZIO 23: (*) In caratteristica 0 se C, D, E hanno lo stesso grado, la Steineriana è indeterminata se e solo se esiste $p \in \mathbb{P}^2$ che è singolare per C, D, E. (Sugg: Teorema di Bertini).

ESERCIZIO 24: (**) (Proiettività normale delle curve liscie)

Sia $F \in \mathbb{K}[x_0, x_1, x_2]$ l'equazione di una curva piana liscia C, $A = \mathbb{K}[x_0, x_1, x_2]/(F)$ e $R(x) \in A[x]$ un polinomio monico. Provare:

1) Dati $P = \hat{P} + P_r$, $Q = \hat{Q} + Q_s$ polinomi in $\mathbb{K}[x_0, x_1, x_2]$ con P_r (risp. Q_s) omogeneo di grado r (risp. s) e $\hat{P}$ (risp. $\hat{Q}$) di grado $< r$ (risp. $< s$). Se P/Q è una radice di R allora vale $\nu_p(F, P_r) \geq \nu_p(F, Q_s)$ per ogni $p \in C$.

2) L'anello A è un dominio integralmente chiuso. (Sugg. Usare il punto 1) ed il teorema $AF + BG$ di Max Noether).

ESERCIZIO 25: Per un DVR arbitrario A con parametro locale t e campo residuo $\mathbb{K} = A/(t)$ si definisce la lunghezza di un A-modulo M come

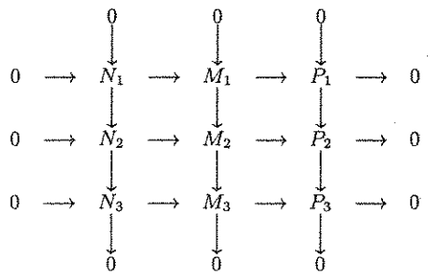
$$l(M) = \sum_{i=0}^{\infty} \dim_{\mathbb{K}} \frac{t^i M}{t^{i+1} M}$$

Provare che con tale definizione il teorema 2.8 continua a valere.

ESERCIZIO 26: Provare che nel teorema 2.5 le valutazioni $\nu(n_{ii})$ sono univocamente determinate da M e non dipendono dalla scelta delle mosse elementari.

ESERCIZIO 27: (lemma del 9)

Si consideri un diagramma commutativo con le colonne esatte



Provare che se due righe sono esatte allora è esatta anche la terza. (Sugg. se la riga centrale è esatta applicare il lemma del serpente altrimenti caccia al diagramma).

Nei seguenti quattro esercizi proponiamo una generalizzazione del teorema V.5.1.

ESERCIZIO 28: Sia $\mathbf{m} \subset \mathbb{K}\{x,y\}$ l'ideale massimale, $f,g \in \mathbf{m}$ senza fattori comuni e $\nu(f,g) = d$. Provare che $\mathbf{m}^d \subset (f,g)$ e quindi che $\mathbb{K}\{x,y\}/(f,g)$ è generato come spazio vettoriale dai monomi $x^a y^b$ con $a+b < d$. (Sugg. l'anello $A = \mathbb{K}\{x,y\}/(f,g)$ è locale noetheriano con ideale massimale $n = \mathbf{m}/(f,g)$, esiste $h \leq d$ tale che $n^h = n^{h+1} = n \cdot n^h$, si usi il lemma di Nakayama).

ESERCIZIO 29: Siano $f,g,h \in \mathbb{K}\{x,y\}$ con f di molteplicità 1. Provare che $h \in (f,g)$ se e solo se $\nu(h,f) \geq \nu(g,f)$.

ESERCIZIO 30: Siano $f_1,..,f_r,g,h \in \mathbb{K}\{x,y\}$ con $f_1,..,f_r$ di molteplicità 1 a tangenti distinte e $f = f_1..f_r$. Provare che se $\nu(h,f_i) \geq \nu(g,f_i) + r - 1$ per ogni $i = 1,..,r$ allora $h \in (f,g)$. (Sugg. induzione su r).

ESERCIZIO 31: Siano $C, D \subset \mathbb{P}^2$ curve fissate senza componenti comuni di equazioni F e G rispettivamente.

Diremo che una curva $E \subset \mathbb{P}^2$ di equazione H soddisfa la condizione $AF + BG$ *globale* se esistono polinomi omogenei A, B tali che $H = AF + BG$.

Diremo che E soddisfa la condizione $AF + BG$ *locale* se per ogni $p \in C \cap D$, dette f,g,h le equazioni di C, D, E in un sistema di coordinate affini x,y centrate in p, si ha $h \in (f,g) \subset \mathbb{K}\{x,y\}$.

Provare che E soddisfa la condizione $AF + BG$ globale se e solo se soddisfa quella locale. (Sugg. Siano n,m i gradi di C e D, provare che se $d \geq nm$ le curve E di grado d che soddisfano la condizione locale formano un sistema lineare di dimensione $\frac{1}{2}d(d+3) - nm$. Ripetere la seconda dimostrazione del teorema V.5.1.)

ESERCIZIO 32: (*) $\mathbb{K}$ campo di caratteristica 0, $f,g \in \mathbb{K}\{x,y\}$ di molteplicità positiva. Se $J = f_x g_y - f_y g_x = 0$ allora f e g hanno gli stessi fattori irriducibili.

ESERCIZIO 33: Sia $f \in \mathbb{K}\{x,y\}$ pseudopolinomio preparato di grado m in y e sia Δ il conucleo del morfismo di algebre $\alpha\colon \mathbb{K}\{u,v\} \to \mathbb{K}\{x,y\}/(f)$, $\alpha(g(u,v)) = g(x,xy)$.

Provare che la dimensione di Δ su $\mathbb{K}$ è uguale a $1 + 2 + ... + (m-1) = \frac{1}{2}m(m-1)$. (Utilizzare il teorema di divisione per dimostrare che i monomi $x^a y^b$, $0 \leq a < b < m$ sono una base di Δ.)

ESERCIZIO 34: (*) (Il numero di punti doppi)

Dato un arco primitivo $\alpha\colon \mathbb{K}\{x,y\} \to \mathbb{K}\{t\}$ la dimensione $\delta(\alpha)$ del conucleo di α è detta *numero di punti doppi* di α. Per ogni $f \in \mathbb{K}\{x,y\}$ si pone:

i) $\delta(f) = \infty$ se f possiede una componente multipla.

ii) $\delta(f) = 0$ se f è invertibile.

iii) Se f è ridotta di molteplicità positiva e $\alpha_1,...,\alpha_k$ sono le parametrizzazioni delle componenti irriducibili di f si pone $\delta(f)$ uguale alla dimensione del conucleo di

$$\mathbb{K}\{x,y\} \xrightarrow{\oplus \alpha_i} \oplus_{i=1}^k \mathbb{K}\{t\}.$$

Dalla definizione segue immediatamente che se f è irriducibile con parametrizzazione α allora $\delta(f) = \delta(\alpha)$. Provare che:

a) Se f è ridotta allora $\delta(f) < \infty$ e $(f) = \cap_i \ker \alpha_i$.

b) Se $\delta(fg) = \delta(f) + \delta(g) + \nu(f,g)$

c) Se $\delta(f) = 0$ se e solo se $m(f) \leq 1$.

d) Nelle notazioni del lemma 1.3 $\delta(\beta) = \delta(\alpha) + \frac{1}{2}\nu(f)(nu(f) - 1)$.

e) $\delta(f) \geq \frac{1}{2}m(f)(m(f)-1)$.

ESERCIZIO 35: Utilizzare il teorema di Bertini per dimostrare che, in caratteristica 0, se V è un fascio di curve piane senza componenti comuni e d è il massimo grado di una componente irriducibile contenuta in una curva del fascio allora esiste al più un numero finito di curve del fascio aventi una componente irriducibile di grado $< d$.

ESERCIZIO 36: Dimostrare la validità della seguente ricetta induttiva per il calcolo della molteplicità di intersezione di due serie irriducibili $f(x,y), g(x,y)$ in funzione delle rispettive parametrizzazioni $\alpha = (\alpha_1, \alpha_2)$, $\beta = (\beta_1, \beta_2)$. Denotiamo $\nu(\alpha,\beta) = \nu(f,g)$ e per ogni arco $\gamma = (\gamma_1, \gamma_2)$ definiamo la sua molteplicità $m(\gamma)$ come il minimo delle molteplicità di γ_1, γ_2.

Con un opportuno cambio lineare sulle coordinate x,y si ha $\nu(\alpha_1) < \nu(\alpha_2)$; in tali ipotesi

i) $\nu(\alpha,\beta) = m(\alpha)m(\beta)$ se $\nu(\beta_1) \geq \nu(\beta_2)$.

ii) $\nu(\alpha,\beta) = m(\alpha)m(\beta) + \nu(\alpha',\beta')$ se $\nu(\beta_1) < \nu(\beta_2)$ dove si è posto $\alpha' = (\alpha_1, \alpha_2\alpha_1^{-1})$, $\beta' = (\beta_1, \beta_2\beta_1^{-1})$.

ESERCIZIO 37: Sia $f \in \mathbb{K}\{t\}$ di molteplicità $\nu(f) > 0$ non divisibile per la caratteristica di $\mathbb{K}$. Provare che

$$\nu\left(x - y, \frac{f(x) - f(y)}{x - y}\right) = \nu(f) - 1$$

VIII. La topologia di Zariski

In tutto il capitolo $\mathbb{K}$ denoterà un campo algebricamente chiuso.

Chiameremo quasicompatto uno spazio topologico tale che ogni ricoprimento aperto ammette un sottoricoprimento finito: il termine compatto è invece riservato agli spazi quasicompatti di Hausdorff.

Una immersione chiusa (risp. aperta) è una applicazione continua, chiusa (risp. aperta) ed iniettiva; in particolare le immersioni chiuse e aperte sono omeomorfismi sull'immagine.

1. Esempi di spazi topologici

Ricordiamo che, preso un ideale $I \subset \mathbb{K}[x_1, ..., x_n]$, si definisce il luogo di zeri di I come

$$V(I) = \{a \in \mathbb{A}^n \mid f(a) = 0 \ \forall f \in I\}$$

e che viceversa, dato un sottoinsieme $X \subset \mathbb{A}^n$ si definisce l'ideale di X come

$$I(X) = \{f \in \mathbb{K}[x_1, ..., x_n] \mid f(a) = 0 \ \forall a \in X\}$$

Il teorema degli zeri di Hilbert afferma che per ogni ideale $J \subset \mathbb{K}[x_1, ..., x_n]$ vale $I(V(J)) = \sqrt{J}$.

Abbiamo inoltre osservato che gli insiemi $V(I) = V(\sqrt{I})$ definiscono i chiusi di una topologia su $\mathbb{A}^n$ detta **topologia di Zariski**.

Un chiuso nonvuoto $X \subset \mathbb{A}^n$ si dice una **ipersuperfice affine** se $X = V(f)$ per qualche polinomio f. Siccome ogni ideale di $\mathbb{K}[x_1, ..., x_n]$ è finitamente generato ogni chiuso di Zariski è intersezione finita di ipersuperfici. Lo stesso argomento prova che gli aperti $D(f) = \mathbb{A}^n - V(f)$, $f \in \mathbb{K}[x_1, ..., x_n]$, formano una base della topologia di Zariski.

ESERCIZIO 1: Provare che $\mathbb{A}^n$ è quasicompatto.

ESERCIZIO 2: Per ogni scelta di $p_1,...,p_s \in \mathbb{K}[x_1,...,x_n]$ l'applicazione $\mathbb{A}^n \to \mathbb{A}^s$, definita da $a \to (p_1(a),...,p_s(a))$ è continua; in particolare le affinità di $\mathbb{A}^n$ in sé sono omeomorfismi.

ESERCIZIO 3: L'applicazione $\mathbb{A}^n \to \mathbb{A}^{n+1}$, $(a_1,...,a_n) \to (a_1,...,a_n,0)$, è una immersione chiusa.

ESERCIZIO 4: La topologia di Zariski su $\mathbb{A}^{n+m} \simeq \mathbb{A}^n \times \mathbb{A}^m$ è più fine della topologia prodotto, in particolare se $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ sono chiusi, allora $X \times Y \subset \mathbb{A}^{n+m}$ è chiuso.

Il fatto che la topologia di Zariski su $\mathbb{A}^{n+m}$ sia strettamente più fine della topologia prodotto permette di supplire a certi inconvenienti tipici delle topologie non-Hausdorff. Ad esempio il grafico dell'applicazione definita nell'esercizio 2 è un sottoinsieme chiuso di $\mathbb{A}^{n+s}$.

Analogamente allo spazio affine è possibile definire la topologia di Zariski anche nello spazio proiettivo. Siano $x_0,...,x_n$ coordinate omogenee su $\mathbb{P}^n$ e $S = \oplus S_d = \mathbb{K}[x_0,...,x_n]$ con S_d lo spazio vettoriale dei polinomi omogenei di grado d.

Dato un polinomio omogeneo $f \in S$ è ben definita **l'ipersuperfice proiettiva**

$$V_{\mathbb{P}}(f) = \{[x] \in \mathbb{P}^n | f(x) = 0\}$$

Si definisce quindi un chiuso come una intersezione di ipersuperfici. Se $I \subset S$ è un ideale omogeneo si definisce $V_{\mathbb{P}}(I)$ come l'intersezione di tutte le ipersuperfici $V_{\mathbb{P}}(f)$ al variare di f tra gli elementi omogenei di I.

La verifica che i $V_{\mathbb{P}}(I)$ sono i chiusi di una topologia è simile al caso affine ed è lasciata per esercizio.

ESERCIZIO 5: Le proiettività sono omeomorfismi e l'applicazione $\mathbb{A}^n \to \mathbb{P}^n$ definita da $(a_1,...,a_n) \to [1,a_1,....,a_n]$ è una immersione aperta.

Sia $\pi: \mathbb{A}^{n+1} - \{0\} \to \mathbb{P}^n$ la proiezione al quoziente, per ogni $X \subset \mathbb{P}^n$ si definisce il **cono affine** di X come

$$C(X) = \pi^{-1}(X) \cup \{0\}$$

Si verifica immediatamente che se $I \subset S_+ := \oplus_{d>0} S_d$ è un ideale omogeneo allora $C(V_{\mathbb{P}}(I)) = V(I)$. Viceversa se $X \subset \mathbb{P}^n$ si definisce $I(X) \subset S_+$ come l'ideale generato dai polinomi omogenei di grado positivo che si annullano su X. Vale in proposito il seguente

Lemma 1.1. *Per ogni chiuso $X \subset \mathbb{P}^n$ vale $I(X) = I(C(X))$.*

Dim. è evidente dalla definizione che $I(X)$ e $I(C(X))$ contengono gli stessi polinomi omogenei, basta quindi dimostrare che l'ideale $I(C(X))$ è omogeneo.

Sia $f \in I(C(X))$ di grado m e $f = f_1 + ... + f_m$ la decomposizione di f nelle sue componenti omogenee, bisogna dimostrare che $f_i \in I(C(X))$ per ogni $i = 1,...,m$.

Dato che $C(X)$ è un cono di centro 0, per ogni $t \in \mathbb{K}$ il polinomio $f_t(x_0,...,x_n) = f(tx_0,...,tx_n)$ appartiene ancora all'ideale $I(C(X))$. Dato che $f_t = tf_1 + ... + t^m f_m$, presi m scalari distinti $t_1,....t_m \in \mathbb{K} - \{0\}$ e invertendo la matrice di Vandermonde (t_i^j) si può scrivere $f_1,...,f_m$ come combinazione lineare dei polinomi $f_{t_1},...,f_{t_m}$. □

Il precedente lemma ed il teorema degli zeri affine ci danno immediatamente il teorema degli zeri proiettivo $I(V_{\mathbb{P}}(J)) = \sqrt{J}$ per ogni ideale omogeneo $J \subset S_+$.

Si osservi che il precedente enunciato del teorema degli zeri non varrebbe senza l'ipotesi $J \subset S_+$, ad esempio $V_{\mathbb{P}}(S) = V_{\mathbb{P}}(S_+) = \emptyset$.

Corollario 1.2. *Sia $J = \oplus J_d \subset S_+$ ideale omogeneo, vale $V_{\mathbb{P}}(J) = \emptyset$ se e solo se $S_d = J_d$ per $d >> 0$.*

Dim. Se $S_d = J_d$ per qualche d allora $V(J) = \emptyset$. Viceversa se $V(J) = \emptyset$ per il teorema degli zeri $\sqrt{J} = S_+$ e dato che S_+ è finitamente generato esiste $d > 0$ tale che $S_+^d \subset J$. □

Corollario 1.3. *Siano $f_0,...,f_r \in S_+$ omogenei di gradi $d_0 \geq d_1 \geq ... \geq d_r$ e sia*

$$\phi_d: S_{d-d_0} \oplus .... \oplus S_{d-d_r} \to S_d$$

l'applicazione lineare $(g_0,...,g_r) \to g_0 f_0 + ... + g_r f_r$. Allora $V(f_0) \cap ... \cap V(f_r) = \emptyset$ se e solo se esiste d tale che ϕ_d è surgettiva.

Dim. Evidente. □

Nota: esiste una versione effettiva del corollario 1.3. Se $V(f_0,...,f_r) = \emptyset$ allora $r \geq n$ e ϕ_d è surgettiva per $d \geq d_0 + d_1 + ... + d_n - n$; per una dimostrazione vedi [Ko, I.7.4].

Siano $f_0,....,f_s \in \mathbb{K}[x_0,...,x_n]$ polinomi omogenei dello stesso grado N. Se gli f_i non hanno zeri comuni, cioè se $V(f_0,...,f_s) = \emptyset$, si può definire una applicazione $f: \mathbb{P}^n \to \mathbb{P}^s$, $f([x]) = [f_0(x),...,f_s(x)]$ che si verifica immediatamente essere continua. Se $f_0,...,f_s$ è una base di S_N la condizione $V(f_0,...,f_s) = \emptyset$ è banalmente soddisfatta e l'applicazione f viene detta **mappa di Veronese**.

Proposizione 1.4. *La mappa di Veronese f è una immersione chiusa.*

Dim. Iniziamo con l'osservare che per ogni proiettività ϕ di $\mathbb{P}^n$ esiste una proiettività indotta ψ su $\mathbb{P}^s$ tale che $f\phi = \psi f$. Dato che f non è costante ed il gruppo delle proiettività di $\mathbb{P}^n$ agisce in modo doppiamente transitivo (significa che $PGL(n+1)$ agisce transitivamente su $\mathbb{P}^n \times \mathbb{P}^n - Diagonale$) ne segue immediatamente che f è iniettiva.

Il fatto che f è una applicazione chiusa può essere dedotto da un risultato generale non costruttivo che dimostreremo in seguito. Per motivi didattici preferiamo dare qui una dimostrazione costruttiva della chiusura di f.

Sia $X = f(\mathbb{P}^n)$, proviamo prima che $f: \mathbb{P}^n \to X$ è un omeomorfismo e poi che X è chiuso in $\mathbb{P}^s$.

Dato che ogni chiuso di $\mathbb{P}^n$ è intersezione di ipersuperfici, è sufficiente provare che $f(V(g))$ è chiuso in X per ogni polinomio omogeneo g. A meno di sostituire g con una sua potenza non è restrittivo supporre che il grado di g sia un multiplo di N. Esiste allora un polinomio $P \in \mathbb{K}[y_0, ..., y_s]$ tale che $P(f_0, ..., f_s) = g$. È allora evidente che $f(V(g)) = X \cap V(P)$.

Proviamo adesso che X è una intersezione di ipersuperfici. A meno di comporre f con una proiettività di $\mathbb{P}^s$ non è restrittivo supporre che $f_0, ..., f_s$ sia la base canonica data dai monomi di grado N nelle variabili $x_0, ..., x_n$ e che le coordinate omogenee di $\mathbb{P}^s$ siano indicizzate dai multiindici $I = (i_0, ..., i_n)$ di grado N. In tale situazione $f(x)$ è il punto di coordinate omogenee $y_I = x^I$, $|I| = N$. Detto

$$Y = \bigcap V(y_{I_1} y_{I_2} \cdots y_{I_r} - y_{J_1} y_{J_2} \cdots y_{J_r}), \quad I_1 + ... + I_r = J_1 + ... + J_r$$

si ha $X \subset Y$, proviamo che vale $X = Y$.

Sia $[y] \in Y$ e sia $I = (i_0, ..., i_n)$ un multiindice tale che $y_I \neq 0$. A meno di permutazioni degli indici si può supporre $i_0 > 0$, detto $I_0 = (n, 0, 0, ..., 0)$ si ha che y_{I_0} divide y_I^n e quindi $y_{I_0} \neq 0$. Si pone $x_0 = y_{(n,0,0,...,0)} = 1$, $x_j = y_{(n-1,0,...,1,...,0)}$ dove 1 è posto alla j-esima posizione; lasciamo per esercizio al lettore la semplice verifica che $f([x_0, ..., x_n]) = [y]$ (Sugg. $y_I y_{I_0}^{n-1} = x^I$). □

ESERCIZIO 6: Il complementare ad una ipersuperfice proiettiva è omeomorfo ad un chiuso di uno spazio affine. (Sugg. Veronese)

Molto utili per le applicazioni sono gli spazi misti affino-multiproiettivi $\mathbb{P}^{n_1} \times .... \times \mathbb{P}^{n_s} \times \mathbb{A}^m$ sui quali è possibile definire in modo naturale la topologia di Zariski. A titolo di esempio consideriamo il caso $\mathbb{P}^n \times \mathbb{A}^m$. Un polinomio $f \in \mathbb{K}[x_0, ..., x_n, y_1, ..., y_m]$ si dice omogeneo rispetto alle variabili x_i se si può scrivere $f(x, y) = \sum h_i(x) k_i(y)$ con i polinomi h_i omogenei dello stesso grado. Per un tale polinomio è ben definita la corrispondente ipersuperfice $V(f) \subset \mathbb{P}^n \times \mathbb{A}^m$. Definiamo i chiusi come le intersezioni di ipersuperfici. Per il teorema della base ogni chiuso è intersezione finita di ipersuperfici.

Teorema 1.5. *La proiezione $\pi: \mathbb{P}^n \to \mathbb{A}^m$ è un'applicazione chiusa.*

Dim. Sia $X \subset \mathbb{P}^n \to \mathbb{A}^m$ un chiuso, X è intersezione di un numero finito di ipersuperfici $V(f_0), ..., V(f_r)$ con i polinomi $f_i(x, y)$ omogenei nelle variabili x_i. Un punto $a \in \mathbb{A}^m$ appartiene a $\pi(X)$ se e solo se i polinomi omogenei $f_0(x, a), ..., f_r(x, a) \in \mathbb{K}[x_0, ..., x_n]$ hanno uno zero comune in $\mathbb{P}^n$ e questo è equivalente a dire che per ogni $d > 0$ l'applicazione lineare $\phi_d(a)$ definita nel corollario 1.3 non è surgettiva.

Se Y_d è l'insieme dei punti a tali che $\phi_d(a)$ non è surgettiva si ha $X = \cap_d Y_d$; basta quindi dimostrare che Y_d è chiuso per ogni d.

$\phi_d(a)$ è rappresentata da una matrice i cui coefficienti dipendono in modo polinomiale da a e la condizione $\phi_d(a)$ non surgettiva equivale all'annullarsi dei minori di ordine uguale alla dimensione di S_d. Questo prova la chiusura di Y_d. □

ESERCIZIO 7: La proiezione $\mathbb{A}^n \to \mathbb{A}^{n-1}$ è aperta.

ESERCIZIO 8: Sia $X \subset \mathbb{A}^n$ chiuso, $I = I(X)$, $f \in \mathbb{K}[x_1, ..., x_n]$ e sia $\Gamma \subset X \times \mathbb{A}^1 \subset \mathbb{A}^{n+1}$ il grafico della applicazione $f: X \to \mathbb{A}^1$. Provare che Γ è chiuso e che $I(\Gamma)$ è l'ideale generato da $I(X)$ e $x_{n+1} - f(x_1, ..., x_n)$.

2. La dimensione combinatorica di uno spazio topologico

In questa sezione svilupperemo alcune nozioni di topologia generale che bene si adattano alle topologie di Zariski.

Definizione 2.1. Uno spazio topologico X si dice **Noetheriano** se ogni famiglia di aperti possiede un elemento massimale rispetto all'inclusione.

Per il lemma di Zorn uno spazio è Noetheriano se e solo se ogni catena ascendente di aperti (risp. discendente di chiusi) è stazionaria. Tutti gli spazi analizzati nel paragrafo 1 sono Noetheriani: infatti, ad una catena discendente di chiusi X_i dello spazio affine $\mathbb{A}^n$ corrisponde una catena ascendente di ideali $I(X_i)$ che per il teorema della base di Hilbert è stazionaria.

Lemma 2.2. *Sia X uno spazio topologico Noetheriano, allora:*

1) X è quasicompatto.

2) Ogni immagine continua di X è Noetheriana.

3) Ogni sottospazio topologico di X è Noetheriano.

Dim. 1) Siano U_i gli aperti di un ricoprimento di X, basta prendere un elemento massimale nella famiglia delle unioni finite di aperti U_i.

2) è banale.

3) Sia $Y \subset X$ un sottospazio, $T(X)$, $T(Y) = \{U \cap Y | U \in T(X)\}$ le famiglie di aperti di X e Y rispettivamente e $r: T(X) \to T(Y)$ la naturale mappa di restrizione.

Sia $\mathcal{F} \subset T(Y)$ e $U \in r^{-1}(\mathcal{F})$ un elemento massimale, proviamo che $r(U) = U \cap Y$ è massimale in F. Se $r(U) \subset r(V)$ allora $U \cup V \in r^{-1}(\mathcal{F})$ e per la massimalità di U vale $V \subset U$ e quindi $r(U) = r(V)$. □

ESERCIZIO 9: Unione finita di spazi Noetheriani è Noetheriana.

Definizione 2.3. Uno spazio topologico si dice **irriducibile** se ogni coppia di aperti nonvuoti ha intersezione non vuota. Equivalentemente uno spazio è irriducibile se non è unione finita di chiusi propri.

Un sottospazio di uno spazio topologico si dice irriducibile se è irriducibile per la topologia indotta.

ESERCIZIO 10: In uno spazio di Hausdorff gli unici sottoinsiemi irriducibili sono i punti.

Lemma 2.4. *Sia X spazio topologico e $Y \subset X$ sottospazio irriducibile; allora:*

i) $\overline{Y}$ è irriducibile.

ii) Se $U \subset X$ aperto allora $Y \cap U$ è irriducibile.

iii) Se $f: X \to Z$ è continua allora $f(Y)$ è irriducibile.

Dim. Semplice esercizio. □

Sia F la famiglia dei chiusi irriducibili di uno spazio X (F non è vuota perché contiene le chiusure dei punti), gli elementi massimali di F si dicono le **componenti irriducibili** di X.

ESERCIZIO 11: Sia $Y_i \subset X$ una catena ascendente di sottospazi irriducibili, allora $\cup Y_i$ è irriducibile. Dedurre che ogni chiuso irriducibile è contenuto in una componente irriducibile.

ESERCIZIO 12: Sia $f: X \to Y$ continua ed aperta. Se le fibre di f sono irriducibili e $Z \subset Y$ è irriducibile allora $f^{-1}(Z)$ è irriducibile.

Teorema 2.5. *Sia X uno spazio topologico Noetheriano. Allora:*

a) X possiede un numero finito di componenti irriducibili $X_1, \dots, X_n$.

b) $X = X_1 \cup \dots \cup X_n$.

c) X_i non è contenuto nell'unione delle componenti X_j, $j \neq i$.

Dim. Dimostriamo per cominciare che ogni chiuso di X si può scrivere come unione finita di chiusi irriducibili; a tal fine si consideri la famiglia C di tutti i chiusi di X e la famiglia $F \subset C$ dei chiusi che sono unioni finite di chiusi irriducibili.

Se per assurdo $F \neq C$, esiste $Z \in C - F$ minimale; Z non è irriducibile e quindi esistono chiusi propri Z_1, Z_2 tali che $Z = Z_1 \cup Z_2$. Per la minimalità di Z si ha che $Z_1, Z_2 \in F$ e quindi anche $Z \in F$.

Possiamo quindi scrivere $X = X_1 \cup \dots \cup X_n$ con X_i chiuso irriducibile in modo tale che la condizione c) sia soddisfatta; rimane quindi da dimostrare che $X_1, \dots, X_n$ sono tutte e sole le componenti irriducibili di X.

Sia $Z \subset X$ un chiuso irriducibile, allora $Z = (Z \cap X_1) \cup \dots \cup (Z \cap X_n)$, tutti i chiusi $Z \cap X_i$ non possono essere propri ed esiste i tale che $Z \subset X_i$. In particolare ogni componente irriducibile è uguale ad un X_i.

Viceversa se X_i non è massimale esiste una inclusione propria $X_i \subset Z$ con Z irriducibile; per l'argomento precedente Z è contenuto in qualche X_j in contraddizione con c). □

Definizione 2.6. Sia X uno spazio topologico e $p \in X$. La **dimensione di Krull**

$$\dim_p X \in \mathbb{N} \cup \{\infty\}$$

di X nel punto p è per definizione l'estremo superiore dell'insieme dei numeri naturali n tali che esiste una catena $p \in Z_n \subset Z_{n-1} \subset \dots \subset Z_0 \subset X$ dove Z_i sono chiusi irriducibili e $Z_i \neq Z_{i-1}$ per ogni i.

Si definisce poi la dimensione di X, $\dim X$ come l'estremo superiore delle dimensioni nei suoi punti. Uno spazio avente la stessa dimensione in tutti i suoi punti è detto equidimensionale o di dimensione pura.

Sebbene la 2.6 ha senso per qualsiasi spazio topologico, essa perde tutto il suo significato geometrico e la sua utilità se applicata a spazi di Hausdorff (con l' ovvia eccezione degli insiemi finiti). Per tale motivo da ora in poi studieremo la dimensione di Krull esclusivamente per spazi Noetheriani.

Lemma 2.7. *La dimensione di Krull è monotona sui sottospazi, cioè se $p \in Y \subset X$ allora* $\dim_p Y \leq \dim_p X$.

Dim. Sia $Z \subset Y$ chiuso irriducibile e $\overline{Z}$ la chiusura di Z in X. Siccome $Z = Y \cap \overline{Z}$ la chiusura in X trasforma inclusioni proprie di chiusi irriducibili di Y in inclusioni proprie di chiusi irriducibili in X. □

Lemma 2.8. *La dimensione è un invariante locale, cioè se $U \subset X$ è un intorno di p vale* $\dim_p U = \dim_p X$.

Dim. Per 2.7 non è restrittivo supporre U aperto, se $p \in Z \subset X$ è un chiuso irriducibile e $Z \cap U = Z_1 \cup Z_2$ con Z_1, Z_2 chiusi di U, allora $Z = (Z - U) \cup \overline{(Z \cap U)} = Z = (Z - U) \cup \overline{Z_1} \cup \overline{Z_2}$ e dato che $p \notin Z - U$ si ha che $Z = \overline{Z_i}$ per qualche i. In particolare $Z \cap U$ è irriducibile e la restrizione ad U trasforma inclusioni proprie di chiusi irriducibili di X contenenti p in inclusioni proprie di chiusi irriducibili di U. □

Essendo la definizione puramente topologica la dimensione di Krull è invariante per omeomorfismo.

Un utile lemma è il seguente:

Lemma 2.9. *Siano $p \in Y \subset X$ con X irriducibile e Y chiuso in X. Se* $\dim_p Y = \dim_p X < \infty$ *allora $Y = X$.*

Dim. Esercizio. □

Attenzione: esistono spazi Noetheriani di dimensione infinita (vedi esercizi).

Lemma 2.10. *Sia $f: X \to Y$ applicazione continua, chiusa e surgettiva tra spazi topologici Noetheriani, $y \in Y$. Allora per ogni intero $n > 0$ esiste $x \in X$, dipendente da n, tale che $f(x) = y$ e $\dim_x X \geq \min(\dim_y Y, n)$.*
In particolare $\dim X \geq \dim Y$ e se $f^{-1}(f(x)) = \{x\}$ allora $\dim_x X \geq \dim_{f(x)} Y$.

Dim. Per ogni catena finita $y \in Z_n \subset ... \subset Z_0$ di chiusi irriducibili di Y costruiamo una catena $H_n \subset ... \subset H_0$ di chiusi irriducibili di X tali che $f(H_i) = Z_i$. Sia $W = f^{-1}(Z_0)$, essendo W un chiuso in uno spazio Noetheriano esso è unione di un numero finito di componenti irriducibili W_j. I chiusi $f(W_j)$ ricoprono Z_0, per l'irriducibilità esiste un indice j_0 tale che $f(W_{j_0}) = Z_0$. Basta quindi porre $H_0 = W_{j_0}$, ripetere il ragionamento per Z_1 e cosi via. □

3. La dimensione dello spazio affine

Dimostriamo adesso che la dimensione di $\mathbb{A}^n$ è uguale a n. Tale risultato, associato all'esistenza delle proiezioni normalizzate, permetterà di trovare una utile caratterizzazione della dimensione dei chiusi affini e proiettivi.

Lemma 3.1. *$X \subset \mathbb{A}^n$ è irriducibile se e solo se $I(X)$ è un ideale primo.*

Dim. Se $X = X_1 \cup X_2$ con X_i chiusi propri esistono $f_i \in I(X_i) - I(X)$, $i = 1, 2$. Chiaramente $f_1 f_2 \in I(X)$ e quindi $I(X)$ non è primo.
Viceversa se $f_1, f_2 \notin I(X)$ e $f_1 f_2 \in I(X)$ allora $X = X_1 \cup X_2$ dove $X_i = X \cap V(f_i)$ è un chiuso proprio e X non è irriducibile. □

Corollario 3.2. *$\mathbb{A}^n$ è uno spazio topologico Noetheriano irriducibile*

Dim. $I(\mathbb{A}^n) = 0$ è un ideale primo. □

Definizione 3.3. Sia $X \subset \mathbb{A}^n$ un chiuso, la proiezione lineare sulle prime $s \leq n$ coordinate $\mathbb{A}^n \to \mathbb{A}^s$ si dice **normalizzata** rispetto a X se per ogni $i = s+1, s+2, .., n$ esiste $f_i \in I(X) \cap \mathbb{K}[x_1, ..., x_s][x_i] \subset \mathbb{K}[x_1, ..., x_n]$ monico rispetto alla variabile x_i.
Segue dal lemma III.3.4 e da una semplice induzione su $n - s$ che se $\pi: \mathbb{A}^n \to \mathbb{A}^s$ è normalizzata rispetto a X allora $\pi: X \to \mathbb{A}^s$ è un'applicazione chiusa e $I(\pi(X)) = I(X) \cap \mathbb{K}[x_1, ..., x_s]$.

Lemma 3.4. *Si assuma che la proiezione sulle prime coordinate $\pi: \mathbb{A}^n \to \mathbb{A}^{n-1}$ sia normalizzata rispetto ad un chiuso irriducibile nonvuoto $X \subset \mathbb{A}^n$. Per ogni chiuso proprio $Z \subset X$ vale $\pi(Z) \neq \pi(X)$.*

Dim. La proiezione $\pi: X \to \mathbb{A}^{n-1}$ è chiusa, dato che $\pi(X)$ è irriducibile e Z è unione finita di irriducibili non è restrittivo supporre Z irriducibile e nonvuoto.
Siccome $I(X) \subset I(Z)$ sono ideali primi, $1 \notin I(Z)$ e $I(X)$ contiene un polinomio monico in x_n per il corollario III.1.11 si ha $I(\pi(X)) = I(X) \cap \mathbb{K}[x_1, ..., x_{n-1}] \neq I(\pi(Z)) = I(Z) \cap \mathbb{K}[x_1, ..., x_{n-1}]$. □

Proposizione 3.5. *Nelle notazioni del lemma 3.4 per ogni punto $p \in X$ vale $\dim_p X \leq \dim_{\pi(p)} \pi(X)$.*

Dim. Per 3.4 la proiezione π manda inclusioni proprie di chiusi irriducibili di X contenenti p in inclusioni proprie di chiusi irriducibili di $\pi(X)$ contenenti $\pi(p)$. □

Siamo adesso in grado di provare il

Teorema 3.6. *La dimensione di $\mathbb{A}^n$ è uguale a n.*

Dim. Dato che le traslazioni sono omeomorfismi lo spazio affine è equidimensionale, cioè ha la stessa dimensione in ogni punto.
Esiste una ovvia catena di chiusi irriducibili $0 = Z_n \subset ... \subset Z_1 \subset Z_0 = \mathbb{A}^n$ dove $Z_i = \{x_1 = .. = x_i = 0\}$, vale quindi $\dim_0 \mathbb{A}^n \geq n$. Gli unici chiusi propri irriducibili di $\mathbb{A}^1$ sono i punti, quindi il teorema è vero per $n = 1$; per induzione possiamo supporre il teorema vero per $\mathbb{A}^{n-1}$.
Rimane da dimostrare che per ogni chiuso proprio irriducibile $X \subset \mathbb{A}^n$ si ha $\dim X < n$, a meno di un cambio lineare di coordinate la proiezione $\pi: \mathbb{A}^n \to \mathbb{A}^{n-1}$ è normalizzata rispetto a X e per 2.10, 3.5 si ha $\dim X = \dim \pi(X) \leq \dim \mathbb{A}^{n-1} = n - 1$.
□

La dimostrazione di 3.6 fornisce anche una ricetta per il calcolo della dimensione di un chiuso affine X; basta infatti eseguire una serie di proiezioni $\pi_1: \mathbb{A}^n \to \mathbb{A}^{n-1}$, $..., \pi_{s+1}: \mathbb{A}^{s+1} \to \mathbb{A}^s$ normalizzate rispetto a X, $\pi_1(X)$, etc... in modo tale che $\pi_{s+1}(...(\pi_1(X))...) = \mathbb{A}^s$. La dimensione di X sarà quindi uguale a s.

Concludiamo il paragrafo analizzando in dettaglio il caso delle ipersuperfici. Abbiamo già osservato che $V(f)$ è irriducibile se e solo se f è irriducibile. In generale se $f_1, ..., f_r$ sono i fattori irriducibili di f vale $V(f) = V(f_1) \cup ... \cup V(f_r)$. Se $f_i \neq f_j$ per $i \neq j$ allora le $V(f_i)$ sono esattamente le componenti irriducibili di $V(f)$.

