CAPITOLO 5 CALCOLO DIFFERENZIALE

versione del (14-4-2002)

1 Derivazioni e differenziali

Vogliamo ora sviluppare alcuni aspetti formali del calcolo differenziale.

1.1 Definizione. *Sia data un algebra A su un anello R ed un $A-$modulo M.*
*Una $R-$**derivazione** D di A in M è una applicazione $D : A \to M$ che sia $R-$lineare e che verifichi[1]:*

$$D(ab) = aD(b) + bD(a), \quad \forall a, b \in A, \qquad \textit{regola di Leibnitz.} \tag{1.2}$$

L'insieme di tutte le derivazioni $R-$lineari di A in M verrà denotato con $Der_R(A, M)$.

Dalla regola di Leibnitz segue immediatamente che $D(1) = 0$. Dato $r \in R$ dalla regola di Leibnitz $D(ra) = aD(r) + rD(a)$. La condizione di R linearità è dunque equivalente a $0 = D(r)$.[2]

La regola fondamentale con cui calcolare è la seguente:

1.3 Lemma. *Dati elementi $a_i \in A$, $i = 1, \dots, n$ un polinomio $f(x_1, \dots, x_n)$ a coefficieenti in R ed $a := f(a_1, \dots, a_n) = f(\underline{a})$ si ha per una derivazione $D : A \to M$:*

$$D(a) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(\underline{a}) D(a_i). \tag{1.4}$$

Dim. Per linearità ci possiamo ridurre al caso di un monomio, lavoriamo per induzione sul grado e applichiamo la formula di Leibnitz, se $f(x_1, \dots, x_n) = x_1 g(x_1, \dots, x_n)$ e $a = a_1 g(a_1, \dots, a_n)$ si ha

$$D(a) = g(\underline{a})D(a_1) + a_1 D(g(\underline{a})) = g(\underline{a})D(a_1) + \sum_{i=1}^{n} a_1 \frac{\partial f}{\partial x_i}(\underline{a}) D(a_i)$$

l'identità segue poiché $\dfrac{\partial f}{\partial x_1} = g + x_1 \dfrac{\partial g}{\partial x_1}$. □

[1] se volessimo essre più generali ed introdurre i concetti che valgono anche nel caso non commutativo, dovremmo considerare M come $A - A$ bimodulo e scrivere in modo più intrinseco l'identità di Leibnitz come $D(ab) = aD(b) + D(a)b$.

[2] intuitivamente R sono le *costanti* con derivate 0.

Nel caso analitico usualmente una derivazione è un campo di vettori ovvero il generatore infinitesimale di un gruppo ad un parametro. Esiste un analogia algebrica formale.

ESERCIZO Sia A costruiamo la *deformazione infinitesimale* di A ovvero l'anello $B := A[x]/(x^2)$. Usualmente si indica con ϵ la classe di x in B quindi $B = A \oplus A\epsilon,\ \epsilon^2 = 0$.

Provare che definire un automorfismo di B che è l'identità modulo ϵ (su A) è equivalente a dare una derivazione di A.

Iniziamo con osservazioni elementari la cui verifica lasciamo al lettore.

1.5 PROPOSIZIONE.
i) Se $D_1, D_2 \in Der_R(A, M),\ a_1, a_2 \in A$ *si ha* $a_1D_1 + a_2D_2 \in Der_R(A, M)$.
ii) Se $D \in Der_R(A, M)$ *e* $f : M \to N$ *è un morfismo di moduli si ha:*
$f \circ D \in Der_R(A, N)$.
iii) Se $D \in Der_R(A, M)$ *e* $f : B \to A$ *è un morfismo di* $R-$*algebre si ha:*
$D \circ f \in Der_R(B, M)$.
iv) Data una derivazione $D : A \to M$, *l'insieme* $S := \{a \in A | D(a) = 0\}$ *è una sottoalgebra.*
v) Se $D_1, D_2 : A \to A$ *sono due derivazioni di* A *allora* $[D_1, D_2] := D_1D_2 - D_2D_1$ *è una derivazione.*[3]

ESEMPIO Sia $A = R[x_1, \ldots, x_n]$ l'anello dei polinomi in n variabili ed M un $A-$modulo. Una derivazione $D : A \to M$ è univocamente determinata dai valori $D(x_i)$ e dati $m_i,\ i = 1, \ldots, n$ la formula:

$$Df(x) := \sum_{i=1}^{n} \frac{\partial f}{\partial x_i} m_i$$

definisce una derivazione con $D(x_i) = m_i$.

DIM. Da iv) della precedente proposizione segue che due deirvazioni che coincidono sui generatori di un algebra coincidono ovunque. D'altra parte è immediato dalla regola di Leibnitz usuale che:

$$D[f(x)g(x)] = \sum_{i=1}^{n} \frac{\partial fg}{\partial x_i} m_i = \sum_{i=1}^{n} g(x) \frac{\partial f}{\partial x_i} m_i + \sum_{i=1}^{n} f(x) \frac{\partial g}{\partial x_i} m_i = gDf + fDg.$$

□

Le due prime proprietà ci dicono che $M \to Der_R(A, M)$ è un funtore covariante dai moduli ai moduli e induce a considerare la soluzione universale del problema della costruzione delle derivazioni, (nel linguaggio delle categorie ci domandiamo se il funtore è rappresentabile).

La risposta è ovviamente si dato che la proprietà è descritta da relazioni algebriche.

[3]questa è la struttura di *algebra di Lie* delle derivazioni, vale per algebre qualunque.