Proposizione 3.7. *Sia $X \subset \mathbb{A}^n$ una ipersuperfice, $p \in X$, allora $\dim_p X = n - 1$. Viceversa se $X \subset \mathbb{A}^n$ è un chiuso irriducibile di dimensione $n - 1$ allora X è un'ipersuperfice.*

Dim. Dato che tutte le componenti irriducibili di X sono ipersuperfici non è restrittivo supporre $X = V(f)$ irriducibile. Se $n = 1$ l'asserto è banale, sia dunque $n > 1$ e H

un iperpiano affine passante per p e non contenuto in X. L'intersezione $X \cap H$ è una ipersuperficie in $H = \mathbb{A}^{n-1}$ e per induzione

$$n - 2 = \dim_p X \cap H < \dim_p X < n = \dim \mathbb{A}^n.$$

Se $X \subset \mathbb{A}^n$ è irriducibile di dimensione $n-1$ l'ideale $I(X) \neq 0$ è primo e contiene un polinomio irriducibile f. Dunque $X \subset V(f)$ e $\dim X = \dim V(f) < \infty$. Dato che $V(f)$ è irriducibile si ha $X = V(f)$ per 2.9. □

4. Intersezione con ipersuperfici e dimensione delle fibre

Una delle caratteristiche fondamentali degli spazi considerati nella geometria algebrica classica (pre teoria degli schemi) è che ogni punto possiede un sistema fondamentale di intorni omeomorfi a chiusi affini. D'altra parte ogni chiuso affine può essere pensato come un aperto di un chiuso proiettivo; è quindi possibile studiare le proprietà locali, come ad esempio la dimensione in un punto, restringendosi all'insieme dei chiusi proiettivi.

Osserviamo innanzitutto che il gruppo delle proiettività agisce transitivamente su $\mathbb{P}^n$ e che quindi $\dim \mathbb{P}^n = \dim_p \mathbb{P}^n$ per ogni punto p. Siccome ogni punto possiede un intorno omeomorfo ad $\mathbb{A}^n$ si deduce immediatamente il

Teorema 4.1. *Lo spazio proiettivo $\mathbb{P}^n$ dotato della topologia di Zariski è uno spazio irriducibile Noetheriano di dimensione pura n.*

Uno dei vantaggi dei chiusi proiettivi è la mancanza di asintoti e quindi la normalizzazione automatica delle proiezioni.

Lemma 4.2. *Sia $X \subset \mathbb{P}^n$ chiuso, $H \subset \mathbb{P}^n$ iperpiano, $o \notin X \cup H$ e $\pi\colon (\mathbb{P}^n - o) \to H$ la proiezione di centro o. Allora $\pi(X)$ è chiuso, $\dim X = \dim \pi(X)$, $\dim_p X \leq \dim_{\pi(p)} \pi(X)$ per ogni $p \in X$ e vale $\dim_p X = \dim_{\pi(p)} \pi(X)$ se X non interseca la retta $\overline{op}$ al di fuori di p.*

Dim. Siano $x_0, ..., x_n$ coordinate omogenee su $\mathbb{P}^n$ tali che $o = [1, 0, .., 0]$ e $H = \{x_0 = 0\}$, la proiezione si esprime in coordinate omogenee $\pi([x_0, ..., x_n]) = [x_1, ..., x_n]$.

Dato che $o \notin X$ esiste un polinomio omogeneo $f \in I(X)$ tale che $f(o) \neq 0$, necessariamente f è monico in x_0, basta quindi applicare i risultati del paragrafo precedente alle restrizioni $\pi_i\colon X \cap \mathbb{A}^n_i \to H \cap \mathbb{A}^n_i = \mathbb{A}^{n-1}$ dove $\mathbb{A}^n_i = \{x_i \neq 0\}$ per ogni $i = 1, .., n$. □

Nel seguente corollario useremo la convenzione che la dimensione dell'insieme vuoto è -1.

Corollario 4.3. *Sia $X \subset \mathbb{P}^n$ chiuso e $\mathcal{F}$ la famiglia dei sottospazi proiettivi di $\mathbb{P}^n$ che non intersecano X. Se $K \in \mathcal{F}$ è un elemento massimale rispetto all'inclusione allora $\dim X + \dim K = n - 1$.*

Dim. Il risultato è banalmente vero se $X = \emptyset, \mathbb{P}^n$ e se $n = 1$. Sia $X \neq \emptyset, \mathbb{P}^n$, prendiamo un punto $o \in K$ e sia $\pi\colon X \to \mathbb{P}^{n-1}$ la proiezione di centro o; per il lemma precedente X e $\pi(X)$ hanno la stessa dimensione e $\dim \pi(K) = \dim K - 1$.

Dato che $\pi(K)$ è chiaramente massimale tra i sottospazi di $\mathbb{P}^{n-1}$ che non intersecano $\pi(X)$ l'induzione su n conclude la dimostrazione. □

Lemma 4.4. *Sia $X \subset \mathbb{P}^n$ chiuso di dimensione $\leq n - 2$, $p \in X$. Esiste un punto $o \neq p$ tale che la retta $\overline{op}$ interseca X solamente nel punto p.*

Dim. Per il corollario precedente esiste una retta L che non interseca X, sia P il piano generato dalla retta L e dal punto p, dato che $(X \cap P) \cap L = \emptyset$ sempre per 4.3 la dimensione di $X \cap P$ è uguale a 0. Dunque $X \cap P$ è un insieme finito di punti ed esistono al più finiti punti $o \in L$ che non soddisfano la condizione richiesta. □

Teorema 4.5. *Sia $X \subset \mathbb{P}^n$ chiuso, H iperpiano e $p \in X \cap H$. Allora:*

a) Sia $p \in Z \subset X$ chiuso irriducibile, allora $\dim_p X \geq \dim Z$. In particolare se X è irriducibile vale $\dim_p X = \dim X$.

b) $\dim_p X \cap H \geq \dim_p X - 1$.

Dim. Se il teorema vale per ogni componente irriducibile di X allora vale anche per X, non è quindi restrittivo assumere X chiuso proprio irriducibile e $Z = X$.

Se $n = 1$ il teorema è evidente, per induzione su n possiamo assumere vero il teorema per chiusi di $\mathbb{P}^{n-1}$. Se X è una ipersuperficie abbiamo già dimostrato che $\dim_p X = \dim X = n - 1$ e $X \cap H$ è ancora una ipersuperfice e quindi $\dim_p X \cap H \geq n - 2$.

Se X non è una ipersuperfice allora per 4.4 ha dimensione $< n - 1$ ed esiste una proiezione $\pi\colon X \to \mathbb{P}^{n-1}$ tale che $\pi^{-1}(\pi(p)) = p$ e per induzione su n si ha

$$\dim_p X = \dim_{\pi(p)} \pi(X) = \dim \pi(X) = \dim X.$$

Sia $Y = X \cap H$, se $X = Y$ il punto 2) è banale, se Y è un chiuso proprio di X allora $\dim Y < \dim X$ e quindi $\dim Y \leq \dim H - 2$. Per 4.4 esiste una proiezione $\pi\colon X \to \mathbb{P}^{n-1}$ di centro $o \in H$ tale che $\pi^{-1}(\pi(p)) = p$. Dunque $\dim_p Y = \dim_{\pi(p)} \pi(Y)$ e la conclusione segue osservando che $\pi(Y)$ è una sezione iperpiana di $\pi(X)$. □

Grazie alla mappa di Veronese che sappiamo essere una immersione chiusa possiamo generalizzare immediatamente e senza fatica i precedenti risultati alle intersezioni di chiusi di $\mathbb{P}^n$ con ipersuperfici. Infatti se $X, V(f) \subset \mathbb{P}^n$ con f polinomio omogeneo di

grado d, possiamo estendere f ad una base $f = f_0, f_1, ..., f_s$ di S_d e considerare la mappa di Veronese $v: \mathbb{P}^n \to \mathbb{P}^s$ data da $v = (f_0, f_1, .., f_s)$.

Allora $v(X \cap V(f))$ è omeomorfo all'intersezione di $v(X)$ con l'iperpiano di $\mathbb{P}^s$ di equazione $y_0 = 0$, si ha quindi in particolare:

Corollario 4.6. *Sia $X \subset \mathbb{P}^n$ chiuso e $H \subset \mathbb{P}^n$ ipersuperfice, allora se $\dim X > 0$ vale $X \cap H \neq \emptyset$ e per ogni $p \in X \cap H$ si ha $\dim_p X \cap H \geq \dim_p X - 1$.*

Corollario 4.7.(Versione geometrica del teorema dell'ideale principale di Krull) *Sia $p \in X \subset \mathbb{A}^n$ chiuso e $p \in H$ ipersuperfice affine. Allora $\dim_p X \cap H \geq \dim_p X - 1$.*

Dim. Immergiamo $\mathbb{A}^n$ in uno spazio proiettivo $\mathbb{P}^n$ e prendiamo le chiusure di X e H. Basta osservare adesso che la chiusura proiettiva di una ipersuperfice è ancora una ipersuperfice, più precisamente se $f \in \mathbb{K}[x_1, ..., x_n]$ ha grado d e $H = V(f)$, la chiusura di H in $\mathbb{P}^n$ è l'ipersuperfice definita dall'omogeneizzato di f in $\mathbb{K}[x_0, x_1, ..., x_n]$. □

Teorema 4.8. *Sia $p \in X \subset \mathbb{A}^n$ chiuso affine, le dimensione di X nel punto p è uguale al minimo intero s tale che esistono s polinomi $f_1, ..., f_s \in \mathbb{K}[x_1, ..., x_n]$ ed un intorno $p \in U \subset X$ tali che $U \cap V(f_1, ..., f_s) = p$.*

Dim. Sia s definito come sopra, per il corollario 4.7 $s \geq \dim_p X$. Viceversa se $\dim_p X = d > 0$ possiamo prendere un iperpiano $H_1 = V(f_1)$ passante per p non contenente nessuna componente irriducibile di X. Avremo $\dim_p X \cap H_1 = \dim_p X - 1$, iterando il ragionamento con $X \cap H_1$ al posto di X possiamo trovare d iperpiani $H_1, .., H_d$ tali che $dim_p X \cap H_1 \cap ... \cap H_d = 0$ e quindi $d \geq s$. □

Nota: Il teorema 4.8 è la versione geometrica del teorema [A-M, 11.14] di algebra commutativa secondo il quale la dimensione di un anello locale Noetheriano con ideale massimale $\mathfrak{m}$ è uguale al minimo numero di generatori di un ideale $\mathfrak{m}$-primario.

Il seguente teorema è noto come teorema sulla dimensione delle fibre ed è la versione moderna dell'ottocentesco **principio di Plücker-Clebsch** sul quale rimandiamo a [E-C, Libro I, p. 149] per maggiori informazioni.

Teorema 4.9. *Sia $X \subset \mathbb{A}^m \times \mathbb{P}^n$ un chiuso, $\pi: X \to \mathbb{A}^m$ la proiezione sul primo fattore. Per ogni $q \in \mathbb{A}^m$ denotiamo $X_q = \pi^{-1}(q) = X \cap \{q\} \times \mathbb{P}^n$.*

a) Per ogni $p \in X$, $q = \pi(p)$ vale $\dim_p X \leq \dim_p X_q + \dim_q \pi(X)$.

b) Gli insiemi $Y_h = \{q \in \mathbb{A}^n \mid \dim X_q \geq h\}$ sono chiusi di Zariski.

c) Se X è irriducibile esiste $q \in \pi(X)$ tale che $\dim X_q = \dim X - \dim \pi(X)$.

Si noti che per i punti a) e b) i punti $q \in \pi(X)$ come al punto c) formano un aperto denso di $\pi(X)$.

Dim. a) Sia $r = \dim_q \pi(X)$, esistono allora r iperpiani $H_1, .., H_r$ di $\mathbb{A}^m$ passanti per q tali che q è un punto isolato di $\pi(X) \cap H_1 \cap ... \cap H_r$; si ha quindi $\dim_p X_q = \dim_p X \cap H_1 \times \mathbb{P}^n \cap ... \cap H_r \times \mathbb{P}^n$ e dato che $H_i \times \mathbb{P}^n$ sono iperpiani si ha che $\dim_p X_q \geq \dim_p X - r$.

b) Sappiamo che π è una applicazione chiusa, per ogni sottoinsieme $Z \subset \pi(X)$ si definisce $d_Z = \min_{q \in Z} \dim X_q$.

Poniamo $X_0 = X$, $Z_0 = \pi(X)$ e sia $q \in Z_0$ tale che $\dim X_q = d_{Z_0}$. Sia $H \subset \mathbb{P}^n$ un sottospazio massimale che non interseca X_q e poniamo $Z_1 = \pi(X_0 \cap \mathbb{A}^m \times H)$, $X_1 = \pi^{-1}(Z_1)$.

Segue immediatamente dalla costruzione che, se $Z_0 \neq \emptyset$, Z_1 è un chiuso proprio di Z_0 e che $\dim X_q = d_{Z_0}$ per ogni $q \in Z_0 - Z_1$.

Ripetiamo il procedimento con X_1, Z_1 al posto di X_0, Z_0 e costruiamo X_2, Z_2 al posto di X_1, Z_1. Iterando il procedimento troviamo una catena discendente di chiusi $...Z_i \subset ... \subset Z_1 \subset Z_0$ con le proprietà che $Z_{i+1} \neq Z_i$, eccetto il caso in cui $Z_i = \emptyset$, e $\dim X_q = d_{Z_i}$ per ogni $q \in Z_i - Z_{i+1}$. Per Noetherianità $Z_i = \emptyset$ per $i >> 0$ e gli insiemi Y_h corrispondono ai chiusi Z_i nei quali $d_{Z_i} > d_{Z_{i-1}}$.

c) Dimostriamo il risultato per induzione su $r = \dim \pi(X)$. Se $r = 0$ allora $\pi(X)$ è un punto e l'asserto è banale. Sia assuma $r > 0$ e sia $s = \dim X$. Sia $H \subset \mathbb{A}^m$ un iperpiano tale che $\emptyset \neq H \cap \pi(X) \neq \pi(X)$, per il corollario 4.7 ogni componente irriducibile di $\pi(X) \cap H$ (risp. $X \cap H \times \mathbb{P}^n$) ha dimensione $r - 1$ (risp. $s - 1$). Sia Z una componente irriducibile fissata di $\pi(X) \cap H$ e scriviamo $X \cap H \times \mathbb{P}^n = X_1 \cup .. \cup X_a \cup Y_1 \cup .. \cup Y_b$ dove X_i, Y_j sono le componenti irriducibili divise in modo tale che $\pi(X_i) = Z$, $\pi(Y_j) \neq Z$. Dato che π è chiusa e Z è irriducibile necessariamente $a > 0$.

Per l'ipotesi induttiva per ogni $i = 1, .., a$ esiste un aperto $U_i \subset Z$ tale che le fibre di X_i sopra U_i hanno dimensione esattamente $s - r$. Per qualsiasi punto $q \in (U_1 \cap .. \cap U_a) - (\pi(Y_1) \cup ... \cup \pi(Y_b))$ vale $\dim X_q = s - r$. □

Proviamo infine un utile corollario di 4.9.

Corollario 4.10. *Nelle notazioni di 4.9 se $Y = \pi(X)$ è irriducibile e le fibre X_q, $q \in Y$, sono tutte irriducibili della stessa dimensione allora X è irriducibile.*

Dim. Siano $Z_1, ..., Z_a, W_1, ..., W_b$ le componenti irriducibili di X ordinate in modo tale che $\pi(Z_i) = Y$, $\pi(W_i) \neq Y$ e $\dim Z_1 \geq \dim Z_i$ per ogni i. Proviamo che $X = Z_1$.

Dato che Y è irriducibile e π è chiusa deve essere $a > 0$, denotiamo con s, r le dimensioni di Z_1, Y rispettivamente.

Per 4.9 esiste un aperto $U \subset Y$ tale che per ogni $q \in U$ vale $(W_i)_q = \emptyset$ e $\dim(Z_i)_q = \dim Z_i - r$, in particolare ne segue che la dimensione delle fibre X_q è esattamente $s - r$.

Dato che le fibre X_q sono per ipotesi tutte irriducibili, $(Z_1)_q \subset X_q$ e $\dim(Z_1)_q \geq s - r = \dim X_q$ per ogni $q \in Y$ si ha che $Z_1 = X$. □

Come primo esempio di applicazione dei precedenti risultati proviamo che, fissato un intero $n > 1$, le curve piane singolari di grado n formano una ipersuperficie irriducibile Y nello spazio proiettivo delle curve piane di grado n $|\mathcal{O}(n)| = \mathbb{P}^N$, $N = \frac{1}{2}n(n+3)$.
Si consideri infatti l'insieme $X \subset \mathbb{P}^2 \times \mathbb{P}^N$ formato dalle coppie (p, C) tali che p è un punto singolare di C. Si vede facilmente che X è un chiuso, infatti la coppia di punti di coordinate omogenee $([x], [F])$, con F equazione di C, appartiene a X se e solo se $F(x) = F_0(x) = F_1(x) = F_2(x) = 0$.
Fissato un punto $p \in \mathbb{P}^2$ le curve piane singolari in p formano un sistema lineare di dimensione $N-3$, per i teoremi 4.9 e 4.10 applicati alla proiezione $X \to \mathbb{P}^2$, o più precisamente alle restrizioni agli aperti affini di $\mathbb{P}^2$, abbiamo che X è irriducibile di dimensione $N-1$.
La fibra di $\pi: X \to \mathbb{P}^N$ sopra la curva C consiste nell'insieme dei punti singolari di C, e siccome esiste almeno una curva di grado n con un punto singolare, per 4.9 ricaviamo che $Y = \pi(X)$ è un chiuso irriducibile di dimensione $N-1$ e quindi una ipersuperfice.
Altre più significative applicazioni di 4.9 e 4.10 saranno esposte prossimamente utilizzando il linguaggio delle varietà algebriche.

5. Esercizi complementari

ESERCIZIO 13: Nelle notazioni del corollario 1.3, se $n = 2, r = 1$ e f_0, f_1 sono senza fattori comuni determinare la dimensione del conucleo di ϕ_d per $d >> 0$.

ESERCIZIO 14: Provare che l'immagine della mappa di Veronese è intersezione di quadriche.

ESERCIZIO 15: Si consideri l'applicazione $\phi: \mathbb{A}^1 \to \mathbb{A}^3$, $\phi(t) = (t, t^2, t^3)$; provare che $X = \phi(\mathbb{A}^1)$ è chiuso e si determini $I(X)$.

ESERCIZIO 16: Enunciare il teorema degli zeri di Hilbert per $\mathbb{P}^n \times \mathbb{P}^m$.

ESERCIZIO 17: Sia $X = X_1 \cup X_2$ con X_1, X_2 aperti irriducibili. X è irriducibile se e solo se $X_1 \cap X_2 \neq \emptyset$.

ESERCIZIO 18: Uno spazio Noetheriano di Hausdorff è finito.

ESERCIZIO 19: Uno spazio topologico si dice Artiniano se ogni famiglia di aperti contiene un elemento minimale. Sia X uno spazio topologico Artiniano, provare che:

i) X contiene un numero finito di punti chiusi.

ii) Ogni chiuso di X è unione finita di componenti irriducibili.

iii) Se X è irriducibile, l' unione dei chiusi propri di X è un chiuso proprio.

iv) (*) Se X è anche Noetheriano allora contiene un numero finito di aperti. (Sugg. uno spazio Artiniano con infiniti chiusi contiene una catena discendente non stazionaria di chiusi)

ESERCIZIO 20: Mostrare che esistono spazi topologici Noetheriani e spazi topologici Artiniani di dimensione infinita.

ESERCIZIO 21: (Spazi di Zariski).
Ricordiamo che uno spazio topologico X si dice T_0 se dati $x \neq y \in X$ si ha $\overline{x} \neq \overline{y}$. Un punto $x \in X$ si dice generico se $\overline{x} = X$. Condizione necessaria affinché esista un punto generico è che X sia irriducibile; se X è T_0 esiste al più un punto generico.
Sia X spazio topologico e per ogni chiuso $C \subset X$ sia $t(C)$ l'insieme dei chiusi irriducibili contenuti in C. Provare:
1) Gli insiemi $t(C)$, $C \subset X$ chiuso, sono i chiusi di una topologia T_0 su $t(X)$.
2) Si consideri l'applicazione naturale $\phi: X \to t(X)$, $\phi(x) = \overline{x}$; vale $\phi^{-1}(t(C)) = C$ per ogni chiuso $C \subset X$, ne segue che ϕ è continua, $\phi(X)$ è denso in $t(X)$ ed è iniettiva se e solo se X è T_0.
3) Se X è irriducibile (risp. Noetheriano) allora $t(X)$ è irriducibile (risp. Noetheriano).
4) Uno spazio topologico si dice **spazio di Zariski** se è T_0, Noetheriano ed ogni chiuso irriducibile contiene un punto generico. Se X è Noetheriano allora $t(X)$ è di Zariski e se X è di Zariski allora ϕ è un omeomorfismo.
5) Ogni applicazione continua $f: X \to Y$ induce una applicazione continua $t(f): t(X) \to t(Y)$ che commuta con $\phi_X: X \to t(X)$ e $\phi_Y: Y \to t(Y)$.

ESERCIZIO 22: Tradurre:
Teorema: Seja E um espaço irredutível e U um aberto não vazio de E. Então, U é denso em E, isto é, o fêcho $\overline{U}$ de U é igual a E.
Demonstração: Se E é aberto e não vazio então, $U = E - F$, onde F é fechado e distinto de E. Como $E = U \cup F = \overline{U} \cup F$ e E é irredutível resulta que $\overline{U} = E$.

ESERCIZIO 23: X spazio topologico Noetheriano, un sottoinsieme $A \subset X$ è aperto se e solo se per ogni chiuso irriducibile $E \subset X$ esiste un sottoinsieme $S \subset E$ aperto in E tale che $A \cap E \subset \overline{S}$. (Sugg. Si consideri la famiglia dei chiusi C di X tali che $C - A$ non è chiuso.)

ESERCIZIO 24: (Lemma di normalizzazione di E. Noether)
a) Siano $\pi_1: \mathbb{A}^n \to \mathbb{A}^s$, $\pi_2: \mathbb{A}^s \to \mathbb{A}^r$ proiezioni normalizzate rispetto a X e $\pi_1(X)$. Allora $\pi_2 \circ \pi_1$ è normalizzata rispetto a X. (Sugg. Estensioni intere per gli esperti, risultante per gli inesperti).
b) Sia $X \subset \mathbb{A}^n$ chiuso di dimensione s, a meno di un cambio lineare di coordinate la proiezione sulle prime s coordinate è normalizzata rispetto a X.

ESERCIZIO 25: (Cono tangente)

Sia $0 \in X \subset \mathbb{A}^n$ un chiuso affine e sia $Y \subset \mathbb{A}^1 \times \mathbb{A}^n$ la chiusura di Zariski dell'insieme delle coppie (t,x) tali che $t \neq 0$ e $tx \in X$. Si definisce $C_0(X) = Y \cap \{0\} \times \mathbb{A}^n$; provare:

i) Y è il luogo di zeri dei polinomi $f(t,x) = g(tx)$ al variare di g in $I(X)$ e $C_0(X) = V(J)$ dove J è l'ideale generato dalle forme iniziali dei polinomi di $I(X)$. (Se $f = f_m + f_{m+1} + ...$ con f_i omogeneo di grado i e $f_m \neq 0$, la forma iniziale di f è per definizione f_m).

ii) Se $0 \in H$ è un sottospazio lineare allora $C_0(X \cap H) = C_0(X) \cap H$.

iii) $\dim_0 X = \dim_0 C_0(X)$.

iv) Mostrare con un esempio che, fissati $g_1, ..., g_r \in I(X)$ generatori, in generale $C_0(X)$ non è definito dalle parti iniziali di $g_1, ..., g_r$.

Il cono $C_0(X)$ si dice *cono tangente* a X nel punto 0.

ESERCIZIO 26: (Lo scoppiamento)

Sia $0 \in X \subset \mathbb{A}^n$ un chiuso, $Y = X - \{0\}$, $\tilde{Y} \subset (\mathbb{A}^n - \{0\}) \times \mathbb{P}^{n-1}$ l'insieme dei punti $\{(y, [y])\}$ al variare di $y \in Y$.

i) Provare che $\tilde{Y}$ è un chiuso omeomorfo a Y. (Sugg. considerare dapprima il caso $X = \mathbb{A}^n$).

Sia $\tilde{X} \subset \mathbb{A}^n \times \mathbb{P}^{n-1}$ la chiusura di Zariski di $\tilde{Y}$ e sia $E = \{0\} \times \mathbb{P}^{n-1} \cap \tilde{X}$.

ii) Descrivere esplicitamente $\tilde{X}$ ed E nei casi $X = \mathbb{A}^n$ e X ipersuperficie.

iii) Se $X = X_1 \cup X_2$ con X_i chiusi contenenti 0 allora $\tilde{X} = \tilde{X}_1 \cup \tilde{X}_2$.

iv) Provare che $\dim_0 X = \dim E + 1$.

v) Il cono affine di E coincide con il cono tangente $C_0(X)$

ESERCIZIO 27: Sia $\pi: \mathbb{A}^n \to \mathbb{A}^m$, $n > m$, la proiezione sulle prime coordinate e sia $s: \mathbb{A}^m \to \mathbb{A}^n$ la sezione nulla $s(x_1, ..., x_m) = (x_1, ..., x_m, 0, .., 0)$.

Per ogni chiuso $X \subset \mathbb{A}^n$ mostrare che la funzione $q \to \dim_{s(q)}(X \cap \pi^{-1}(q))$ è semicontinua superiormente.(Sugg. scoppiamento lungo la sezione).

ESERCIZIO 28: Siano $X, Z \subset \mathbb{A}^m \times \mathbb{P}^n$ chiusi, si definisce il prodotto fibrato di X e Z sopra $\mathbb{A}^m$ come

$$W = X \times_{\mathbb{A}^m} Z = \{(y,x,z) \in \mathbb{A}^m \times \mathbb{P}^n \times \mathbb{P}^n \,|\, (y,x) \in X, (y,z) \in Z\}$$

Provare che W è chiuso. Dire a cosa corrispondono le fibre delle proiezioni naturali $W \to X$, $W \to Z$ e $W \to \mathbb{A}^m$.

ESERCIZIO 29: $(\star)$ Nelle stesse notazioni del teorema 4.9 si provi che la funzione $p \to \dim_p X_{\pi(p)}$ è semicontinua superiormente su X. (Sugg. usare i due esercizi precedenti).

ESERCIZIO 30: Sia $X \subset \mathbb{A}^n$ un chiuso e $\pi: \mathbb{A}^n \to \mathbb{A}^{n-1}$ la proiezione sulle prime $n-1$ coordinate.

Sia $f = \sum_{i \geq 0} g_i(x_1, ..., x_{n-1}) x_n^{d-i} \in I(X)$, allora $D(g_0) \cap \pi(X)$ è chiuso in $D(g_0) = \mathbb{A}^{n-1} - V(g_0)$. Dedurre che $\pi(X)$ contiene un aperto di $Y = \overline{\pi(X)}$. (Sugg. Si può ripetere sostanzialmente la dimostrazione del lemma di proiezione oppure si può considerare $\tilde{X} \subset \mathbb{A}^n \times \mathbb{A}$ definito da $I(X)$ e $1 - tg_0$ e $tf \in I(\tilde{(X)})$.)

ESERCIZIO 31: Provare che $\mathbb{A}^2$ e $\mathbb{P}^2$, dotati della topologia di Zariski, non sono omeomorfi. Più in generale se $n \geq 2$ e $X \subset \mathbb{P}^n$ chiuso di dimensione $\leq n-3$ si provi che $\mathbb{A}^n$ e $\mathbb{P}^n - X$ non sono omeomorfi.

ESERCIZIO 32: Sia $\mathbb{P}^{14} = |\mathcal{O}(4)|$ lo spazio proiettivo delle quartiche piane. Sia $U \subset \mathbb{P}^{14}$ l'insieme delle quartiche liscie C tali che per ogni $p \in C$ e per ogni retta $L \subset \mathbb{P}^2$ si ha $\nu_p(C, L) \leq 3$. Provare che U è un aperto nonvuoto.

ESERCIZIO 33: Sia $X \subset \mathbb{A}^3$ il chiuso definito dalle equazioni $xy - z^2 = y^3 - x^5 = 0$. Provare che X ha due componenti irriducibili.

ESERCIZIO 34: Caratteristica 0. Sia $F(x_1, ..., x_n)$ un polinomio omogeneo di grado $m > 0$; poniamo $C = V(F) \subset \mathbb{A}^n$, $\mathcal{A}$ l'insieme dei sottospazi affini di $\mathbb{A}^n$ contenuti in C e definiamo C_0 come l'intersezione dei sottospazi in $\mathcal{A}$ che sono massimali rispetto all'inclusione. Provare:

i) C_0 è un sottospazio affine contenente l'origine $(0, ..., 0)$.

ii) A meno di un cambio lineare di coordinate si può assumere che esista $s \leq n$ tale che $\frac{\partial F}{\partial x_i} = 0$ per ogni $i > s$ e $\frac{\partial F}{\partial x_1}, ..., \frac{\partial F}{\partial x_s}$ linearmente indipendenti in $\mathbb{K}[x_1, ..., x_n]$.

iii) $(\star)$ In un sistema di coordinate come al punto ii) vale $C_0 = \{x_1 = ... = x_s = 0\}$.

ESERCIZIO 35: $(\star\star)$ Sia $\mathbb{K} = \mathbb{C}$, $X \subset \mathbb{C}^n$ un chiuso irriducibile di Zariski e $U \subset X$ un aperto nonvuoto di Zariski. Provare che la chiusura di U nella topologia classica è uguale a X.

(Sugg. Provare l'esercizio dapprima nel caso $X = \mathbb{C}^n$, dopodiché considerare una proiezione normalizzata e ripetere il ragionamento fatto nella dimostrazione del lemma degli archi selezionati. Per un altra dimostrazione vedi [Mu, Th. 2.33])

ESERCIZIO 36: $(\star\star?)$ Sia $\mathbb{K} = \mathbb{C}$, $X \subset \mathbb{C}^n$ un chiuso di Zariski dotato della topologia classica: allora ogni punto di X è un retratto per deformazione di un suo intorno.

IX. Varietà algebriche: nozioni base

Quando si parla di varietà si intende generalmente uno spazio topologico dotato di strutture accessorie. Lo scopo principale di questo capitolo è quello di mostrare che i sottoinsiemi localmente chiusi di $\mathbb{P}^n$, oltre alla topologia di sottospazio, ereditano anche una struttura di "varietà quasiproiettiva".
Iniziamo questo viaggio studiando alcune possibili strutture sui chiusi affini; per tutto il capitolo assumeremo salvo avviso contrario che $\mathbb{K}$ sia un campo fissato algebricamente chiuso.

1. Applicazioni regolari tra chiusi affini

Sia $X \subset \mathbb{A}^n$ un chiuso, una funzione $f: X \to \mathbb{K}$ si dice **regolare** se è la restrizione di una funzione polinomiale su $\mathbb{A}^n$, più precisamente f è regolare se esiste $F \in \mathbb{K}[x_1, ..., x_n]$ tale che $F(x) = f(x)$ per ogni $x \in X$.
Le funzioni regolari su X formano una $\mathbb{K}$-algebra $\mathbb{K}[X]$, il morfismo naturale di restrizione $\mathbb{K}[x_1, ..., x_n] \to \mathbb{K}[X]$ è surgettivo per definizione ed ha come nucleo esattamente l'ideale $I(X)$.

Esempio 1.1. Sia $X \subset \mathbb{A}^2$ la curva di equazione $x_1^2 = x_2^3$; l'applicazione $\phi: \mathbb{K} \to X$, $\phi(t) = (t^3, t^2)$ è un omeomorfismo ma $\phi^{-1}: X \to \mathbb{K}$ non è regolare. Infatti se esistesse $P \in \mathbb{K}[x, y]$ tale che $P(x) = \phi^{-1}(x)$ per ogni $x \in X$ si avrebbe $P(t^3, t^2) = t$ per ogni $t \in \mathbb{K}$.

Se X è un chiuso affine $\mathbb{K}[X]$ è una $\mathbb{K}$-algebra finitamente generata senza nilpotenti ed è quindi Noetheriana. Viceversa se A è una $\mathbb{K}$-algebra finitamente generata senza nilpotenti si può scrivere $A = \mathbb{K}[x_1, ..., x_n]/J$ con $J = \sqrt{J}$ e quindi $A = \mathbb{K}[X]$ dove $X = V(J) \subset \mathbb{A}^n$.
Le funzioni regolari su un chiuso affine X sono continue, in particolare per ogni ideale $J \subset \mathbb{K}[X]$ l'insieme $V_X(J) = \{x \in X \mid f(x) = 0 \ \forall f \in J\}$ è un chiuso di X. Viceversa se $Z \subset X$ chiuso si definisce $I_X(Z) \subset \mathbb{K}[X]$ come l'ideale delle funzioni regolari che si annullano su Z; detta $\pi: \mathbb{K}[x_1, ..., x_n] \to \mathbb{K}[X]$ la proiezione naturale i seguenti fatti sono di semplice verifica:

1) $V_X(J) = V(\pi^{-1}(J))$ per ogni ideale $J \subset \mathbb{K}[X]$.

2) $\pi^{-1}(I_X(Z)) = I(Z)$ per ogni $Z \subset X$.

3) $\pi^{-1}(\sqrt{J}) = \sqrt{\pi^{-1}(J)}$ per ogni ideale $J \subset \mathbb{K}[X]$ (qui bisogna usare il fatto che $\mathbb{K}[X]$ è ridotta, cioè senza nilpotenti).

Dalle precedenti proprietà 1) 2) e 3) segue che i chiusi di X sono tutti e soli in sottoinsiemi $V_X(J)$ per J ideale di $\mathbb{K}[X]$ e che le corrispondenze V_X, I_X soddisfano proprietà analoghe a quelle di V e I definite sullo spazio affine. In particolare $V_X(I_X(Z)) = Z$ per ogni $Z \subset X$ chiuso e vale il

Teorema 1.2.(degli zeri) *Sia X un chiuso affine e $J \subset \mathbb{K}[X]$ un ideale, allora vale l'uguaglianza $I_X(V_X(J)) = \sqrt{J}$. In particolare gli ideali massimali di $\mathbb{K}[X]$ sono tutti e soli quelli della forma $I_X(x)$, $x \in X$.*

Dim. Evidente. □

Come prima conseguenza di 1.2 osserviamo che se $F, G \in \mathbb{K}[x_1, ..., x_n]$ e $G(x) \neq 0$ per ogni $x \in X$ allora la restrizione di G a X è invertibile in $\mathbb{K}[X]$ e quindi la funzione $f(x) = F(x)G(x)^{-1}$ è regolare su X.

Se $f \in \mathbb{K}[X]$ l'aperto $X_f = \{x \in X \mid f(x) \neq 0\}$ si dice un **aperto principale** di X. Per ogni ideale $J \subset \mathbb{K}[X]$ si ha $X - V_X(J) = \cup_{f \in J} X_f$ e quindi gli aperti principali formano una base per la topologia di X.

ESERCIZIO 1: $f, g \in \mathbb{K}[X]$, allora $X_f \subset X_g$ se e solo se g divide una potenza di f.

Definizione 1.3. Siano $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ chiusi, una applicazione $f: X \to Y$ si dice **regolare** se è la restrizione di una applicazione polinomiale $F: \mathbb{A}^n \to \mathbb{A}^m$. In altri termini f è regolare se e solo se esistono $F_1, ..., F_m \in \mathbb{K}[x_1, .., x_n]$ tali che $f(x) = (F_1(x), ..., F_m(x))$ per ogni $x \in X$. È tautologico osservare che se $f = (f_1, ..., f_m)$, $f_i: X \to \mathbb{K}$ allora f è regolare se e solo se f_i è regolare per ogni i. Le applicazioni regolari sono continue.

Denotiamo con $\mathbb{K}^X$ (risp. $\mathbb{K}^Y$) la $\mathbb{K}$-algebra di tutte le funzioni su X (risp. Y) a valori in $\mathbb{K}$. Ogni applicazione $f: X \to Y$ definisce per composizione un morfismo di $\mathbb{K}$-algebre $f^*: \mathbb{K}^Y \to \mathbb{K}^X$.

Lemma 1.4. *Nelle notazioni precedenti una applicazione $f: X \to Y$ è regolare se e solo se $f^*\mathbb{K}[Y] \subset \mathbb{K}[X]$.*

Dim. Siano $y_1, ..., y_n \in \mathbb{K}[Y]$ le restrizioni a Y delle coordinate sullo spazio affine $\mathbb{A}^m$, detto $f_i = f^*y_i$ si ha $f = (f_1, .., f_m)$ e f è regolare se e solo se $f^*y_i \in \mathbb{K}[X]$ per ogni i. Basta adesso osservare che le y_i generano $\mathbb{K}[Y]$ come $\mathbb{K}$-algebra. □

Proposizione 1.5. *Siano X, Y chiusi affini, esiste una bigezione naturale tra l'insieme dei morfismi regolari $f: X \to Y$ e l'insieme dei morfismi di $\mathbb{K}$-algebre $f^*: \mathbb{K}[Y] \to \mathbb{K}[X]$.*

Dim. Si assuma $Y \subset \mathbb{A}^m$, $\pi: \mathbb{K}[\mathbb{A}^m] \to \mathbb{K}[Y]$ la proiezione naturale e siano $y_1, ..., y_m \in \mathbb{K}[\mathbb{A}^m]$ le coordinate affini. Preso un omomorfismo di $\mathbb{K}$-algebre $\phi: \mathbb{K}[Y] \to \mathbb{K}[X]$ siano $f_i = \phi\pi(y_i)$, l'applicazione $f = (f_1, ..., f_m): X \to \mathbb{A}^m$ è regolare e $f^* = \phi\pi$.

Se $g \in I(Y)$ allora $f^*g = 0$ e quindi $f(X) \subset V(g)$, quindi l'immagine di f è contenuta in Y. Lasciamo per esercizio la semplice verifica che l'applicazione $\phi \to f$ così definita è l'inversa della applicazione $f \to f^*$. □

Definizione 1.6. Un morfismo regolare tra chiusi affini si dice un **isomorfismo regolare** se è bigettivo con inverso regolare.

Corollario 1.7. *Un morfismo regolare $f: X \to Y$ tra chiusi affini è un isomorfismo se e solo se $f^*: \mathbb{K}[Y] \to \mathbb{K}[X]$ è un isomorfismo.*

Dim. Immediata conseguenza di 1.5. □

Esempio 1.8. La retta $\mathbb{A}^1$ e l'iperbole $X = V(xy - 1) \subset \mathbb{A}^2$ non sono isomorfe. Infatti, se lo fossero avremo un isomorfismo di $\mathbb{K}$-algebre $\mathbb{K}[t] = \mathbb{K}[\mathbb{A}^1] = \mathbb{K}[X] = \mathbb{K}[x, y]/(xy - 1)$ e questo non è possibile dato che x è invertibile in $\mathbb{K}[X]$ mentre ogni invertibile di $\mathbb{K}[\mathbb{A}^1]$ è costante.

Esempio 1.9. Sia $X \subset \mathbb{A}^n$ chiuso affine e $f: X \to \mathbb{A}^m$ applicazione regolare. Sia $Y = \{(x, f(x)) \in \mathbb{A}^{n+m} \mid x \in X\}$ il grafico di f e $\pi: Y \to X$ la proiezione. Allora Y è chiuso e π è un isomorfismo regolare.

Infatti se $x_1, ..., x_n$ sono le coordinate su $\mathbb{A}^n$ e $y_1, ..., y_m$ sono le coordinate su $\mathbb{A}^m$ e posto $f_i = f^*y_i$ si ha che $Y = V(J)$ dove $J \subset \mathbb{K}[x_1, .., x_n, y_1, ..., y_m]$ è l'ideale generato da $I(X)$ e $y_i - f_i$ e quindi Y è chiuso. La proiezione π è evidentemente regolare e bigettiva con inversa $\pi^{-1} = (x_1, ..., x_n, f_1, ..., f_m)$ regolare.

ESERCIZIO 2: Nelle notazioni di 1.9 provare che $J = I(Y)$.

ESERCIZIO 3: $f: X \to Y$ regolare. Provare che:

i) $f(X)$ è denso in Y se e solo se f^* è iniettiva.

ii) $f(X) \subset V_Y(\ker f^*)$.

iii) Se f^* è surgettiva allora f è una immersione chiusa.

iv) Mostrare con un esempio che il viceversa del punto iii) è generalmente falso.

Esempio 1.10. Sia $X \subset \mathbb{A}^n$ chiuso, $f \in \mathbb{K}[X]$ e $Y = \{(x, t) \in \mathbb{A}^{n+1} \mid x \in X, tf(x) = 1\}$. $Y = V(I(X), 1 - tf)$ è un chiuso e la proiezione $\pi: Y \to X$ induce una bigezione tra Y e l'aperto principale X_f. Il morfismo $\pi^*: \mathbb{K}[X] \to \mathbb{K}[Y]$ ha le seguenti proprietà:

1) $h = \pi^*(f)$ è invertibile in $\mathbb{K}[Y]$.

2) Per ogni $g \in \mathbb{K}[Y]$ vale $h^s g \in \pi^*\mathbb{K}[X]$ per $s >> 0$.

3) $\pi^*(a) = 0$ se e solo se $f^s a = 0$ per $s >> 0$.

La verifica di 1) e 3) è immediata in quanto $ht = 1$ e $\pi^*(a) = 0$ se e solo se $a(x) = 0$ per ogni $x \in X_f$.

Il morfismo $\mathbb{K}[X][t] \to \mathbb{K}[Y]$ è surgettivo e quindi ogni $g \in \mathbb{K}[Y]$ si può esprimere come un polinomio nella variabile t a coefficienti in $\pi^*\mathbb{K}[X]$ ed il punto 2) segue dal fatto che $ht = 1$.

Possiamo decomporre il morfismo $\pi^* = \beta\alpha$ con $\alpha: \mathbb{K}[X] \to \mathbb{K}[X][t]/(1-tf)$ morfismo naturale e $\beta: \mathbb{K}[X][t]/(1-tf) \to \mathbb{K}[Y]$. Si osserva che il morfismo α soddisfa le stesse proprietà 1), 2) e 3) di π^*. Le proprietà 1) e 2) sono banali, dimostriamo che vale 3). Se $f^s a = 0$ per $s >> 0$ allora $a = (1-tf)(\sum_{i\geq 0} t^i f^i a)$ e quindi $\alpha(a) = 0$. Viceversa se $\alpha(a) = 0$ allora esistono $b_0, ..., b_s \in \mathbb{K}[X]$ tali che $a = (1-tf)(\sum b_i t^i)$ e quindi $b_0 = a$, $b_1 = fa, ..., b_s = f^s a$, $f^{s+1}a = 0$.

Possiamo adesso provare che β è un isomorfismo: dato che π^* soddisfa 2) si ha che β è surgettiva. Se $\beta(g) = 0$ allora esiste $s > 0$ tale che $f^s g = \alpha(h)$ con $\pi^*(h) = 0$ e quindi esiste $r > 0$ tale che $f^r h = 0$. A maggior ragione $f^{s+r} g = 0$ e dato che f è invertibile in $\mathbb{K}[X][t]/(1-tf)$ necessariamente $g = 0$ e β risulta iniettiva.

L'esempio 1.10 rende doveroso richiamare le nozioni di base sulla localizzazione degli anelli commutativi con unità; per ulteriori approfondimenti rimandiamo ai testi di algebra commutativa.

Sia A un anello, un sottoinsieme $S \subset A$ si dice una parte moltiplicativa se $1 \in S$ e S è chiuso per il prodotto, cioè se $st \in S$ ogniqualvolta $t, s \in S$.

Data una parte moltiplicativa $S \subset A$ si definisce $S^{-1}A$ come il quoziente di $A \times S$ per la relazione: $(a, s) \sim (b, t)$ se e solo se esiste $r \in S$ tale che $r(at - bs) = 0$. Per comprensibili motivi si denota con $\frac{a}{s} \in S^{-1}A$ la classe di equivalenza della coppia (a, s). Lasciamo per esercizio al lettore la verifica che $\sim$ è una relazione di equivalenza e che $S^{-1}A$ è un anello commutativo con zero $\frac{0}{1}$ e unità $\frac{1}{1}$ rispetto alle operazioni

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}$$

Si noti che $S^{-1}A = 0$ se e solo se $1 = 0$ in $S^{-1}A$ se e solo se $0 \in S$.

È consuetudine denotare:

i) $S^{-1}A = A_P$ se $S = A - P$ con P ideale primo.

ii) $S^{-1}A = A_f$ se $S = \{f^s\}_{s\geq 0}$ con $f \in A$.

iii) $S^{-1}A = Fraz(A)$ se $S = A - \{$ divisori di $0\}$.

L'anello $Fraz(A)$ si dice anello delle frazioni globali di A e coincide con il campo delle frazioni quando A è un dominio di integrità.

Esiste un omomorfismo naturale di anelli $l: A \to S^{-1}A$, $l(a) = \frac{a}{1}$; è immediato verificare che

1) $l(s)$ è invertibile in $S^{-1}A$ per ogni $s \in S$.

2) Per ogni $g \in S^{-1}A$ vale $l(s)g = l(a)$ per qualche $s \in S$, $a \in A$.

3) $l(a) = 0$ se e solo se $sa = 0$ per qualche $s \in S$.

ESERCIZIO 4: L'omomorfismo l è iniettivo se e solo se S non contiene divisori di 0; l è isomorfismo se e solo se ogni elemento di S è invertibile in A.

Teorema 1.11. *Sia $S \subset A$ parte moltiplicativa e $\phi: A \to B$ un morfismo di anelli tale che:*

1) $\phi(s)$ è invertibile per ogni $s \in S$.

Allora esiste unico un morfismo $\beta: S^{-1}A \to B$ tale che $\phi = \beta l$.

Se inoltre vale:

2) Per ogni $b \in B$ vale $\phi(s)b = \phi(a)$ per qualche $s \in S$, $a \in A$.

3) $\phi(a) = 0$ se e solo se $sa = 0$ per qualche $s \in S$.

Allora β è un isomorfismo.

Dim. Si assuma 1), se esiste β deve necessariamente essere $\beta(\frac{a}{s}) = \phi(a)\phi(s)^{-1}$ e quindi β è unico. Inoltre se $(a, s) \sim (b, t)$ allora $\phi(a)\phi(s)^{-1} = \phi(b)\phi(t)^{-1}$ e quindi la precedente è una buona definizione di β.

Se vale 1) e 2) è evidente che β è surgettiva. La condizione 3) equivale a dire che ϕ e l hanno lo stesso nucleo, dunque se vale 1) e 3) e $\beta(\frac{a}{s}) = 0$ allora $\phi(a) = 0$ e $\frac{a}{s} = \frac{1}{s} l(a) = 0$. □

ESERCIZIO 5: Sia $I \subset S^{-1}A$ un ideale e sia $E \subset A$ un insieme di generatori di $l^{-1}(I)$. Mostrare che $l(E)$ genera I; in particolare se A è Noetheriano allora anche $S^{-1}A$ è Noetheriano.

La stesso argomento usato nell'esempio 1.10 mostra che per ogni anello A e $f \in A$ vale $A_f = A[t]/(1-tf)$.

Si consideri adesso un chiuso affine X ed un aperto $U \subset X$, si definisce $\mathcal{O}_X(U) \subset \mathbb{K}^U$ come la sottoalgebra delle funzioni che sono localmente quoziente di funzioni regolari su X, più precisamente $f: U \to \mathbb{K}$ appartiene a $\mathcal{O}_X(U)$ se e solo se per ogni $x \in U$ esiste un intorno $x \in V \subset U$ e funzioni regolari $F, G \in \mathbb{K}[X]$ tali che per ogni $y \in V$ vale $G(y) \neq 0$ e $f(y) = \frac{F(y)}{G(y)}$.

Definizione 1.12. L'applicazione $\mathcal{O}_X: \{$ aperti di $X\} \to \{\mathbb{K}$-algebre $\}$ si dice **fascio strutturale** di X.

Il fascio strutturale è caratterizzato dalle seguenti proprietà:

F1) Per ogni coppia di aperti $V \subset U$ la esiste un morfismo di $\mathbb{K}$-algebre $\rho_V^U: \mathcal{O}_X(U) \to \mathcal{O}_X(V)$; se $W \subset V \subset U$ sono aperti allora $\rho_W^U = \rho_W^V \rho_V^U$ e $\rho_U^U = Id$.

I morfismi ρ_V^U sono indotti dalla restrizione delle funzioni all'aperto V, scriveremo spesso $f_{|V}$ al posto di $\rho_V^U(f)$.

F2) Se $U = \cup_{i\in I} U_i$ è un ricoprimento aperto, $f \in \mathcal{O}_X$ è tale che $f_{|U_i} = 0$ per ogni $i \in I$ allora $f = 0$.

F3) Se $U = \cup_{i\in I} U_i$ è un ricoprimento aperto e $f_i \in \mathcal{O}_X(U_i)$, $i \in I$, sono tali che $f_{i|U_i\cap U_j} = f_{j|U_i\cap U_j}$ per ogni $i,j \in I$ allora esiste $f \in \mathcal{O}_X(U)$ tale che $f_{|U_i} = f_i$ per ogni i.

Le condizioni F1), F2) e F3) si dicono **assiomi di fascio.** Più in generale ogni applicazione definita sugli aperti di uno spazio topologico a valori gruppi abeliani che soddisfa i tre assiomi si dice un fascio.

Si noti che la funzione f come al punto F3) è unica in obbedienza al punto F2). La condizione F1) esprime il fatto che, se pensiamo gli aperti di X come gli oggetti di una categoria i cui morfismi sono le inclusioni, allora $\mathcal{O}_X$ è un funtore controvariante.

Non è difficile calcolare $\mathcal{O}_X(U)$ per gli aperti principali.

Teorema 1.13. *Sia X chiuso affine, $f \in \mathbb{K}[X]$. Allora $\mathcal{O}_X(X_f) = \mathbb{K}[X]_f = \mathbb{K}[X][t]/(1-tf)$. In particolare per $f = 1$ si ottiene $\mathcal{O}_X(X) = \mathbb{K}[X]$.*

Dim. Basta verificare che il morfismo naturale $\phi\colon \mathbb{K}[X] \to \mathcal{O}_X(X_f)$ soddisfa le condizioni 1), 2) e 3) del teorema 1.11 rispetto alla parte moltiplicativa $\{f^n\}_{n\geq 0}$. La 1) e la 3) sono immediate in quanto $f^s \in \mathcal{O}_X(X_f)$ per ogni $s \in \mathbb{Z}$ e $\phi(a) = 0$ se e solo se $a(x) = 0$ per ogni $x \in X_f$ e quindi se e solo se $af^s = 0$ per qualche $s \geq 0$.

Rimane da dimostrare che se $g \in \mathcal{O}_X(X_f)$ allora $f^s g \in \mathbb{K}[X]$ per $s >> 0$. Per definizione di $\mathcal{O}_X$ esiste un ricoprimento aperto $X_f = \cup_{i\in I} U_i$ e funzioni regolari $F_i, G_i \in \mathbb{K}[X]$ tali che, se $x \in U_i$ allora $G_i(x) \neq 0$ e $gG_i(x) = F_i(x)$. Non è restrittivo assumere gli aperti U_i principali, diciamo $U_i = X_{u_i}$ e a meno di considerare $F_i u_i$ e $G_i u_i$ al posto di F_i, G_i possiamo assumere che $gG_i = F_i$ su tutto X. Infine X_f è quasi compatto e possiamo supporre il ricoprimento finito e $I = \{1,\dots,r\}$.

Dato che $V(G_1,\dots,G_r) \subset V(f)$ per il teorema degli zeri esiste $s > 0$ ed una relazione $f^s = \sum H_i G_i$, $H_i \in \mathbb{K}[X]$. Moltiplicando ambo i membri per g si ottiene $f^s g = \sum H_i G_i g = \sum H_i F_i \in \mathbb{K}[X]$. □

Chiameremo quindi $\mathcal{O}_X(U)$ algebra delle funzioni regolari su U; in generale non si tratta di una $\mathbb{K}$-algebra finitamente generata.

Proposizione 1.14. *Siano X, Y chiusi affini e $f\colon X \to Y$ continua.*

Se f è regolare allora $f^*\mathcal{O}_Y(U) \subset \mathcal{O}_X(f^{-1}(U))$ per ogni aperto $U \subset Y$.

Se $Y = \cup U_i$ è un ricoprimento aperto e $f^*\mathcal{O}_Y(U_i) \subset \mathcal{O}_X(f^{-1}(U_i))$ per ogni i allora f è regolare.

Dim. Se f è regolare allora f^* trasforma funzioni localmente quoziente di elementi di $\mathbb{K}[Y]$ in funzioni localmente quoziente di elementi di $f^*\mathbb{K}[Y] \subset \mathbb{K}[X]$ e quindi $f^*\mathcal{O}_Y(U) \subset \mathcal{O}_X(f^{-1}(U))$ per ogni aperto $U \subset Y$.

Viceversa sia $g \in \mathbb{K}[Y]$, allora $(f^*g)_{|f^{-1}(U_i)} = f^*(g_{|U_i}) \in \mathcal{O}_X(f^{-1}(U_i))$ e per l'assiome F3) si ha $f^*g \in \mathcal{O}_X(X) = \mathbb{K}[X]$. Dunque $f^*\mathbb{K}[Y] \subset \mathbb{K}[X]$ e f è regolare per 1.4. □

Esempio 1.15. Nelle stesse notazioni dell'esempio 1.10 per ogni aperto $U \subset X_f$ l'omomorfismo $\pi^*\colon \mathcal{O}_X(U) \to \mathcal{O}_Y(\pi^{-1}(U))$ è un isomorfismo. Infatti l'applicazione $s\colon X_f \to Y$, $s(x) = (x, f(x)^{-1})$ è l'inversa di π e ogni $g \in \mathbb{K}[Y]$ è rappresentata da un polinomio in t a coefficienti in $\mathbb{K}[X]$ e quindi vale $s^*g = g_1 f^{-s}$ per qualche $g_1 \in \mathbb{K}[X]$, $s \geq 0$.

Quindi s^* trasforma funzioni localmente quoziente di elementi di $\mathbb{K}[Y]$ in funzioni localmente quoziente di elementi di $\mathbb{K}[X]$; da questo segue che per ogni $U \subset X_f$ aperto $s^*\colon \mathcal{O}_Y(s(U)) \to \mathcal{O}_X(U)$ è esattamente l'inverso di $\pi^*\colon \mathcal{O}_X(U) \to \mathcal{O}_Y(\pi^{-1}(U))$.

ESERCIZIO 6: Per ogni $n \geq 2$ vale $\mathcal{O}_{\mathbb{A}^n}(\mathbb{A}^n - \{0\}) = \mathbb{K}[\mathbb{A}^n]$ (Sugg. $\mathbb{K}[\mathbb{A}^n]$ è un dominio a fattorizzazione unica).

Dunque per ogni chiuso affine X si ha $\mathbb{K}[X]_f = \mathcal{O}_X(X_f)$ per ogni $f \in \mathbb{K}[X]$. Sorge spontaneo chiedersi se per ogni ideale primo $P \subset \mathbb{K}[X]$ esiste una descrizione geometrica dell'anello $\mathbb{K}[X]_P$. Daremo adesso una risposta affermativa fornendo una descrizione di $\mathbb{K}[X]_P$ che utilizza il fascio strutturale $\mathcal{O}_X$.

Sia X chiuso affine e $Z \subset X$ un chiuso irriducibile, $P = I_X(Z)$ ideale primo di Z.

Si definisce $\mathcal{O}_{Z,X}$ come l'insieme delle coppie (U,f) con $U \subset X$ aperto tale che $U \cap Z \neq \emptyset$ e $f \in \mathcal{O}_X(U)$ quozientato per la relazione di equivalenza $(U,f) \sim (V,g)$ se esiste un aperto $W \subset U \cap V$ tale che $W \cap Z \neq \emptyset$ e $f_{|W} = g_{|W}$.

L'irriducibilità di Z implica che su $\mathcal{O}_{Z,X}$ è ben definita una struttura di anello rispetto alle operazioni

$$(U,f) + (V,g) = (U \cap V, f+g), \qquad (U,f)(V,g) = (U \cap V, fg)$$

Definiamo inoltre $m_{Z,X} = \{(U,f) \in \mathcal{O}_{Z,X} \mid f_{|Z\cap U} = 0\}$, di nuovo la verifica che si tratta di una buona definizione richiede che Z sia irriducibile. $m_{Z,X}$ è chiaramente un ideale e se $(U,f) \notin m_{Z,X}$ allora $U_f \cap Z \neq \emptyset$ e (U,f) è invertibile in $\mathcal{O}_{Z,X}$ con inverso (U_f, f^{-1}). Questo implica che $\mathcal{O}_{Z,X}$ è un anello locale con ideale massimale $m_{Z,X}$.

Definizione 1.16. Se X è irriducibile si denota $\mathbb{K}(X) = \mathcal{O}_{X,X}$. Il campo $\mathbb{K}(X)$ si chiama **campo delle funzioni razionali** su X. Se $x \in X$ l'anello $\mathcal{O}_{x,X}$ si dice anello dei **germi di funzioni regolari** nel punto x.

Si faccia attenzione al fatto che le cosiddette funzioni razionali su X non sono delle vere funzioni su X ma sono funzioni definite su aperti densi di X. È consuetudine indicare graficamente le funzioni razionali con delle frecce discontinue, $f\colon X \dashrightarrow \mathbb{K}$.

Ogni elemento di $\mathcal{O}_{x,X}$ si rappresenta con una coppia del tipo (X_g, fg^{-1}) con $f, g \in \mathbb{K}[X]$ e $g(x) \neq 0$.

Teorema 1.17. *Per ogni chiuso irriducibile $Z \subset X$ con ideale $P = I_X(Z)$ l'omomorfismo naturale $\phi\colon \mathbb{K}[X] \to \mathcal{O}_{Z,X}$ induce un isomorfismo di $\mathbb{K}$-algebre $\mathbb{K}[X]_P = \mathcal{O}_{Z,X}$.*

Dim. Basta dimostrare che ϕ soddisfa le condizioni 1), 2) e 3) del teorema 1.11 rispetto alla parte moltiplicativa $S = \mathbb{K}[X] - P$. Se $f \in S$ allora $X_f \cap Z \neq \emptyset$ e quindi $\phi(f) = (X, f)$ è invertibile con inverso (X_f, f^{-1}).

Se $\phi(a) = 0$ significa che esiste un aperto U tale che $U \cap Z \neq \emptyset$ e $a(x) = 0$ per ogni $x \in U$. Dato che U è unione di aperti principali non è restrittivo supporre $U = X_f$ per qualche $f \in S$ e quindi $fa = 0$. Viceversa se $af = 0$ per qualche $f \in S$ allora $\phi(a) = (X_f, 0) = 0$.

Sia infine $b \in \mathcal{O}_{Z,X}$, possiamo rappresentare g con una coppia (X_f, g) per qualche $f \in S$ e $g \in \mathcal{O}_X(X_f) = \mathbb{K}[X]_f$; esiste quindi $s > 0$ tale che $gf^s \in \mathbb{K}[X]$ e quindi $b = \phi(gf^s)\phi(f)^{-s}$. □

Corollario 1.18. *Gli anelli $\mathcal{O}_{Z,X}$ sono Noetheriani.*

Dim. Esercizio. □

ESERCIZIO 7: Se $f: X \to Y$ morfismo regolare, $Z \subset X$ chiuso irriducibile e $W = \overline{f(Z)}$ allora è definito $f^*: \mathcal{O}_{W,Y} \to \mathcal{O}_{Z,X}$.

ESERCIZIO 8: X chiuso affine, $U \subset X$ aperto irriducibile. Per ogni aperto $V \subset U$, l'applicazione $\mathcal{O}_X(U) \to \mathcal{O}_X(V)$ è iniettiva.

ESERCIZIO 9: (*) Sia $\pi: X \to Y$ un morfismo regolare di chiusi affini irriducibili. Se $\pi(X)$ è denso in Y allora $\pi(X)$ contiene un aperto.

(Sugg. Ridursi al caso $Y \subset \mathbb{A}^n$, $X \subset \mathbb{A}^{n+s}$ chiusi e π indotta dalla proiezione sulle prime n coordinate. Usare induzione su s.

Se $s = 0$ o se $X = \pi^{-1}(Y)$ non c'è nulla da dimostrare, altrimenti sia $F \neq 0$ appartenente al nucleo di $\mathbb{K}[Y][x_{n+1}, ..., x_{n+s}] \to \mathbb{K}[X]$; se d è il grado di F, a meno di un cambio lineare di coordinate si ha $F = fx_{n+s}^d +$ termini di grado minore in x_{n+s} con $f \in \mathbb{K}[Y]$. Se f è invertibile e $p: \mathbb{A}^{n+s} \to \mathbb{A}^{n+s-1}$ è la proiezione sulle prime coordinate allora $p(X)$ è chiuso. Se f non è invertibile si consideri i chiusi $Y_f \subset \mathbb{A}^{n+1}$ e $X_f \subset \mathbb{A}^{n+1+s}$.)

2. Varietà quasiaffini e quasiproiettive

Sia $X \subset \mathbb{A}^n$ un chiuso e $U \subset X$ un aperto, possiamo definire il fascio strutturale di U, $\mathcal{O}_U$: { aperti di U} $\to$ {$\mathbb{K}$ − algebre} ponendo semplicemente $\mathcal{O}_U(V) = \mathcal{O}_X(V)$ per ogni $V \subset U$ aperto. Si vede subito che $\mathcal{O}_U(V)$ è l'anello delle funzioni $f: V \to \mathbb{K}$ che si esprimono localmente come quoziente di polinomi in $\mathbb{K}[\mathbb{A}^n]$, in particolare $\mathcal{O}_U$ non dipende da X ed è ben definito per ogni $U \subset \mathbb{A}^n$ localmente chiuso.

Definizione 2.1. Se $U \subset \mathbb{A}^n$ è un sottoinsieme localmente chiuso la coppia $(U, \mathcal{O}_U)$ si dice **varietà quasiaffine**.

In modo completamente simile se $X \subset \mathbb{P}^n$ è localmente chiuso si ha, per ogni $V \subset X$ aperto, una $\mathbb{K}$-algebra $\mathcal{O}_X(V) \subset \{f: V \to \mathbb{K}\}$; per definizione $f \in \mathcal{O}_X(V)$ se per ogni $x \in V$ esistono $F, G \in \mathbb{K}[x_0, ..., x_n]$ polinomi omogenei dello stesso grado tali che $G(x) \neq 0$ e $f = \frac{F}{G}$ in un intorno di x. È evidente che la definizione di $\mathcal{O}_X$ non dipende dalla scelta del sistema di coordinate omogenee di $\mathbb{P}^n$.

Definizione 2.2. Se $X \subset \mathbb{P}^n$ è localmente chiuso, la coppia $(X, \mathcal{O}_X)$ si dice **varietà quasiproiettiva**.

Se $x_0, ..., x_n$ sono coordinate omogenee su $\mathbb{P}^n$ e $\mathbb{A}^n = \{x_0 \neq 0\}$ allora $y_i = x_i x_0^{-1}$ sono coordinate affini su $\mathbb{A}^n$. Dati due polinomi $f, g \in \mathbb{K}[y_1, ..., y_n]$, per $d >> 0$

$$\frac{f(y_1, ..., y_n)}{g(y_1, ..., y_n)} = \frac{x_0^d f(x_1 x_0^{-1}, ..., x_n x_0^{-1})}{x_0^d g(x_1 x_0^{-1}, ..., x_n x_0^{-1})} = \frac{F(x_0, ..., x_n)}{G(x_0, ..., x_n)}$$

con F, G polinomi omogenei di grado d. Viceversa dati $F, G \in \mathbb{K}[x_0, ..., x_n]$ omogenei dello stesso grado si ha che

$$\frac{F(x_0, ..., x_n)}{G(x_0, ..., x_n)} = \frac{F(1, y_1 ..., y_n)}{G(1, y_1, ..., y_n)} = \frac{f(y_1, ..., y_n)}{g(y_1, ..., y_n)}$$

Se $X \subset \mathbb{A}^n$ è localmente chiuso, allora X è localmente chiuso anche in $\mathbb{P}^n$ e possiamo considerare X sia come varietà quasiaffine che quasiproiettiva. le precedenti osservazioni su omogeneizzazione e disomogeneizzazione mostrano che il fascio strutturale $\mathcal{O}_X$ non dipende da come si considera X.

Se X è una varietà quasiproiettiva e $U \subset X$ è un aperto, U è a sua volta una varietà quasiproiettiva e $\mathcal{O}_U(V) = \mathcal{O}_X(V)$ per ogni aperto $V \subset U$.

È immediato verificare che per ogni $(X, \mathcal{O}_X)$ quasiproiettiva allora $\mathcal{O}_X$ soddisfa gli assiomi di fascio F1, F2 e F3. Da ora in poi per semplicità notazionale indicheremo una varietà $(X, \mathcal{O}_X)$ solamente con il simbolo X lasciando sottinteso il fascio strutturale.

Abbiamo definito gli oggetti della categoria delle varietà quasiproiettive, definiamo adesso i morfismi in modo tale che la categoria dei chiusi affini definita nel paragrafo 1 sia una sottocategoria piena.

Definizione 2.3. Siano X, Y varietà quasiproiettive, una applicazione $f: X \to Y$ si dice **regolare** o **algebrica** se per ogni aperto $U \subset Y$ e per ogni $x \in f^{-1}(U)$ esiste un aperto $x \in V \subset X$ tale che $f(V) \subset U$ e $f^*_{|V} \mathcal{O}_Y(U) \subset \mathcal{O}_X(V)$.

Si noti che:

1) Le applicazioni regolari sono continue.

2) Per stabilire che $f: X \to Y$ è regolare basta verificare le condizioni di 2.3 per gli aperti U di una base di Y.

3) Una applicazione è regolare se e soltanto se è localmente regolare, cioè $f: X \to Y$ è regolare se e solo se per ogni $x \in X$ esistono aperti $x \in V \subset X$ e $f(x) \in U \subset Y$ tali che $f(V) \subset U$ e $f: V \to U$ è regolare.

4) Una applicazione continua $f: X \to Y$ è regolare se e solo se per ogni aperto $U \subset Y$ si ha $f^*\mathcal{O}_Y(U) \subset \mathcal{O}_X(f^{-1}(U))$.

5) Se $Y \subset X \subset \mathbb{P}^n$ sono sottoinsiemi localmente chiusi allora l'inclusione $Y \to X$ è regolare.

6) Siano X, Y varietà quasiproiettive con $Y \subset \mathbb{P}^n$ localmente chiuso, una applicazione $f: X \to Y$ è regolare se e solo se è regolare la composizione $X \to \mathbb{P}^n$ di f con l'inclusione $Y \to \mathbb{P}^n$.

Definizione 2.4. Un morfismo tra varietà quasiproiettive si dice un **isomorfismo regolare** se è regolare, bigettivo ed ha inverso regolare.

Ad esempio le proiettività sono isomorfismi regolari di $\mathbb{P}^n$.

Definizione 2.5. Una varietà quasiproiettiva si dice **affine** (risp.: **proiettiva**) se è isomorfa ad un chiuso di uno spazio affine (risp.: proiettivo).

Esempio 2.6. Sia $X \subset \mathbb{A}^n$ chiuso e $f \in \mathbb{K}[X]$, la varietà quasiaffine $X_f = X - V(f)$ è affine; essa è infatti isomorfa alla varietà Y degli esempi 1.10 e 1.15.

Lemma 2.7. *Ogni varietà quasiproiettiva possiede una base di aperti affini.*

Dim. Precisiamo che con il termine aperto affine di X intendiamo un aperto che, con la struttura di varietà indotta da X, è una varietà affine.

Sia X una varietà quasiproiettiva, siccome X è unione finita di aperti quasiaffini non è restrittivo assumere $X \subset \mathbb{A}^n$ quasiaffine, sia $\overline{X}$ la chiusura di X in $\mathbb{A}^n$, $Y = \overline{X} - X$. Una base di X è allora data dagli aperti $\overline{X}_f$, $f \in V(Y) \subset \mathbb{K}[\overline{X}]$ che sono affini per 2.6. □

Un utile criterio per stabilire la regolarità di una applicazione è il seguente:

Lemma 2.8. *Sia $f: X \to Y$ applicazione tra varietà quasiproiettive e $Y = \cup Y_i$ ricoprimento di aperti affini.*

Allora f è regolare se e solo se $V_i = f^{-1}(Y_i)$ è aperto per ogni i e $f^*\mathbb{K}[Y_i] \subset \mathcal{O}_X(V_i)$.

Dim. Immediata conseguenza di 1.14. □

ESERCIZIO 10: Sia X varietà quasiproiettiva e Y varietà affine; esiste una bigezione naturale tra l'insieme delle applicazioni regolari $X \to Y$ e l'insieme degli omomorfismi di $\mathbb{K}$-algebre $\mathbb{K}[Y] \to \mathcal{O}_X(X)$.

Esempio 2.9. Siano $F_0, \ldots, F_m \in \mathbb{K}[x_0, \ldots, x_n]$ omogenei dello stesso grado e sia $U \subset \mathbb{P}^n$ un aperto tale che $U \cap V(F_0, \ldots, F_m) = \emptyset$; l'applicazione $F: U \to \mathbb{P}^m$, $F([x]) = [F_0(x), \ldots, F_m(x)]$ è regolare. Viceversa vale il:

Teorema 2.10. *Sia $U = \mathbb{P}^n - Z$ un aperto nonvuoto e sia $\phi: U \to \mathbb{P}^m$ un morfismo regolare. Allora esistono, unici a meno di invertibili, $F_0, \ldots, F_m \in \mathbb{K}[x_0, \ldots, x_n]$ omogenei dello stesso grado e senza fattori comuni tali che $V(F_0, \ldots, F_m) \subset Z$ e $\phi = [F_0, \ldots, F_m]$ (vedi 2.9). In particolare $(n - m - 1) \leq \dim Z$ e ogni automorfismo regolare di $\mathbb{P}^n$ è una proiettività.*

Dim. Dimostriamo per prima cosa che per ogni $p \in U$ esiste un aperto $p \in V \subset U$ tale che l'enunciato del teorema vale per la restrizione di ϕ a V. Prendiamo coordinate omogenee x_i su $\mathbb{P}^n$ e y_j su $\mathbb{P}^m$ tali che $p = [1, 0, \ldots, 0]$ e $\phi(p) = [1, 0, \ldots, 0]$, dunque $p \in \mathbb{A}^n_0 = \{x_0 \neq 0\}$ ed esiste $f \in \mathbb{K}[\mathbb{A}^n_0] = \mathbb{K}[x_1, \ldots, x_n]$ tale che $f(p) \neq 0$, $\mathbb{A}^n_f = \mathbb{A}^n_0 - V(f) \subset U$ e $\phi(\mathbb{A}^n_f) \subset \mathbb{A}^m_0$.

Esistono $g_1, \ldots, g_m \in \mathbb{K}[x_1, \ldots, x_n]$ ed un intero $s > 0$ tali che $\phi^* y_i = \frac{g_i}{f^s}$ per ogni i, a meno di sostituire f^s con f non è restrittivo assumere $s = 1$ e quindi $\phi = [f, g_1, \ldots, g_m]$ su $\mathbb{A}^n_f$. Basta adesso porre $V = \mathbb{A}^n_f$ ed $F_0, \ldots, F_m$ gli omogeneizzati di $f, g_1, \ldots, g_m$ divisi per il loro massimo comune divisore.

Siano adesso $p, q \in U$ e $F_0, \ldots, F_m, G_0, \ldots, G_m \in \mathbb{K}[x_0, \ldots, x_n]$ omogenei tali che:

i) $\deg F_i = \deg F_j$, $\deg G_i = \deg G_j$ per ogni i, j.

ii) $M.C.D.(F_0, \ldots, F_m) = M.C.D.(G_0, \ldots, G_m) = 1$.

iii) $p \notin V(F_0, \ldots F_m)$, $q \notin V(G_0, \ldots, G_m)$.

iv) $\phi = [F_0, \ldots, F_m]$ in un intorno di p e $\phi = [G_0, \ldots, G_m]$ in un intorno di q.

Dato che U è uno spazio irriducibile esiste un aperto $W \subset U$ dove vale $[F_0, \ldots, F_m] = [G_0, \ldots, G_m]: W \to \mathbb{P}^m$ e quindi $F_i G_j = F_j G_i$ per ogni i, j.

Sia $F_0 = \prod H_i^{r_i}$ la decomposizione in fattori irriducibili, esiste allora $j > 0$ tale che H_1 non divide F_j e dato che $H_1^{r_1}$ divide $G_0 F_j = F_0 G_j$ si ha che $H_1^{r_1}$ divide G_0. Ripetendo per ogni fattore irriducibile di F_0 si deduce che F_0 divide G_0 e per simmetria esiste una costante a tale che $F_i = a G_i$ per ogni i.

La disuguaglianza $n - m - 1 \leq \dim_z Z$ segue dal fatto che, detto $Y = V(F_0, \ldots, F_m)$ si ha $Y \subset Z$ e $\dim Y \geq n - m - 1$ per il teorema VIII.4.6.

Un applicazione regolare $[F_0, \ldots, F_n]: \mathbb{P}^n \to \mathbb{P}^n$ può essere un isomorfismo solo se i polinomi F_i hanno grado 1. □

ESERCIZIO 11: Sia $L \subset \mathbb{P}^n$ sottospazio di dimensione $n - m - 1$, la proiezione di centro L, $\mathbb{P}^n - L \to \mathbb{P}^m$ non può essere estesa ad una applicazione regolare su un aperto contenente strettamente $\mathbb{P}^n - L$.

Esempio 2.12.(Le Grassmaniane) Sia V uno spazio vettoriale di dimensione n sul campo $\mathbb{K}$ e sia $0 \leq s \leq n$ un intero. Vogliamo adesso far vedere che esiste una bigezione naturale tra l'insieme $G(s, V)$ dei sottospazi s-dimensionali di V ed una varietà proiettiva irriducibile di dimensione $s(n-s)$ detta Grassmaniana. Mostreremo inoltre che $G(s, V)$ possiede un ricoprimento di aperti isomorfi a $\mathbb{A}^{s(n-s)}$.

Chiaramente se $G(1, V) = \mathbb{P}(V)$, $G(n-1, V) = \mathbb{P}(V^\vee)$ e quindi per $s = 1, n-1$ la situazione è chiara.

In generale sia $X \subset \mathbb{P}(\bigwedge^s V)$ l'insieme delle classi di omotetia dei vettori totalmente decomponibili di $\bigwedge^s V - 0$. Un vettore $v \in \bigwedge^s V$ si dice **totalmente decomponibile** se esistono $v_1, ..., v_s \in V$ tali che $v = v_1 \wedge v_2 \wedge .... \wedge v_s$.

Esiste una bigezione naturale $P: G(s,V) \to X$ data da $P(W) = [w_1 \wedge ... \wedge w_s]$ dove $w_1, ..., w_s$ è una base di W. Se $v_1, ..., v_s$ è un altra base di W si ha $w_1 \wedge ... \wedge w_s = dv_1 \wedge ... \wedge v_s$ dove d è il determinante della matrice di cambiamento di base; questo prova che P, detta **mappa di Plücker**, è ben definita. Lasciamo per esercizio al lettore la semplice verifica che P è bigettiva.

Da ora in poi identifichiamo X e $G(s,V)$ tramite P. Sia $H \subset V$ un sottospazio di dimensione $n-s$ e poniamo $X_H = \{W \in X \,|\, W \cap H = 0\}$.

Fissiamo una base $e_1, ..., e_n$ di V tale che H è generato da $e_{s+1}, ..., e_n$, ogni elemento di $\bigwedge^s V$ si scrive in modo unico come $\sum p_I e_I$, $p_I \in \mathbb{K}$, $I \in \wedge^s\{1, ..., n\}$ dove $\wedge^s\{1, ..., n\}$ indica l'insieme, di cardinalità $\binom{n}{s}$, dei sottoinsiemi di $\{1, ..., n\}$ contenenti s elementi e se $I = \{i_1, ..., i_s\}$ allora $e_I = e_{i_1} \wedge ... \wedge e_{i_s}$.

Le p_I sono coordinate omogenee su $\mathbb{P}(\bigwedge^s V) = \mathbb{P}^N$, $N = \binom{n}{s} - 1$ e sono dette **coordinate Plückeriane** su $G(s,V)$ rispetto alla base $e_1, ..., e_n$.

Sia $I_0 = \{1, 2, ..., s\}$, allora $X_H = \{[p_I] \in X \,|\, p_{I_0} \neq 0\}$, infatti se $W \cap H = 0$ allora esistono unici $v_1, ..., v_s \in H$ tali che W è generato da $e_1 + v_1, ..., e_s + v_s$ e quindi $p_{I_0}(W) \neq 0$. Viceversa se $W \cap H \neq 0$ possiamo prendere una base $w_1, ..., w_s$ di W tale che $w_1 \in H$ e quindi $p_{I_0}(W) = 0$.

Dunque X_H è un aperto in X, dette $y_{i,j}$, $i = 1, ..., s$, $j = s+1, ..., n$ coordinate affini su $\mathbb{A}^{s(n-s)}$ esiste una morfismo regolare bigettivo $f: \mathbb{A}^{s(n-s)} \to X_H \subset \mathbb{P}^N$ dato da

$$f(y_{i,j}) = [(e_1 + \sum_j y_{1,j} e_j) \wedge .... \wedge (e_s + \sum_j y_{s,j} e_j)]$$

Nelle coordinate affini $x_I = p_I p_{I_0}^{-1}$ su $\mathbb{A}^N_{I_0}$ per ogni punto di X_H vale

$$y_{ij} = (-1)^{s-i} x_{\{1,..,i-1,i+1,..,s,j\}}$$

e quindi X_H non è altro che il grafico di una applicazione regolare da $\mathbb{A}^{s(n-s)}$ e $\mathbb{A}^{N-s(n-s)}$, questo prova che X_H è chiuso in $\mathbb{A}^N_{I_0}$ ed è isomorfo come varietà affine a $\mathbb{A}^{s(n-s)}$.

In conclusione si può quindi affermare che X è chiuso in $\mathbb{P}^N$, e dato che $X = \cup X_H$, $H \in G(n-s, V)$ e $X_H \cap X_K \neq \emptyset$ per ogni H, K ne segue che X è pure irriducibile.

Chiameremo in seguito gli aperti $X_H \subset X = G(s,V)$ gli aperti fondamentali della Grassmaniana.

Ulteriori caratteristiche della Grassmaniana e delle coordinate Plückeriane sono esposte negli esercizi.