La soluzione formalmente si ottiene prendendo l'$A-$modulo libero A^A generato da simboli $D[a],\ a \in A$. A diviene una base di tale modulo e le applicazioni lineari di A^A in N coincidono con le applicazioni di A in N. Le derivazioni sono quelle applicazioni che svaniscono sul sottomodulo delle *relazioni* generato dagli elementi

$$D[a+b] - D[a] - D[b],\ D[ab] - aD[b] - bD[a],\ a,b \in A,\ D[r],\ r \in R.$$

1.6 Definizione. *L'$A-$ modulo dato con generatori $D[a]$ e relazioni*

$$D[a+b] - D[a] - D[b],\ D[ab] - aD[b] - bD[a],\ D[r], \qquad a,b \in A,\ r \in R$$

di dice **modulo dei differenziali di Kähler** *di A e viene denotato con $\Omega_{A/R}$, la classe di $D[a]$ viene denotata con da e detta differenziale totale di a.*

Per costruzione $d : A \to \Omega_{A/R}$ è una derivazione universale.

Da iv) di 1.5 segue la funtorialità in A data dal diagramma commutativo:

$$\begin{array}{ccc} A & \xrightarrow{d} & \Omega_{A/R} \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle dp} \\ B & \xrightarrow{d} & \Omega_{B/R} \end{array} \tag{1.7}$$

Dove p è un omomorfismo di algebre e dp è un morfismo di moduli su p nel senso che $dp(am) = p(a)dp(m)$.

OSSERVAZIONE Se A è un algebra su B a sua volta un algebra su R abbiamo per definizione, che i due moduli $\Omega_{A/R}, \Omega_{A/B}$ sono dati dagli stessi generatori e che per $\Omega_{A/B}$ dobbiamo aggiungere le relazioni $D[b],\ \forall b \in B$, ne deduciamo una successione esatta:

$$A \otimes_B \Omega_{B/R} \to \Omega_{A/R} \to \Omega_{A/B} \to 0. \tag{1.8}$$

Se $A = A_1 \oplus A_2$ si ha:

$$\Omega_{A/R} = \Omega_{A_1/R} \oplus \Omega_{A_2/R}. \tag{1.9}$$

Finiamo con una descrizione alternativa del modulo $\Omega_{A/R}$.

Consideriamo dunque $A \otimes_R A$ con l'omomorfismo di moltiplicazione:

$$m : A \otimes_R A \to A,\ m(a \otimes b) := ab, \quad \text{poniamo} \quad I := \ker m.$$

1.10 Lemma. *I è l'ideale generato dagli elementi $a \otimes 1 - 1 \otimes a,\ a \in A$.*

Dim. Se $\sum_i a_i \otimes b_i \in I$ si ha $\sum_i a_i b_i = 0$ e dunque:

$$\sum_i a_i \otimes b_i = \sum_i a_i \otimes b_i - 1 \otimes \sum_i a_i b_i = \sum_i (a_i \otimes 1 - 1 \otimes a_i) 1 \otimes b_i$$

□

$A \otimes_R A$ è un A modulo in due modi diversi, che possiamo scrivere a destra e sinistra, $a(c \otimes b) := ac \otimes b, \quad (c \otimes b)a := c \otimes ba$. Consideriamo I/I^2, questo è in modo naturale un A modulo perché modulo I^2 le due moltiplicazioni coincidono.

1.11 LEMMA. *L'applicazione* $\delta : A \to I/I^2,\ \delta(a) := 1 \otimes a - a \otimes 1$ *è una derivazione.*

DIM.

$$\delta(ab) := 1 \otimes ab - ab \otimes 1 = (1 \otimes a - a \otimes 1)b + a(1 \otimes b - b \otimes 1), \quad \text{mod } I^2$$

□

1.12 TEOREMA. *L'applicazione* $\delta : A \to I/I^2,\ \delta(a) := 1 \otimes a - a \otimes 1$ *induce un isomorfismo di* I/I^2 *con* $\Omega_{A/R}$.

DIM. Dalla propeietà universale abbiamo un morfismo $p : \Omega_{A/R} \to I/I^2, p(da) = a \otimes 1 - 1 \otimes a$.

Viceversa possiamo fare una costruzione formale, dato a=un anello A ed un suo modulo M si ha costruzione di *idealizzare* M, ovvero si costruisce un anello che come gruppo è $A \oplus M$ e la moltiplicazione è definita da $(a, m)(b, n) := (ab, am + bn)$ (in particolare $M^2 = 0$). facciamola per $\Omega_{A/R}$ e costruiamo $A \oplus \Omega_{A/R}$, Costruiamo l'applicazione:

$$\phi : A \times A \to A \oplus \Omega_{A/R},\ \phi(a, b) := (ab, ad(b)).$$

ϕ è R bilineare ed induce un morfismo (che denotiamo ancora con ϕ),

$$\phi : A \otimes A \to A \oplus \Omega_{A/R},\ \phi(a \otimes b) := (ab, ad(b)).$$

Si verifica facilmente che ϕ è un omomorfismo di anelli. per definizione $\phi(I) \subset \Omega_{A/R}$ e dato che $\Omega^2_{A/R} = 0$ si ha un morfismo indotto $\overline{\phi} : I/I^2 \to \Omega_{A/R}, \overline{\phi}(1 \otimes a - a \otimes 1) = (1a, 1d(a)) - (a1, ad(1)) = (0, da)$. Si vede facilmente che p e $\overline{\phi}$ sono inversi. □

2 Calcolo differenziale

Come usuale, una definizione cosí astratta non ci dice nulla su come è fatto tale modulo, bisogna perciò iniziare a fare qualche calcolo esplicito.

2.1 TEOREMA. *Se* $A = R[x_1, \ldots, x_n]$ *è l'anello dei polinomi in n variabili,* $\Omega_{A/R}$ *è un modulo libero sugli n differenziali* dx_i.

Più in generale se $A = B[x_1, \ldots, x_n]$ *è l'anello dei polinomi in n variabili su una R algebra B,*

$$\Omega_{A/R} = A \otimes_B \Omega_{A/R} \oplus \oplus_{i=1}^n Ad(x_i),$$

DIM. Sfrutteremo la proprietà universale. Sia $F = \oplus_{i=1}^n Au_i$ modulo libero.

Definiamo una derivazione $d : A \to F$ data da $Df(x) := \sum_{i=1}^{n} \frac{\partial f}{\partial x_i} u_i$, la definizione è tale che $d(x_i) = u_i$.

Se $D : A \to N$ è una derivazione definiamo l'applicazione lineare $f : F \to N,\ f(u_i) := D(x_i)$. Dallo studio dell'esempio precedente segue che $D = f \circ d$ come richiesto.

Più in generale, facciamolo in una variabile x poniamo $d(\sum_j a_j x^j) := \sum_j x^j d(a_j) + \sum_j j a_j x^{j-1} d(x)$. □

Dato un anello A ed un suo ideale I, posto $\overline{A} := A/I$, vediamo che relazione vi è fra $\Omega_{A/R}$ e $\Omega_{\overline{A}/R}$. Abbiamo che il diagramma si completa:

$$\begin{array}{ccc} A & \xrightarrow{d} & \Omega_{A/R} \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle dp} \\ A/I = \overline{A} & \xrightarrow{d} & \Omega_{\overline{A}/R} \end{array}$$

Si ha che dp è 0 su $dI + I\Omega_{A/R}$. Poichè $adi = d(ai) - ida$ è chiaro che $dI + I\Omega_{A/R}$ è un $A-$sottomodulo e che $\Omega_{A/R}/(dI + I\Omega_{A/R})$ è un $A/I-$modulo, infine la applicazione indotta $d : A/I \to \Omega_{A/R}/(dI + I\Omega_{A/R})$ è una derivazione e dalla proprietà universale si ottiene un isomorfismo:

$$\Omega_{A/R}/(dI + I\Omega_{A/R}) \cong \Omega_{\overline{A}/R}. \tag{2.2}$$

Possiamo rienunciare 2.2 in altro modo $\Omega_{A/R}/I\Omega_{A/R} = A/I \otimes_A \Omega_{\overline{A}/R}$, se $I = (f_1, \ldots, f_m)$ abbiamo che la immagine di dI in $A/I \otimes_A \Omega_{\overline{A}/R}$ è l'A/I sottomodulo generato dagli elementi df_i quindi:

$$\Omega_R(A/I) = A/I \otimes_A \Omega_{A/R}/(\sum_i A/I df_i). \tag{2.3}$$

Nel caso di un algebra finitamente presentata abbiamo:

2.4 Teorema. *Se $A = R[x_1, \ldots, x_n]$ e l'algebra $B := R[a_1, \ldots, a_n]$ è presentata come $B = R[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$ abbiamo una presentazione (esatta):*

$$B^m \xrightarrow{J} B^n \to \Omega_{B/R} \to 0. \tag{2.5}$$

con J la matrice Jacobiana.

Dim. $A/I \otimes_A \Omega_{A/R} = \oplus_{i=1}^{n} B dx_i = B^n$, il sottomodulo $\sum_i B df_i$ è il sottomodulo di B^n immagine del morfismo $J : B^m \to B^n$ con matrice la matrice Jacobiana di colonna $i-$esima $\frac{\partial f_i}{\partial x_j},\ j = 1, \ldots, n$. □

Consideriamo un caso importante, sia $B = A[x]/(f(x))$ con $f(x) = \sum_{i=0}^{n} a_i x^i$ un polinomio, la matrice Jacobiana si riduce alla derivata $f'(x)$, e

$$\Omega_{B/R} = B \otimes_{A[x]} \Omega_{A[x]/R}/Bdf(x) = B \otimes_A \Omega_{A/R} \oplus Bd(x)/B(\sum_{i=0}^{n} x^i d(a_i) + f'(x)d(x))$$

Se in B si ha $f'(x)$ invertibile si deduce che:

$$\Omega_{B/R} = B \otimes_A \Omega_{A/R}, \qquad d(x) = -(f'(x))^{-1}(\sum_{i=0}^{n-1} x^i d(a_i)). \tag{2.6}$$

Applichiamo questa analisi ad una estensione algebrica semplice di campi $K := k[x]/(f(x))$ con $f(x)$ irriducibile.

2.7 LEMMA. *Per una estensione algebrica semplice di campi $K := k[a] = k[x]/(f(x))$ si ha $\Omega_{K/k} = 0$ se e solo se $f'(x) \neq 0$, altrimenti* $\dim_K \Omega_{K/k} = 1$.

DIM. Da 2.4 se $f'(x) \neq 0$ si ha $f'(a)$ invertibile e $\Omega_{K/k} = K \otimes_k \Omega_{k/k} = 0$, altrimenti le formule generali danno $\Omega_{K/k} = Kda$. □

3 Localizzazione dei differenziali

Una proprietà importante del modulo dei differenziali è che si localizza e si commuta con i cambiamenti di base:

3.1 PROPOSIZIONE.
i) Dato un sistema moltiplicativo S in A abbiamo l'isomorfismo:

$$\Omega_{A[S^{-1}]/R} = \Omega_{A/R}[S^{-1}] \tag{3.2}$$

ii) Se B è una $R-$algebra si ha:

$$\Omega_{A\otimes_R B/B} = \Omega_{A/R} \otimes_R B \tag{3.3}$$

DIM. i) Dal diagramma

$$\begin{array}{ccc} A & \xrightarrow{d} & \Omega_{A/R} \\ {\scriptstyle p}\downarrow & & {\scriptstyle dp}\downarrow \\ A[S^{-1}] & \xrightarrow{d} & \Omega_{A[S^{-1}]/R} \end{array}$$

e dalla proprietà universale della localizzazione otteniamo un morfismo

$$dp[S^{-1}] : \Omega_{A/R}[S^{-1}] \to \Omega_{A[S^{-1}]/R},$$

d'altra parte vogliamo definire una derivazione $\delta : A[S^{-1}] \to \Omega_{A/R}[S^{-1}]$ definita da

$$\delta(a/s) := \frac{sd(a) - ad(s)}{s^2}$$

bisogna provare che è compatibile con la equivalenza.