ESERCIZIO 12: Ogni automorfismo lineare di V induce un automorfismo regolare di $G(s,V)$.

3. Prodotti e morfismi proiettivi

Siano $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ due chiusi con ideali $I(X) \subset \mathbb{K}[x_1, ..., x_n]$, $I(Y) \subset \mathbb{K}[y_1, ..., y_m]$. Denotiamo con $J \subset \mathbb{K}[x_1, ..., x_n, y_1, ..., y_m]$ l'ideale generato da $I(X)$ e $I(Y)$. È immediato osservare che $V(J) = X \times Y \subset \mathbb{A}^{n+m}$.

Lemma 3.1. *Siano X, Y, J come sopra, per ogni $f(x,y) \in \mathbb{K}[x_1, ..., x_n, y_1, ..., y_m]$ possiamo scrivere (in modo non unico)*

$$f(x,y) = \sum_{i=1}^{r} f_i(x) g_i(y) + h(x,y) \qquad (*)$$

con $h \in J$ e $r \geq 0$ minimo possibile.

Detta $\pi: X \times Y \to X$ la proiezione sul primo fattore si ha

$$\pi(\mathbb{A}^{n+m}_f \cap X \times Y) = X \cap (\cup_{i=1}^r \mathbb{A}^n_{f_i})$$

in particolare π è aperta e $J = I(X \times Y)$.

Dim. L'inclusione $\subset$ è ovvia, viceversa sia $p \in X$ tale che $f_r(p) \neq 0$ e si assuma per assurdo che $f(p,y) = 0$ per ogni $y \in Y$, allora $\sum_{i=1}^r f_i(p) g_i(y) \in I(Y)$ e quindi

$$g_r(y) - \frac{1}{f_r(p)} \sum_{i=1}^{r-1} f_i(p) g_i(y) \in I(Y) \subset J$$

Sostituendo in $(*)$ e semplificando si ottiene

$$f(x,y) - \sum_{i=1}^{r-1} (f_i(x) - \frac{f_i(p)}{f_r(p)} g_i(y)) \in J$$

Dato che r era il minimo possibile si ottiene una contraddizione. Se $f \in I(X \times Y)$ si ha $\mathbb{A}^{n+m}_f \cap X = \emptyset$ e quindi necessariamente $r = 0$. □

È utile osservare che, per ogni $f \in \mathbb{K}[X]$, $g \in \mathbb{K}[Y]$, si ha $X_f \times Y_g = (X \times Y)_{fg}$ e quindi $\mathcal{O}_{X\times Y}(X_f \times Y_g)$ è la sottoalgebra di $\mathbb{K}^{X_f \times Y_g}$ generata da $\mathcal{O}_X(X_f)$ e $\mathcal{O}_Y(Y_g)$. Questo prova in particolare che la struttura di varietà su $X \times Y$ non dipende dalla scelta delle immersioni chiuse $X \subset \mathbb{A}^n$ e $Y \subset \mathbb{A}^m$. Più in generale se $U \subset X$ e $V \subset Y$ sono aperti affini e $X_f \subset U$, $Y_g \subset V$ allora $X_f = U_f$, $Y_g = V_g$ e quindi la sottovarietà aperta $U \times V \subset X \times Y$ è isomorfa alla varietà prodotto $U \times V$.

Sia adesso Z una varietà quasiproiettiva, $f: Z \to X \times Y$ una applicazione e $f_X: Z \to X$, $f_Y: Z \to Y$ le composizioni di f con le proiezioni sui fattori.

Dato che $f=(f_1,..,f_{n+m})\colon Z\to X\times Y\subset \mathbb{A}^{n+m}$ è regolare se e solo se $f_i\in \mathcal{O}_Z(Z)$ per ogni i si ha che f è regolare se e solo se f_X e f_Y sono entrambe regolari.

Chiameremo $X\times Y$ **varietà affine prodotto** di X e Y. Se $X'\subset \mathbb{A}^{n'}$, $Y'\subset \mathbb{A}^{m'}$ sono chiusi isomorfi a X e Y rispettivamente allora $X\times Y$ è isomorfa a $X'\times Y'$.

La definizione di varietà prodotto si estende in modo naturale alle varietà quasiaffini. Infatti se $X\subset \mathbb{A}^n$, $Y\subset \mathbb{A}^m$ sono localmente chiusi allora anche $X\times Y$ è localmente chiuso in $\mathbb{A}^{n+m}$ ed eredita una struttura di varietà quasiaffine tale che per ogni coppia di aperti $U\subset X$, $V\subset Y$ la sottovarietà aperta $U\times V\subset X\times Y$ è isomorfa alla varietà prodotto $U\times V$.

La definizione del prodotto di due varietà quasiproiettive richiede lo studio preliminare delle cosiddette immersioni di Segre.

Siano n,m interi positivi fissati, $N=(n+1)(m+1)-1$ e si consideri gli spazi proiettivi $\mathbb{P}^n$, $\mathbb{P}^m$ e $\mathbb{P}^N$ con i rispettivi sistemi di coordinate omogenee x_i, $i=0,..,n$, y_j, $j=0,..,m$ e $w_{i,j}$, $i=0,..,n$ $j=0,..,m$.

La mappa di Segre $s\colon \mathbb{P}^n\times\mathbb{P}^m\to\mathbb{P}^N$ è definita come $s([x],[y])=[w]$, $w_{i,j}=x_iy_j$.

In termini astratti se V,W sono spazi vettoriali la mappa di Segre $s\colon \mathbb{P}(V)\times\mathbb{P}(W)\to \mathbb{P}(V\otimes W)$ si definisce come $s([a],[b])=[a\otimes b]$.

Denotiamo con S l'immagine della mappa di Segre, si ha $s^{-1}(S\cap\{w_{i,j}\neq 0\})=\{x_iy_j\neq 0\}$. Sugli spazi affini

$$\mathbb{A}^n_i=\{[x]\in\mathbb{P}^n|x_i\neq 0\},\qquad \mathbb{A}^m_j=\{[y]\in\mathbb{P}^n|y_j\neq 0\},\qquad \mathbb{A}^N_{i,j}=\{[w]\in\mathbb{P}^n|w_{i,j}\neq 0\}$$

si hanno le coordinate affini $\frac{x_h}{x_i}$, $h\neq i$, $\frac{y_k}{y_j}$, $k\neq j$, $\frac{w_{h,k}}{w_{i,j}}$, $(h,k)\neq(i,j)$ nelle quali la mappa di Segre $s\colon \mathbb{A}^n_i\times\mathbb{A}^m_j\to S\cap\mathbb{A}^N_{i,j}$ si scrive come $\frac{w_{h,k}}{w_{i,j}}=\frac{x_h}{x_i}\frac{y_k}{y_j}$.

In particolare $\frac{w_{h,j}}{w_{i,j}}=\frac{x_h}{x_i}$ e $\frac{w_{i,k}}{w_{i,j}}=\frac{y_k}{y_j}$ e quindi $S\cap\mathbb{A}^N_{i,j}$ è il chiuso definito dalle equazioni $\frac{w_{h,k}}{w_{i,j}}=\frac{w_{h,k}}{w_{h,j}}\frac{w_{i,k}}{w_{i,j}}$ ed è isomorfo, tramite s, a $\mathbb{A}^n_i\times\mathbb{A}^m_j$.

Abbiamo quindi dimostrato la:

Proposizione 3.2. *La mappa di Segre induce una struttura di varietà proiettiva su $\mathbb{P}^n\times\mathbb{P}^m$ tale che le sottovarietà aperte $\{x_iy_j\neq 0\}$ sono isomorfe a $\mathbb{A}^n\times\mathbb{A}^m$.*

Lasciamo per esercizio la verifica che la topologia indotta su $\mathbb{P}^n\times\mathbb{P}^m$ dalla mappa di Segre coincide con la topologia di Zariski degli spazi multiproiettivi definita nel capitolo VIII.

Se $X\subset\mathbb{P}^n$, $Y\subset\mathbb{P}^m$ sono sottoinsiemi localmente chiusi allora anche $X\times Y$ è localmente chiuso in $\mathbb{P}^n\times\mathbb{P}^m$ e quindi anche in $\mathbb{P}^N$.

Definizione 3.3. Date due varietà quasiproiettive $X\subset\mathbb{P}^n$, $Y\subset\mathbb{P}^m$ si definisce la **varietà prodotto** come $X\times Y$ dotata della struttura di varietà quasiproiettiva indotta dall'inclusione $X\times Y\subset\mathbb{P}^n\times\mathbb{P}^m$ e dalla mappa di Segre.

Dalla proprietà della mappa di Segre segue inoltre che se X e Y sono contenuti nel complementare di un iperpiano allora $X\times Y$, pensato come il prodotto di varietà quasiproiettive coincide con il prodotto come varietà quasiaffini; se ne ricava il seguente

Teorema 3.4. *Date due varietà quasiproiettive X e Y esiste una unica struttura di varietà quasiproiettiva su $X\times Y$ tale che se $U\subset X$, $V\subset Y$ sono aperti affini allora $U\times V$ è un aperto affine di $X\times Y$ e $\mathcal{O}_{X\times Y}(U\times V)=\mathbb{K}[U\times V]$ è la sottoalgebra generata da $\mathbb{K}[U]$ e $\mathbb{K}[V]$.*

In particolare per ogni coppia di aperti $X'\subset X$, $Y'\subset Y$ si ha che $X'\times Y'$ è una sottovarietà aperta di $X\times Y$ isomorfa alla varietà prodotto $X'\times Y'$.

Dim. Si osservi innanzitutto che, in virtù degli assiomi di fascio che deve soddisfare $\mathcal{O}_{X\times Y}$, la proprietà espressa in 3.4 implica l'unicità della struttura di varietà su $X\times Y$. Siccome la 3.4 vale se U e V sono contenuti nel complementare di un iperpiano possiamo supporre di aver dimostrato il teorema per gli aperti affini appartenenti a basi fissate di X e Y. Il teorema segue adesso dalle proprietà di incollamento e dall'analogo risultato per il prodotto di varietà affini. □

Vediamo adesso alcune semplici conseguenze di 3.4:

a) La proiezione $X\times Y\to X$ è un morfismo regolare e aperto. Basta infatti ridursi al caso affine e applicare 3.1.

b) Siano X,Y,Z varietà quasiproiettive, $f\colon Z\to X\times Y$ e $f_X\colon Z\to X$, $f_Y\colon Z\to Y$ le composizioni di f con le proiezioni. Allora f è regolare se e solo se f_X e f_Y sono regolari. Di nuovo possiamo ridurre il problema al caso affine.

c) Dati due morfismi regolari $f\colon X\to Z$, $g\colon Y\to W$ il morfismo prodotto $f\times g\colon X\times Y\to Z\times W$ è regolare. Questo segue immediatamente da b).

d) La diagonale $\Delta_X\subset X\times X$ è chiusa. Si verifica direttamente se $X=\mathbb{P}^n$ e in generale se $X\subset\mathbb{P}^n$ si ha che $\Delta_X=\Delta_{\mathbb{P}^n}\cap X\times X$.

e) Dati due morfismi regolari $f,g\colon X\to Y$ ed un sottoinsieme denso $D\subset X$, se $f=g$ su D allora $f=g$. Infatti $(f,g)\colon X\to Y\times Y$ è regolare e $(f,g)^{-1}(\Delta_Y)$ è un chiuso che contiene D.

f) Il grafico $G_f\subset X\times Y$ di un morfismo regolare $f\colon X\to Y$ è chiuso e la proiezione $G_f\to X$ è un isomorfismo. Infatti G_f è la controimmagine di Δ_Y mediante il morfismo $f\times Id_Y$ ed il morfismo $(id,f)\colon X\to G_f$ è l'inverso regolare della proiezione.

La proprietà e) si esprime dicendo che le varietà quasiproiettive sono **separate**.

ESERCIZIO 13: Se U,V sono aperti affini di una varietà X allora $U\cap V$ è affine.

Una variante del prodotto è il prodotto fibrato; dati due morfismi regolari $f\colon X\to Z$ e $g\colon Y\to Z$ si definisce

$$X\times_Z Y=\{(x,y)\in X\times Y|\,f(x)=g(y)\}=(f\times g)^{-1}(\Delta_Z)$$

si tratta evidentemente di una sottovarietà chiusa del prodotto usuale.

Definizione 3.5. Un morfismo di varietà $f: X \to Y$ si dice **proiettivo** se per ogni $y \in Y$ esiste un aperto $y \in U \subset Y$, un intero $n \geq 0$ ed una immersione chiusa $h: f^{-1}(U) \to U \times \mathbb{P}^n$ tale che $f_{|U}$ è la composizione di h e della proiezione sul primo fattore.

Si noti che se X è una varietà proiettiva allora ogni applicazione regolare $X \to Y$ è proiettiva.

ESERCIZIO 14: La composizione di morfismi proiettivi è ancora un morfismo proiettivo.

ESERCIZIO 15: Se $f: X \to Y$ è proiettivo e $g: Z \to Y$ è regolare allora $X \times_Y Z \to Z$ è proiettivo

Proposizione 3.7. *Ogni morfismo proiettivo è chiuso.*

Dim. Siccome la restrizione di un morfismo proiettivo $f: X \to Y$ ad un chiuso di X è ancora proiettivo basta dimostrare che esiste un ricoprimento affine $Y = U_i$ tale che $f(X) \cap U_i = f(f^{-1}(U_i))$ è chiuso in U_i per ogni i. Non è quindi restrittivo assumere $Y \subset \mathbb{A}^m$ chiuso affine e $X \subset Y \times \mathbb{P}^n$; la dimostrazione segue da VIII.1.5 e dal fatto che $Y \times \mathbb{P}^n$ è chiuso in $\mathbb{A}^m \times \mathbb{P}^n$. □

Corollario 3.8. *Sia X una varietà proiettiva irriducibile , allora $\mathcal{O}_X(X) = \mathbb{K}$. Più in generale ogni morfismo da una varietà proiettiva irriducibile ad una varietà affine è costante.*

Dim. Sia $Y \subset \mathbb{A}^n$ una varietà affine e $f: X \to Y$ regolare; componendo f con l'inclusione $Y \subset \mathbb{P}^n$ otteniamo un morfismo proiettivo $g: X \to \mathbb{P}^n$. Per 3.7 $g(X)$ è un chiuso di $\mathbb{P}^n$ che non interseca l'iperpiano all'infinito e quindi deve avere dimensione 0.

Le funzioni regolari su X possono essere pensate come morfismi regolari a valori in $\mathbb{A}^1$. □

Teorema 3.9. *Sia $f: X \to Y$ un morfismo regolare di varietà quasiproiettive; per ogni $y \in Y$ denotiamo $X_y = f^{-1}(y)$. Si ha:*

1) *Per ogni $y \in Y$, $x \in X_y$ vale $\dim_x X \leq \dim_x X_y + \dim_y \overline{f(X)}$.*
2) *Se X è irriducibile esiste un aperto nonvuoto $U \subset f(X)$ tale che per ogni $y \in U$ vale $\dim X = \dim \overline{f(X)} + \dim X_y$.*

Se inoltre f è proiettivo allora vale anche:

3) *L'applicazione $y \to \dim X_y$ è semicontinua superiormente.*
4) *Se Y è irriducibile e le fibre X_y sono tutte irriducibili della stessa dimensione allora X è irriducibile.*

Dim. Possiamo tranquillamente assumere che $f(X)$ sia denso in Y. Proviamo dapprima i 4 enunciati nel caso in cui f è proiettivo; dato che basta dimostrare il teorema

per le restrizioni di f ad un ricoprimento aperto di Y non è restrittivo supporre Y affine e X chiuso in $\mathbb{P}^n \times Y$. Il teorema segue quindi da VIII.4.9 e VIII.4.10.

Se f non è proiettiva si consideri $X \subset \overline{X}$ una chiusura proiettiva (ricordiamo che X è aperto in $\overline{X}$) e sia Z la chiusura del grafico di f in $\overline{X} \times Y$ e $f: Z \to Y$ il morfismo indotto dalla proiezione.

Dato che per ogni $y \in Y$ X_y è un aperto (possibilmente vuoto) di Z_y il punto 1) segue immediatamente dal caso proiettivo. Se X è irriducibile anche Z è irriducibile ed esiste un aperto $U \subset Y$ tale che per ogni $y \in U$ e per ogni $z \in Z_y$ vale $\dim_z Z_y = \dim Z - \dim Y = \dim X - \dim Y$. Siccome $f(X)$ è denso esso interseca U e questo prova il punto 2). □

Corollario 3.10. *Siano X, Y varietà quasiproiettive irriducibili, allora $X \times Y$ è irriducibile e $\dim X \times Y = \dim X + \dim Y$.*

Dim. X e Y sono aperte nelle loro chiusure proiettive, non è quindi restrittivo supporre X e Y proiettive. In questo caso basta applicare 3.9 al morfismo di proiezione $X \times Y \to Y$. □

ESERCIZIO 16: Provare direttamente che se X_i sono le componenti irriducibili di X e Y_j sono le componenti irriducibili di Y allora $X_i \times Y_j$ sono le componenti irriducibili di $X \times Y$.

Corollario 3.11. *Sia $X \subset \mathbb{P}^n$ chiuso e $C(X) \subset \mathbb{A}^{n+1}$ il cono affine. Allora $\dim_0 C(X) = \dim C(X) = \dim X + 1$.*

Dim. Non è restrittivo assumere X irriducibile e non vuoto, dato che $C(X) - 0$ è denso in $C(X)$ basta dimostrare che $C(X) - 0$ è irriducibile di dimensione uguale a $\dim X + 1$.

Sia $p \in C(X) - 0$ e siano $x_0, ..., x_n$ coordinate affini si $\mathbb{A}^{n+1}$ (e quindi omogenee su $\mathbb{P}^n$) tali che $p \in U = X \cap \{x_0 \neq 0\}$. Il morfismo $(x_0, ..., x_n) \to ([x_0, ..., x_n], x_0)$ induce un isomorfismo tra $C(U)$ e $U \times (\mathbb{K} - 0)$; in particolare $C(U)$ è irriducibile di dimensione $\dim X + 1$. Siccome il punto p è arbitrario tutto segue. □

Corollario 3.12. *Siano $X, Y \subset \mathbb{P}^n$ chiusi, allora vale la formula*

$$\dim X \cap Y \geq \dim X + \dim Y - n.$$

Dim. Il cono affine di $X \cap Y$ è isomorfo all'intersezione di $C(X) \times C(Y)$ con la diagonale di $\Delta \subset \mathbb{A}^{n+1} \times \mathbb{A}^{n+1}$. Dato che Δ è intersezione di $n+1$ iperpiani si ha $\dim_0 C(X \cap Y) \geq \dim(C(X) \times C(Y)) - n - 1$. □

ESERCIZIO 17: Sia $X \subset \mathbb{P}^n$ chiuso di dimensione > 0. Provare che $C(X) - 0$ non è isomorfo a $X \times (\mathbb{K} - 0)$.

ESERCIZIO 18: (Teorema di Hopf)

Siano A, B, C spazi vettoriali di dimensione finita su un campo algebricamente chiuso e $\mu: A \otimes B \to C$ lineare e separatamente iniettiva, cioè tale che se $a, b \neq 0$ allora $\mu(a \otimes b) \neq 0$. Provare che $\dim C > \dim B$.

(Sugg. Sia K il nucleo di $A \otimes B \to C$; $\mathbb{P}(K)$ non interseca la varietà di Segre $\mathbb{P}(A) \times \mathbb{P}(B) \subset \mathbb{P}(A \otimes B)$).

4. Punti lisci e singolari, spazio tangente di Zariski

Sia $X \subset \mathbb{A}^n$ un chiuso e $x \in X$, in analogia con il caso delle curve piane diremo che un vettore $v = (v_1, ..., v_n) \in \mathbb{K}^n$ è **tangente** a X nel punto x se per ogni $f \in I(X)$, il polinomio $f_v(t) = f(x+tv)$ ha una radice multipla per $t = 0$. Derivando rispetto a t si ottiene che v è tangente a X in x se e solo se

$$< v, df(x) >= \sum v_i \frac{\partial f}{\partial x_i}(x) = 0, \qquad \text{per ogni } f \in I(X)$$

L'insieme $T_xX \subset \mathbb{K}^n$ dei vettori tangenti a X in x è un sottospazio vettoriale detto **spazio tangente di Zariski**.

Ecco qua alcune semplici osservazioni:

1) Se $x \in X \subset Y$, $X, Y \subset \mathbb{A}^n$ chiusi, allora $I(Y) \subset I(X)$ e $T_xX \subset T_xY$.

2) Se $x \in X \cap Y$, $X, Y \subset \mathbb{A}^n$ chiusi, allora $I(X) + I(Y) \subset I(X \cap Y)$ a quindi $T_x(X \cap Y) \subset T_xX \cap T_xY$.

3) T_xX dipende solo dal germe di X in x, più precisamente se Y è un altro chiuso ed esiste un intorno $x \in U \subset \mathbb{A}^n$ tale che $X \cap U = Y \cap U$ allora $T_xX = T_xY$. Infatti non è restrittivo supporre $X = \overline{X \cap U}$ e quindi $X \subset Y$ e $T_xX \subset T_xY$. Sia $v \in T_xY$ e $f \in I(X)$, esiste g tale che $g(x) = 1$ e $fg \in I(Y)$. Dalla regola di Leibnitz segue che $f(x + tv)$ possiede una radice multipla in $t = 0$.

4) Se l'ideale $I(X)$ è generato da $f_1, ..., f_s$, per la regola di Leibnitz $v \in T_xX$ se e solo se $< v, df_i(x) >= 0$ per $i = 1, .., s$ e quindi T_xX è il nucleo dell'applicazione lineare $\mathbb{K}^n \to \mathbb{K}^s$ rappresentata dalla matrice jacobiana $(\frac{\partial f_i}{\partial x_j})$.

5) L'applicazione $x \to \dim T_xX$ è semicontinua superiormente in X; infatti, presi $f_1, ..., f_s$ generatori di $I(X)$ e detto $J_h \subset \mathbb{K}[X]$ l'ideale generato dai determinanti dei minori $(n - h + 1) \times (n - h + 1)$ della matrice jacobiana di $f_1, .., f_s$ si ha che $\dim T_xX \geq h$ se e solo se $x \in V(J_h)$.

6) Se $f: X \to Y$ è un'applicazione regolare tra chiusi affini, $x \in X$, $y = f(x)$, è definito in modo naturale il differenziale $df(x): T_xX \to T_yY$.

Infatti se $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ sono chiusi, allora f è la restrizione di una applicazione regolare $(F_1, ..., F_m): \mathbb{A}^n \to \mathbb{A}^m$ dove i polinomi F_i sono unicamente determinati modulo $I(X)$.

Sia $v = (v_1, .., v_n) \in T_xX$ e definiamo

$$w = dF(x)v, \qquad w_j = \sum_{i=1}^{n} \frac{\partial F_j}{\partial x_i} v_i$$

Per definizione di T_xX il vettore w non dipende dalla scelta dei polinomi F_i. Se $g \in I(Y)$ allora $g(F_1, ..., F_m) \in I(X)$ e la regola di derivazione della funzione composta mostra che $< w, dg(y) >= 0$.

Come conseguenza di 6) la dimensione di T_xX dipende solo dalla coppia (X, x) e non dalla particolare immersione chiusa $X \subset \mathbb{A}^n$, vedremo negli esercizi una caratterizzazione intrinseca dello spazio tangente di Zariski.

Lemma 4.1. *Sia $X \subset \mathbb{A}^n$ chiuso, $x \in X$, allora $\dim T_xX \geq \dim_x X$.*

Dim. Induzione su $d = \dim_x X$. Se $d = 0$ non c'è nulla da dimostrare. Se $d > 0$, per VIII.4.7 esiste un iperpiano $H \subset \mathbb{A}^n$ passante per x tale che T_xX non è contenuto in T_xH e $\dim_x(X \cap H) = \dim_x X - 1$; per l'ipotesi induttiva

$$\dim T_xX > \dim(T_xX \cap T_xH) \geq \dim T_x(X \cap H) \geq \dim_x(X \cap H) = \dim_x X - 1.$$

□

Lemma 4.2. *Sia X varietà affine, $Y \subset X$ aperto affine; allora l'inclusione $Y \subset X$ induce un isomorfismo tra gli spazi tangenti di Zariski.*

Dim. Sia $x \in Y$ e sia f funzione regolare su X tale che $f(x) \neq 0$ e $X_f \subset Y$. Siccome X_f e Y_f sono varietà affini isomorfe basta dimostrare il lemma nel caso in cui $Y = X_f$.

Sia $X \subset \mathbb{A}^n$ una immersione chiusa, abbiamo visto che esiste una immersione chiusa $X_f \subset \mathbb{A}^{n+1}$ e che $I(X_f)$ è generato da $I(X)$ e $1 - x_{n+1}f$. Quindi per ogni $(x, x_{n+1}) \in X_f$ si ha che $(v_1, ..., v_{n+1}) \in T_{(x,x_{n+1})}X_f$ se e solo se $(v_1, ..., v_n) \in T_xX$ e $v_{n+1} = -\frac{1}{f(x)^2} \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(x) v_i$. □

Definizione 4.3. Sia X varietà quasiproiettiva. Diremo che un punto $x \in X$ è **singolare** se preso un aperto affine U contenente x vale $\dim T_xU > \dim_x U$, altrimenti si dice **liscio**.

Per 4.2 la dimensione di T_xU non dipende dalla scelta di U e quindi la 4.3 è una buona definizione.

Se X è equidimensionale (e.g. se X è irriducibile), dalla semicontinuità della dimensione di T_xX e dal lemma 4.1 segue che l'insieme dei punti lisci è un aperto.

Si consideri ad esempio una ipersuperficie $X \subset \mathbb{A}^n$, $I(X) = (F)$. Sappiamo che X ha dimensione pura $n-1$ e quindi un punto $x \in X$ è singolare se e solo se annulla tutte le derivate parziali di F.

Dato che $\mathbb{K}$ è perfetto, F è ridotto e non ha fattori in comune con le derivate parziali; per il teorema degli zeri ogni componente irriducibile di X contiene punti lisci.

Similmente si prova che se F è un polinomio omogeneo senza fattori multipli, un punto della ipersuperficie proiettiva definita da F è singolare se e solo se tutte le derivate parziali di F si annullano in X.

Più in generale si ha il:

Teorema 4.4. *Sia X varietà quasiproiettiva, allora l'aperto dei punti lisci è non vuoto.*

Dim. Non è restrittivo supporre $X \subset \mathbb{A}^n$ chiuso irriducibile. Lavoriamo per induzione su n essendo il risultato banalmente vero se $n = 0$ e se $X = \mathbb{A}^n$. Si assuma quindi $n > 0$ e X chiuso proprio; prendiamo un polinomio $f \in I(X) - 0$ di grado minimo. Essendo $I(X)$ un ideale primo necessariamente f è irriducibile e quindi con almeno una derivata parziale, diciamo $\dfrac{\partial f}{\partial x_n}$, non nulla.

Si consideri adesso un generico cambio di coordinate del tipo $x_n = y_n$, $x_i = y_i + a_i y_n$, $a_i \in \mathbb{K}$; si ha

$$\frac{\partial f}{\partial y_n} = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}\frac{\partial x_i}{\partial y_n} = \frac{\partial f}{\partial x_n} + \sum_{i=1}^{n-1} a_i \frac{\partial f}{\partial x_i}$$

Tutto questo mostra che a meno di un cambio lineare di coordinate possiamo supporre f monico rispetto a x_n e $\dfrac{\partial f}{\partial x_n} \neq 0$. Per ragioni di grado $\dfrac{\partial f}{\partial x_n} \notin I(X)$ e $Z = X \cap V(\dfrac{\partial f}{\partial x_n})$ è un chiuso proprio di X.

Sia $\pi\colon \mathbb{A}^n \to \mathbb{A}^{n-1}$ la proiezione sulle prime coordinate, per i ben noti risultati sulle proiezioni normalizzate si ha che $Y = \pi(X)$ è chiuso irriducibile di dimensione uguale a dimensione di X e $\pi(Z)$ è un chiuso proprio di Y.

Per induzione esiste $y \in Y - \pi(Z)$ punto liscio, proviamo che se $x \in X$, $\pi(x) = y$ allora la proiezione $d\pi\colon T_x X \to T_y Y$ è iniettiva e quindi $\dim T_x X \leq \dim T_y Y = \dim Y = \dim X$ che implica la liscezza di x.

Un vettore $(v_1, \ldots, v_n)$ appartiene al nucleo di π se e solo se $v_1 = \ldots = v_{n-1} = 0$ e dato che $\dfrac{\partial f}{\partial x_n}(x) \neq 0$ una tale vettore non può essere tangente a X. □

Proposizione 4.5. *Siano $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ chiusi, per ogni $x \in X$, $y \in Y$ vale $T_{(x,y)} X \times Y = T_x X \times T_y Y$. In particolare (x, y) è un punto liscio di $X \times Y$ se e solo se x e y sono punti lisci di X e Y rispettivamente.*

Dim. Sappiamo che $I(X \times Y)$ è generato da $I(X)$ e $I(Y)$. □

5. Funzioni razionali

La definizione degli anelli locali $\mathcal{O}_{Z,X}$ data nel §1 per le varietà affini si estende senza variazioni sostanziali alle varietà quasiproiettive; in particolare se X è una varietà quasiproiettiva irriducibile, il campo $\mathbb{K}(X)$ delle funzioni razionali su X si definisce come l'insieme delle coppie (U, f), $U \subset X$ aperto, $f \in \mathcal{O}_X(U)$, modulo la relazione di equivalenza $(U, f) \sim (V, g)$ se f e g coincidono su un aperto $W \subset U \cap V$.

Si noti che, essendo X irriducibile, per ogni aperto nonvuoto U esiste una naturale inclusione $\mathcal{O}_X(U) \subset \mathbb{K}(U) = \mathbb{K}(X)$, in particolare per ogni aperto affine $U \subset X$ si ha che $\mathbb{K}(X)$ è naturalmente isomorfo al campo delle frazioni globali del dominio di integrità $\mathbb{K}[U]$.

Diremo che una funzione razionale $f \in \mathbb{K}(X)$ **è definita** in un punto $x \in X$ se è rappresentata da una coppia (U, f) con $x \in U$. È ovvio che l'insieme dei punti dove una funzione razionale è definita è una aperto detto **aperto di definizione** ed è facile vedere che se U è l'aperto di definizione di una funzione razionale f allora f è rappresentata da una coppia (U, f).

Definizione 5.1. Un morfismo $\phi\colon X \to Y$ tra varietà irriducibili si dice **dominante** se $f(X)$ è denso in Y.

La restrizione di un morfismo dominante ad ogni aperto è ancora dominante; abbiamo visto negli esercizi che l'immagine di un morfismo dominante contiene un aperto.

Sia dunque $\phi\colon X \to Y$ un morfismo dominante di varietà irriducibili e sia $f \in \mathbb{K}(Y)$ rappresentata da una coppia (U, f); l'aperto $\phi^{-1}(U)$ è nonvuoto e si definisce $\phi^* f \in \mathbb{K}(X)$ come la funzione razionale definita dalla coppia $(\phi^{-1}(U), \phi^* f)$. Lasciamo per esercizio la semplice verifica che $\phi^*\colon \mathbb{K}(Y) \to \mathbb{K}(X)$ è un omomorfismo di campi ben definito e che è l'identità su $\mathbb{K}$.

Definizione 5.2. Un morfismo dominante si dice **birazionale** se induce un isomorfismo tra i campi delle funzioni razionali.

Teorema 5.3. *Un morfismo $\psi\colon X \to Y$ tra varietà quasiproiettive irriducibili è birazionale se e soltanto se esistono aperti $U \subset X$, $V \subset Y$ tali che $\psi\colon U \to V$ è un isomorfismo.*

Dim. Siccome il campo delle funzioni razionali è invariante per restrizione ad un aperto, se ψ induce un isomorfismo tra aperti allora ψ è birazionale.

Viceversa supponiamo ψ birazionale, possiamo supporre senza perdita di generalità che X, Y siano varietà affini.

Siccome ψ è dominante $\psi^*\colon \mathbb{K}[Y] \to \mathbb{K}[X]$ è iniettiva e possiamo identificare $\mathbb{K}[Y]$ con la sua immagine in $\mathbb{K}[X]$, la condizione di birazionalità è allora equivalente al fatto che i domini di integrità $\mathbb{K}[X]$ ed $\mathbb{K}[Y]$ hanno lo stesso campo delle frazioni.

Sia $u_1,..,u_n \in \mathbb{K}[X]$ un insieme di generatori come $\mathbb{K}$-algebra, possiamo considerare $u_1,..,u_n$ come funzioni razionali su Y, sia $V \subset Y$ un qualsiasi aperto dove le u_i sono regolari.
Esistono dunque delle ovvie inclusioni

$$\mathbb{K}[Y] \subset \mathbb{K}[X] \subset \mathbb{K}[V] \subset \mathbb{K}(Y) = \mathbb{K}(X)$$

Poniamo $U = \psi^{-1}V$ e dimostriamo che $\psi: U \to V$ è un isomorfismo.
Siccome X è affine esiste un morfismo dominante $\gamma: V \to X$ che induce l'inclusione $\mathbb{K}[X] \subset \mathbb{K}[V]$ e siccome anche Y è affine la composizione $\psi \circ \gamma: V \to Y$ induce l'inclusione $\mathbb{K}[Y] \subset \mathbb{K}[V]$ e quindi deve essere $\psi \circ \gamma = Id_V$.
Chiaramente $\gamma(V) \subset U$ e quindi per concludere la dimostrazione è sufficiente dimostrare che il morfismo $\gamma \circ \psi: U \to U$ è l'identità sul sottoinsieme denso $\gamma(V) \subset U$.
Se $x = \gamma(y)$ allora $\gamma \circ \psi(x) = \gamma(\psi \circ \gamma(y) = \gamma(y) = x$. □

Definizione 5.4. Siano X, Y varietà, X irriducibile; una **applicazione razionale** ϕ da X in Y è una classe di equivalenza di coppie (U, ϕ) con $U \subset X$ aperto nonvuoto e $\phi: U \to Y$ morfismo regolare modulo la relazione $(U, \phi) \sim (V, \psi)$ se $\phi = \psi$ in un sottoinsieme aperto di $U \cap V$.

Una applicazione razionale si denota graficamente con una freccia tratteggiata $- \to$. Diremo che una applicazione razionale $\phi: X - \to Y$ è dominante se i suoi rappresentanti $\phi: U \to Y$ sono dominanti. Come sopra una applicazione razionale dominante $\phi: X - \to Y$ tra varietà irriducibili induce un omomorfismo di campi $\phi^*: \mathbb{K}(Y) \to \mathbb{K}(X)$. Di nuovo una applicazione razionale si dice birazionale se è dominante e induce un isomorfismo tra i campi di funzioni razionali. Segue immediatamente da 5.3 che una applicazione razionale dominante è birazionale se e solo se possiede un inversa razionale.

Proposizione 5.5. *La dimensione di una varietà quasiproiettiva irriducibile è il massimo intero n tale che esiste una applicazione razionale dominante $\phi: X - \to \mathbb{A}^n$.*

Dim. Non è restrittivo assumere X affine, abbiamo già dimostrato che se $\dim X = n$ esiste un morfismo chiuso e surgettivo $X \to \mathbb{A}^n$.
Viceversa sia $\phi: X - \to \mathbb{A}^n$ dominante, a meno di restringere X ad un aperto possiamo supporre ϕ regolare; segue dunque dal teorema 3.9 che $\dim X \geq n$. □

La condizione espressa in 5.5 può essere espressa in termini puramente algebrici; ricordiamo che il grado di trascendenza di una estensione di campi $\mathbb{K} \subset L$ è il massimo intero n tale che esiste un omomorfismo iniettivo di $\mathbb{K}$-algebre, $\mathbb{K}[t_1,...,t_n] \to L$. Si ha quindi il

Corollario 5.6. *La dimensione di una varietà quasiproiettiva X è uguale al grado di trascendenza dell'estensione $\mathbb{K} \subset \mathbb{K}(X)$.*

Dim. Se $\dim X = n$ esiste un applicazione razionale dominante $X - \to \mathbb{A}^n$ che induce un omomorfismo iniettivo $\mathbb{K}[\mathbb{A}^n] \to \mathbb{K}(X)$.
Viceversa se $\mathbb{K}[t_0,...,t_n] \subset \mathbb{K}(X)$, preso un aperto affine $U \subset X$ dove le t_i sono definite, l'inclusione $\mathbb{K}[t_0,...,t_n] \subset \mathbb{K}[U]$ è indotta da un morfismo dominante $U \to \mathbb{A}^n$. □

Un utile criterio di birazionalità è il seguente:

Teorema 5.7. *Un morfismo proiettivo dominante $\phi: X \to Y$ è birazionale se e solo se esiste $x \in X$ tale che $\phi^{-1}(\phi(x)) = x$ e $d\phi: T_xX \to T_{\phi(x)}Y$ è iniettivo.*

Premettiamo alla dimostrazione alcuni risultati preliminari.

Sia $S_d \subset \mathbb{K}[t_0, t_1]$ il sottospazio vettoriale dei polinomi omogenei di grado d e per $n \geq m \geq h \geq 1$ interi fissati sia $\Sigma_h \subset \mathbb{P}(S_n) \times \mathbb{P}(S_m)$ l'insieme delle coppie $([f],[g])$ tali che i polinomi f, g hanno un fattore comune di grado $\geq h$. In altri termini Σ_h è l'immagine del morfismo $\phi: \mathbb{P}(S_h) \times \mathbb{P}(S_{n-h}) \times \mathbb{P}(S_{m-h}) \to \mathbb{P}(S_n) \times \mathbb{P}(S_m)$, $\phi([h],[f],[g]) = ([hf],[hg])$. Dato che ϕ è regolare, proiettivo e iniettivo su $\Sigma_h - \Sigma_{h+1}$ abbiamo dimostrato il

Lemma 5.8. *Nelle notazioni precedenti Σ_h è un chiuso di dimensione $n + m - h$.*

Lemma 5.9. *Sia Y varietà affine, $X \subset Y \times \mathbb{P}^1$ chiuso e sia $x \in X$ tale che:*
a) La proiezione sul primo fattore $\pi: X \to Y$ è surgettiva.
b) Detto $\pi(x) = y$ si ha $\pi^{-1}(y) = x$ e $\pi: T_xX \to T_yY$ iniettiva.
Allora π è birazionale e $\pi: T_xX \to T_yY$ è un isomorfismo.