Prima di tutto notiamo che, se $sa = 0,\ s \in S$ si ha in $\Omega_{A/R}$ che $sda + ads = 0$ localizzando ad S in $\Omega_{A/R}[S^{-1}]$ poiché $a = 0$ ed s è invertibile si deduce $da = 0$.

Possiamo quindi ridurci ad $A/I,\ I := \{a \in A | \exists s \in S,\ sa = 0\}$. Ora l'equivalenza $a/s \cong b/t$ implica

$$ta - sb = 0, \qquad \Longrightarrow \qquad td(a) - sd(b) = bd(s) - ad(t).$$

Dobbiamo provare che, in $\Omega_{A/R}[S^{-1}]$ si ha: $t^2sd(a) - t^2ad(s) = s^2(td(b) - bd(t))$.

Sia $C := t^2sd(a) - t^2ad(s) - s^2(td(b) + bd(t))$, dobbiamo provare $C = 0$.

$$C = ts(td(a) - sd(b)) - t^2ad(s) + s^2bd(t) = ts(bd(s) - ad(t)) - t^2ad(s) + s^2bd(t) =$$
$$= stbd(s) - t^2ad(s) - tsad(t) + s^2bd(t) = (sb - ta)[td(s) + sd(t)] = 0$$

Il lettore ora può verificare che δ è una derivazione e che quindi induce un morfismo $q : \Omega_{A/R}[S^{-1}] \to \Omega_{A[S^{-1}]/R}$ che si vede immediatamente essere inverso di $dp[S^{-1}]$.

ii) L'applicazione $d \otimes 1 : A \otimes_R B \to \Omega_{A/R} \otimes_R B$ è chiaramente una $B-$derivazone, dobbiamo provare che soddissfa la proprietà universale. Dato un $A \otimes_R B$ modulo M ed una $B-$derivazone $A \otimes_R B \xrightarrow{D} M$ si ha che M è anche un A modulo e $D(a \otimes 1)$ è una $R-$derivazione, esiste dunque un morfismo di $A-$moduli $\Omega_{A/R} \xrightarrow{f} M$ con $D(a \otimes 1) = f(da)$. Evidentemente f induce un $A \otimes_R B$ morfismo $\overline{f}$ da $\Omega_{A/R} \otimes_R B$ ad M definito da $\overline{f}(u \otimes b) = (1 \otimes b)f(u)$ e $D = \overline{f} \circ d \otimes 1$. □

4 Separabilità

Applichiamo la localizzazione al caso in cui A è un dominio, algebra su un campo k, e K il suo campo delle frazioni ed abbiamo dunque $K \otimes_A \Omega_{A/k} = \Omega_{K/k}$.

Vogliamo dunque studiare $\Omega_{K/k}$ come spazio vettoriale su K.

Dobbiamo ricordare alcuni elementi di Teoria di Galois.

4.1 DEFINIZIONE. *Date due estensioni $K \subset E$, $K \subset G$ con K, E, G campi un $K-$isomorfismo di E in G è semplicemente un omomorfismo non nullo (e quindi iniettivo) e $K-$lineare, $\phi : E \to G$. Se $[E : K] < \infty$ e $G = \overline{K}$ è una chiusura algebrica di K parliamo semplicemente di K isomorfismi.*

Una estensione $K \subset E$ di campi si dice **normale** *o* **quasi Galoisiana** *se per ogni $K-$isomorfismo di $\phi : E \to \overline{E}$ nella chiusura algebrica di E si ha $\phi(E) \subset E$.*

Se $E = K[a] = K[x]/(f(x))$ è una estensione semplice dare, un $K-$isomorfismo $\phi : E \to \overline{K}$ è equivalente a scegliere una radice di $f(x)$. Quante sono le radici di $f(x)$?. Sia n il grado di $f(x)$ che è un polinomio irriducibile su K. Una radice di $f(x)$ è miltipla se e solo se è anche radice di $f'(x)$, quindi $f(x)$ ha radici multiple se e solo se il massimo comun divisore di $f(x), f'(x)$ ha grado positivo. Poiché $f(x)$ è irriducibile questo avviene se e solo se $f'(x) = 0$, a sua volta questo avviene se e solo se la caratteristica del campo è $p > 0$ e $f(x) = g(x^p)$. In questo ultimo caso possiamo ovviamente scrivere $f(x) = h(x^{p^k})$ con $h'(x) \neq 0$ di grado m ed $n = mp^k$. Poichè l'applicazione $a \to a^{p^k}$ è un automorfismo di $\overline{K}$, si ha che $f(x)$ ha esattamente m radici. Quando $f'(x) \neq 0$ diremo che a è separabile su K,altrimenti inseparabile. All'opposto se $m = 1$ ed $f(x) = x^{p^k} - b$ ovvero $a^{p^k} = b$ e k è l'esponente minimo per cui $a^{p^k} \in k$ diremo che a è puramente inseparabile su K, il numero m è il grado di separabilità di a o di $f(x)$ su K. Più in generale, se $f(x) = \sum_{i=0}^{n} a_i x^i$, dato un isomorfismo $\phi : K \to \overline{K}$, esso si estende ad un isomorfismo di $K[a]$ in $\overline{K}$ in esattamente m modi.