Dim. Consideriamo una immersione $Y \subset \mathbb{A}^n$ tale che il punto y corrisponde allo $0 \in \mathbb{A}^n$, e sia t una coordinata affine su $\mathbb{P}^1$ tale che il punto x corrisponde a $(0,0) \in \mathbb{A}^n \times \mathbb{A}^1$. A meno di restringere Y ad un aperto affine possiamo supporre X interamente contenuto nella parte affine $t \neq \infty$ di $\mathbb{A}^n \times \mathbb{P}^1$. Siccome il vettore $(0,..,0,1)$ non è tangente a X in 0 ne segue che esistono $g, f(x_1,...,x_n,t) \in I(X)$ polinomi monici in t tali che t è una radice semplice di $f(0,t)$ e $f(0,t), g(0,t)$ non hanno radici in comune per $t \neq 0$.
Proviamo che $T_0X \to T_0Y$ è surgettivo, sia $v = (v_1,...,v_n) \in T_0Y$ e sia $t - f_1(x_1,...,x_n)$ la parte lineare di f; proviamo che il vettore $w = (v_1,...,v_n, f_1(v))$ appartiene a T_0X. Per costruzione $< w, df(0) >= 0$, si assuma per assurdo che esista $h \in I(X)$ tale che $< w, dh(0) > \neq 0$, a meno di sostituire ad h una opportuna combinazione lineare $h + af + bt^s g$ con $s \geq 2$ e $a, b \in \mathbb{K}$ possiamo assumere senza perdita di generalità che h sia monico in t, $h(0,t)$ e $f(0,t)$ senza zeri comuni per $t \neq 0$ e che t non compaia nella parte lineare di h.
Proviamo che, a meno di una costante moltiplicativa invertibile, la parte lineare del risultante $R(f,h) \in I(Y)$ è uguale alla parte lineare di h. Conviene in proposito lavorare nell'anello delle serie formali $\mathbb{K}[[x_1,...,x_n]]$, per il lemma di Hensel possiamo

scrivere $f = (t - \phi(x_1, ..., x_n))\tilde{f}$ e quindi per le proprietà di bilinearità del risultante $R(f,h) = h(x_1, .., x_n, \phi)R(\tilde{f}, h)$ con $R(\tilde{f}, h)(0) \neq 0$.

Proviamo adesso che $\pi: X \to Y$ è birazionale, si consideri innanzitutto i sottoinsiemi Y_h, $h \in \mathbb{Z}$, definiti come l'insieme dei punti y tali che i polinomi $f(y,t), g(y,t)$ hanno almeno h radici in comune contate con molteplicità, per ipotesi $Y_1 = Y$ e $0 \notin Y_2$. Gli insiemi Y_h sono chiusi in quanto sono la controimmagine degli insiemi Σ_h considerati nel lemma precedente per un morfismo regolare. A meno di restringere Y possiamo supporre $Y_2 = \emptyset$.

Sia $h \in \mathbb{K}(Y)[t]$ il massimo comune divisore (monico) di f, g, a meno di restringere Y possiamo supporre $h \in \mathbb{K}[Y][t]$ e che h divida f e g in $\mathbb{K}[Y][t]$. Necessariamente h ha grado 1, e $X = V(h)$ è il grafico di un morfismo regolare $Y \to \mathbb{A}^1$. □

Dimostrazione di 5.7. Sia $f: X \to Y$ come in 5.7, a meno di restringere Y non è restrittivo assumere Y affine e $X \subset Y \times \mathbb{P}^n$ e $x = (y, p)$. Usiamo induzione su n avendo dimostrato il risultato per $n = 1$. Se $n > 1$ prendiamo un punto $q \in \mathbb{P}^n$, $p \neq q$ e si consideri la proiezione di centro q, $\pi: Y \times (\mathbb{P}^n - q) \to Y \times \mathbb{P}^{n-1}$, a meno di restringere Y π è definita su X. Per il caso $n = 1$ segue che $X \to \pi(X)$ è birazionale e $T_{pi(x)}\pi(X) \to T_y Y$ è ancora iniettiva (dettagli lasciati per esercizio al lettore). □

Corollario 5.9. *Sia $X \subset \mathbb{P}^n$ varietà proiettiva irriducibile di codimensione ≥ 2, allora la generica proiezione $X \to \mathbb{P}^{n-1}$ è birazionale sull'immagine. In particolare per ogni varietà quasiproiettiva irriducibile X esiste un morfismo birazionale $X \to H$ con H ipersuperfice proiettiva.*

Dim. Esercizio.

6. Esercizi complementari

ESERCIZIO 19: Sia M una varietà differenziabile compatta, $\mathcal{C}$ la famiglia dei chiusi di M e $\mathcal{I}$ la famiglia degli ideali di $C^\infty(M, \mathbb{C})$. In analogia con il caso affine definire $V: \mathcal{I} \to \mathcal{C}$, $I: \mathcal{C} \to \mathcal{I}$. Provare che vale la forma debole del teorema degli zeri, cioè se $J \neq (1)$ allora $V(J) \neq \emptyset$.

Se $J \in \mathcal{I}$ si definisce J' come l'ideale generato da tutte le funzioni $h \circ f$, $f \in J$, $h \in C^\infty(\mathbb{C}, \mathbb{C})$, $h(0) = 0$. Provare che $\sqrt{J'} \subset I(V(J))$ ma che in generale non vale l'inclusione opposta.

ESERCIZIO 20: Sia $S \subset A$ una parte moltiplicativa e $l: A \to S^{-1}A$ l'omomorfismo naturale. Se $T = 1 + \ker l$, allora T è una parte moltiplicativa ed esiste un morfismo $T^{-1}A \to S^{-1}A$.

ESERCIZIO 21: Sia $E \subset A$ insieme finito e $S \subset A$ la più piccola parte moltiplicativa contenente E. Mostrare che $S^{-1}A$ è finitamente generata come A-algebra.

ESERCIZIO 22: Sia $R \to B$ un morfismo di anelli e I_n, $n \in \mathbb{Z}$, una successione di ideali di B tali che $I_a I_b \subset I_{a+b}$ per ogni $a, b \in \mathbb{Z}$ e $I_n = B$ per ogni $n \leq 0$. Provare che $A = \oplus_{n \in \mathbb{Z}} I_{-n} t^n$ è una $R[t]$-algebra e descrivere $A/(t)$ e A_t. Se $X \subset \mathbb{A}^n$ chiuso, $x_1, ..., x_n$ coordinate affini su $\mathbb{A}^n$, $R = \mathbb{K}$, $B = \mathbb{K}[X]$ e $I_a = (x_1^a)$ per ogni $a \geq 0$ si dia una interpretazione geometrica di A, $A/(t)$ e A_t.

ESERCIZIO 23: Sia A un dominio di integrità con campo delle frazioni globali $\mathbb{K}$, per ogni ideale massimale $m \subset A$ interpretiamo il localizzato A_m come un sottoanello di $\mathbb{K}$. Provare che $\cap A_m = A$ dove l'intersezione è presa su tutti gli ideali massimali.

ESERCIZIO 24: Se $Z \subset \mathbb{A}^n$ è una ipersuperfice irriducibile e $I(Z) = (f)$ l'anello $\mathcal{O}_{Z,X}$ è un anello di valutazione discreta con parametro locale f.

ESERCIZIO 25: Sia X varietà, per ogni chiuso irriducibile $Z \subset X$ vale $\mathcal{O}_{Z,X}/m_{Z,X} = \mathbb{K}(Z)$.

ESERCIZIO 26: (**) Sia X una varietà quasiproiettiva ed $A = \mathcal{O}_X(X)$. Diremo che X soddisfa il teorema degli zeri se per ogni ideale $J \subset A$ si ha che $I(V(J)) = \sqrt{J}$, dove lasciamo per esercizio al lettore di definire in analogia al caso dei chiusi affini gli operatori I e V.

Provare che una varietà quasiaffine X è affine se e solo se soddisfa il teorema degli zeri e la $\mathbb{K}$-algebra $\mathcal{O}_X(X)$ è finitamente generata. (Sugg. Vedi esercizio II.2.17 in [Ha]).

ESERCIZIO 27: Sia $F \in \mathbb{K}[x_0, ..., x_n]$ omogeneo di grado $d > 0$ e $U = \mathbb{P}^n - V(F)$. Provare che ogni funzione di $\mathcal{O}_{\mathbb{P}^n}(U)$ è della forma GF^{-a} con $a \geq 0$ e $G \in \mathbb{K}[x_0, ..., x_n]$ omogeneo di grado ad.

ESERCIZIO 28: Sia $Y \subset M(n, s, \mathbb{K}) = \mathbb{A}^{sn}$, $s \leq n$, l'aperto delle matrici di rango massimo s e per ogni $A \in Y$ sia $f(A) \in G(s, \mathbb{K}^n) = X$ il sottospazio generato dai vettori colonna di A. Provare:

i) L'applicazione $f: Y \to X$ è regolare ed aperta.

ii) $f(A) = f(B)$ se e solo se esiste $C \in GL(s, \mathbb{K})$ tale che $A = BC$.

iii) Sia $U \subset X$ aperto, $f^*: \mathcal{O}_X(U) \to \mathcal{O}_Y(f^{-1}(U))$ è iniettiva ed ha come immagine esattamente

$$\mathcal{O}_Y(f^{-1}(U))^{GL(s)} = \{g \in \mathcal{O}_Y(f^{-1}(U)) \mid g(AC) = g(A) \forall A \in f^{-1}(U), \forall C \in GL(s, \mathbb{K})\}$$

ESERCIZIO 29: Sia $\phi: \bigwedge^s V \to \mathrm{Hom}(V, \bigwedge^{s+1} V)$ definita da $\phi(w)(v) = w \wedge v$ per ogni $v \in V$. Provare che ϕ è lineare e che $\phi(w)$ ha rango $\leq \dim V - s$ se e solo se w è totalmente decomponibile. (Sugg. se $v \neq 0$ provare che $\phi(w)(v) = 0$ se e solo se esiste $h \in \bigwedge^{s-1} V$ tale che $w = h \wedge v$; dedurre che $w \neq 0$ è totalmente decomponibile se e solo se $\ker \phi(w)$ ha dimensione s).

ESERCIZIO 30: Sia $H \subset V$ sottospazio di dimensione l, provare che il morfismo naturale $G(s-l, V/H) \to G(s,V)$ è regolare.

ESERCIZIO 31: Sia $H \subset V$ sottospazio e $l \geq 0$ un intero. Provare che

$$\Omega_l(H) = \{W \in G(s,V) \,|\, \dim(W \cap H) \geq l\}$$

è l'intersezione di $G(s,V)$ con un sottospazio proiettivo di $\mathbb{P}(\bigwedge^s V)$. (Sugg. Sia $e_1, ..., e_m$ base di H e si consideri l'insieme dei vettori $v \in \bigwedge^s V$ tali che $v \wedge h = 0$ per ogni $h \in \bigwedge^{m-l+1} H$).

ESERCIZIO 32: (Varietà di Schubert, [K-L]).

Sia $A_1 \subset A_2 \subset ... \subset A_s \subset V$, $A_i \neq A_{i+1}$ una catena di sottospazi vettoriali di V tali che $i \leq \dim A_i \leq n-s+i$. Poniamo $\Omega(A_1, ..., A_s) = \{W \in G(s,V) \,|\, \dim(W \cap A_i) \geq i\}$; si noti che $\Omega(A_1, ..., A_s)$ dipende, a meno di automorfismi regolari di $G(s,V)$ dalle dimensioni d_i dei sottospazi A_i.

Provare che $\Omega(A_1, ..., A_s)$ è un chiuso irriducibile della Grassmaniana e se ne calcoli la dimensione in funzione di $d_1, ..., d_s$.

ESERCIZIO 33: Fissati m sottospazi $L_1, ..., L_m \subset \mathbb{P}^n$, di dimensione $d_1, ..., d_m \leq n-2$, provare che l'insieme delle rette di $\mathbb{P}^n$ che intersecano $L_1, ..., L_m$ è non vuoto se

$$\sum_{i=1}^{m} \binom{n-d_i}{2} \leq 2(n-1)$$

ESERCIZIO 34: In alcuni testi scolastici si trova la seguente definizione: dati due punti distinti (x,y,z), (x',y',z') di una retta $L \subset \mathbb{A}^3$, si dicono coordinate Plückeriane di L i sei numeri:

$$\alpha_1 = x'-x, \quad \alpha_2 = y'-y, \quad \alpha_3 = z'-z$$

$$p_1 = y'z - z'y, \quad p_2 = z'x - x'z, \quad p_3 = x'y - y'x$$

Conciliare questa definizione con quella descritta nelle note.

ESERCIZIO 35: (caratteristica $\neq 2$) Provare che i vettori totalmente decomponibili di $\bigwedge^2 V$ coincidono con i vettori isotropi della applicazione bilineare simmetrica $\bigwedge^2 V \times \bigwedge^2 V \to \bigwedge^4 V$, $(v,w) \to v \wedge w$. Dedurre che $G(2,V)$ è intersezione di quadriche in $\mathbb{P}(\bigwedge^2 V)$.

ESERCIZIO 36: (**) Ricordiamo che esiste un isomorfismo naturale $\bigwedge^s V^\vee = (\bigwedge^s V)^\vee$ tramite l'accoppiamento di dualità che estende per bilinearità la relazione

$$< v_1 \wedge ... \wedge v_s, \phi_1 \wedge ... \wedge \phi_s > = \sum_{\sigma \in \Sigma_s} (-1)^\sigma \phi_1(v_{\sigma(1)}) ... \phi_s(v_{\sigma(s)})$$

Presa una base $\epsilon_1, ..., \epsilon_n$ di $V^\vee$, provare che $v \in \bigwedge^s V$ è totalmente decomponibile se per ogni scelta di $i_1, ... i_{s-1}, j_1, ..., j_{s+1} \in \{1, ..., n\}$ vale

$$\sum_{\lambda=1}^{s+1} (-1)^\lambda < \epsilon_{i_1} \wedge ... \wedge \epsilon_{i_{s-1}} \wedge \epsilon_{j_\lambda}, v > < \epsilon_{j_1} \wedge ... \wedge \widehat{\epsilon_{j_\lambda}} \wedge ... \wedge \epsilon_{j_{s+1}}, v >$$

Tali relazioni sono dette relazioni quadratiche di Plücker. (Sugg. vedi [Hr], [G-H] per una descrizione astratta, [K-L] e [Cat] per una dimostrazione dettagliata.)

ESERCIZIO 37: Sia S l'immagine della mappa di Segre $s: \mathbb{P}^n \times \mathbb{P}^m \to S \subset \mathbb{P}^N$ e $L \subset S$ una retta. Provare che $s^{-1}(L)$ è contenuta in una fibra di una delle due proiezioni $\mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^n$, $\mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^m$. Dedurre che l'insieme delle rette in S è un sottoinsieme sconnesso di $G(2, N+1)$.

ESERCIZIO 38: Un morfismo regolare $f: X \to Y$ si dice **universalmente chiuso**, se per ogni morfismo regolare $g: Z \to Y$ il morfismo di proiezione $X \times_Y Z \to Z$ è chiuso. Un morfismo universalmente chiuso è chiuso, il viceversa è falso in generale.

ESERCIZIO 39: (*) Sia $X \subset \mathbb{P}^n$ localmente chiuso.

Un morfismo $f: X \to Y$ è proiettivo se e solo se G_f è chiuso in $Y \times \mathbb{P}^n$. (Sugg. provare che se f è proiettivo allora anche $(i,f): X \to \mathbb{P}^n \times Y$ è proiettivo).

ESERCIZIO 40: (*) Sia $f: X \to Y$ un morfismo di varietà quasiproiettive. Provare che f è proiettivo se e solo se è universalmente chiuso. (Sugg. Sia $\overline{X}$ la chiusura proiettiva di X e $\overline{G} \subset \overline{X} \times Y$ la chiusura del grafo. Provare che $\{((x,f(x)),x) \in \overline{G} \times_Y X \,|\, x \in X\}$ è un chiuso.)

ESERCIZIO 41: Mostrare che in generale i punti 3) e 4) di 3.9 non valgono se il morfismo non è proiettivo.

ESERCIZIO 42: Sia $S_d \subset \mathbb{K}[x_0, x_1]$ lo spazio vettoriale delle forma binarie di grado d, e per ogni $h > 0$, sia $\Sigma_h \subset S_d$ l'insieme delle forme aventi un fattore multiplo di grado h. Provare che Σ_h è un chiuso irriducibile di Zariski di $S_d = \mathbb{A}^{d+1}$ e se ne calcoli la dimensione.

ESERCIZIO 43: Utilizzare 3.9 per dimostrare che, dato un morfismo $f: X \to Y$ tra varietà quasiproiettive irriducibili tale che $\overline{f(X)} = Y$ allora $f(X)$ contiene un aperto. (Sugg. Sia $g: \overline{X} \to Y$ una chiusura proiettiva di f e sia $Z = \overline{X} - X$. Si consideri l'insieme dei punti $y \in Y$ tali che $\dim Z_y < \dim X - \dim Y$.)

ESERCIZIO 44: (Superfici di Segre-Hirzebruch).

In tutto l'esercizio $k \geq 0$ è in intero fissato.

a) Sia $v: \mathbb{P}^1_x \to \mathbb{P}^{k+1}_y$ la mappa di Veronese, $y_i = x_0^{k+1-i} x_1^i$, $i = 0, .., k+1$, e sia $C_{k+1} \subset \mathbb{P}^{k+1}$ l'immagine di v. Provare direttamente che C_{k+1} è chiuso e trovare un insieme finito di equazioni che lo definiscono. (Sugg. Descrivere C_{k+1} come il luogo dove si abbassa il rango di ua opportuna matrice a coefficienti forme lineari nelle coordinate y_i).

b) Siano $x_0, x_1, y_0, ..., y_{k+1}$ coordinate omogenee su $\mathbb{P}^{k+3}$ e $\mathbb{P}^1 = \{y_0 = ... = y_{k+1} = 0\}$, $\mathbb{P}^{k+1} = \{x_0 = x_1 = 0\}$. Definiamo $S_k \subset \mathbb{P}^{k+3}$ come l'unione, al variare di $p \in \mathbb{P}^1$, delle rette congiungenti p e $v(p) \in C_{k+1} \subset \mathbb{P}^{k+1}$. Provare che S_k è chiuso e determinare un insieme finito di equazioni che lo definiscono.

c) Definiamo astrattamente un spazio topologico quoziente $\mathbb{F}_k = (\mathbb{A}^2 - 0) \times (\mathbb{A}^2 - 0)/\sim$ dove la relazione di equivalenza è definita

$$(l_0, l_1, t_0, t_1) \sim (\lambda l_0, \lambda l_1, \mu t_0, \mu \lambda^k t_1), \qquad \lambda, \mu \in \mathbb{K} - 0.$$

Determinare un morfismo regolare $(\mathbb{A}^2 - 0) \times (\mathbb{A}^2 - 0) \to \mathbb{P}^{k+3}$ che induce per passaggio al quoziente un omeomorfismo $s\colon \mathbb{F}_k \to S_k$ tale che, nella struttura di varietà proiettiva indotta su $\mathbb{F}_k$, gli aperti $U_{ij} = \{l_i t_j \neq 0\}$ siano isomorfi a $\mathbb{A}^2$.

d) (**) Se $a \neq b$ allora S_a non è isomorfo a S_b. (Sugg. Studiare i gruppi degli automorfismi regolari delle varietà S_k).

ESERCIZIO 45: (**?) Sia $f\colon X \to Y$ un morfismo regolare aperto di varietà affini, provare che il morfismo $f \times id\colon X \times \mathbb{A}^1 \to Y \times \mathbb{A}^1$ è ancora aperto.

ESERCIZIO 46: Dato un anello locale Noetheriano A con ideale massimale m si definisce l'anello graduato associato

$$G(A) = \oplus_{n \geq 0} \frac{m^n}{m^{n+1}}$$

Provare che se $G(A)$ è un dominio di integrità allora anche A è un dominio di integrità. Il viceversa è invece falso in generale. (Sugg. Usare il lemma di Nakayama per provare che $\cap_{n>0} m^n = 0$. Per il viceversa suggeriamo $A = \mathbb{K}[x,y]/(y^2 - x^2 - x^3))$ come controesempio.

ESERCIZIO 47: (*) Sia X varietà affine e $x \in X$ un punto liscio. Provare che se $\dim_x X = \dim T_x X = n$ allora l'anello graduato (vedi esercizio precedente) $G(\mathcal{O}_{x,X})$ è isomorfo all'anello dei polinomi $\mathbb{K}[x_1, ..., x_n]$.

In particolare $\mathcal{O}_{x,X}$ è un dominio di integrità. (Sugg. Un punto è liscio se e solo se il cono tangente è uguale allo spazio tangente).

ESERCIZIO 48: Se $x \in X$ è un punto liscio il completamento m-adico di $\mathcal{O}_{x,X}$ è un'algebra di serie di potenze formali.

ESERCIZIO 49: (Definizione intrinseca dello spazio tangente di Zariski).

a) Sia A una $\mathbb{K}$-algebra locale con ideale massimale m e campo residuo $\mathbb{K}$.

Sia $Der_{\mathbb{K}}(A, \mathbb{K})$ il $\mathbb{K}$-spazio vettoriale delle $\mathbb{K}$-derivazioni. Provare che esiste un isomorfismo naturale di spazi vettoriali $Der_{\mathbb{K}}(A, \mathbb{K}) \to \mathrm{Hom}_{\mathbb{K}}(m/m^2, \mathbb{K})$.

b) Sia $X \subset \mathbb{A}^n$ chiuso affine, $x \in X$ e $x\colon \mathbb{K}[X] \to \mathbb{K}$ l'omomorfismo corrispondente, $x(f) = f(x) \in \mathbb{K}$. Provare che il morfismo di localizzazione $\mathbb{K}[X] \to \mathcal{O}_{x,X}$ induce un isomorfismo $Der_{\mathbb{K}}(\mathcal{O}_{x,X}, \mathbb{K}) \to Der_{\mathbb{K}}(\mathbb{K}[X], \mathbb{K})$.

c) Provare che esiste un isomorfismo naturale $T_x X \to Der_{\mathbb{K}}(\mathbb{K}[X], \mathbb{K})$.

d) Per ogni varietà quasiproiettiva $(X, \mathcal{O}_X)$, $x \in X$ è possibile definire $T_x X$ in modo intrinseco come lo spazio vettoriale duale di m_x/m_x^2 dove m_x è l'ideale massimale di $\mathcal{O}_{x,X}$.

ESERCIZIO 50: Sia $X \subset \mathbb{P}^n$ varietà proiettiva irriducibile di dimensione m, $H \subset \mathbb{P}^n$ sottospazio proiettivo di dimensione $n-m$ e $p \in X \cap H$. Provare che se p è l'unico punto di intersezione di X e H e se $T_p X \cap T_p H = 0$ allora X è un sottospazio proiettivo. (sugg. Sia $Y \subset \mathbb{P}^{n-1}$ la chiusura dell'immagine della proiezione di centro p, $\pi\colon X - \{p\} \to \mathbb{P}^{n-1}$. Provare che $Y \cap \pi(H) = \emptyset$ e quindi che $\dim Y < \dim X$.)

ESERCIZIO 51: Sia $n > m$, provare che non esistono chiusi di $\mathbb{P}^m \times \mathbb{P}^m$ omeomorfi a $\mathbb{P}^n$.

ESERCIZIO 52: Sia $\mathbb{K}$ campo algebricamente chiuso e $\mathbb{K} \subset L$ una estensione finitamente generata di campi. Esistono allora $x_1, ..., x_n \in L$ tali che $\mathbb{K}(x_1, ..., x_n) = L$, $x_1, ..., x_{n-1}$ sono algebricamente indipendenti su $\mathbb{K}$ e x_n è algebrico separabile su $\mathbb{K}(x_1, .., x_{n-1})$. (Sugg. Un tale campo L è il campo delle funzioni razionali di una varietà).

Nota: Il risultato dell'esercizio precedente è vero più in generale per ogni campo perfetto $\mathbb{K}$ (cf. [Ha] p. 27).

ESERCIZIO 53: (caratteristica $\neq 2, 3$). Sia $C \subset \mathbb{P}^2$ una cubica piana liscia, definiamo un'applicazione $j\colon C \to \mathbb{K}$ ponendo $j(p)$ l'invariante j della quaterna di Salmon di (C, p). Provare che j è una funzione regolare e si usi questo fatto per una dimostrazione alternativa del teorema di Salmon V.3.6.

ESERCIZIO 54: (caratteristica $\neq 2$) Sia $X \simeq \mathbb{P}^5$ il sistema lineare completo delle coniche di $\mathbb{P}^2$ e $Y \simeq \mathbb{P}^5$ il sistema lineare completo delle coniche di $(\mathbb{P}^2)^\vee$. Siano inoltre $U \subset X$ e $V \subset Y$ gli aperti delle coniche liscie. Provare che U e V sono varietà affini e che l'applicazione $\phi\colon U \to V$, $\phi(C) = C^\vee$, è un isomorfismo regolare di varietà.

ESERCIZIO 55: L'insieme dei punti lisci su una varietà quasiproiettiva è un aperto (Sugg. usare il risultato dell'esercizio 47).

ESERCIZIO 56: (*) $\mathbb{K} = \mathbb{C}$. Provare che ogni varietà quasiproiettiva irriducibile complessa dotata della topologia classica è uno spazio topologico connesso per archi, cf. [Mu, 4.16]. (Sugg. basta dimostrare che esiste un sottoinsieme aperto di Zariski che è connesso per archi)

X. Varietà algebriche: argomenti scelti

1. Le varietà di incidenza

Sia V uno spazio vettoriale di dimensione n su $\mathbb{K}$, si definisce il **fibrato tautologico lineare** sulla Grassmaniana $G(s,V)$ come

$$S = \{(W,v) \in G(s,V) \times V \,|\, v \in W\}$$

Denotiamo inoltre con $p\colon S \to G(s,V)$, $q\colon S \to V$ le proiezioni sui fattori.
Diremo che un morfismo $\phi\colon X \to Y$ di varietà algebriche è localmente un prodotto con fibra Z se esiste un ricoprimento aperto $Y = \cup U_i$ ed isomorfismi $h_i\colon \phi^{-1}(U_i) \to U_i \times Z$ tali che p è localmente la composizione di h_i e della proiezione sul primo fattore. I morfismi localmente prodotto sono aperti e stabili per cambio di base.

Lemma 1.1. *S è un chiuso di $G(s,V)\times V$ e $p\colon S \to G(s,V)$ è localmente un prodotto a fibra $\mathbb{K}^s$.*

Dim. se pensiamo la Grassmaniana immersa in $\mathbb{P}(\bigwedge^s V)$ tramite la mappa di Plücker si ha che

$$S = \{([w],v) \in \mathbb{P}(\bigwedge^s V) \times V \,|\, v \wedge w = 0, [w] \in G(s,V)\}$$

da cui segue che S è chiuso.
Si consideri adesso una decomposizione $V = W \oplus H$, $W \in G(s,V)$ e sia $U \subset G(s,V)$ l'aperto dei sottospazi che hanno intersezione nulla con H e $r\colon S \to W$ la composizione di q e della proiezione $\pi\colon V \to W$.
Proviamo che il morfismo regolare $p^{-1}(U) \xrightarrow{(p,r)} U \times W$, è un isomorfismo. Per questo basta ricordare che U è isomorfo al sottospazio di $\mathrm{Hom}(W,V)$ delle mappe α tali che $\pi\alpha = Id$. L'inversa di (p,r) è quindi data da $(\alpha,v) = (\alpha, \alpha(v))$. □

Definiamo con $G(s,\mathbb{P}(V))$ la Grassmaniana dei sottospazi proiettivi di $\mathbb{P}(V)$ di dimensione s, esiste una ovvia identificazione $G(s,\mathbb{P}(V)) = G(s+1,V)$. In modo completamente analogo si definisce il **fibrato tautologico proiettivo**

$$Z = \{(W,v) \in G(s,\mathbb{P}(V)) \times \mathbb{P}(V) \,|\, v \in W\}, \qquad p\colon Z \to G(s,\mathbb{P}(V))$$

e si dimostra il

Lemma 1.2. *Z è una varietà proiettiva liscia irriducibile di dimensione $s+(s+1)(\dim V-s-1)$ e p è localmente prodotto a fibra $\mathbb{P}^s$.*

Siamo adesso in grado di dimostrare che i sottospazi lineari contenuti in una varietà proiettiva sono un sottoinsieme chiuso della Grassmaniana, più in generale vale

Proposizione 1.3. *Sia T una varietà quasiproiettiva e $X\subset\mathbb{P}^n\times T$ un chiuso, denotiamo con X_t la fibra di X sopra il punto $t\in T$. Il sottoinsieme*

$$H=\{(W,t)\in G(s,\mathbb{P}^n)\times T\,|\,W\subset X_t\}$$

è chiuso in $G(s,\mathbb{P}^n)\times T$.

Dim. La proiezione $p\colon Z\times T\to G(s,\mathbb{P}^n)\times T$ è localmente prodotto e quindi aperta, chiaramente H è il complementare di $p(Z\times T-G(s,\mathbb{P}^n)\times X)$. □

Siano $x_0,\dots,x_n$ coordinate omogenee su $\mathbb{P}^n$ e $S_d\subset\mathbb{K}[x_0,\dots,x_n]$ il sottospazio vettoriale dei polinomi omogenei di grado d; il proiettivizzato $\mathbb{P}(S_d)$ può essere pensato come lo spazio delle ipersuperfici proiettive di grado d in $\mathbb{P}^n$. Esiste una famiglia universale di ipersuperfici

$$X_d=\{([F],[x_0,\dots,x_n])\in\mathbb{P}(S_d)\times\mathbb{P}^n\,|\,F(x_0,\dots,x_n)=0\}$$

X_d è chiaramente un chiuso, lasciamo come esercizio di dimostrare che X_d è una ipersuperficie liscia irriducibile di bigrado $(1,d)$.
Possiamo applicare la proposizione 1.3 alla famiglia $X_d\to\mathbb{P}(S_d)$ e otteniamo che

$$I_d(s,\mathbb{P}^n)=\{(W,[F])\in G(s,\mathbb{P}^n)\times\mathbb{P}(S_d)\,|\,W\subset V(F)\}$$

è una varietà proiettiva detta **varietà di incidenza**

Lemma 1.4. *$I_d(s,\mathbb{P}^n)$ è una varietà irriducibile di codimensione $\binom{s+d}{d}$ del prodotto $G(s,\mathbb{P}^n)\times\mathbb{P}(S_d)$.*

Dim. Si consideri la proiezione $p\colon I_d(s,\mathbb{P}^n)\to G(s,\mathbb{P}^n)$, la fibra $p^{-1}(W)$ è composta dal sistema lineare di ipersuperfici che contengono W e quindi ha codimensione uguale alla dimensione dello spazio delle forme omogenee di grado d su W che è uguale a $\binom{s+d}{d}$. La irriducibilità di $I_d(s,\mathbb{P}^n)$ segue allora dal teorema IX.3.9. □

ESERCIZIO 1: Provare che $p\colon I_d(s,\mathbb{P}^n)\to G(s,\mathbb{P}^n)$ è localmente un prodotto.

Consideriamo il caso $s=1$, $n=3$, e consideriamo la proiezione sul secondo fattore $q\colon I_d=I_d(1,\mathbb{P}^3)\to\mathbb{P}(S_d)$. Dato $[F]\in\mathbb{P}(S_d)$, $q^{-1}([F])$ è l'insieme delle rette contenute in $V(F)$. Vale il

Lemma 1.5. *Nelle notazioni precedenti se $d\geq 3$, $q(I_d)\subset\mathbb{P}(S_d)$ è un chiuso di codimensione $d-3$.*

Dim. Siccome $G(1,\mathbb{P}^3)$ ha dimensione 4 e I_d ha codimensione $d+1$ la codimensione di $q(I_d)$ è $\geq d+1-4=d-3$ e vale $=$ se e solo se esiste una fibra di $q\colon I_d\to\mathbb{P}(S_d)$ di dimensione 0. Preso $F=x_0x_1x_2^{d-2}-x_3^d$ si vede facilmente (esercizio) che $V(F)$ contiene esattamente tre rette L_0,L_1,L_2, $L_i=\{x_i=x_3=0\}$. □

Abbiamo quindi dimostrato il

Teorema 1.6. *Ogni superfice di grado 3 in $\mathbb{P}^3$ contiene almeno una retta. La generica superfice di grado $d>3$ non contiene rette.*

2. Il teorema delle 27 rette

In questa sezione dimostriamo il seguente

Teorema 2.1. *Sia $S\subset\mathbb{P}^3$ superficie liscia di grado 3 su un campo algebricamente chiuso $\mathbb{K}$ di caratteristica $\neq 2$. Allora S contiene esattamente 27 rette ognuna delle quali ne interseca altre 10.*

La dimostrazione di 2.1 è divisa in vari passi, il punto di partenza è il teorema 1.6 secondo il quale S contiene almeno una retta.
Introduciamo alcune notazioni, sia $x_0,..,x_3$ un sistema di coordinate omogenee su $\mathbb{P}^3$ e $F(x_0,\dots,x_3)$ l'equazione di S, per ipotesi F è omogeneo di grado 3 e le derivate parziali $\dfrac{\partial F}{\partial x_i}$, $i=0,\dots,3$ non hanno zeri comuni su S. Se $H\subset\mathbb{P}^3$ è un piano si denoterà con $H\cdot S$ la cubica piana la cui equazione è la restrizione di F ad H. Per ogni $p\in S$ denotiamo con $T_pS\subset\mathbb{P}^3$ il piano tangente a S nel punto p, l'equazione di T_pS è $\sum x_i\dfrac{\partial F}{\partial x_i}(p)=0$.

Lemma 2.2. *Sia $H\subset\mathbb{P}^3$ un piano, $p\in H\cap S$, vale $H=T_pS$ se e solo se p è un punto singolare di $H\cdot S$.*

Dim. In opportune coordinate omogenee tali che $p=[1,0,0,0]$ e $H=\{x_3=0\}$, l'equazione di $H\cdot S$ è data da $F(x_0,x_1,x_2,0)$ ed il punto p è singolare per $H\cdot S$ se e solo se $\dfrac{\partial F}{\partial x_i}(p)=0$, $i=0,1,2$. □

Lemma 2.3. *La cubica $H\cdot S$ è ridotta per ogni piano H.*

Dim. Si assuma per assurdo che $H\cdot S=2L+M$ con L,M rette in H, per il lemma 2.2 vale $H=T_pS$ per ogni $p\in L\subset S$. Sia H' un qualsiasi piano contenente la retta L, si ha allora $H'\cdot S=L+C$ per una opportuna conica C; se $q\in L\cap C$ per 2.2 si ha $H'=T_pS$. Quindi $H'=H$ che è alquanto assurdo. □

Lemma 2.4. *Sia $Q(s,x_0,x_1,x_2)$ un polinomio a coefficienti in un campo algebricamente chiuso di caratteristica $\neq 2$, omogeneo di grado 2 nelle variabili x_i e sia $\delta(s)$ il determinante della matrice Hessiana $(\frac{\partial^2 Q}{\partial x_i \partial x_j})$.*
Fissato un punto $p=(s_0,[v_0,v_1,v_2])\in \mathbb{A}^1\times\mathbb{P}^2$, se la conica piana di equazione $Q(s_0,x_0,x_1,x_2)$ è ridotta con un punto singolare in $[v_0,v_1,v_2]$ vale

$$\frac{d\delta}{ds}(s_0)=0 \Leftrightarrow \frac{\partial Q}{\partial s}(p)=0$$

Dim. (cf. [Sh] II.6.4) A meno di un cambio di coordinate si può supporre $p=(0,[0,0,1])$, e $Q(0,x_0,x_1,x_2)=x_0x_1$. Dunque $\delta(0)=0$ ed un semplice conto mostra che $\frac{d\delta}{ds}(0)=-\frac{\partial^3 Q}{\partial s\partial x_2^2}$ mentre per la formula di Eulero $\frac{\partial Q}{\partial s}(p)=\frac{1}{2}\frac{\partial^3 Q}{\partial s\partial x_2^2}$. □

Si consideri una retta fissata $L\subset S$ e sia j il numero di rette $M\neq L$ contenute in S che intersecano L. Grazie a 2.3 sappiamo che j è uguale al doppio del numero di piani H contenenti L e tali che, se $H\cdot S=L+C$, la conica C è singolare.

Lemma 2.5. *Nelle notazioni precedenti $j=10$.*

Dim. Fissiamo un sistema di coordinate omogenee tali che $L=\{x_0=x_1=0\}$. In tali coordinate l'equazione di S è

$$F=x_0A(x_2,x_3)+x_1B(x_2,x_3)+x_0^2m(x_2,x_3)+x_1^2n(x_2,x_3)+x_0x_1p(x_2,x_3)+G(x_0,x_1)$$

con m,n,p forme lineari, A,B forme quadratiche e G omogeneo di grado 3.
Dato che S è liscia in ogni punto di L le due forme binarie $\frac{\partial F}{\partial x_0}(0,0,x_2,x_3)=A(x_2,x_3)$, $\frac{\partial F}{\partial x_1}(0,0,x_2,x_3)=B(x_2,x_3)$ non hanno zeri comuni.
Per ogni $a=(a_0,a_1)\in\mathbb{K}^2-0$ sia H_a il piano di equazione $a_1x_0=a_0x_1$ e sia $\phi_a\colon\mathbb{P}^2\to H_a$ la proiettività $\phi_a([y_1,y_2,y_3])=[a_0y_1,a_1y_1,y_2,y_3]$. Si ha quindi $H_a\cdot S=L+C_a$ dove C_a è la conica di equazione

$$Q=a_0A+a_1B+y_1(a_0^2m+a_1^2n+a_0a_1p)+y_1^2G(a_0,a_1)$$

Il discriminante $\Delta(a_0,a_1)$ di C_a è il determinante della matrice

$$\begin{pmatrix} 2G(a_0,a_1) & a_0^2m_2+a_1^2n_2+a_0a_1p_2 & a_0^2m_3+a_1^2n_3+a_0a_1p_3\\ a_0^2m_2+a_1^2n_2+a_0a_1p_2 & a_0A_{22}+a_1B_{22} & a_0A_{23}+a_1B_{23}\\ a_0^2m_3+a_1^2n_3+a_0a_1p_3 & a_0A_{32}+a_1B_{32} & a_0A_{33}+a_1B_{33}\end{pmatrix}.$$

Si vede subito che $\Delta(a_0,a_1)$ è omogeneo di grado 5. Rimane da dimostrare che Δ non ha fattori multipli. Poniamo $\delta(s)=\Delta(1,s)$ e proviamo che δ non ha radici multiple, seguirà per simmetria che anche $\Delta(s,1)$ non ha radici multiple.

Si osservi innanzitutto che l'ipersuperfice $Z\subset\mathbb{A}^1\times\mathbb{P}^2$ di equazione $Q(1,s,y_1,y_2,y_3)=0$ è liscia. Infatti, se esistesse un punto $(1,s,v_1,v_2,v_3)\in Z$ che annulla tutte le derivate parziali di Q, siccome A e B non hanno zeri comuni deve necessariamente essere $v_1\neq 0$, possiamo quindi restringerci all'aperto affine $y_1=1$ dove Q ha equazione $Q(1,s,y_2,y_3)=F(1,s,y_2,y_3)$ e tutto segue dalla liscezza di S.
Basta applicare adesso il lemma 2.4. □

Dimostrazione di 2.1. Abbiamo visto che esiste un piano H tale che $H\cdot S=L_1+L_2+L_3$ con le L_i rette contenute in S e che $H=T_{p_{ij}}S$ dove $p_{ij}=L_i\cap L_j$. Ogni altra retta M contenuta in S interseca H e quindi almeno una delle rette L_i, d'altra parte se $p\in L_i\cap M$ allora $M\subset T_pS$ e quindi M interseca al più una delle rette L_i. Tenendo presente che ogni retta L_i interseca altre 8 rette contenute in S ma non in H ne segue che il numero totale delle rette in S è uguale a $3+3\cdot 8=3+24=27$. □

3. Il teorema di Bertini-Sard

Definizione 3.1. Sia $\phi\colon X\to Y$ un morfismo regolare tra varietà algebriche irriducibili, diremo che un punto $x\in X$ è **critico** se $d\phi\colon T_xX\to T_{\phi(x)}Y$ non è surgettiva.