4.2 LEMMA. *Data una estensione $K \subset E$ con $n = [E : K] < \infty$, l'insieme $\mathcal{I}_{E/K}$ dei $K-$isomorfismi di E in $\overline{K}$ ha $n-$elementi in caratteristica 0, e m elementi con $n = mp^k$ in caratteristica $p > 0$.*

In questo ultimo caso, $m = n$ se e solo se ogni elemento $a \in E$ è separabile su K e si dice che E è **separabile** *su K.*

DIM. Per induzione, usando le osservazioni precedenti sul numero di isomorfismi che estendono uno dato.

Se $K \subset E$ è normale, l'insieme dei $K-$isomorfismi di E nella chiusura algebrica coincide con il gruppo di automorfismi G della estensione. Se $F := E^G$ è il campo dei punti fissi di G si vede facilmente che $K \subset F$ è puramente inseparabile. In gnerale data $K \subset E$ una estensione finita e $\phi_j,\ j = 1, \ldots, m$ i $K-$isomorfismi di E nella chiusura algebrica, il sottocampo generato dai campi $\phi_j(E)$ è finito su K ed è la minima estensione normale contenente K. □

Da 2.7 abbiamo il criterio differenziale di separabilità:

4.3 PROPOSIZIONE. *Data una estensione $K \subset E$ con $n = [E : K] < \infty$ si ha che E è separabile su K se e solo se $\Omega_{E/K} = 0$.*

Le seguenti asserzioni seguono facilmente:

4.4 Teorema. *i) Se $K \subset E \subset F$ si ha che F è separabile su K se e solo se E è separabile su K e F è separabile su E.*

ii) Se E è separabile su K, il campo K è l'insieme degli elementi di E fissati dai $K-$isomorfismi di E.

iii) Se E è separabile su K si ha $E = K[a]$.

iv) Se $[E : K] = n$ e $\overline{K}$ è una chiusura algebrica di K, si ha che E è separabile su K se e solo se $E \otimes_K \overline{K} = \overline{K}^{\oplus n}$, è somma diretta di n copie di $\overline{K}$. Altrimenti $E \otimes_K \overline{K}$ contiene elementi nilpotenti non nulli.

Vi è un ultimo criterio utile per la separabilità, ricordiamo che data una estensione finta $E \supset K$ abbiamo una funzione $k-$lineare $Tr_{E/K} : E \to K$. Con tale funzione costruiamo la forma quadratica $Q(x) := Tr_{E/K}(x^2)$.

4.5 Proposizione. *Data una estensione $K \subset E$ con $n = [E : K] < \infty$ si ha che E è separabile su K se e solo se la forma quadratica $Q(x) := Tr_{E/K}(x^2)$ è non degenere.*

Dim. Per definizione $Tr_{E/K}(a)$ è la traccia dell'operatore di moltiplicazione per l'elemento a. Si estende a $Tr_{E\otimes_K \overline{K}/\overline{K}} : E \otimes_K \overline{K} \to \overline{K}$. Se E è separabile su K si ha $E \otimes_K \overline{K} = \overline{K}^{\oplus n}$. Un elemento $x = (k_1, \ldots, k_n) \in \overline{K}^{\oplus n}$ come operatore è diagonale e la sua traccia è $\sum_{i=1}^n k_i$ e quindi, $Q(x) = \sum_{i=1}^n X_i^2$. La forma è non degenere. Altrimenti nel caso non separabile $E \otimes_K \overline{K}$ contiene elementi non nulli a e nilpotenti, è chiaro che un tale a è nel nucleo delle forma bilineare associata a $Q(x)$. □

Dato un elemento a che soddisfa un polinomio minimo $g(x^{p^k})$ su K con $g' \neq 0$ si ha che a^{p^k} è separabile, pertanto una estensione $E \supset K$ si può costruire in due passi. Prima una estensione separabile $F \supset K$ poi una puramente inseparabile $E \supset F$.

Passiamo ora ad estensioni finitamente generate ma non necessariamente algebriche.

Il primo esempio è ovviamente $K = k(x_1, \ldots, x_m)$ il campo delle funzioni razionali in m variabili e quindi $\Omega_{K/k}$ è lo spazio vettoriale su K con base gli elementi dx_i.

4.6 Lemma. *Sia $K = k(a_1, \ldots, a_m)$ una estensione finitamente generata di campi. $\Omega_{K/k} = 0$ se e solo se K è algebrico e separabile su k.*

Dim. Sia i minimo con la proprietà che K è algebrico e separabile su $K_i := k(a_1, \ldots, a_i)$. Da si ha $\Omega_{K/k} = K \otimes_{K_i} \Omega_{K_i/k} = 0$ e quindi $\Omega_{K_i/k} = 0$ se $i = 0$ abbiamo $K_0 = k$ ed abbiamo concluso, altrimenti $\Omega_{K_i/K_{i-1}} = 0$ che, dal Lemma 2.7 e la analisi del caso delle funzioni razionali, implica che a_i è algebrico separabile su K_{i-1}. Ma queso implica che anche K è algebrico separabile su K_{i-1}, una contraddizione. □

In questo caso appare già un fenomeno peculiare alla caratteristica $p > 0$ ovvero una distinzione fra estensioni separabili ed inseparabili.