Lemma 3.2. *Sia $\phi\colon X\to Y$ un morfismo regolare di varietà quasiproiettive; per ogni $x\in X$ sia $V_x\subset T_xX$ il nucleo del differenziale di ϕ. Allora la funzione $x\to\dim V_x$ è semicontinua superiormente su X.*
Se inoltre X è liscia l'insieme dei punti critici è chiuso.

Dim. Possiamo assumere X,Y affini, a meno di comporre ϕ con una immersione chiusa di Y in uno spazio affine possiamo supporre $Y=\mathbb{A}^m$ ed a meno di sostituire X con il grafico di ϕ si può assumere che X sia un chiuso di $\mathbb{A}^{n+m}$ e che ϕ sia la proiezione sulle ultime coordinate.
Se $f_1,\dots,f_r\in\mathbb{K}[x_1,\dots,x_n,y_1,\dots,y_m]$ è un insieme di generatori dell'ideale $I(X)$, un vettore $v=(v_1,\dots,v_n,w_1,\dots,w_m)$ appartiene a V_x se e solo se $w_i=0$ per ogni i e

$$\sum_{i=1}^n v_i\frac{\partial f_j}{\partial x_i}=0,\qquad j=1,\dots,r$$

la semicontinuità è adesso chiara.
Se X è liscia un punto x è critico se e solo se $\dim V_x+\dim T_{\phi(x)}>\dim X$. □

Teorema 3.3.(Bertini-Sard) *Sia $\phi\colon X\to Y$ un morfismo regolare tra varietà quasiproiettive irriducibili definite su un campo $\mathbb{K}$ algebricamente chiuso di* **caratteristica**

0. *Sia $Z \subset X$ l'insieme dei punti critici, allora $\phi(Z)$ è contenuto in un chiuso proprio di Y.*

Osservazioni:

1) Sui complessi i chiusi propri (nella topologia di Zariski) di varietà irriducibili non hanno parte interna (nella topologia euclidea) ed hanno misura nulla [1] .

2) In caratteristica positiva il risultato è falso: si consideri ad esempio un campo di caratteristica $p > 0$ ed il morfismo $\phi\colon \mathbb{A}^1 \to \mathbb{A}^1$, $\phi(x) = x^p$. Si tratta di un morfismo bigettivo ma tutti i punti del dominio sono critici.

3) In alcune applicazioni pratiche si riesce a dimostrare direttamente che $\dim \overline{Z} < \dim Y$, in questo caso il teorema 3.2 è banalmente vero senza ipotesi sulla caratteristica del campo.

4) Se X è nonsingolare, ϕ è surgettiva e $y \notin \phi(Z)$ allora la fibra $V = \phi^{-1}(y)$ è liscia: infatti per ogni $x \in V$ vale

$$\dim T_x V \leq \dim T_x X - \dim T_y Y \leq \dim X - \dim Y \leq \dim_x V$$

Da cui segue che y è un punto liscio di Y e x un punto liscio di V.

Lemma 3.4. *In caratteristica 0, se $\phi\colon X \to Y$ è un morfismo dominante di varietà quasiproiettive irriducibili allora i punti critici di ϕ sono contenuti in un chiuso proprio di X.*

Dim. Riconduciamoci con opportune semplificazioni ad un caso particolare in cui dimostrare 3.4. A tal fine osserviamo che:

a) Siano $U \subset X$, $V \subset Y$ aperti tali che $\phi(U) \subset V$, se il lemma è vero per la restrizione $\phi_{|U}$ allora è vero anche per ϕ, in particolare si può assumere X, Y varietà affini nonsingolari.

b) sia ϕ la composizione di due morfismi dominanti $\alpha\colon X \to Z$, $\beta\colon Z \to Y$ (Z è necessariamente irriducibile). Se il lemma è vero per α e β allora è vero anche per ϕ.

A meno di cambiare X con il grafico di ϕ si può assumere $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ chiusi, $m \leq n$ e ϕ la proiezione sulle prime n-coordinate.

Se $n = m$ non c'è nulla da dimostrare, se $m = n - 1$ sono possibili due casi:

i) $X = Y \times \mathbb{A}^1$, in tal caso non esistono punti critici.

ii) Se X è un chiuso proprio di $Y \times \mathbb{A}^1$ si ha $\dim X = \dim Y$ $I(Y) = I(X) \cap \mathbb{K}[x_1, ..., x_m]$ e l'insieme dei polinomi $f = \sum f_i(x_1, .., x_m) x_n^i \in I(X)$ tali che $f_i \notin I(Y)$ per ogni i è non vuoto; sia g un tale polinomio di grado in x_n minimo ed uguale a $d > 0$.

[1] Rimandiamo a [G-H] pp. 27-33 per i fondamentali di teoria della misura sulle varietà algebriche complesse

Chiaramente $\dfrac{\partial g}{\partial x_n}$ non appartiene a $I(X)$ e quindi $Z = X \cap V(\dfrac{\partial g}{\partial x_n})$ è un chiuso proprio di X. Ragionando come in IX.4.4, se $x \in X - Z$ la proiezione $T_x X \to T_{\phi(x)} Y$ è iniettiva e siccome X e Y sono varietà lisce della stessa dimensione il differenziale è anche surgettivo.

Infine se $n > m + 1$ allora ϕ è la composizione di α e β dove $\alpha\colon \mathbb{A}^n \to \mathbb{A}^{n-1}$, $\beta\colon \mathbb{A}^{n-1} \to \mathbb{A}^m$ sono le proiezioni sulle prime coordinate. Posto $Z \subset \mathbb{A}^{n-1}$ la chiusura di $\alpha(X)$, chiaramente $Z \subset \beta^{-1}(Y)$ ed i morfismi $\alpha\colon X \to Z$ e $\beta\colon Z \to Y$ sono dominanti. Per l'ipotesi induttiva il lemma è vero per α e β e quindi anche per ϕ. □

Dimostrazione di 3.3 Se ϕ non è dominante non c'è nulla da dimostrare. Se ϕ è dominante siano $Z_1, ..., Z_r$ le componenti irriducibili di Z e poniamo $W_i \subset X$ la chiusura di Z, per 3.5 W_i è un chiuso proprio e Z_i è denso in W_i, dato che per ogni $x \in W_i$ vale $T_x W_i \subset T_x X$, i punti critici di $\phi\colon W_i \to Y$ non sono contenuti in nessun chiuso proprio e per 3.5 $\phi(W_i)$ è contenuto in un chiuso proprio di Y. □

ESERCIZIO 2: In caratteristica 0 ogni morfismo iniettivo tra varietà irriducibili della stessa dimensione è birazionale.

Corollario 3.6. *Sia V un sistema lineare di curve piane di grado d e $BS(V) \subset \mathbb{P}^2$ i punti base di V. Se il campo ha caratteristica 0 esiste un aperto nonvuoto $U \subset V$ i cui punti corrispondono a curve liscie su $\mathbb{P}^2 - BS(V)$.*

Dim. Sia $d > 0$ la dimensione di V e siano $F_0, ..., F_d$ le equazioni di una base di V. Le combinazioni lineari di $F_0, ..., F_d$ sono tutte e sole le equazioni delle curve del sistema lineare e $BS(V) = V(F_0, .., F_d)$.

Sia $X \subset \mathbb{P}^d_y \times \mathbb{P}^2_x$ l'ipersuperfice definita da $y_0 F_0(x_0, x_1, x_2) + ... + y_d F_d(x_0, x_1, x_2) = 0$ e $\phi\colon X \to \mathbb{P}^d$ la proiezione sul primo fattore.

Se $[C] \in \mathbb{P}^d \simeq V$ è il punto corrispondente ad una curva C si ha $\phi^{-1}([C]) = \{[C]\} \times C$. I punti singolari di X sono contenuti in $\mathbb{P}^d \times BS(V)$ e quindi la curva C è liscia al di fuori dei punti base se e solo se $[C]$ non appartiene all'immagine dei punti critici di $\phi\colon X - (\mathbb{P}^d \times BS(V)) \to \mathbb{P}^d$. □

4. Esercizi complementari

ESERCIZIO 3: Sia $X \subset G(s, \mathbb{P}^n) \times G(r, \mathbb{P}^n)$ l'insieme delle coppie (V, W) tali che $\dim V \cap W \geq h$. Provare che X è un chiuso irriducibile e se ne calcoli la dimensione.

ESERCIZIO 4: Sia V un sistema lineare di curve piane di grado d, provare che l'insieme delle curve di V che hanno al più nodi come singolarità è un aperto di Zariski.

ESERCIZIO 5: Sia $S \subset \mathbb{P}^3$ superfice cubica liscia, $L \subset S$ retta e $\mathbb{P}^1$ il fascio di piani contenenti L, provare che l'applicazione $\phi_L: S \to \mathbb{P}^1$ definita da $\phi_L(p) = L + p$ se $p \notin L$ e $\phi_L(p) = T_p S$ se $p \in L$ è un morfismo regolare.

ESERCIZIO 6: Siano L, M rette sghembe contenute in una superfice cubica $S \subset \mathbb{P}^3$.

a) provare che esistono esattamente 5 rette $R_1, ...R_5$ in S che intersecano L e M.

b) Provare che l'applicazione $\phi_L \times \phi_M: S \to \mathbb{P}^1 \times \mathbb{P}^1$ è surgettiva, contrae le rette R_i a dei punti p_i ed è iniettiva su $S - (R_1 \cup ... \cup R_5)$.

c) I punti p_i sono in posizione generica, più precisamente ogni corrispondenza su $\mathbb{P}^1 \times \mathbb{P}^1$ di tipo $(1,0)$, $(0,1)$, $(1,1)$ contiene rispettivamente al più $1, 1, 3$ punti p_i.

d) Descrivere in funzione dei punti $p_1, ..., p_5$ le curve di $\mathbb{P}^1 \times \mathbb{P}^1$ che sono immagine tramite $\phi_L \times \phi_M$ delle 27 rette in S.

ESERCIZIO 7: (caratteristica $\neq 2$) Sia $\mathbb{P}^5$ lo spazio delle coniche di $\mathbb{P}^2$, $\Delta \subset \mathbb{P}^5$ l'ipersuperfice cubica delle coniche singolari e $V \subset \Delta$ la varietà (di Veronese) delle rette doppie. Provare che i punti di V sono tutti e soli i punti singolari di Δ. (Sugg. Siccome $Aut(\mathbb{P}^2)$ agisce transitivamente su V basta dimostrare che $\emptyset \neq Sing(\Delta) \subset V$.)

ESERCIZIO 8: Trovare un esempio di morfismo regolare tra varietà irriducibili tale che i punti critici non siano un chiuso.

ESERCIZIO 9: Sia C una quartica piana liscia senza iperflessi; provare che C possiede almeno una bitangente. (Sugg. Sia L una retta fissata, $\mathbb{P}^{14}$ lo spazio delle quartiche e $B_L \subset \mathbb{P}^{14}$ l'insieme delle quartiche C tali che o L è bitangente a C oppure esiste $p \in C$ tale che $\nu_p(C, L) \geq 4$. Provare che B_L è un chiuso irriducibile di dimensione 12).

ESERCIZIO 10: (**) (Le 28 bitangenti)

Caratteristica $\neq 2, 3$. Sia $C \subset \mathbb{P}^2$ una quartica liscia senza iperflessi e sia L una retta bitangente a C (cf. esercizio precedente).

Esiste un sistema di coordinate omogenee x_0, x_1, x_2 tali che le equazioni di L e C sono rispettivamente $x_0 = 0$ e $x_1^2 x_2^2 - 4 x_0 g(x_0, x_1, x_2) = 0$.

Si consideri $\mathbb{P}^2$ come il piano di $\mathbb{P}^3$ di equazione $x_3 = 0$, $o = [0,0,0,1] \in \mathbb{P}^3$ e denotiamo con $\pi: \mathbb{P}^3 - o \to \mathbb{P}^2$ la proiezione di centro o. Sia $S \subset \mathbb{P}^3$ la cubica di equazione $x_0 x_3^2 + x_1 x_2 x_3 + g(x_0, x_1, x_2)$, la curva C coincide con l'insieme dei valori critici della proiezione $\pi: S - o \to \mathbb{P}^2$.

Sia $R = \pi^{-1}(C) \subset S - o$ l'insieme dei punti critici, provare che S è liscia al di fuori di R. Sia $p \in R$, $q = \pi(p)$ ed $H \subset \mathbb{P}^2$ una retta per q, se $q \notin L$ provare che H è tangente a C in q se e solo se $S \cdot \pi^{-1}(H)$ è singolare in p, in particolare S è una cubica liscia (sugg. usare V.3.2).

Dedurre che esiste una bigezione tra le rette contenute in S e le bitangenti a C diverse da L.

ESERCIZIO 11: (**) (Hesse, 1853)

In questo lungo esercizio esaminiamo un diverso approccio alle 28 bitangenti alla quartica generica piana che mette in risalto il fatto che $28 = \binom{8}{2}$ anziché $28 = 27 + 1$. Si lavora su di un campo algebricamente chiuso di caratteristica $\neq 2, 3$.

Sia $V \simeq \mathbb{P}^2$ una rete generica di quadriche di $\mathbb{P}^3$ e denotiamo con $C \subset V$ il luogo discriminante delle quadriche singolari. Provare:

a) V non contiene quadriche riducibili. (Sugg. lo spazio delle quadriche di $\mathbb{P}^3$ ha dimensione 9 mentre quello delle quadriche formate da due piani ha dimensione 6).

b) Si assuma come evidente che V ha esattamente 8 punti base $p_1, .., p_8$ e che in ogni punto p_i non esistano vettori tangenti non nulli tangenti ad ogni quadrica della rete; provare che i punti p_i sono 4 a 4 non contenuti in nessun piano e quindi a maggior ragione 3 a 3 non allineati.

c) Una quadrica irriducibile singolare è un cono quadrico, cioè il cono proiettivo di una conica piana liscia.

d) Sia $Q \in V$ cono quadrico, e $L \subset V$ una retta per Q. Provare che L è tangente a C in Q se e solo se il vertice di Q è un punto base del fascio di quadriche L. In particolare C è liscia e dati due coni quadrici $Q_1, Q_2 \in V$ la retta $Q_1 + Q_2$ è bitangente a C se e solo se il vertice di Q_1 appartiene a Q_2 e viceversa.

e) La generica quartica piana si ottiene come discriminante di una generica rete di quadriche, in particolare C non contiene iperflessi.

f) Sia $L_{ij} \subset V$ il luogo delle quadriche contenenti la retta $p_i + p_j$; provare che L_{ij} è una retta bitangente a C e che $L_{ij} = L_{hk}$ se e solo se $p_i + p_j = p_h + p_k$. (Sugg. è facile dimostrare che L_{ij} è una retta, sia $Q \in L_{ij}$ cono quadrico, necessariamente il vertice di Q è contenuto in $p_i + p_j$ e quindi nel luogo base del fascio L_{ij}.)

g) Viceversa sia $L \subset V$ una retta bitangente a C in Q_1, Q_2, e $H \subset \mathbb{P}^3$ la retta contenente i vertici di Q_1 e Q_2; provare che H è contenuta nel luogo base di L e che quindi $H = p_i + p_j$ per qualche coppia i, j.

h) Utilizzare i punti F) e G) per dedurre che C contiene esattamente $\binom{8}{2} = 28$ bitangenti.

Nota. Nessuno dei due esercizi precedenti descrive il metodo classico di determinazione del numero delle bitangenti ad una quartica liscia. Il metodo più frequentemente usato (in caratteristica 0) è descritto in [Wa, p.154] e fa uso del teorema di dualità e delle formule di Plücker.

ESERCIZIO 12: (*) Caratteristica $\neq 2, 3$. Siano $Q_1, Q_2 \subset \mathbb{P}^3$ coni quadrici tali che il vertice dell'uno sia contenuto nell'altro e tali che la generica quadrica del fascio generato da Q_1, Q_2 sia nonsingolare. Provare che esistono coordinate omogenee su $\mathbb{P}^3$ nelle quali le equazioni di Q_1 e Q_2 sono rispettivamente $x_0 x_2 = x_1^2$, $x_1 x_3 = x_2^2$. In particolare $Q_1 \cap Q_2$ è l'unione di una retta e della curva razionale proiettivamente normale di grado 3.

(Sugg. Siano v_1, v_2 i vertici di Q_1, Q_2, provare per prima cosa che $v_1 \neq v_2$ e che per un piano generico $H \subset \mathbb{P}^3$ le coniche $Q_1 \cap H$ e $Q_2 \cap H$ sono liscie e si intersecano in quattro punti distinti $p_0 = H \cap (v_1 + v_2)$, p_1, p_2, p_3.

Fissato un piano H come sopra ed una radice terza di -1 ξ, si può prendere un sistema di coordinate omogenee tali che $v_1 = [0,0,0,1]$, $v_2 = [1,0,0,0]$, $p_1 = [1,-1,1,-1]$, $p_2 = [1,\xi,\xi^2,-1]$, $p_3 = [1,\xi^2,-\xi,-1]$; scrivere adesso le possibili equazioni dei due coni e giocare con cambi di coordinate dei seguenti tre tipi

i) $x_1 \to x_2$, $x_2 \to -x_1$.

ii) $x_0 \to x_0 - ax_1 - bx_2$.

iii) $x_3 \to x_3 - cx_1 - dx_2$.

fino a quando non si arriva alle equazioni cercate).

ESERCIZIO 13: Caratteristica 0. Sia $S \subset \mathbb{P}^3$ superfice cubica liscia e H piano tale che la cubica piana $C = H \cdot S$ sia liscia. Sia $o \in C$ un flesso e si consideri la legge di gruppo di C avente o come elemento neutro. Provare che la somma dei 27 punti di intersezione di C con le 27 rette in S è uguale a o.

ESERCIZIO 14: (*) Sia $U \subset \mathbb{A}^n$ un aperto e $X \subset U \times \mathbb{P}^m$ chiuso tale che la proiezione $\pi : X \to U$ sia surgettiva e con il differenziale bigettivo in ogni punto. Provare che le fibre di π hanno cardinalità costante. (Sugg. Utilizzare IX.5.9 e induzione su m per ricondursi al caso $m = 1$. Si consideri poi la chiusura $\overline{X}$ di X in $\mathbb{A}^n \times \mathbb{P}^1$ e provare che per ogni $p \in \mathbb{P}^1$ l'ideale di $\overline{X} \cap \mathbb{A}^n \times (\mathbb{P}^1 - p)$ è principale).

Nota: il risultato dell'esercizio 14 continua ad essere vero sotto le ipotesi che U sia una varietà liscia irriducibile ma la dimostrazione richiede strumenti tecnici che non sono presenti nelle note.

ESERCIZIO 15: Mostrare con un esempio che il risultato dell'esercizio precedente è generalmente falso se U è singolare. (Sugg. sia $\mathbb{A}^2 \to aff^2$ data da $(x,y) \to (x^2,y)$ e si prenda X una quartica generica singolare nei punti $(1,0),(-1,0)$).

ESERCIZIO 16: (*) (caratteristica $\neq 2,3$) Sia $U \subset \mathbb{P}^{19}$ l'aperto delle ipersuperfici cubiche liscie di $\mathbb{P}^3$ e sia $X \subset U \times G(1,\mathbb{P}^3)$ l'insieme delle coppie (S,L) tali che $L \subset S$. Provare che X è una varietà liscia e che la proiezione $X \to U$ ha il differenziale bigettivo in ogni punto. Dedurre, utilizzando gli esercizi precedenti che il numero di rette in una superfice cubica liscia è costante e che può essere calcolato in un caso particolare.

ESERCIZIO 17: (*) Si consideri l'anello $A = \mathbb{K}[x,y,z]/(y^2 - p(x), z^2 - q(x))$ con $p, q \in \mathbb{K}[x]$ tali che il prodotto pq sia un polinomio di grado dispari senza radici multiple. Provare che A non è generato ciclicamente su $\mathbb{K}[x]$, cioè che non esiste alcun $f \in A$ tale che $A = \mathbb{K}[x,f]$. (Sugg. Sia per assurdo $f = ay + bz + cyz$, $a,b,c \in \mathbb{K}[x]$, come sopra e sia α una radice di $a^2p - b^2q$. Provare che la mappa maturale $\mathbb{K}[x,f] \to \mathbb{K}[y,z]/(y^2 - p(\alpha), z^2 - q(\alpha))$, $x \to \alpha$, non è surgettiva.)

ESERCIZIO 18: (Teorema di Bertini delle sezioni iperpiane)
Sia $X \subset \mathbb{P}^n$ una varietà proiettiva liscia di dimensione positiva; provare che la generica sezione iperpiana è una varietà liscia. (Sugg. Se $X \neq \mathbb{P}^n$ si consideri $Y \subset X \times (\mathbb{P}^n)^\vee$ l'insieme delle coppie (x,H) tali che $x \in X \cap H$; provare che il luogo Z dei punti critici della proiezione $Y \to (\mathbb{P}^n)^\vee$ è un chiuso irriducibile di dimensione $n-1$.)

XI. Il teorema di Riemann-Roch per curve liscie proiettive

In questo capitolo si assumerà che il lettore abbia una conoscenza di base di algebra commutativa, e.g. [A-M].

Con $\mathbb{K}$ denoteremo un campo algebricamente chiuso fissato.

Con il termine curva intenderemo una varietà quasiproiettiva irriducibile di dimensione 1.

Per ogni varietà irriducibile X denotiamo con $\mathbb{K}(X)$ il campo delle funzioni razionali su X. Se $x \in X$ identificheremo liberamente l'anello $\mathcal{O}_{x,X}$ con il sottoanello di $\mathbb{K}(X)$ formato dalle funzioni razionali che sono definite in x. Denoteremo inoltre $m_x \subset \mathcal{O}_{x,X}$ l'ideale massimale.

1. Grado di un morfismo.

Per facilitare il lettore richiamiamo alcuni risultati di algebra commutativa.

Lemma 1.1. *Sia A un dominio locale Noetheriano di dimensione 1 con ideale massimale m. Le seguenti condizioni sono equivalenti:*

1) m è principale. (3)

2) A è un dominio ad ideali principali.

3) ogni ideale è una potenza di m.

4) A è integralmente chiuso nel suo campo delle frazioni.

5) A è un anello di valutazione discreta.

Dim. [A-M] 9.2. □

(3) Un anello locale Noetheriano di dimensione d tale che l'ideale massimale è generato da d elementi si dice regolare ed è necessariamente un dominio di integrità ([A-M] 11.22).

È istruttivo riportare qui la definizione di anello di valutazione discreta e l'equivalenza 1) $\Leftrightarrow$ 5).

Definizione 1.2. Un dominio di integrità A si dice un anello di valutazione discreta se, detto K il suo campo delle frazioni esiste una funzione $v\colon K^* \to \mathbb{Z}$ tale che:

1) $v(xy) = v(x) + v(y)$.
2) Se $x + y \neq 0$, $v(x+y) \geq \min(v(x), v(y))$.
3) $A = \{x \in K^* | v(x) \geq 0\} \cup \{0\}$.

Una funzione v che soddisfa le condizioni 1) e 2) si chiama una valutazione discreta, usualmente si pone per convenzione $v(0) = \infty$.

Sia A un anello di valutazione discreta con valutazione v e sia $m = \{x \in A | v(x) > 0\}$. m è un ideale e se $x \notin m$ allora $v(x) = v(x^{-1}) = 0$, cioè $x^{-1} \in A$, dunque A è un anello locale con ideale massimale m.

Sia $t \in m$ tale che $v(t)$ è minimo, allora per ogni $x \in m$ vale $v(xt^{-1}) \geq 0$ e dunque $x = ty$ per qualche $y \in A$.

Viceversa supponiamo A dominio Noetheriano di dimensione 1 con ideale massimale principale $m = (t)$. Sia $x \in A$, siccome gli unici ideali primi di A sono 0 e m, se $x \neq 0$ il radicale di (x) è necessariamente m e quindi è ben definito il numero intero $v(x) = \min\{n | m^n \subset (x)\}$.

Se $n = v(x)$ allora esiste $y \in A$ tale che $t^n = xy$. y è un elemento invertibile, altrimenti si avrebbe $y = tz$ e n non sarebbe minimo.

Dunque $v(x) = n$ se e soltanto se $x = t^n y$ con $y \notin m$.

Infine si estende in modo naturale v ad una funzione $K^* \to \mathbb{Z}$ ponendo $v(\frac{x}{y}) = v(x) - v(y)$. Si vede immediatamente che v è la valutazione cercata e per ogni $x \in K^*$ vale $x = t^{v(x)}y$, $y \in A$ invertibile.

Se p è un punto liscio di una curva C, la valutazione associata ad $\mathcal{O}_{p,C}$ si indica usualmente con ord_p.

Lemma 1.3. *Sia A un anello di valutazione discreta con campo delle frazioni K e parametro locale t. Se esiste un sottocampo $\mathbb{K} \subset A$ isomorfo al campo residuo A/m allora per ogni $f \in K$ esiste unico un polinomio P a coefficienti in $\mathbb{K}$ tale che $f - P(t^{-1}) \in m$.*

Dim. Esercizio. □

Il lemma 1.3 si applica in particolare nel caso in cui A è l'anello locale di una curva liscia e K il campo delle funzioni razionali.

Lemma 1.4. *Sia C una curva e $p \in C$. C è liscia in p se e solo se l'ideale $\mathcal{O}_{p,X}$ è un anello di valutazione discreta.*

Dim. Esercizio. □

Definizione 1.5. Sia C una curva Una funzione razionale $t \in \mathbb{K}(C)$ si dice un **parametro locale in** p se $m_p = t\mathcal{O}_{p,C}$.

ESERCIZIO 1: Se A è un anello locale Noetheriano con campo residuo $\mathbb{K}$, l'ideale massimale m è principale se e solo se m/m^2 è uno spazio vettoriale di dimensione 1 su $\mathbb{K}$. (Sugg. Lemma di Nakayama).

ESERCIZIO 2: Sia $X \subset \mathbb{A}^n$ un chiuso irriducibile e siano $f_1, ..., f_s$ generatori dell'ideale $I(X)$. Per ogni $p \in X$ esiste una successione esatta di spazi vettoriali su $\mathbb{K}$

$$\mathbb{K}^s \xrightarrow{J} \mathbb{K}^n \longrightarrow m_p/m_p^2 \longrightarrow 0$$

dove J è la matrice di coefficienti $J_{i,j} = \dfrac{\partial f_j}{\partial x_i}$.

(Sugg. Se p è il punto di coordinate $(a_1, ..., a_n)$ e $M_p \subset k[x_1, ..., x_n]$ è l'ideale generato da $x_1 - a_1, ..., x_n - a_n$ si dimostri che $m_p/m_p^2 = M_p/(I(X) + M_p^2)$ e si consideri lo sviluppo di Taylor dei polinomi f_j nel punto p.)

La retta affine $\mathbb{A}^1$ è una curva liscia, infatti se t è una coordinata affine, $t - a$ genera l'deale massimale nel punto di coordinata a.

$\mathbb{P}^1$ è ricoperto da aperti isomorfi alla retta affine ed è quindi liscio.

Se $F(x_0, x_1, x_2)$ è un polinomio omogeneo irriducibile di grado d, F definisce una curva $X \subset \mathbb{P}^2$, $X = \{x | F(x) = 0\}$.

Un punto $p \in X$ è nonsingolare se le derivate parziali di F rispetto alle coordinate x_0, x_1, x_2 non sono tutte nulle. Infatti, supponiamo per esempio che il punto p sia contenuto nell'aperto affine $\mathbb{A}^2_0 = \{x_0 \neq 0\}$, allora dette $u = \frac{x_1}{x_0}, v = \frac{x_2}{x_0}$ lo sviluppo di Taylor di $F(1, u, v)$ nel punto $p = (u_0, v_0)$ è

$$F(1, u, v) = \alpha(u - u_0) + \beta(v - v_0) + O(2) \qquad (*)$$

dove con $O(2)$ si intende una combinazione lineare di termini di grado ≥ 2.

$u - u_0, v - v_0$ generano l'ideale massimale m_p e $\alpha(u-u_0) + \beta(v-v_0)$ è l'unica relazione di dipendenza lineare in m_p/m_p^2. Dunque $u - u_0$ (risp.: $v - v_0$) è un parametro locale se e soltanto se $\beta \neq 0$ (risp.: $\alpha \neq 0$).

Confrontando $(*)$ con lo sviluppo di Taylor di $F(x_0, x_1, x_2)$ si ha $\alpha = \dfrac{\partial F}{\partial x_1}(1, u_0, v_0)$, $\beta = \dfrac{\partial F}{\partial x_2}(1, u_0, v_0)$ e la tesi segue dalla formula di Eulero

$$x_0 \frac{\partial F}{\partial x_0} + x_1 \frac{\partial F}{\partial x_1} + x_2 \frac{\partial F}{\partial x_2} = deg(F)F$$

Teorema 1.6. *Sia C una curva liscia, $U \subset C$ un aperto e $\phi\colon U \to \mathbb{P}^n$ un morfismo regolare. Allora ϕ si estende ad un unico morfismo $\phi\colon C \to \mathbb{P}^n$.*

Dim. Il problema è locale, posiamo quindi supporre C, U aperti affini e che $\phi(U)$ sia contenuto nel complementare di un iperpiano. Esistono allora $f_0, ..., f_n \in \mathbb{K}[U] \subset \mathbb{K}(C)$ senza zeri comuni in U e tali che in coordinate omogenee $\phi = (f_0, ..., f_n)$.
Sia $p \in C$ e siano $a_i = ord_p(f_i)$, $a = \min(a_i)$. Esiste allora un intorno V di p dove le funzioni razionali $t^a f_i$ sono regolari e senza zeri comuni e quindi $t^a\phi: V \to \mathbb{P}^n$ è un morfismo che estende ϕ. □

Si osservi che se $\phi(U)$ è contenuto in una varietà proiettiva $Y \subset \mathbb{P}^n$ allora anche $\phi(X) \subset Y$, infatti $\phi(X) = \phi(\overline{U}) \subset \overline{Y} = Y$.

Corollario 1.7. *Ogni morfismo birazionale tra due curve liscie proiettive è un isomorfismo.*

Dim. Esercizio. □

Si consideri adesso un morfismo $\phi: X \to Y$ tra curve proiettive. Siccome X è proiettiva ed irriducibile $\phi(X)$ è un sottoinsieme chiuso irriducibile di Y e siccome $\dim Y = 1$ le uniche possibilità sono o ϕ costante oppure ϕ surgettiva.
Consideriamo adesso il caso in cui ϕ è surgettiva, per ogni $q \in Y$, $\phi^{-1}(q)$ è una unione finita di chiusi irriducibili e quindi è un insieme finito di punti.
ϕ è in particolare dominante e quindi induce una estensione di campi $\mathbb{K}(Y) \subset \mathbb{K}(X)$. Siccome $\mathbb{K}(Y), \mathbb{K}(X)$ sono entrambi finitamente generati e di grado di trascendenza 1 su $\mathbb{K}$ necessariamente $\mathbb{K}(X)$ è una estensione algebrica finita di $\mathbb{K}(Y)$.

Definizione 1.8. Il grado di ϕ è la dimensione $deg\phi = [\mathbb{K}(X) : \mathbb{K}(Y)]$ di $\mathbb{K}(X)$ come $\mathbb{K}(Y)$ spazio vettoriale.
Oss: Con la stessa definizione si può definire il grado di un qualsiasi morfismo dominante fra varietà quasiproiettive irriducibili della stessa dimensione.

Ricordiamo il seguente risultato di algebra commutativa

Teorema 1.9.(cf. [Ha] I.3.9A) *Sia F un campo e A una F-algebra finitamente generata. Se A è un dominio di integrità con campo delle frazioni K e $K \subset L$ è una estensione finita di campi allora la chiusura integrale B di A in L è un A-modulo finitamente generato. In particolare B è una F-algebra finitamente generata.*

Dim. [Mat] §33, □

Si ricorda che la chiusura integrale è l'insieme degli elementi di L che sono radici di un polinomio monico a coefficienti in A.

Teorema 1.10. *Sia $\phi: X \to Y$ un morfismo surgettivo tra curve proiettive con X liscia. Allora per ogni aperto affine $U \subset Y$, $V = \phi^{-1}(U)$ è affine e $\mathbb{K}[V]$ è un $\mathbb{K}[U]$-modulo finito.*

Dim. Identifichiamo tramite ϕ $\mathbb{K}(Y)$ con un sottocampo di $\mathbb{K}(X)$ e sia $B \subset \mathbb{K}(X)$ la chiusura integrale di $\mathbb{K}[U]$ in $\mathbb{K}(X)$. Abbiamo visto che B è finito come $\mathbb{K}[U]$-modulo, in particolare B è una $\mathbb{K}$-algebra finitamente generata ed esiste una varietà affine Z tale che $B = \mathbb{K}[Z]$.
$\mathbb{K}(X)$ è algebrico su $\mathbb{K}(Y)$, in particolare per ogni $f \in \mathbb{K}(X)$ esiste $g \in A$ tale che gf è intero su A. Ne segue che $\mathbb{K}(X)$ è il campo delle frazioni di B e che Z ha dimensione 1.
Inoltre B è integralmente chiuso, in accordo con ([A-M] 5.12) ogni suo localizzato è integralmente chiuso e Z è nonsingolare.
Infine se $q \in V$, $\mathcal{O}_{q,X}$ è integralmente chiuso e contiene $\mathbb{K}[U]$, quindi $B \subset \mathcal{O}_{q,X}$ ed esistono inclusioni di $\mathbb{K}$-algebre

$$\mathbb{K}[U] \subset B \subset \mathcal{O}_X(V) = \cap_{q \in V} \mathcal{O}_{q,X}$$

che sono indotte, essendo U, Z affini, da dei morfismi

$$V \xrightarrow{\gamma} Z \xrightarrow{\mu} U \qquad \phi = \mu \circ \gamma$$

γ è un morfismo birazionale e siccome Z è liscia e X proiettiva per il teorema 1.6 esiste un inversa $\gamma^{-1}: Z \to X$. Siccome $\gamma^{-1} \circ \phi = \mu$ deve necessariamente essere $\gamma^{-1}(Z) \subset V$ e $\gamma \circ \gamma^{-1} = Id_Z$.
Infine $\gamma^{-1} \circ \gamma: V \to V$ è l'identità sul sottoinsieme denso $\gamma^{-1}(Z)$ e quindi è l'identità ovunque. □

2. Divisori e sistemi lineari.

Sia X una varietà affine su $\mathbb{K}$ algebricamente chiuso, $A = \mathbb{K}[X]$. Per ogni ideale $J \subset A$ si indica con $V(J) \subset X$ il sottoinsieme chiuso dei punti che annullano J e per ogni sottoinsieme $Z \subset X$ si indica con $I(Z)$ l'ideale delle funzioni regolari nulle su Z.
Il teorema degli zeri afferma che per ogni ideale J $I(Z(J)) = \sqrt{J}$, in particolare gli ideali massimali di A sono tutti e soli quelli della forma $I(p)$, $p \in X$.
Se M è un A-modulo e $p \in X$ si pone $M_p = (A - I(p))^{-1}M$ (cf. [A-M] capitolo 3). M_p è un $\mathcal{O}_{p,X} = A_p$ modulo naturalmente isomorfo a $M \otimes_A \mathcal{O}_{p,X}$ ([A-M] 3.3).

Definizione 2.1. Il **supporto** di M, $Supp(M) \subset X$ è l'insieme dei punti p tali che $M_p \neq 0$.
Si noti che $M_p = 0$ se e soltanto se per ogni $x \in M$ esiste $f \in A$ tale che $f(p) \neq 0$ e $fx = 0$. In particolare se M è finitamente generato $M_p = 0$ se e soltanto se esiste $f \in Ann(M)$ tale che $f(p) \neq 0$, segue quindi immediatamente il

Lemma 2.2. *Per ogni A-modulo Noetheriano M, $Supp(M) = V(Ann(M))$.*

A noi interessano i moduli a supporto finito.

Lemma 2.2. *Sia M un A-modulo Noetheriano tale che $Supp(M) = \{p_1, ..., p_n\}$. Allora esiste un isomorfismo naturale $M = \oplus_{i=1}^n M_{p_i}$ indotto dai morfismi $M \to M_p$, $m \to \frac{m}{1} = m \otimes 1$.*

Dim. Sia $I = Ann(M)$, siccome $M = M \otimes_A \frac{A}{I}$ è sufficiente dimostrare che $\frac{A}{I} = \oplus_{i=1}^n (\frac{A}{I})_{p_i}$.

Dato che $p_1, ..., p_n$ sono le uniche sottovarietà irriducibili di $Supp(M)$ esistono elementi $f_1, ..., f_n \in A$ tali che $f_i(p_j) = \delta_j^i$, $\sum_{i=1}^n f_i = 1$ ed a meno di passare a potenze si può supporre $f_i f_j \in I$ se $i \neq j$; si considera quindi

$$Q_i = (I : f_i) = \{g | g f_i \in I\}$$

Si verifica facilmente che $Z(Q_i) = p_i$ e che esiste un isomorfismo naturale

$$\frac{A}{I} = \oplus_i (\frac{A}{Q_i}) \qquad (*)$$

Si noti che $I = Q_1 \cap ..... \cap Q_n$ è la decomposizione primaria di I ([A-M] cap. 4) e che l'inverso del morfismo naturale $\frac{A}{I} \to \oplus_i (\frac{A}{Q_i})$ è dato da $(g_1, ..., g_n) \to \sum f_i g_i$.

Si osservi infine che per $i \neq j$ $(\frac{A}{Q_j})_{p_i} = 0$ (perché $Q_j \not\subset I(p_i)$), mentre $(\frac{A}{Q_i})_{p_i} = \frac{A}{Q_i}$ (perché è già un anello locale con ideale massimale $I(p_i)/Q_i$).

Le tesi segue quindi considerando le localizzazioni di $(*)$ nei punti p_i. □

Data una curva liscia X si definisce il gruppo dei divisori di X, $Div(X)$ come il gruppo abeliano libero generato dai punti di X. Gli elementi di $Div(X)$ si dicono **divisori**.

Per ogni $p \in X$ esiste un unico omomorfismo $ord_p: Div(X) \to \mathbb{Z}$ tale che $ord_p(p) = 1$ e $ord_p(q) = 0$ se $p \neq q$. ord_p si dice anche la **valutazione** in p.

Il grado di un divisore è la somma di tutte le valutazioni

$$deg(D) = \sum_{p \in X} ord_p(D)$$

Si indica con $Div^0(X)$ il sottogruppo dei divisori di grado 0.

Su $Div(X)$ esiste un ordinamento parziale naturale, $D_1 \leq D_2$ se e soltanto se $ord_p(D_1) \leq ord_p(D_2)$ per ogni $p \in X$. Un divisore ≥ 0 si dice **effettivo**.