Se $a_1, \ldots, a_m \in K$ sono elementi per cui $d(a_1), \ldots, d(a_m) \in \Omega_{K/k}$ sono linearmente indipendenti su K, vorremmo dedurre che gli elementi a_i sono algebricamente indipendenti su k. Questo non è vero in generale un semplice esempio si ha con una estensione semplice non separabile.

Se $charK = p > 0$ dobbiamo supporre che k è *perfetto* ovvero che $\forall a \in k,\ \exists b \in k,\ a = b^p$.

4.7 LEMMA. *Se $a_1, \ldots, a_m \in K$ sono elementi per cui $d(a_1), \ldots, d(a_m) \in \Omega_{K/k}$ sono linearmente indipendenti su K e k è perfetto, gli elementi a_i sono algebricamente indipendenti su k.*

DIM. Sia per assurdo $f(x_1, \ldots, x_n)$ un polinomio di grado minimo su k che svanisce sugli a_i.

Si ha $df(a_1, \ldots, a_n) = \sum_{i=1}^n \dfrac{\partial f(a_1, \ldots, a_n)}{\partial x_i} da_i = 0$. Dall'indipendenza lineare dei da_i otteniamo che $\dfrac{\partial f(a_1, \ldots, a_n)}{\partial x_i} = 0,\ \forall i$. Dalla minimalità del grado otteniamo che tutte le derivate parziali di f sono nulle ovvero che f è un polinomio $g(x_1^p, \ldots, x_n^p)$.

Poiché il campo k è perfetto possiamo estrarre le radici $p-$esime dei coefficienti e scrivere infine $f = h^p$. Una contraddizione perché h diviene una relazione di grado più basso per gli a_i. □

4.8 TEOREMA. *Sia k perfetto e $K = k(x_1, \ldots, x_m)$ una estensione finitamente generata di campi.*

i) $\dim_K \Omega_{K/k} = Trdeg(K/k)$.

ii) dati $a_1, \ldots, a_n \in K$ gli elementi $da_1, \ldots, da_n$ sono una base di $\Omega_{K/k}$ su K se e solo se $a_1, \ldots, a_n$ sono una base di trascendenza di K su k e l'estensione $K \supset k(a_1, \ldots, a_n)$ è algebrica separabile.

DIM. Dalla analisi precedente abbiamo visto che $\dim_K \Omega_{K/k} \leq Trdeg(K/k)$, e se $da_1, \ldots, da_n$ sono una base di $\Omega_{K/k}$ su K gli elementi a_i sono algebricamente indipendenti su k. Ora calcoliamo $\Omega_{K/k(a_1,\ldots,a_n)}$. Per costruzione è il quoziente di $\Omega_{K/k}$ modulo il sottospazio generato dai da_i e quindi è 0. Ora applichiamo il Lemma 4.6 e vediamo che $K \supset k(a_1, \ldots, a_n)$ è algebrica separabile.

Viceversa se $K \supset k(a_1, \ldots, a_n)$ è algebrica separabile si ha (da 2.6):

$$\Omega_{K/k} = K \otimes_{k(a_1,\ldots,a_n)} \Omega_{k(a_1,\ldots,a_n)/k} = \oplus_{i=1}^n K da_i.$$

□

Nella teoria dei campi data una estensione $K \supset k$ ed elementi a_i algebricamente indipendenti su k con $K \supset k(a_1, \ldots, a_n)$ algebrica separabile, è detta *estensione separabile*.

Una tale base di trascendenza è detta *base separante*. In generale in caratteristica $p > 0$ non tutte le estensioni sono separabili. Abbiamo provato che:

COROLLARIO. *Se k è perfetto e K è finitamente generato allora K è separabile e le sue basi separanti sono gli insiemi di elementi a_i per cui i differenziali da_i sono una base lineare di $\Omega_{K/k}$ su K.*

Riprendiamo ora lo studio dei punti regolari di una varietà affine. Sia

$$A = R[a_1, \ldots, a_n] = k[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$$

e $B := R[a_1, \ldots, a_n]$ è presentata come $B = R[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$ abbiamo visto in 2.5 che si ha la successione esatta $A^m \xrightarrow{J} A^n \to \Omega_{A/k} \to 0$, che presenta, tramite la matrice Jacobiana J, il modulo dei differenziali.

Assumiano k perfetto, A un dominio di dimensione d e K il suo campo delle frazioni. Da 4.8 abbiamo $d = \dim_K \Omega_{K/k} = K \otimes_A \Omega_{A/k}$.

Come in Cap. 2, 5.8 abbiamo un $f \neq 0$ per cui $\Omega_{A/k}[1/f]$ è un modulo libero di rango d, l'aperto dove $f \neq 0$ è quindi formato da punti regolari. In altri termini, la matrice J pensata come matrice a coefficienti in K ha rango $n - d$ quindi i suoi minori di ordine $n - d + 1$ sono nulli in K e quindi in A, i minori di ordine $n - d$ non sono tutti nulli e generano un ideale J_{n-d} che definisce la sottovarietà dei punti singolari. Abbiamo provato:

4.9 Teorema. *Data una varietà irriducibile di dimensione d l'insieme dei punti regolari è un aperto non vuoto su cui il modulo $\Omega_{K/k}$ induce un fibrato vettoriale di dimensione d (il fibrato cotangente).*

Vediamo cosa vuol dire, per una algebra finitamente generata $A = k[a_1, \ldots, a_n]$ su un campo k che $\Omega_{A/k} = 0$.

4.10 Teorema. *Sia $A = k[a_1, \ldots, a_n]$, $\Omega_{A/k} = 0$ se e solo se A è somma diretta finita di campi di dimensione finita e separabili su k.*

Dim. Se A è somma diretta finita di campi di dimensione finita e separabili su k si ha $\Omega_{A/k} = 0$ da 1.9, 2.7.

Viceversa, sia $\Omega_{A/k} = 0$. Presa una chiusura algebrica $\overline{k}$ di k si ha A è somma diretta finita di campi di dimensione finita e separabili su k se e solo se $\overline{k} \otimes_k A$ è somma diretta finita di copie di $\overline{k}$. Si ha $\Omega_{\overline{k} \otimes_k A/\overline{k}} = 0$ ci riduciamo al caso k algebricamente chiuso.

Sia P un ideale primo di A e sia K il campo delle frazioni di A/P. Si ha che (2.3, 3.2) $\Omega_{K/k} = 0$ e quindi da 4.6, $K = A/P$ è di dimensione finita e separabile su k e quindi $A/P = k$. Dunque $A = \oplus_i A_i$ dove gli A_i sono anelli locali. Dobbiamo dunque vedere che, se A è un anello locale di dimensione finita su k e $\Omega_{A/k} = 0$ allora A non ha elementi nilpotenti. Sia $\overline{m}$ il radicale, se $\overline{m} \neq 0$ vi è un ideale $\overline{n}$ per cui $\dim_k \overline{m}/\overline{n} = 1$. Abbiamo dunque $A/\overline{n}$ è l'algebra $k[\epsilon]$, $\epsilon^2 = 0$ finalmente che $\Omega_{k[\epsilon]/k} \neq 0$. □

5 Anelli regolari, prime proprietà.

Se A è un anello locale regolare di dimensione n ed M il suo ideale massimale, diremo *parametri regolari* n elementi $(a_1, \ldots, a_n)$ per cui $M = (a_1, \ldots, a_n)$. Dal Lemma di Nakayama questo è equivalente a dire che $a_1, \ldots, a_n \in M$ sono una base modulo M^2 dello spazio vettoriale M/M^2 su A/M.

5.1 Teorema. *i) Dati parametri regolari $(a_1, \ldots, a_n)$ e posto $P = (a_1, \ldots, a_i)$ si ha che A/P è locale regolare di dimensione $n - i$.*

ii) Sia A un anello locale regolare di dimensione n e P un suo ideale tale che A/P è locale regolare di dimensione $n - i$. Allora esistono parametri regolari $(a_1, \ldots, a_n)$ per cui $P = (a_1, \ldots, a_i)$.

Dim. i) Dal teorema dll'ideale principale A/P è locale di dimensione $\geq n - i$. L'ideale massimale $\overline{M}$ di A/P si identifica a M/P e $\overline{M}/\overline{M}^2 = M/M^2 + P$ e per costruzione $\dim_{A/M} \overline{M}/\overline{M}^2 = n - i$ e si ha anche che $\dim A/P \leq n - i$, quindi A/P è locale regolare di dimensione $n - i$.

ii) Viceversa sia P tale che A/P è un anello locale regolare di dimensione $n - i$. Dal Corollario di 7.3 Cap. 4, P è un ideale primo.

Poiché $\dim_{A/M} \overline{M}/\overline{M}^2 = n - i$ e $\overline{M}/\overline{M}^2 = M/M^2 + P$ vi sono i elementi $a_1, \ldots, a_i \in P$ che si completano ad un sistema di elementi regolari $(a_1, \ldots, a_n)$ per A.

Dalla prima parte $A/(a_1, \ldots, a_i)$ è un dominio di dimensione $n - i$ e A/P un suo quoziente sempre di dimensione $n - i$. Pertanto $P = (a_1, \ldots, a_i)$. □

5.2 Definizione. *Un anello Noetheriano A si dice regolare se, per ogni ideale massimale M si ha che A_M è un anello locale regolare.*

È stato a lungo un problema aperto di provare che, se A è regolare e P è un ideale primo anche A_P è regolare. Questo è stato alla fine provato con una caratterizzazione omologica degli anelli regolari.

Possiamo però prima di tutto analizzare il caso geometrico.

5.3 Lemma. *Sia A un anello Noetheriano e P un ideale primo di codimensione d. A_P è regolare (di dimensione d) se e solo se esiste $f \notin P$ e $a_1, \ldots, a_d \in P$ con $(a_1, \ldots, a_d) = P[1/f]$ in $A[1/f]$. Ovvero P è generato localmente da d elementi.*

Dim. A_P è regolare (di dimensione d) se e solo se esistono $a_1, \ldots, a_d \in P$ con $(a_1, \ldots, a_d) = PA_P$ in A_P. Dai principi dilocalizzazione (e.g. Cap 2, 5.7) segue il Lemma. □

5.4 Teorema. *A è regolare se e solo se $A[x]$ è regolare.*

Dim. Sia A regolare e P un ideale di $A[x]$, posto $Q := P \cap A$ si ha che A_Q è regorale e possiamo passare a $A_Q[x]$. Supporre dunque A locale regolare di dimensione d e di ideale massimale $Q = (a_1, \ldots, a_d)$ e $P \cap A = Q$. Se $F = A/Q$ si ha che P induce in $F[x]$ un ideale primo che quindi o è 0 ovvero è della forma $(f(x))$ con $(f(x))$ irriducibile. Nel primo caso P è un ideale primo di codimensione d generato dai $d-$elementi $a_1, \ldots, a_d$. Nel secondo se $u(x) \in P$ solleva $f(x)$, P è un ideale primo di codimensione $d+1$ generato dai $d-$elementi $a_1, \ldots, a_d, u(x)$. In entrambi i casi il Lemma precedente si applica.