Si consideri adesso un morfismo surgettivo $\phi: X \to Y$ di curve liscie proiettive, per ogni $p \in X$ si definisce **l'indice di ramificazione** e_p di ϕ in p nel modo seguente.

Sia $q = \phi(p)$, $m_q \subset \mathcal{O}_{q,Y}$ l'ideale massimale, si pone $e_p = \dim_{\mathbb{K}} \frac{\mathcal{O}_{p,X}}{(\phi^* m_q)}$.

ESERCIZIO 3: Se t è un parametro locale in q, vale $e_p = ord_p(\phi^* t)$.

Un punto $p \in X$ si dice di **ramificazione** (per ϕ) se $e_p > 1$. Dimostreremo più avanti che se l'estensione $\mathbb{K}(Y) \subset \mathbb{K}(X)$ è separabile allora esistono al più un numero finito di punti di ramificazione.

ESERCIZIO 4: Supponiamo che $\mathbb{K}$ abbia caratteristica $p > 0$, si consideri il morfismo $\mathbb{P}^1 \to \mathbb{P}^1$ definito in coordinate omogenee da $(x_0, x_1) \to (x_0^p, x_1^p)$. Dimostrare che l'indice di ramificazione in ogni punto è uguale a p.

Si definiscono due morfismi di gruppi abeliani

$$\phi^*: Div(Y) \to Div(X), \qquad \phi_*: Div(X) \to Div(Y)$$

ponendo per ogni $q \in Y$, $p \in X$

$$\phi^* q = \sum_{p \in \phi^{-1}(q)} e_p \cdot (p), \qquad \phi_* p = \phi(p)$$

ed estendendo per linearità.

Teorema 2.3. *Nelle notazioni precedenti, per ogni $D \in Div(Y)$ vale $deg(\phi^*(D)) = deg(D) deg(\phi)$.*

Dim. Basta chiaramente dimostrare che per ogni $q \in Y$ vale $deg(\phi^*(q)) = deg(\phi)$.

Sia t un parametro locale in q e sia $U \subset Y$ un aperto affine contenente q dove t è regolare e invertibile in $U - q$.

Sia $B = \mathcal{O}_X(\phi^{-1}(U))$, allora per il lemma 2.2 il grado di $\phi^*(q)$ è uguale alla dimensione di $B/(\phi^* t)$ come $\mathbb{K}$-spazio vettoriale.

Siano $u_1, ..., u_d$ elementi di B che inducono una $\mathbb{K}$-base di $B/(\phi^* t)$ e dimostriamo che sono una $\mathbb{K}(Y)$-base di $\mathbb{K}(X)$.

Per semplicità di notazione identifichiamo $\mathbb{K}(Y)$ con la sua immagine $\phi^* \mathbb{K}(Y) \subset \mathbb{K}(X)$.

1) $u_1, ..., u_d$ sono $\mathbb{K}(Y)$ linearmente indipendenti.

Sia per assurdo $\sum f_i u_i = 0$ con $f_i \in \mathbb{K}(Y)$ non tutti nulli, moltiplicando per un denominatore comune posso supporre $f_i \in \mathcal{O}_Y(U)$ e dividendo per una opportuna potenza di t posso supporre che $f_i(q)$ non siano tutti nulli. La riduzione modulo t è allora una relazione di equivalenza lineare in $B/(t)$.

2) $u_1, ..., u_s$ generano $\mathbb{K}(X)$.

Sia $S = \mathcal{O}_Y(U) - I(q)$, S è una parte moltiplicativa e $S^{-1}B$ è un $\mathcal{O}_{q,Y}$ modulo finito, per il lemma di Nakayama $u_1, ..., u_d$ generano $S^{-1}B$. Si conclude osservando

che essendo $S^{-1}B$ la chiusura integrale di $\mathcal{O}_{q,Y}$, $S^{-1}B$ genera $\mathbb{K}(X)$ come $\mathbb{K}(Y)$ spazio vettoriale. □

Se f è una funzione razionale su una curva liscia X posso definire il divisore associato $div(f) = \sum_p ord_p(f)$.

Corollario 2.4. *Se X è liscia e proiettiva e $f \in \mathbb{K}(X)$ allora $div(f)$ ha grado 0.*

Dim. Si può considerare f come un morfismo $f: X \to \mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ e $div(f) = f^*((0) - (\infty))$. □

Definizione 2.5. Il divisore di una funzione razionale si dice **principale**, i divisori principali su una curva liscia proiettiva formano un sottogruppo $P(X) \subset Div^0(X)$.
Si pone infine $Pic(X) = Div(X)/P(X)$, $Pic^0(X) = Div^0(X)/P(X)$. Due divisori si dicono linearmente (o razionalmente) equivalenti se la loro differenza è un divisore principale, dunque $Pic(X)$ classifica i divisori modulo equivalenza lineare.
Due divisori linearmente equivalenti hanno lo stesso grado, il viceversa è in generale falso, vale infatti

Proposizione 2.6. *$\mathbb{P}^1$ è l'unica curva liscia proiettiva tale che $Pic^0 = 0$.*

Dim. Se t è una coordinata affine allora il divisore della funzione razionale $t - a$ è $(a) - (\infty)$. Dunque tutti i punti sono equivalenti a ∞ e ogni divisore di grado d è linearmente equivalente a $d(\infty)$.
Viceversa, se $Pic^0(X) = 0$, presi due punti $q \neq p$ in X esiste una funzione razionale non costante f tale che $div(f) = p - q$. Se pensiamo f come un morfismo $f: X \to \mathbb{P}^1$ è $f^*((0) - (\infty)) = p - q$ e l'unica possibilità è che $f^*(0) = p$. In particolare $deg(f) = 1$ e f è un morfismo birazionale, quindi un isomorfismo. □

Uno dei problemi più importanti nello studio delle curve algebriche è quello di determinare l'insieme dei divisori effettivi linearmente equivalenti ad un divisore dato.
Sia X una curva liscia proiettiva fissata, per ogni divisore D su X si definisce

$$H^0(D) = \{f \in \mathbb{K}(X) \mid div(f) + D \geq 0\}$$

H^0 è un $\mathbb{K}$-sottospazio vettoriale di $\mathbb{K}(X)$ ed esiste una bigezione tra il proiettivizzato $\mathbb{P}(H^0(D))$ e l'insieme $|D|$ dei divisori effettivi linearmente equivalenti a D.
Si consideri infatti l'applicazione $\gamma: H^0(D) - \{0\} \to |D|$ che ad ogni funzione razionale f associa il divisore effettivo $D + div(f)$.
γ è surgettiva per costruzione, viceversa se $\gamma(f) = \gamma(g)$ allora $div(fg^{-1}) = 0$, cioè fg^{-1} è una funzione regolare su X e quindi costante.
Si noti che se il grado di D è negativo allora $|D| = \emptyset$ e $H^0(D) = 0$.

Proposizione 2.7. *Sia D un divisore qualsiasi ed E un divisore effettivo su una curva liscia proiettiva. Allora i $\mathbb{K}$-spazi vettoriali $H^0(D), H^0(D+E)$ hanno dimensione finita e vale*

$$\dim H^0(D+E) \leq H^0(D) + deg(E).$$

In particolare $\dim H^0(E) \leq deg(E) + 1$.

Dim. $H^0(0)$ è lo spazio delle funzioni regolari su X e quindi $H^0(0) = \mathbb{K}$. Per induzione su $deg(E)$ basta dimostrare la proposizione nel caso $E = p$.
Sia dunque $E = p$ e sia $ord_p(D) = a$, allora se t è un parametro locale in p, tutte le funzioni di $H^0(D+p)$ si possono scrivere come $t^{-a-1}g$ con $g \in \mathcal{O}_p$.
Chiaramente $H^0(D) \subset H^0(D+p)$ è esattamente il nucleo dell'applicazione lineare $H^0(D+p) \to \mathbb{K}$, data da $t^{-a-1}g \to g(p)$. Quindi ha codimensione al più 1. □
Se $D' = D + div(f)$ è un divisore linearmente equivalente a D allora $fH^0(D') = H^0(D)$. Si pone $h^0(D) = \dim H^0(D)$. Il seguente corollario è quindi immediato

Corollario 2.8. *Se $D \sim D'$ allora $h^0(D) = h^0(D') \leq \max(0, deg(D) + 1)$*

Dato un divisore D, un sottospazio proiettivo L di $|D|$ si dice un **sistema lineare** su X. Se $L = |D|$ il sistema lineare si dice **completo**.
Anticamente L veniva chiamato un g^l_d se $deg(D) = d$, $dim(L) = l$ e la proposizione 2.7 si enunciava dicendo che non esistevano g^l_d con $l > d$.

ESERCIZIO 5: $X = \mathbb{P}^1$ se e soltanto se esiste un g^1_1.

Esempio 2.9. Se $X = \mathbb{P}^1$ e $deg(D) = d > 0$ allora $h^0(D) = d + 1$. Infatti divisori dello stesso grado sono linearmente equivalenti e per il corollario 2.8 è sufficiente dimostrare che $h^0(d(\infty)) = d + 1$.
$H^0(d(\infty))$ è lo spazio vettoriale delle funzioni regolari su $\mathbb{A}^1$ che hanno un polo di ordine al più d all'infinito. Tali funzioni sono tutti e soli i polinomi di grado $\leq d$ in una coordinata affine.

Esempio 2.10. Sia C una curva piana liscia, per il teorema del resto V.5.2 i divisori aggiunti di grado fissato su C formano un sistema lineare completo.

Come nel caso delle curve piane se X è una curva liscia proiettiva e $o \in X$ è un punto fissato per ogni $s > 0$ si definisce una mappa

$$\mu_s: X^s \to Pic^0(X), \qquad \mu_s(p_1, ..., p_s) = p_1 + ... + p_s - so$$

Dimostreremo nella prossima sezione che μ_s è surgettiva per $s >> 0$, ha senso quindi dare la seguente

Definizione 2.11.(Weierstrass) Il minimo intero $g = g(X)$ tale che la mappa μ_g è surgettiva si dice **genere** della curva X.

3. Il Teorema di Riemann-Roch. Prima parte.

Sia X una curva liscia proiettiva fissata, nella sezione precedente abbiamo dimostrato che per ogni coppia di divisori D, E con E effettivo vale $h^0(D+E) \leq h^0(D) + deg(E)$.

Definizione 3.1. Un divisore D si dice **speciale**[1] se esiste un divisore effettivo E tale che $h^0(D+E) < h^0(D) + deg(E)$.

Definizione 3.2. Un divisore speciale massimale (rispetto all'ordinamento usuale di $Div(X)$) si dice **canonico**.

Si noti che un divisore linearmente equivalente ad un divisore speciale (canonico) è ancora speciale (canonico).

Se $X = \mathbb{P}^1$ un divisore è speciale se e soltanto se ha grado ≤ -2.

Questa sezione è interamente dedicata alla dimostrazione del seguente

Teorema 3.3.(Riemann-Roch, prima parte) *X curva liscia proiettiva su campo $\mathbb{K}$ algebricamente chiuso.*
1) Esiste un divisore canonico $K \in Div(X)$ unico a meno di equivalenza lineare e $g(X) = h^0(K)$.
2) Per ogni divisore D su X vale

$$h^0(D) - h^0(K-D) = deg(D) + 1 - g(X)$$

Il punto essenziale della dimostrazione è il seguente

Lemma 3.4. *Esiste su X un divisore effettivo non speciale.*

Dim. Assumiamo per assurdo che ogni divisore effettivo sia speciale, esiste allora trovare una catena infinita $0 < D_1 < D_2 < .. < D_n < ..$ di divisori effettivi tali che per ogni n, $h^0(D_n) \leq deg(D_n) + 1 - n$.
Prendiamo una qualsiasi funzione razionale $f: X \to \mathbb{P}^1$ non costante e poniamo $Q_n = f^* f_* D_n$. Se d è il grado di f e d_n il grado di D_n allora $Q_n - D_n$ è un divisore effettivo di grado $(d-1)d_n$ e quindi per 2.7 $h^0(Q_n) \leq dd_n + 1 - n$.
Sia $g_1, ..., g_d$ una base di $\mathbb{K}(X)$ come $\mathbb{K}(f) = \mathbb{K}(\mathbb{P}^1)$-spazio vettoriale e sia G un divisore effettivo tale che $g_1, ..., g_d \in H^0(G)$ (basta prendere come G la somma dei divisori di polo delle g_i). Per il solito lemma 2.7 $h^0(Q_n + G) \leq dd_n + 1 - n + deg(G)$.
D'altra parte per ogni i vale $g_i H^0(f_* D_n) \subset H^0(Q_n + G)$ e siccome le g_i sono linearmente indipendenti vale $h^0(Q_n + G) \geq d h^0(f_* D_n) = d(d_n + 1)$, il che non è possibile per $n \geq deg(G)$. □

[1] questa definizione differisce da quella che si trova usualmente in letteratura dove ad un divisore speciale si richiede di essere anche effettivo

Esiste un criterio di specialità basato sulle classi di ripartizione (cf. [Se1]). L'introduzione delle ripartizioni è suggerita dalla teoria delle adele di Weil [We].

Definizione 3.5. Una **ripartizione** è una applicazione $r: X \to \mathbb{K}(X)$ tale che $ord_p(r(p)) \geq 0$ eccetto un numero finito di punti.
Denotiamo con R il $\mathbb{K}(X)$-spazio vettoriale delle ripartizioni e identifichiamo $\mathbb{K}(X)$ con il sottospazio di R delle ripartizioni costanti.
Se D è un divisore si definisce $R(D) = \{r \in R | \, ord_p(D) + ord_p(r(p)) \geq 0, \forall p \in X\}$.
$R(D)$ è uno spazio vettoriale su $\mathbb{K}$ ma non su $\mathbb{K}(X)$, infatti per ogni $f \in \mathbb{K}(X)$ vale $fR(D) = R(D - div(f))$.
Una classe di ripartizione è un elemento del $\mathbb{K}$-spazio vettoriale

$$I(D) = \frac{R}{R(D) + \mathbb{K}(X)}$$

Se $f \in \mathbb{K}(X)$ la moltiplicazione per f induce un isomorfismo $fI(D) = I(D - div(f))$ mentre se $D_1 \leq D_2$ esiste una proiezione naturale $I(D_1) \to I(D_2)$.
È quindi possibile definire per ogni coppia di divisori D_1, D_2 un applicazione $\mathbb{K}$-bilineare

$$H^0(D_1) \times I(D_2) \to I(D_1 + D_2).$$

Infatti se $r \in I(D_2)$ allora $fr \in I(D_2 - div(f))$ e se $f \in H^0(D_1)$ esiste una proiezione naturale $I(D_2 - div(f)) \to I(D_1 + D_2)$.

Lemma 3.6. *Se $I(D) \neq 0$ allora D è speciale.*

Dim. Basta dimostrare che esiste un punto $p \in X$ ed un intero positivo h tale che $H^0(D + hp) = H^0(D + (h-1)p)$.
Per ogni $r \in R$ definiamo

$$N(r, D) = \{p \in X | \, ord_p(r) + ord_p(D) < 0\}$$

$$n(r, D) = -\sum_{p \in N(r,D)} (ord_p(r(p)) + ord_p(D))$$

Per definizione $r \in R(D)$ se e soltanto se $n(r, D) = 0$.
Sia $r \notin R(D) + \mathbb{K}(X)$ una ripartizione che minimizza $n(r, D)$, scegliamo $p \in N(r, D)$ e prendiamo $h = -(ord_p(r(p)) + ord_p(D))$. Se per assurdo $H^0(D+hp) \neq H^0(D+(h-1)p)$ allora esiste una $f \in H^0(D+hp)$ tale che $ord_p(f) = -ord_p(D) - h = ord_p(r(p))$.
Quindi è possibile trovare $\alpha \in \mathbb{K}$ tale che $ord_p(r(p) - \alpha f) > ord_p(r(p))$.
Se $q \neq p$, $ord_q(f) + ord_q(D) \geq 0$, $ord_q(r(q) - \alpha f) + ord_q(D) \geq ord_q(r(q)) + ord_q(D)$ e quindi $N(r - \alpha f, D) \subset N(r, D)$, $n(r + f, D) < n(r, D)$ in contraddizione con la scelta di r. □

Corollario 3.7. *Esiste un divisore effettivo D tale che $I(D) = 0$.*

Lemma 3.8. *Per ogni divisore D e per ogni punto $p \in X$ esiste una successione esatta*

$$0 \longrightarrow H^0(D) \longrightarrow H^0(D+p) \xrightarrow{\alpha} k \xrightarrow{\overline{\beta}} I(D) \longrightarrow I(D+p) \longrightarrow 0$$

Dim. Sia $h = ord_p(D)$ e t un parametro locale in p, per ogni $f \in H^0(D+p)$ si pone $\alpha(f) = a$ dove a è l'unica costante tale che $ord_p(f - at^{-(h+1)}) \geq -h$.
Se $a \in \mathbb{K}$ si pone $\overline{\beta}(a)$ come la classe della ripartizione $\beta(a)\colon X \to \mathbb{K}(X)$ che vale 0 per $q \neq p$ e $at^{-(h+1)}$ nel punto p.
L'esattezza della successione in $H^0(D), H^0(D+p), I(D+p)$ è banale.
Se $f \in H^0(D+p)$ allora $\beta(\alpha(f)) - f \in R(D)$ e quindi $\beta(\alpha(f)) \in R(D) + \mathbb{K}(X)$ e $\overline{\beta} \circ \alpha = 0$.
Si osservi che $R(D+p)/R(D) = \mathbb{K}$ ed è generato da $\beta(1)$, quindi $\overline{\beta}$ induce una applicazione surgettiva fra $\mathbb{K}$ e il nucleo della proiezione $I(D) \to I(D+p)$ che è isomorfo a $(R(D+p) + \mathbb{K}(X))/(R(D) + \mathbb{K}(X))$.
Rimane da dimostrare che se $\overline{\beta}(1) = 0$ allora α è surgettiva, ma se $\beta(a) = r + f$ con $f \in \mathbb{K}(X), r \in r(D)$ allora necessariamente $f \in H^0(D+p)$ e $\alpha(f) = a$. □

Corollario 3.9. *Per ogni D, $h^1(D) = \dim_k I(D) < \infty$ e vale la formula*

$$h^0(D) - h^1(D) = deg(D) + 1 - h^1(0)$$

Dim. Se E è un divisore effettivo non speciale allora $h^1(E) = 0$ e possiamo passare da 0 ad E in un numero finito di passi, aggiungendo un punto ad ogni passo, se segue che, per la successione esatta precedente, $h^1(0) \leq deg(E)$.
Analogamente possiamo raggiungere ogni divisore da 0 in un numero finito di passi ogni volta aggiungendo o togliendo un punto, per la successione esatta la quantità $h^0(D) - h^1(D) - deg(D)$ resta costante. □

Corollario 3.10. *Un divisore D è speciale se e soltanto se $I(D) \neq 0$.*

Dim. Se $I(D) = 0$ allora per ogni divisore effettivo E, $I(D+E) = 0$ e per il corollario 6 $h^0(D+E) - h^0(D) = deg(E)$. □

Corollario 3.11. *Esiste un intero N tale che ogni divisore speciale ha grado minore o uguale a N.*

Dim. Sia E un divisore effettivo non speciale e poniamo $N = deg(E) + h^1(0)$. Se $deg(D) \geq N$ per il corollario 3.9 $h^0(D-E) > 0$ ed esiste un divisore effettivo D_0 tale che D è linearmente equivalente a $E + D_0$ che non è speciale. □

Corollario 3.12. *Esistono divisori canonici e per ogni divisore canonico K vale $h^1(K) = 1$.*

Dim. L'esistenza segue immediatamente da 3.11, mentre per il corollario 3.10 $h^1(K) > 0$.
Se fosse $h^1(K) > 1$ allora per ogni punto p si avrebbe $h^1(K+p) \neq 0$ in contraddizione con la massimalità di K. □

Consideriamo adesso l'insieme J delle applicazioni $\mathbb{K}$-lineari $\phi\colon R \to \mathbb{K}$ tali che $\phi = 0$ su $R(D) + \mathbb{K}(X)$ per qualche divisore D, dipendente da ϕ. Per ogni divisore D, $I(D)^\vee = \mathrm{Hom}(I(D), \mathbb{K})$ è i modo naturale un sottospazio di $R^\vee$ e J è l'unione di tutti gli $I(D)^\vee$ al variare di $D \in Div(X)$.
J ha una struttura di $\mathbb{K}(X)$ spazio vettoriale indotta dal prodotto $f\phi(r) = \phi(fr)$, $f \in \mathbb{K}(X)$, $r \in R$.

Lemma 3.13. *J è uno spazio vettoriale di dimensione 1 su $\mathbb{K}(X)$.*

Dim. Se D ha grado ≤ -2 allora $I(D) \neq 0$ e quindi $J \neq 0$, assumiamo per assurdo che esistano $\phi_1, \phi_2 \in J$ linearmente indipendenti su $\mathbb{K}(X)$.
Sia D un divisore tale che $\phi_1, \phi_2 \in I(D)^\vee$, allora per ogni coppia $f_1, f_2 \in H^0(E)$ vale $f_1\phi_1 + f_2\phi_2 \in I(D-E)^\vee$ e siccome ϕ_1, ϕ_2 sono indipendenti si ha $2h^0(E) \leq h^1(D-E)$, facendo tendere il grado di E all'infinito otteniamo una contraddizione per il corollario 3.9. □

Sia K un divisore canonico e sia π un generatore di $I(K)^\vee \simeq \mathbb{K}$. π è allora anche un generatore di J come spazio vettoriale su $\mathbb{K}(X)$.

Lemma 3.14. *Nelle notazioni precedenti sia $f \in \mathbb{K}(X)$. Vale $f\pi \in I(K-D)^\vee$ se e soltanto se $f \in H^0(D)$. In particolare per ogni divisore D vale $h^0(D) = h^1(K-D)$.*

Dim. Abbiamo già visto che se $f \in H^0(D)$ allora $f\pi \in I(K-D)^\vee$. Viceversa supponiamo che $f\pi \in I(K-D)^\vee$, questo significa che per ogni $r \in R(K-D) + \mathbb{K}(X)$, $\pi(fr) = 0$, cioè $fr \in R(K) + \mathbb{K}(X)$.
Sia $p \in X$ e supponiamo per assurdo che $ord_p(f) + ord_p(D) < 0$. Denotiamo con $a = ord_p(f)$, $b = ord_p(D)$, $c = ord_p(K)$, siccome $I(K+p) = 0$, la successione esatta del lemma 3.8 implica che se t è un parametro locale in p, allora la ripartizione $r(p) = t^{-(c+1)}$, $r(q) = 0$ se $q \neq p$ non appartiene a $R(K) + \mathbb{K}(X)$.
Osserviamo però che, essendo $-a - c - 1 \geq b - c$ la ripartizione $f^{-1}r$ appartiene a $R(K-D)$ in contraddizione con le ipotesi. □

Lemma 3.15. *Nelle notazioni precedenti μ_s è surgettiva se e solo se $s \geq h^1(0)$ e quindi $h^1(0)$ è uguale al genere di X.*

Dim. Per definizione μ_s è surgettiva se e solo se $h^0(D) > 0$ per ogni divisore D di grado s. Se $deg(D) \geq h^1(0)$ per 3.9 si ha $h^0(D) \geq \deg(D) + 1 - h^1(0) > 0$. Viceversa

se $s < h^1(0)$ e D_1, D_2 sono divisori effettivi generici di grado $d, d-s$ rispettivamente con $d >> 0$ si ha $h^0(D_1 - D_2) = \max(0, h^0(D_1) - \deg(D_2)) = 0$. □

Dimostrazione del teorema 3.3. Se K_1, K_2 sono divisori canonici allora per il lemma 3.13 $h^0(K_1 - K_2) = h^1(K_2) = 1$, e $K_1 - K_2$ è linearmente equivalente ad un divisore effettivo E con $deg(E) = deg(K_1) - deg(K_2)$, similmente $h^0(K_2 - K_1) = 1$ e quindi $deg(E) \leq 0$, ma l'unico divisore effettivo di grado 0 è il divisore nullo. Questo prova che K_1 e K_2 sono linearmente equivalenti. Sempre per il lemma 3.13 $h^0(K) = h^1(0)$ e basta applicare 3.9 e 3.15. □

4. Estensioni separabili e differenziali razionali.

Ricordiamo che, dato un campo $\mathbb{K}$, un polinomio irriducibile $P \in \mathbb{K}[x]$ si dice separabile se non ha radici multiple nel suo campo di spezzamento. P irriducibile è separabile se e soltanto la sua derivata P' rispetto alla variabile x è non nulla.

Sia $\mathbb{K} \subset K$ una estensione algebrica, un elemento $a \in K$ si dice separabile su $\mathbb{K}$ se è separabile il suo polinomio minimo $\mu_a \in \mathbb{K}[x]$. K si dice separabile su $\mathbb{K}$ se è separabile ogni suo elemento.

Un campo si dice **perfetto** se ogni sua estensione algebrica è separabile. In caratteristica 0 ogni campo è separabile mentre in caratteristica positiva p un campo $\mathbb{K}$ è perfetto se e soltanto se $\mathbb{K} = \mathbb{K}^p$.

Se $\mathbb{K} \subset K \subset L$ sono estensioni algebriche con K separabile su $\mathbb{K}$ e L separabile su K allora L è separabile su $\mathbb{K}$.

Una estensione algebrica $\mathbb{K} \subset K$ si dice puramente inseparabile se nessun elemento di $K - \mathbb{K}$ è separabile su $\mathbb{K}$, si vede facilmente che una estensione è puramente inseparabile se e soltanto se il polinomio minimo di ogni elemento è del tipo $x^{p^a} - b$, $p =$caratteristica.

Data una estensione algebrica $\mathbb{K} \subset K$ esiste unico un campo intermedio E detto **chiusura separabile** tale che E è separabile su $\mathbb{K}$ e K è puramente inseparabile su E. Se $[K : \mathbb{K}] < \infty$ si pone $[K : \mathbb{K}]_s = [E : \mathbb{K}]$ grado separabile, $[K : \mathbb{K}]_i = [K : E]$ grado inseparabile, il grado inseparabile è sempre una potenza di p.

Una estensione non necessariamente algebrica $\mathbb{K} \subset K$ si dice separabile se esiste una fattorizzazione $\mathbb{K} \subset E \subset K$ con $\mathbb{K} \subset E$ trascendente pura e K separabile su E.

Teorema 4.1. *Sia $\mathbb{K} \subset K$ una estensione finitamente generata di campi di caratteristica $p > 0$ e sia $\mathbb{K}^{\frac{1}{p}}$ il campo delle radici p-esime degli elementi di $\mathbb{K}$.*

K è separabile su $\mathbb{K}$ se e soltanto se la $\mathbb{K}$-algebra $K \otimes_{\mathbb{K}} \mathbb{K}^{\frac{1}{p}}$ non ha nilpotenti.

Dim. [Mat] 26.2 oppure [La] capitolo 10. □

Corollario 4.2. *Ogni estensione finitamente generata di un campo perfetto $\mathbb{K}$ è separabile.*

Dim. In caratteristica 0 non c'è nulla da dimostrare, in caratteristica p, siccome $\mathbb{K}$ è perfetto $\mathbb{K} = \mathbb{K}^{\frac{1}{p}}$. □

Per estensioni con grado di trascendenza 1 è possibile migliorare il corollario precedente

Teorema 4.3. *Sia $\mathbb{K}$ campo perfetto di caratteristica $p > 0$, $\mathbb{K} \subset K$ una estensione finitamente generata con grado di trascendenza 1.*

Sia $t \in K$ trascendente su $\mathbb{K}$, allora K è separabile su $\mathbb{K}(t)$ se e soltanto se $t \notin K^p$.

Dim. La dimostrazione si divide in 5 passi.

1) $[K : K^p] = p$. Sia $a_1, ..., a_n$ una $\mathbb{K}(t)$-base di K, allora $a_1^p, ..., a_n^p$ è una $\mathbb{K}(t)^p$ base di K^p. $\mathbb{K}$ è perfetto, dunque $\mathbb{K}(t)^p = \mathbb{K}(t^p)$ e quindi

$$np = [K : \mathbb{K}(t)][\mathbb{K}(t) : \mathbb{K}(t^p)] = [K : K^p][K^p : \mathbb{K}(t^p)]$$

2) Se $a \in K - K^p$ il suo polinomio minimo su K^p è $x^p - a^p$.

Sia $\mu_a \in K^p[x]$ il polinomio minimo di a, è evidente che μ_a divide $x^p - a^p = (x-a)^p$ e quindi possiede una sola radice nel suo campo di spezzamento. Se avesse grado minore di p allora $\mu_a' \neq 0$ e quindi a sarebbe separabile su K^p.

3) K non è separabile su K^p e se $a \in K - K^p$ allora $K^p(a) = K$.

Segue banalmente da 1) e 2).

4) Se $t \in K^p$ allora K non è separabile su $\mathbb{K}(t)$.

Infatti $\mathbb{K}(t) \subset K^p$ e la tesi segue dal punto 3.

5) Se $t \notin K^p$ allora K è separabile su $\mathbb{K}(t)$.

Sia $E \subset K$ la chiusura separabile di $\mathbb{K}(t)$, K è finitamente generato e quindi esiste $a \geq 0$ tale che $K^{p^a} \subset E$. Per i punti 1), 2) e 3) vale $K^{p^a}(t) = K \subset E$. □

Corollario 4.4. *Sia X una curva liscia proiettiva su un campo algebricamente chiuso $\mathbb{K}$ di caratteristica p e sia $f \in \mathbb{K}(X)$ tale che $div(f)$ non è p-divisibile in $Div(X)$, allora $\mathbb{K}(f) \subset \mathbb{K}(X)$ è separabile.*

Siano $A \subset B$ anelli commutativi con 1 e sia M un B-modulo. Una applicazione $\partial: B \to M$ si dice una A-derivazione se:

i) ∂ è A-lineare.

ii) $\partial(b_1 b_2) = b_1 \partial(b_2) + b_2 \partial(b_1)$ $\forall b_1, b_2 \in B$ (regola di Leibnitz).

Si noti che per ii) $\partial(1) = \partial(1) + \partial(1) = 0$ e per i) $\partial(a) = 0$ per ogni $a \in A$.

ESERCIZIO 6: Una $\mathbb{Z}$-derivazione $\partial: B \to M$ è una A-derivazione se e solo se $\partial(a) = 0$ per ogni $a \in A$.

Se $\partial: B \to M$ è una A-derivazione e $b \in B$ anche $b\partial$ è una A-derivazione e più in generale per ogni morfismo di B-moduli $\phi: M \to N$ la composizione $\phi \circ \partial$ è ancora una A-derivazione. L'insieme delle A-derivazioni da B in M forma un B-modulo $Der_A(B, M)$.

Esiste una derivazione universale $B \xrightarrow{d} \Omega_{B/A}$ tale che per ogni A-derivazione $\partial: B \to M$ esiste unico un morfismo di B-moduli $\phi: \Omega_{B/A} \to M$ tale che $\partial = \phi \circ d$.

Un possibile modo di costruire $\Omega_{B/A}$ è il seguente: Si consideri la struttura di B-modulo su $B \otimes_A B$ indotta dalla moltiplicazione a sinistra e si prenda $\Omega_{B/A} = B \otimes_A B/R$ dove R è il B-sottomodulo generato dalle relazioni

$$1 \otimes b_1 b_2 - b_1 \otimes b_2 - b_2 \otimes b_1 \qquad \forall b_1, b_2 \in B$$

L'applicazione $d: B \to \Omega_{B/A}$, $db = 1 \otimes b$ è una A-derivazione e gode della proprietà universale (esercizio).

Si noti che se $b_1, ..., b_s$ generano B come A-algebra allora $db_1, ..., db_s$ generano $\Omega_{B/A}$ come B-modulo.

ESERCIZIO 7: Se $S \subset B$ è una parte moltiplicativa allora $\Omega_{S^{-1}B/A} = S^{-1}\Omega_{B/A}$.

Per ogni B-modulo M esiste un accoppiamento B-bilineare

$$<,>: \Omega_{B/A} \times Der_A(B, M) \to M$$

tale che $< db, \partial >= \partial b$ per ogni $b \in B$, definito nel modo seguente: Se $\partial = \phi \circ d \in Der_A(B, M)$, si pone $< \omega, \partial >= \phi(\omega) \in M$.

Esempio 4.5. Se $\mathbb{K} \subset \mathbb{K}(t_1, ..., t_d) = K$ è una estensione puramente trascendente di campi allora $dt_1, ..., dt_n$ sono una K-base di $\Omega_{K/\mathbb{K}}$.

Infatti una $\mathbb{K}$-derivazione $\partial: K \to V$ è unicamente determinata dai ∂t_i e quindi $dt_1, ..., dt_n$ è un sistema di generatori. D'altra parte le derivate parziali rispetto alle variabili t_i sono $\mathbb{K}$-derivazioni, $< dt_i, \dfrac{\partial}{\partial t_j} >= \delta_{ij}$ e quindi $dt_1, ..., dt_n$ sono linearmente indipendenti.

Ogni morfismo di A-algebre $\phi: B \to C$, composto con la derivazione universale di C definisce una derivazione $B \to \Omega_{C/A}$ e per la proprietà universale di $\Omega_{B/A}$ esiste unico un morfismo di C-moduli $\phi_*: C \otimes_B \Omega_{B/A} \to \Omega_{C/A}$ tale che $\phi_*(db) = d(\phi b)$ per ogni $b \in B$.

ESERCIZIO 8: Se $A \subset B \subset C$ esiste una successione esatta

$$C \otimes_B \Omega_{B/A} \longrightarrow \Omega_{C/A} \longrightarrow \Omega_{C/B} \longrightarrow 0$$

Esempio 4.6. $\mathbb{K}$ campo di caratteristica $p > 0$, $\mathbb{K} \subset \mathbb{K}(t) = K$ estensione trascendente pura. Sia $\phi: K \to K$ l'omomorfismo di $\mathbb{K}$-algebre tale che $\phi(t) = t^p$,

allora il morfismo indotto $\phi_*: \Omega_{K/\mathbb{K}} \to \Omega_{K/\mathbb{K}}$ è nullo. Infatti dt genera il modulo dei differenziali e $\phi_*(dt) = dt^p = 0$.

Lemma 4.7. *Sia $\mathbb{K} \subset K \subset L$ estensione di campi con L algebrico separabile su K, allora esiste un isomorfismo naturale $\Omega_{L/\mathbb{K}} = L \otimes_K \Omega_{K/\mathbb{K}}$.*

Dim. Denotiamo con $\alpha: L \otimes \Omega_{K/\mathbb{K}} \to \Omega_{L/\mathbb{K}}$ il morfismo indotto dall'inclusione $K \subset L$.

1) α è surgettiva.

Basta dimostrare che ogni dl, $l \in L$ è una combinazione lineare a coefficienti in L di elementi df, $f \in K$.

Sia $l \in L$ e sia $\mu_l = \sum f_i x^i$ il suo polinomio minimo su K, allora $0 = d\mu_l(l) = \sum df_i l^i + \mu_l'(l)dl$ ed essendo l separabile $\mu_l'(l) \neq 0$.

2) α è iniettiva.

Basta trovare una derivazione $\partial: L \to L \otimes_K \Omega_{K/\mathbb{K}}$ che estende $1 \otimes d: K \to L \otimes_K \Omega_{K/\mathbb{K}}$. Tale derivazione indurrà un morfismo L lineare $\beta: \Omega_{L/\mathbb{K}} \to L \otimes_K \Omega_{K/\mathbb{K}}$ che sarà l'inverso a sinistra di α.

Per il lemma di Zorn esiste un sottocampo $K \subset E \subset L$ ed una derivazione $\partial: E \to L \otimes_K \Omega_{K/\mathbb{K}}$ che estende $1 \otimes d$ e tale che (E, ∂) è massimale tra le coppie aventi la stessa proprietà.

Assumiamo per assurdo $E \neq L$ e sia $l \notin E$, sia $\mu_l \in E[x]$ il suo polinomio minimo su E.

Consideriamo la struttura di $E[x]$ modulo su $L \otimes_K \Omega_{K/\mathbb{K}}$ indotta dal morfismo $E[x] \to E[l] \subset L$. Estendiamo ∂ ad una derivazione $\tilde{\partial}$ su $E[x]$ ponendo $\tilde{\partial}(x) = 0$, più in generale, scelto un qualsiasi elemento $y \in L \otimes_K \Omega_{K/\mathbb{K}}$ possiamo estendere ∂ ad una derivazione $\delta: E[x] \to L \otimes_K \Omega_{K/\mathbb{K}}$ tale che $\delta(x) = y$, se accade che $\delta(\mu_l) = 0$ allora δ si fattorizza ad una derivazione su $E[l]$ in contraddizione alla massimalità.

Essendo l separabile su E ciò è certamente possibile perché $\mu_l'(l) \neq 0$ e $\delta(\mu_l) = (\tilde{\partial}\mu_l)(l) + \mu_l'(l)\delta(x)$. □

Definizione 4.8. Sia X una varietà quasiproiettiva irriducibile di dimensione d su un campo algebricamente chiuso $\mathbb{K}$. Un **differenziale razionale** su X è un elemento di $\Omega_X = \Omega_{\mathbb{K}(X)/\mathbb{K}}$. Per i risultati precedenti Ω_X è un $\mathbb{K}(X)$-spazio vettoriale di dimensione d.

Definizione 4.9. Dati $p \in X$, $\omega \in \Omega_X$, il differenziale ω si dice *regolare* in p se esistono $f_1, ..., f_n, g_1, ..., g_n \in \mathcal{O}_{p,X} \subset \mathbb{K}(X)$ tali che $\omega = \sum f_i dg_i$. In altre parole ω è regolare in p se appartiene all'immagine dell'applicazione naturale $\Omega_{\mathcal{O}_{p,X}/\mathbb{K}} \to \Omega_X$. Per ogni aperto U si indica $\Omega_X(U)$ il modulo su $\mathcal{O}_X(U)$ dei differenziali regolari in ogni punto di U.

Si noti che per ogni differenziale ω, l'insieme dei punti dove ω è regolare è un aperto denso di X.

Vediamo adesso il caso delle curve liscie.

Sia X curva liscia e t un parametro locale, per il corollario 4.4 $\mathbb{K}(X)$ è separabile su $\mathbb{K}(t)$ e quindi $dt \neq 0$ e genera Ω_X come $\mathbb{K}(X)$-spazio vettoriale. In particolare per ogni $f \in \mathbb{K}(X)$ esiste unica una funzione razionale $\frac{df}{dt}$ tale che $df = \frac{df}{dt}dt$.

Lemma 4.10.(cf. [Ha] II.8.8) *Se t è un parametro locale in $p \in X$ e $f \in \mathcal{O}_{p,X}$ allora $\frac{df}{dt} \in \mathcal{O}_{p,X}$.*

Dim. Sia U un intorno affine di p e siano $x_1, ..., x_n$ generatori di $\mathcal{O}_X(U)$ come $\mathbb{K}$-algebra. Per ogni $g \in \mathcal{O}_{p,X}$ esistono polinomi P, Q nelle x_i tali che $Q(p) \neq 0$, $g = PQ^{-1}$.