Viceversa se $A[x]$ è regolare e Q è un ideale primo di codimensione d in A si ha che $P = Q[x] + (x)$ è un ideale primo di codimensione $d + 1$ in $A[x]$ e $A_Q = A[x]_P/(x)$. Basta provare che, se M è l'ideale massimale di $A[x]_P$, $x \notin M^2$ questo si verifica immediatamente passando modulo $Q[x]$. □

5.5 Teorema. *Se A è un campo o $A = \mathbb{Z}$ si ha $A[x_1, \ldots, x_n]$ è regolare.*

5.6 Teorema. *Se $V \supset W$ sono varietà irriducibili, $k[V]$ l'anello di coordinate di V e P l'ideale primo definente W si ha $k[V]_P$ è regolare se e solo se W contiene almeno un punto liscio di V.*

Dim. Se $k[V]_P$ è regolare di dimensione d in un aperto affine P è generato da d elementi, resringiamoci a tale aperto e supponiamo

□

6 Morfismi lisci ed étale

Vogliamo generalizzare le nozioni di non singolarità ad una idea di morfismi lisci.

Intuitivamente un morfismo $f : X \to Y$ di varietà analitiche è liscio se in coordinate locali X è il prodotto di Y con un aperto dello spazio e f è la proiezione.

Per algebrizzare questa idea prendiamo prima di tutto la definizione locale delle varietà non singolari. Sia dunque A un anello $f_1(x), \ldots, f_n(x) \in A[x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+k}]$, n polinomi in $m = n + k$ variabili. Sia $\Delta := \det(\frac{\partial f_i}{\partial x_j}),\ i, j = 1, \ldots, n.$

6.1 Definizione. *L'algebra*

$$B := A[x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+k}]/(f_1(x), \ldots, f_n(x))[\Delta^{-1}]$$

è detta algebra standard liscia di dimensione k su A.

Se $k = 0$ parleremo di algebra étale standard su A.

Questa definizione può essere globalizzata come segue.

6.2 Definizione. *Data un algebra B su A ed un punto $P \in Spec(B)$ diremo che B è liscia (risp étale) su A in P se esiste un intorno di P in cui l'algebra $B[1/f]$ è standard liscia di dimensione k (risp. étale standard) su A.*

B è liscia (risp étale) su A se lo è in ogni suo punto.

È meglio pensare in termini di morfismi, il morfismo di algebre è pensato come un *comorfismo* $f^* : A \to B$ indotto da un morfismo di schemi affini $f : X \to Y$, $X := Spec(B)$, $Y := Spec(A)$. Vediamo le prime proprietà della definizione:

6.3 Lemma.

i) Se C è un'algebra liscia standard su B di dimensione k e B è un'algebra liscia standard su A di dimensione h allora C è un'algebra liscia standard su A di dimensione $h + k$.

ii) Se B è un'algebra liscia standard su A di dimensione h e C è una $A-$algebra allora $C \otimes_A B$ è un'algebra liscia standard su B di dimensione h.

iii) Se B, C sono due algebre liscie standard su A di dimensione h, k allora $B \otimes_A C$ è un'algebra liscia standard su A di dimensione $h + k$.

DIM. i) Siano

$$B := A[x_1, \dots, x_n, \dots, x_{n+h}]/(f_1(x), \dots, f_n(x))[\Delta^{-1}], \Delta := \det(\frac{\partial f_i}{\partial x_j}),\ i, j = 1, \dots, n,$$

$$C := B[y_1, \dots, y_m, \dots, y_{m+k}]/(g_1(y), \dots, g_m(y))[\Gamma^{-1}], \Gamma := \det(\frac{\partial g_i}{\partial y_j}),\ i, j = 1, \dots, m.$$

pur di moltiplicare per una potenza di δ possiamo sollevare i $g_i(y)$ a polinomi $G_i(x, y)$ a coefficienti in A e Γ si solleva a $\Phi := \det(\frac{\partial G_i}{\partial y_j}),\ i, j = 1, \dots, m$:

$$C := A[x_1, \dots, x_{n+h}, y_1, \dots, y_{m+k}]/(g_1(y), \dots, g_m(y))[(\Delta\Phi)^{-1}],$$

Evidentemente il prodotto $\Delta\Phi$ è il determinante della matrice Jacobiana dei polinomi $f_1(x), \dots, f_n(x), G_1(x, y), \dots, G_m(x, y)$ rispetto alle variabili $x_1, \dots, x_n, y_1, \dots, y_m$.

ii) Se $B := A[x_1, \dots, x_n, \dots, x_{n+h}]/(f_1(x), \dots, f_n(x))[\Delta^{-1}]$ si ha

$$C \otimes_A B = B := C[x_1, \dots, x_n, \dots, x_{n+h}]/(f_1(x), \dots, f_n(x))[\Delta^{-1}]$$

iii) Segue dai due precedenti. □

6.4 TEOREMA.

(1) *Dati morfismi $X \xrightarrow{f} Y \xrightarrow{g} Z$, $X := Spec(C)$, $Y := Spec(B)$, $Z := Spec(A)$. Se f è liscia (risp. étale) in un punto $P \in Spec(C)$ e g è liscia (risp étale) in $f(P)$ si ha che $g \circ f$ è liscia (risp. étale) in P.*

(2) *Dato un prodotto fibrato:*

$$\begin{array}{ccc} X \times_Z Y & \xrightarrow{g} & Y \\ {\scriptstyle q}\downarrow & & \downarrow{\scriptstyle p} \\ X & \xrightarrow{f} & Z \end{array} \tag{6.5}$$

se f è liscia (risp. étale) lo è anche g.

(3) *Se in 5.5 anche p è liscia (risp. étale) lo è anche $p \circ g = f \circ q : X \times_Z Y \to Z$.*

DIM. Segue dalla localizzazione ed il Lemma precedente.

□