Differenziando $dg = Q^{-2}\sum G_i dx_i$ con G_i polinomio nelle x_i.

Detto dunque $a = \min_i\{ord_p(\frac{dx_i}{dt})\}$ per ogni $g \in \mathcal{O}_{p,X}$ vale $ord_p(\frac{dg}{dt}) \geq a$.

Sia ora $f \in \mathcal{O}_{p,X}$ e b un intero positivo tale che $b + a > 0$, esiste allora un polinomio $P(t)$ ed una $g \in \mathcal{O}_{p,X}$ tale che $f = P(t) + t^b g$, differenziando si dimostra la tesi. □

Lemma 4.11. *$p \in X$, t parametro locale in p. Il differenziale fdt è regolare in p se e soltanto se f è regolare in p.*

Dim. Se f è regolare allora fdt è regolare per definizione.

Viceversa se $fdt = \sum f_i dg_i$, $f_i, g_i \in \mathcal{O}_{p,X}$ allora $f = \sum f_i \frac{dg_i}{dt}$ e la tesi segue dal lemma 4.10. □

Se $\omega \in \Omega_X$ e $p \in X$ definiamo $ord_p(\omega) = ord_p(f)$ dove $\omega = fdt$, t parametro locale in p. Una semplice applicazione dei lemmi precedenti mostra che è una buona definizione e che $ord_p(\omega) \geq 0$ se e soltanto se ω è regolare in p.

Lemma 4.12. *Se $\omega \neq 0$ allora $ord_p(\omega) = 0$ eccetto un numero finito di punti.*

Dim. Basta chiaramente dimostrare il lemma per il differenziale dt con t parametro locale. Abbiamo già dimostrato che esiste un aperto denso dove $ord_p(dt) \geq 0$. Sia U un aperto affine di X, siccome $X - U$ è finito basta dimostrare che dt possiede un numero finito di zeri in U.

Se $U \subset \mathbb{A}^n$ chiuso irriducibile con $x_1, ..., x_n$ coordinate affini. A meno di permutazioni negli indici possiamo supporre che esista $s \leq n$ tale che $dx_i = 0$ se e soltanto se $i > s$.

Se $p = (a_1, ..., a_n) \in U$ le funzioni $x_i - a_i$, $i = 1, ..., n$ generano l'ideale massimale e quindi, essendo $d(x_i - a_i) = dx_i = \frac{dx_i}{dt}dt$ esiste un intero $j \leq s$ tale che $x_j - a_j$ è un parametro locale in p.

Dunque gli zeri di dt in U sono contenuti nell'unione dei poli delle funzioni razionali $\frac{dx_i}{dt}$, $i = 1, ..., s$, e sono in numero finito. □

Ad ogni differenziale razionale ω su di una curva liscia X possiamo associare un divisore $div(\omega) = \sum ord_p(\omega)p$. Se $f \in \mathbb{K}(X)$ vale $div(f\omega) = div(f) + div(\omega)$ e quindi i divisori dei differenziali sono tutti linearmente equivalenti tra loro.

Un morfismo $\phi: X \to Y$ dominante di curve liscie si dice separabile (inseparabile, puramente inseparabile) se l'estensione di campi $\mathbb{K}(Y) \subset \mathbb{K}(X)$ ha la medesima proprietà.

ϕ induce un morfismo $\phi^*: \Omega_Y \to \Omega_X$ $\mathbb{K}(Y)$-lineare e tale che per ogni $f \in \mathbb{K}(Y)$, $\phi^*(df) = d\phi^*(f)$. Per il lemma 4.7 se ϕ è separabile ϕ^* è iniettivo.

Sia ora $\omega \in \Omega_Y$ e $p \in X$ un punto fissato, vogliamo determinare $ord_p(\phi^*\omega)$. Sia $q = \phi(p)$, $a = ord_q(\omega)$, t un parametro locale in p, s parametro locale in q ed e l'indice di ramificazione di ϕ in p.

Si ha $\omega = gs^a ds$, $g(q) \neq 0$, $s = ht^e$, $h(p) \neq 0$, $\phi^*\omega = gh^a t^{ae}(et^{e-1}h + t^e\frac{dh}{dt})dt$ e quindi $ord_p(\phi^*\omega) \geq ae + e - 1$ e vale $=$ se e soltanto se e non è divisibile per la caratteristica del campo. Per il lemma 4.12 $\phi^*\omega \neq 0$ se e soltanto se $e_p = 1$ eccetto un numero finito di punti.

Definizione 4.13. $\phi: X \to Y$ si dice **docilmente ramificato** se la caratteristica del campo non divide l'indice di ramificazione in nessun punto.

Proposizione 4.14. *Nelle notazioni precedenti sia i il grado di inseparabilità di ϕ, allora $e_p(\phi) \geq i$ per ogni $p \in X$ e vale $=$ eccetto un numero finito di punti.*

Dim. Se ϕ è separabile allora ϕ^* è iniettiva e la tesi segue dalle osservazioni precedenti.

Supponiamo quindi $i > 1$ e sia $l > 0$ la caratteristica del campo.

In generale se $\psi: Y \to Z$ è un morfismo dominante di curve liscie vale la formula $e_p(\psi\phi) = e_p(\phi)e_{\phi(p)}(\psi)$. Prendendo quindi $\psi: Y \to \mathbb{P}^1$ separabile possiamo supporre senza perdita di generalità $Y = \mathbb{P}^1$.

Sia s coordinata affine su $\mathbb{P}^1$ e sia $a \geq 0$ il massimo intero tale che $s \in \mathbb{K}(X)^{l^a}$. Se $s = t^{l^a}$ allora $t \notin \mathbb{K}(X)^l$, l'estensione $\mathbb{K}(t) \subset \mathbb{K}(X)$ è separabile e $\mathbb{K}(s) \subset \mathbb{K}(t)$ è puramente inseparabile di grado l^a. In particolare $i = l^a$.

Se consideriamo t come un morfismo su $\mathbb{P}^1$ ho una fattorizzazione $\phi: X \xrightarrow{t} \mathbb{P}^1 \xrightarrow{\gamma} \mathbb{P}^1$ dove $\gamma(t) = t^{l^a}$ e l'indice di ramificazione di γ è uguale ad i in ogni punto. □

5. Residui astratti.

Sia V uno spazio vettoriale su un campo $\mathbb{K}$, se $A, B \subset V$ sono sottospazi vettoriali diremo che A non è molto più grande di B e scriveremo $A < B$ se esiste un sottospazio F di dimensione finita tale che $A \subset B + F$. Si vede subito che si tratta

di una relazione di ordine e quindi $A \sim B \Leftrightarrow A < B, B < A$ è una relazione di equivalenza.

ESERCIZIO 9: Se $A < B$ allora $f(A) < f(B)$ per ogni f applicazione lineare.

ESERCIZIO 10: $\sum_{i=1}^{n} A_i < \cap_{j=1}^{m} B_j$ se e soltanto se $A_i < B_j$ per ogni i, j.

Fissato un sottospazio $A \subset V$ si definisce

$$E = \{f \in \mathrm{Hom}_{\mathbb{K}}(V,V) | \, f(A) < A\}$$

$$E_1 = \{f \in E | \, f(V) < A\}$$

$$E_2 = \{f \in E | \, f(A) < 0\}$$

$$E_0 = E_1 \cap E_2$$

Si vede immediatamente che E, E_0, E_1, E_2 dipendono solo dalla classe di equivalenza di A.

ESERCIZIO 11: E_1 determina unicamente la classe di equivalenza di A.

ESERCIZIO 12: $f \in E$ se e soltanto se $A \cap f^{-1}(A) \sim A$.

Lemma 5.1. *E_0, E_1, E_2 sono ideali bilateri della $\mathbb{K}$-algebra E e $E_1 + E_2 = E$.*

Dim. La verifica che gli E_i sono ideali bilateri di E è banale ed è lasciata al lettore. Dunque $E_1 + E_2$ è un ideale ed è sufficiente dimostrare che $1 \in E_1 + E_2$, se $\pi: V \to A$ è una proiezione allora $\pi \in E_1, 1 - \pi \in E_2$ e $1 = \pi + (1 - \pi)$. □

Se $F \subset E_0$ è un sottospazio vettoriale di dimensione finita è possibile trovare sottospazi $C \subset A \subset B$ tali che $C \sim B$, $f(V) \subset B$, $f(C) = 0$ per ogni $f \in F$ e si definisce una applicazione lineare $Tr_V: F \to \mathbb{K}$ definita da

$$Tr_V(f) = Traccia_{B/C}(f)$$

Dalle proprietà dell'operatore traccia negli spazi vettoriali di dimensione finita segue facilmente che Tr_V non dipende dalla particolare scelta di C e B e passando al limite inverso si definisce una applicazione lineare $Tr_V: E_0 \to \mathbb{K}$.

Lemma 5.2. *Siano $f, g \in E$ tali che $fg, gf \in E_0$ (ad esempio se $f \in E_1$, $g \in E_2$). Allora $Tr_V(fg) = Tr_V(gf)$.*

Dim. Sia $C \subset A$, $C \sim A$ tale che $fg(C) = gf(C) = 0$, a meno di sostituire C con $C \cap f^{-1}(A) \cap g^{-1}(A) \sim C$ possiamo supporre $f(C), g(C) \subset A$.
Esistono allora morfismi fra spazi vettoriali di dimensione finita

$$\frac{A + f(A) + fg(V)}{C + f(C)} \underset{f}{\overset{g}{\rightleftarrows}} \frac{A + g(A) + gf(V)}{C + g(C)}$$

e si usano le ben note proprietà della traccia. □

Sia $K \subset E$ una $\mathbb{K}$-sottoalgebra **commutativa**, V è allora un K-modulo ed A un sottospazio tale che $fA < A$ per ogni $f \in K$.
Il nostro prossimo obbiettivo è quello di associare alla classe di equivalenza di A una applicazione $\mathbb{K}$-lineare

$$res_A^V: \Omega_{K/\mathbb{K}} \longrightarrow \mathbb{K}$$

Siano $f, g \in K$, per il lemma 5.1 è possibile scrivere (in modo non unico) $f = f_1 + f_2$, $g = g_1 + g_2$, $f_i, g_i \in E_i$. Si noti che $[f_1, g_1] \in E_1$ e che $[f_1, g_1] \equiv [f, g] = 0 \mod(E_2)$, dunque $[f_1, g_1] \in E_0$ ed è ben definito $Tr_V[f_1, g_1]$. Si noti che per il lemma 5.2 la traccia di $[f_1, g_1]$ non dipende dalla particolare scelta di f_1, g_1 e che è chiaramente bilineare in f e g.
Si pone per definizione $res_A^V(fdg) = Tr_V[f_1, g_1]$, per verificare che si tratta di una buona definizione bisogna dimostrare che l'applicazione lineare

$$Tr_V[-_1, -_1]: K \otimes_{\mathbb{K}} K \to \mathbb{K}$$

si annulla sul $\mathbb{K}$-sottospazio vettoriale generato dalle espressioni $f \otimes hg - fh \otimes g - gf \otimes h$. Fissati f_1, g_1, h_1 si può prendere $(hg)_1 = h_1 g_1$, $(fh)_1 = f_1 h_1$, $(gf)_1 = g_1 f_1$ e l'annullamento segue dalla relazione

$$[f_1, h_1 g_1] - [f_1 h_1, g_1] - [g_1 f_1, h_1] = 0.$$

Si noti che se $A_1 \sim A_2$ allora $res_{A_1}^V = res_{A_2}^V$.

Esiste una utile formula per il calcolo del residuo, se $\pi: V \to A$ è una proiezione si può prendere $f_1 = \pi f$, $g_1 = \pi g$ e quindi

$$res_A^V(fdg) = Traccia_{A/C}[\pi f, \pi g] \tag{5.3}$$

dove $C = \{x \in A | \, f(x), g(x) \in A\} \sim A$. Infatti $[\pi f, \pi g](V) \subset A$ e se $x \in C$ allora $[\pi f, \pi g]x = \pi[f, g]x = 0$.
In particolare se $V \subset V'$ è una inclusione di K-moduli allora $res_A^V = res_A^{V'}$.
Si noti anche che $res_A^V(fdg) + res_A^V(gdf) = 0$ per ogni $f, g \in K$.

Proposizione 5.4. *Nelle notazioni precedenti:*

1) *Se $f(A) \subset A$, $g(A) \subset A$ allora $res_A^V(fdg) = 0$, in particolare se A è un K-sottomodulo di V il residuo è identicamente nullo.*
2) *Per ogni $g \in K$, $n \geq 0$ vale $res_A^V(g^n dg) = 0$.*
3) *Se $g \in K$ è invertibile e $n \leq -2$, $res_A^V(g^n dg) = 0$.*
4) *Se $g \in K$ è invertibile e $g(A) \subset A$ allora $res_A^V(g^{-1} dg)$ è uguale alla traccia dell'identità in $A/g(A)$.*

Dim. Il punto 1) segue immediatamente dalla formula 5.3. Nel punto 2), fissato g_1 si può prendere $(g^n)_1 = g_1^n$ e quindi $[g_1^n, g_1] = 0$. Se si pone $h = g^{-1}$ al punto 3) si ha $g^n dg = -h^{-2-n} dh$ e la tesi segue dal punto 2.
Per dimostrare 4) si applica la formula 5.3, si ha quindi $C = g(A)$ e per ogni $x \in A$, $[\pi g^{-1}, \pi g]x = x - g(\pi g^{-1} x)$. □

Vediamo infine come si comportano i residui con le successioni esatte.

Proposizione 5.5. *Sia* $0 \longrightarrow U \longrightarrow V \xrightarrow{p} W \longrightarrow 0$ *una successione esatta di* K*-moduli e sia* $A \subset V$ *un* $\mathbb{K}$*-sottospazio tale che* $f(A) < A$ *per ogni* $f \in K$. *Siano* $A_1 = A \cap U$, $A_2 = p(A)$, *allora* $f(A_i) < A_i$ *per ogni* $i = 1, 2$ *e* $f \in K$ *e vale*

$$res_A^V = res_{A_1}^U + res_{A_2}^W$$

Dim. Sia $F \sim 0$ un sottospazio di V tale che $f(A) \subset A + F$, è allora ovvio che $f(A_2) \subset A_2 + p(F)$, $f(A_1) \subset U \cap (A + F)$. Un semplice conto di algebra lineare che lasciamo per esercizio mostra che

$$\dim_k \frac{U \cap (A+F)}{A_1} \leq \dim_k F$$

e quindi $f(A_1) < A_1$.
Fissiamo delle proiezioni π, π_1, π_2 tali che il seguente diagramma sia commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U & \longrightarrow & V & \xrightarrow{p} & W & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi_2} & & \\ 0 & \longrightarrow & A_1 & \longrightarrow & A & \xrightarrow{p} & A_2 & \longrightarrow & 0 \end{array}$$

Siano $f, g \in K$ fissati e sia $C = \{x \in A \,|\, f(x), g(x) \in A\}$. Allora C è contenuto nel nucleo di $[\pi f, \pi g]$ e quindi $C \cap U \subset \ker[\pi_1 f, \pi_1 g]$, $p(C) \subset [\pi_2 f, \pi_2 g]$. Una semplice verifica mostra infine che il seguente diagramma è commutativo con le righe esatte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \dfrac{A_1}{A_1 \cap C} & \longrightarrow & \dfrac{A}{C} & \xrightarrow{p} & \dfrac{A_2}{p(C)} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle [\pi_1 f, \pi_1 g]} & & \downarrow{\scriptstyle [\pi f, \pi g]} & & \downarrow{\scriptstyle [\pi_2 f, \pi_2 g]} & & \\ 0 & \longrightarrow & \dfrac{A_1}{A_1 \cap C} & \longrightarrow & \dfrac{A}{C} & \xrightarrow{p} & \dfrac{A_2}{p(C)} & \longrightarrow & 0 \end{array}$$

La tesi segue dunque dalla formula 5.3 e dal comportamento della traccia rispetto alle successioni esatte di spazi vettoriali di dimensione finita. □

Corollario 5.6. *Siano* $A, B \subset V$ *sottospazi tali che* $f(A) < A$, $f(B) < B$ *per ogni* $f \in K$, *allora anche* $f(A \cap B) < A \cap B$, $f(A + B) < A + B$ *per ogni* $f \in K$ *e vale*

$$res_A^V + res_B^V = res_{A \cap B}^V + res_{A+B}^V.$$

Dim. Si consideri $A \oplus B \subset V \oplus V$, è chiaro che $f(A \oplus B) < A \oplus B$ per ogni $f \in K$ e per la proposizione 5.5, $res_{A \oplus B}^{V \oplus V} = res_A^V + res_B^V$.
Applicando invece la proposizione 5.5 alla successione esatta

$$0 \longrightarrow V \longrightarrow V \oplus V \xrightarrow{p} V \longrightarrow 0, \qquad p(x, y) = x - y$$

si ottiene $p(A \oplus B) = A + B$, $V \cap (A \oplus B) = A \cap B$ e quindi $res_{A \oplus B}^{V \oplus V} = res_{A+B}^V + res_{A \cap B}^V$.
□

Nota: le definizioni ed i risultati di questa sezione sono tratti da [Ta].

6. Il teorema dei residui e seconda parte del teorema di Riemann-Roch.

Sia X una curva liscia proiettiva su un campo $\mathbb{K}$ algebricamente chiuso e sia $K = \mathbb{K}(X)$. Nelle notazioni della sezione 5 per ogni $f \in K$, $p \in X$ vale $f\mathcal{O}_{p,X} < \mathcal{O}_{p,X}$ ed è possibile definire il residuo

$$res_p : \Omega_X \to \mathbb{K} \qquad res_p := res_{\mathcal{O}_{p,X}}^K$$

Siccome $f\mathcal{O}_{p,X} \subset \mathcal{O}_{p,X}$ se e soltanto se f è regolare in p, dalla proposizione 5.4 segue immediatamente che se ω è una forma differenziale regolare in p allora $res_p(\omega) = 0$.
Sempre per la proposizione 5.4 se t è un parametro locale in p vale

$$res_p(t^n dt) = \begin{cases} 1 & \text{se } n = -1 \\ 0 & \text{altrimenti} \end{cases}$$

Se $S \subset X$ è un qualsiasi sottoinsieme si pone

$$\mathcal{O}_X(S) = \cap_{p \in S} \mathcal{O}_{p,X}, \qquad res_S = res_{\mathcal{O}_X(S)}^K$$

Si noti che $\mathcal{O}_X(X) = \mathbb{K} \sim 0$ e quindi $res_X = res_{\mathbb{K}}^K = res_0^K \equiv 0$.

Teorema 6.1. *Per ogni* $\omega \in \Omega_X$, $S \subset X$ *vale*

$$res_S(\omega) = \sum_{p \in S} res_p(\omega).$$

Dim. ω è regolare in S eccetto al più in un numero finito di punti e quindi la formula precedente ha perfettamente senso.
Sia $R_S \subset R$ il K-sottospazio vettoriale delle ripartizioni su S, l'inclusione $S \subset X$ induce una proiezione naturale $R \xrightarrow{p} R_S \longrightarrow 0$. Si identifichi K con il sottospazio di R_S delle ripartizioni costanti, per i risultati della sezione 5 si ha $res_S = res_{\mathcal{O}_X(S)}^{R_S}$.

Per ogni divisore $D \in Div(X)$ si pone $R_S(D) = p(R(D)) \subset R_S$, si noti che $\mathcal{O}_X(S) = K \cap R_S(0)$ e quindi per il corollario 5.6

$$res_S = res_K^{R_S} + res_{R_S(0)}^{R_S} - res_{R_S(0)+K}^{R_S}$$

$K \subset R_S$ è un K-sottomodulo e quindi $res_K^{R_S} \equiv 0$. La proiezione p induce una applicazione surgettiva $R/(R(0)+K) \longrightarrow R_S/(R_S(0)+K)$ dalla quale si deduce che $R_S(0)+K$ ha codimensione finita in R_S e quindi $res_{R_S(0)+K}^{R_S} = res_{R_S}^{R_S} \equiv 0$.
Resta quindi da dimostrare la formula

$$res_{R_S(0)}^{R_S}(\omega) = \sum_{p \in S} res_{\mathcal{O}_p}^{R_S}(\omega) = \sum_{p \in S} res_p(\omega)$$

Siano $f, g \in K$ tali che $\omega = fdg$ e sia $T \subset S$ il sottoinsieme dei punti dove f e g sono regolari, $S - T$ è un insieme finito di punti e vale $R_S(0) = R_T(0) \oplus \bigoplus_{p \in S-T} \mathcal{O}_p$.
Per il corollario 5.6

$$res_{R_S(0)}^{R_S}(fdg) = res_{R_T(0)}^{R_S}(fdg) + \sum_{p \in S-T} res_{\mathcal{O}_p}^{R_S}(fdg)$$

e siccome $fR_T(0) + gR_T(0) \subset R_T(0)$ per la proposizione 5.4 il primo termine della sommatoria è nullo e la dimostrazione è conclusa. □

Corollario 6.2.(Teorema dei residui) *Per ogni* $\omega \in \Omega_X$, $\sum_{p \in X} res_p(\omega) = 0$.

Dim. Per il teorema 6.1 tale somma è uguale a $res_X(\omega) = 0$. □

Il teorema dei residui permette di definire in modo canonico un isomorfismo di $\mathbb{K}(X)$-spazi vettoriali monodimensionali $\Omega_X = J$ dove per $\omega \in \Omega_X$ e $r \in R$ si pone $\omega(r) = \sum_{p \in X} res_p(r(p)\omega)$.
Infatti la definizione mostra immediatamente che ω definisce un elemento del $\mathbb{K}$-duale di R, dalle proprietà elementari dei residui segue che $\omega = 0$ su $R(div(\omega))$ mentre per il teorema dei residui $\omega = 0$ su $\mathbb{K}(X)$. Dunque $\omega \in I(div(\omega))^\vee \subset J$.
Sia K un divisore canonico e sia $\omega \in I(K)^\vee$ un differenziale non nullo, allora, siccome $R(K) + \mathbb{K}(X)$ ha codimensione 1 deve necessariamente essere $R(K) + \mathbb{K}(X) = \ker \omega$.
Vogliamo dimostrare che $K = div(\omega)$.
Sia $p \in X$, t parametro locale in p e sia $h = ord_p(K)$, abbiamo visto che, dato un intero $s \leq h$, la classe della ripartizione r_s: $r(q) = 0$ se $q \neq p$, $r(p) = t^{-s-1}$ è una base di $I(K)$ per $s = h$ mentre se $s < h$ è $r_s \in R(K)$, dunque $\omega(r_s) = res_p(t^{-s-1}\omega) \neq 0$ se e soltanto se $s = h$ e quindi necessariamente $ord_p(\omega) = h$.
Abbiamo quindi dimostrato

Teorema 6.3. *X curva liscia proiettiva, un divisore è canonico se e soltanto se è il divisore di un differenziale razionale.*

Corollario 6.4. *X curva liscia proiettiva, sia data per ogni $p \in X$ una applicazione $\mathbb{K}$-lineare $s_p: \Omega_X \to \mathbb{K}$ con le seguenti proprietà:*

1) $s_p(\omega) = 0$ se ω è regolare in p.

2) $\sum_{p \in X} s_p(\omega) = 0$ per ogni $\omega \in \Omega_X$.

Allora esiste una costante $a \in \mathbb{K}$ tale che per ogni punto p vale $s_p = ares_p$.

Dim. Ripetendo il ragionamento fatto nella dimostrazione del teorema 6.3 si dimostra che le funzioni s_p possono essere utilizzate per costruire un morfismo $\Omega_X \to J \subset R^\vee$ e siccome J ha dimensione 1 su $\mathbb{K}(X)$ esiste una funzione razionale f tale che per ogni $p \in X$, $\omega \in \Omega_X$, $r \in \mathbb{K}(X)$ vale $s_p(r\omega) = res_p(fr\omega)$ e dalla proprietà 1) segue immediatamente che f non possiede poli e quindi è una funzione costante. □

Corollario 6.5. *Il divisore di un differenziale razionale ha grado $2g-2$.*

Dim. Per il teorema 6.3 il divisore di un differenziale è canonico, se K è canonico per Riemann-Roch vale

$$g - 1 = h^0(K) - h^0(0) = deg(K) + 1 - g$$

da cui $deg(K) = 2g - 2$. □

Corollario 6.6.(Formula di Hurwitz) *Sia $f: X \to Y$ un morfismo separabile docilmente ramificato tra curve liscie proiettive, allora*

$$2g(X) - 2 = deg(f)(2g(Y) - 2) + \sum_{p \in X} (e_p(f) - 1).$$

Dim. Se $\omega \in \Omega_Y$, $\omega \neq 0$ allora $f^*\omega \neq 0$ e per i risultati della lezione 4 vale

$$div(f^*\omega) = f^* div(\omega) + \sum_{p \in X} (e_p(f) - 1)p$$

Si noti che se f è separabile ma non docilmente ramificato vale comunque la relazione

$$div(f^*\omega) \geq f^* div(\omega) + \sum_{p \in X} (e_p(f) - 1)p$$ □

Corollario 6.7. *Il $\mathbb{K}$-spazio vettoriale dei differenziali che sono regolari in ogni punto di X ha dimensione g.*

Dim. Sia $\omega \neq 0$ un differenziale razionale fissato e $f \in \mathbb{K}(X)$, allora $f\omega$ è regolare in ogni punto di X se e soltanto se $f \in H^0(div(\omega))$. □

Lemma 6.8. *Siano A, B divisori su X tali che $h^0(A) > 0, h^0(B) > 0$, allora vale*

$$h^0(A + B) \geq h^0(A) + h^0(B) - 1.$$

Dim. (cf. Esercizio III.25) Se $p \in X$ è un punto tale che $h^0(A-p) = h^0(A)$ ed il lemma vale per $A-p, B$ allora a maggior ragione vale per A, B. Possiamo quindi supporre senza perdita di generalità che per ogni $p \in X$, $h^0(A-p) < h^0(A)$. In particolare, essendo k infinito, per ogni sottoinsieme finito $S \subset X$ esiste $g \in H^0(A)$ tale che, detto $A_g = A + div(g)$, $ord_p(A_g) = 0$ per ogni $p \in S$.
Sia dunque $f_1, .., f_b$ una base di $H^0(B)$, $g_1, ..., g_a$ una base di $H^0(A)$ tale che per ogni $p \in X$

$$ord_p(A + div(g_1)) \cdot ord_p(B + div(f_1)) = 0 \qquad (*)$$

Cioè i divisori effettivi A_{g_1}, B_{f_1} hanno supporti disgiunti.
È sufficiente dimostrare che le funzioni razionali $f_1g_1, f_1g_2, ..., f_1g_a, f_2g_1, ..., f_bg_1$ sono linearmente indipendenti. Sia $f_1(\sum_{i\geq 1}\alpha_i g_i) = (\sum_{j\geq 2}\beta_j f_j)g_1$, se tutti i β_j sono nulli allora, siccome $f_1 \neq 0$ ed i g_i sono linearmente indipendenti deve essere $\alpha_i = 0$ per ogni i.
Se i β_j non sono tutti nulli si ha

$$(B + div(f_1)) + (A + div(\sum \alpha_i g_i)) = (B + div(\sum \beta_j f_j)) + (A + div(g_1))$$

e dalla relazione $(*)$ segue che $B + div(f_1) \leq B + div(\sum \beta_j f_j)$, $f_1^{-1}(\sum \beta_j f_j)$ non ha poli ed è quindi una costante. □

Teorema 6.9.(Clifford) *Se D è un divisore speciale effettivo allora*

$$h^0(D) \leq \frac{1}{2}deg(D) + 1$$

Dim. Speciale effettivo significa che $h^0(D) > 0$, $h^0(K-D) > 0$, per il lemma 6.8 e per il teorema di Riemann-Roch

$$h^0(D) - h^0(K-D) = deg(D) + 1 - g$$

$$h^0(D) + h^0(K-D) \leq h^0(K) + 1 = g + 1$$

Sommando membro a membro $2h^0(D) \leq deg(D) + 2$. □
È possibile dimostrare ([Ha] p. 344) che se per un divisore effettivo speciale $D \neq 0, K$ vale $2h^0(D) = deg(D) + 2$ allora esiste un morfismo $f: X \to \mathbb{P}^1$ di grado 2 ed un divisore $Q \in Div(\mathbb{P}^1)$ tale che $D = f^*Q$.

7. Esercizi complementari

ESERCIZIO 13: Se X è una curva liscia proiettiva, dimostrare che tutti anelli di valutazione di $\mathbb{K}(X)$ contenenti $\mathbb{K}$ sono $\mathbb{K}(X)$ e gli anelli locali $\mathcal{O}_{p,X}$, $p \in X$.

(Sugg.: Utilizzare i risultati del capitolo 5 di [A-M]. Cf. anche ([Ha, Es.II.4.12]).

ESERCIZIO 14: Sia $\mathbb{K}$ di caratteristica 0, senza utilizzare i risultati del capitolo V, si provi che la curva $X \subset \mathbb{P}^2$ di equazione $x_0^n + x_1^n + x_2^n = 0$ non è isomorfa a $\mathbb{P}^1$ per $n \geq 3$. (Sugg: Si assuma per assurdo che $X = \mathbb{P}^1$, allora tutti i parametri locali sono espressioni razionali l'uno dell'altro. Scrivere le x_i come polinomi in un parametro locale t e derivare.).

ESERCIZIO 15: Dato un morfismo surgettivo $\phi: X \to Y$ tra curve liscie proiettive e due funzioni razionali $f \in \mathbb{K}(X), g \in \mathbb{K}(Y)$ si ha $\phi_*(div(f)) = div(det_\phi(f))$, $div(\phi^* g) = \phi^*(div(g))$, dove si intende con $det_\phi: \mathbb{K}(X) \to \mathbb{K}(Y)$ il determinante.

ESERCIZIO 16: Utilizzare gli argomenti usati nella dimostrazione del teorema 4.3 per dimostrare che un campo $\mathbb{K}$ di caratteristica $p > 0$ è perfetto se e soltanto se $\mathbb{K}^p = \mathbb{K}$.

ESERCIZIO 17: Dare una dimostrazione alternativa del teorema 4.3 utilizzando il teorema 4.1.

ESERCIZIO 18: Dimostrare la seguente generalizzazione del teorema 4.3.
Sia $\mathbb{K}$ perfetto di caratteristica p, $\mathbb{K} \subset K$ estensione finitamente generata e sia $t_1, ..., t_d$ una base di trascendenza tale che per ogni i, $t_i \notin K^p(t_1, ..., t_{i-1})$.
Allora K è separabile su $\mathbb{K}(t_1, ..., t_d)$.

ESERCIZIO 19: Se $U \subset X$ è un aperto affine $\Omega_X(U)$ è un $\mathcal{O}_X(U)$-modulo Noetheriano isomorfo a $\Omega_{\mathcal{O}_X(U)/\mathbb{K}}/torsione$. (Sugg: Se $U \subset \mathbb{A}^n$ e $x_1, ..., x_n$ sono coordinate affini, mostrare utilizzando la partizione dell'unità che $dx_1, ..., dx_n$ sono generatori).

ESERCIZIO 20: Trovare una varietà affine irriducibile X tale che $\Omega_{\mathcal{O}_X(X)/\mathbb{K}}$ possiede torsione come $\mathcal{O}_X(X)$-modulo. (Sugg: Provare con $X \subset \mathbb{A}^2$ curva singolare).

ESERCIZIO 21: Utilizzare ([Ha] I.6.12) per dimostrare che ogni morfismo dominante di curve liscie proiettive è la composizione di un morfismo puramente inseparabile e di un morfismo separabile.

ESERCIZIO 22: La nozione di traccia di un endomorfismo di uno spazio di dimensione finita si estende in modo naturale agli endomorfismi di potenza finita di V, cioè agli endomorfismi θ tali che per $n >> 0$, θ^n ha rango finito.

ESERCIZIO 23: Nelle notazioni della proposizione 5.4, se $fA_1 < A_1$, $fA_2 < A_2$ è vero che $fA < A$?

ESERCIZIO 24: (Teorema di Lüroth)
Sia $f: X \to Y$ un morfismo surgettivo di curve liscie proiettive, allora $g(X) \geq g(Y)$. (Sugg.: Se f non è separabile si fattorizzi con il Frobenius).

ESERCIZIO 25: (Teorema di Weber, 1878)
In caratteristica 0 ogni applicazione razionale noncostante tra due curve liscie proiettive di genere $g > 0$ è un isomorfismo.

Riferimenti

Testi introduttivi e/o antichi:

[An] A. Andreotti: *Note su un corso di geometria algebrica* Scuola Normale Superiore a.a. 1977/78. (Una bellissima introduzione alla geometria algebrica dal punto di vista dell'analisi complessa; meriterebbe sicuramente di essere teXXato e pubblicato)

[A-M] M.F. Atiyah, I.G. Macdonald: *Introduction to commutative algebra.* Addison-Wesley, Reading, Mass. (1969).(Esiste una traduzione italiana, ormai introvabile in libreria, edita da Feltrinelli)

[B-K] E. Brieskorn, H. Knörrer: *Plane algebraic curves* Birkhäuser, Basel (1986). (Interessante introduzione alle curve piane con molto folklore. Bella la parte sulla risoluzione delle singolarità e la riproduzione di alcune lettere di Newton)

[Cat] F. Catanese: *Introduzione alla geometria algebrica.* Note scritte (1980 ?).

[Cre] L. Cremona: *Introduzione ad una teoria geometrica delle curve piane* Bologna (1862). (Praticamente l'inizio della scuola Italiana di Geometria Algebrica. Contiene interessanti ragionamenti geometrici; molto carente in rigore)

[Co] J. Coolidge: *A treatise on Algebraic Plane Curves.* Oxford University press (1931).

[Die] J. Dieudonné: *Cours de géométrie algébrique* Presses Universitaires de France (1974). (Il volume I contiene la storia della Geometria Algebrica dalle origini fino a Serre e Grothendieck:)

[Enr] F. Enriques: *Lezioni di geometria proiettiva* Zanichelli (1898).

[E-C] F. Enriques, O. Chisini: *Lezioni sulla teoria geometrica delle equazioni e delle funzioni algebriche.* I,II,III,IV, Zanichelli Bologna (1915),(1918),(1924),(1934).

[Ful] W. Fulton: *Algebraic Curves: an introduction to algebraic geometry.* Benjamin (1969).

[G-R-T] F. Gerardelli, L.A. Rosati, G. Tomassini: Lezioni di Geometria (2 volumi) Cedam Padova (1980).

[G-H] P. Griffiths, J. Harris: *Principles of Algebraic Geometry.* Wiley-Interscience publication (1978).

[Hr] J. Harris: *Algebraic Geometry: a first course* Springer Verlag GTM **133** (1992).

[He] I.N. Herstein: *Algebra* Editori Riuniti (1982).

[Hilb] D. Hilbert: *Theory of algebraic invariants.* Cambridge Univ. Press (1993).

[Hu] J. Humphreis: *Introduction to lie algebras and representation theory.* Springer.

[La] S. Lang: *Algebra.* Addison-Wesley, second edition (1984).

[Mu] D. Mumford: *Algebraic geometry I Complex Projective Varieties* Springer-Verlag GMW **221** (1976).

[Reid] M. Reid: *Undergraduate algebraic geometry.* Cambridge Univ. Press (1988).

[Sev] F. Severi: *Complementi di geometria proiettiva.* Zanichelli (1906).

[Sh] I.R. Shafarevich: *Basic algebraic geometry.* Springer-Verlag (1972).

[Wa] R.J. Walker: *Algebraic curves.* Princeton (1950).

Articoli e testi avanzati:

[A-C-G-H] E. Arbarello, M. Cornalba, P. Griffiths, J. Harris: *Geometry of algebraic curves, I.* Springer (1984).

[Ar] M. Artin: *On the solutions of analytic equations.* Inv. Math. **5** (1968) 277-291.

[Cay] A. Cayley: *On the porism of the in-and-circumscibed polygon and the* $(2,2)$ *correspondence of points on a conic* Quart. Math. Jour. t. XI (1871) 83-91.

[Fu2] W. Fulton: *Intersection theory.* Springer-Verlag Ergebnisse der Mathematik **2** (1984).

[G-K-Z] I. Gelfand, M. Kapranov, A. Zelevinsky: *Discriminants, resultants and multidimensional determinants.* Birkhäuser Boston (1994).

[Ha] R. Hartshorne: *Algebraic geometry.* Springer Verlag GTM **52** (1977).

[K-L] S.L. Kleiman D. Laksov: *Schubert calculus.* Amer. Math. Monthly **79** (1972) 1061-1082.

[Ko] J. Kollár: *Rational curves on algebraic varieties* Springer-Verlag Ergeb. **32** (1996).

[K-R] J. Kung, G. Rota. *The invariant theory of binary forms.* Bull. A.M.S. **10** (1984) 27-85.

[Mat] H. Matsumura: *Commutative Ring Theory.* Cambridge University Press (1986)

[Se1] J.P. Serre: *Groupes algébriques et corps de classes.* Hermann Paris (1959).

[Se2] J.P. Serre: *Géométrie algébrique et géométrie analytique.* Ann. Inst. Fourier **6** (1956) 1-42.

[Si] J.H. Silverman: *The arithmetic of elliptic curves.* Springer-Verlag New York (1986).

[St] B. Sturmfels: *Introduction to resultants* Proc. Symp. Appl. Math. **53** (1998) 25-39.(Il risultante dal punto di vista della computer algebra)

[Ta] J. Tate: *Residues of differentials on curves.* Ann. scient. Éc. Norm. Sup. **1** (1968) 149-159.

[We] A. Weil: *Adeles and algebraic groups* Lectures at I.A.S. Princeton 1959-60. Ripubblicato da Birkhäuser Progress in Math. **23** (1982).

Elenco dei volumi della collana
"Appunti"
pubblicati dall'Anno Accademico 1994/95

GIUSEPPE BERTIN (a cura di), *Seminario di Astrofisica*, 1995.

EDOARDO VESENTINI, *Introduction to continuous semigroups*, 1996.

LUIGI AMBROSIO, *Corso introduttivo alla Teoria Geometrica della Misura ed alle Superfici Minime*, 1997.

CARLO PETRONIO, *A Theorem of Eliashberg and Thurston on Foliations and Contact Structures*, 1997.

MARIO TOSI, *Introduction to Statistical Mechanics and Thermodynamics*, 1997.

MARIO TOSI, *Introduction to the Theory of Many-Body Systems*, 1997.

PAOLO ALUFFI (a cura di), *Quantum cohomology at the Mittag-Leffler Institute*, 1997.

GILBERTO BINI, CORRADO DE CONCINI, MARZIA POLITO, CLAUDIO PROCESI, *On the Work of Givental Relative to Mirror Symmetry*, 1998

GIUSEPPE DA PRATO, *Introduction to differential stochastic equations*, 1998

HUYÊN PHAM, *Imperfections de Marchés et Méthodes d'Evaluation et Couverture d'Options*, 1998

MARCO MANETTI, *Corso introduttivo alla Geometria Algebrica*, 1998