PROPRIETA' DELL' ANELLO GENERICO

Seminario tenuto dal
prof. ANDERS KOCK (Aarhus)

come visiting professor del CNR all'Istituto di Matematica "Guido Castelnuovo" dell'Università di Roma nel mese di maggio 1977.

Appunti raccolti da Anna Barbara VEIT RICCIOLI.

I N D I C E

PARTE PRIMA : L'algebra commutativa in un topos

1. Introduzione

Nel corso di questo seminario lavoreremo prevalentemente nelle categorie

- $\mathcal{S}^{\mathcal{A}}$, la categoria dei funtori dalla categoria $\mathcal{A}$ degli anelli(*) finitamente presentati(**) alla categoria degli insiemi $\mathcal{S}$;
- $\mathcal{X}$, il topos di Zariski che definiremo nel seguito; $\mathcal{X}$ è una sottocategoria piena di $\mathcal{S}^{\mathcal{A}}$.

L'importanza di $\mathcal{S}^{\mathcal{A}}$ nella geometria algebrica deriva dal fatto che la maggior parte delle costruzioni che si considerano in questa disciplina dipende <u>funtorialmente</u> dall'anello di base. Così, per esempio, dato un anello A, consideriamo

- $S^1(A) =: \{(x,y) \in A^2 \mid x^2+y^2 = 1\}$, la <u>circonferenza</u> di A;
- $V^{1,2}(A) =: \{(x,y) \in A^2 \mid \exists\, t,s \in A \quad tx+sy=1\}$, l'insieme delle coppie di elementi di A che **generano tutto A.**

Ogni omomorfismo $f: A \longrightarrow B$ da A in un altro anello B induce un'applicazione $S^1(f) : S^1(A) \longrightarrow S^1(B)$,
rispettivamente $V^{1,2}(f) : V^{1,2}(A) \longrightarrow V^{1,2}(B)$,
e si vede così che S^1 e $V^{1,2}$ danno luogo a funtori. Potremmo considerare il funtore S come la <u>circonferenza universale</u>. (Cfr. il testo di Gabriel e Demazure [GD]). Accanto agli oggetti S^1 e $V^{1,2}$ di $\mathcal{S}^{\mathcal{A}}$, consideriamo il <u>funtore distratto</u> $\mathbb{A}: \mathcal{A} \longrightarrow \mathcal{S}$ che associa ad ogni $B \in \mathcal{A}$ il suo insieme di sostegno. Chiameremo il funtore $\mathbb{A}$ <u>la retta</u> (affine): esso associa al campo dei numeri

---

(*) Quando parliamo di anelli, sottintendiamo sempre: anelli commutativi con unità 1.

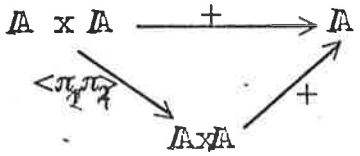
(**) Un anello è finitamente presentato, se è del tipo A/I, dove A è un anello libero con un numero finito di generatori, cioè $A \cong \mathbb{Z}[X_1,\ldots,X_n]$, e I un ideale di A, anch'esso con un numero finito di generatori.

reali precisamente la retta reale. $\mathbb{A}$ è un anello in $\mathscr{A}$: abbiamo le trasformazioni naturali

$$\begin{array}{rcl} \mathbb{A}\times\mathbb{A} & \xrightarrow{+} & \mathbb{A} \\ \mathbb{A}\times\mathbb{A} & \xrightarrow{\cdot} & \mathbb{A} \\ \mathbb{A} & \xrightarrow{-} & \mathbb{A} \\ 1 & \xrightarrow{\ulcorner 1 \urcorner} & \mathbb{A} \\ 1 & \xrightarrow{\ulcorner 0 \urcorner} & \mathbb{A}; \end{array}$$

per esempio, $\mathbb{A}\times\mathbb{A} \xrightarrow{+} \mathbb{A}$ associa ad ogni $B \in \mathscr{A}$ l'addizione in B: $(\mathbb{A}\times\mathbb{A})(B) \cong \mathbb{A}(B)\times\mathbb{A}(B) = B\times B \xrightarrow{+} B = \mathbb{A}(B)$.

Poichè gli assiomi di anello sono equazionali, possiamo esprimerci in termini di commutatività di certi diagrammi, per esempio la commutatività dell'addizione si esprime dicendo che il triangolo



è commutativo.

Accanto a questo approccio funtoriale alla geometria algebrica, consideriamo anche il seguente: dato un anello A in una categoria $\mathscr{C}$ con limiti finiti, possiamo concepire ogni espressione polinomiale in (al più) n variabili ($n \geqslant 0$) come un morfismo da A^n a A; così, per esempio, concepiamo l'espressione x^2+y^2 come il seguente morfismo:

$$AxA \xrightarrow{qxq} AxA \xrightarrow{+} A,$$

dove q è il morfismo "quadrato" corrispondente all'espressione x^2, cioè

$$q = A \xrightarrow{\Delta} AxA \xrightarrow{\cdot} A\ .$$

Possiamo quindi ancora definire la circonferenza di A ponendo

$$S^1(A) =: \{(x,y) \in A^2 \mid x^2+y^2 = 1\},$$

purchè interpretiamo in modo opportuno questo simbolismo "insiemistico", intendendo ci è l'espressione a destra come l'egualizzatore dei due morfismi $A^2 \xrightarrow{x^2+y^2} A$ e $A^2 \longrightarrow 1 \xrightarrow{\lceil 1 \rceil} A$.

Chiaramente, questa tecnica permette di interpretare ogni formula del tipo $\{(x_1,\ldots,x_n) \in A^n \mid f(x_1,\ldots,x_n) = g(x_1,\ldots,x_n)\}$; dove f e g sono espressioni polinomiali in al più n variabili. Una definizione analoga di $V^{1,2}$ è tuttavia complicata dal fatto che, nella definizione originale di $V^{1,2}$ compare il quantificatore esistenziale $\exists$. Ma se $\mathscr{C}$ ammette una "buona" fattorizzazione dei morfismi in un epi seguito da un mono, cioè se $\mathscr{C}$ possiede immagini (come $\mathscr{S}$ per esempio), possiamo definire anche $V^{1,2}$ e altri oggetti nella cui definizione compare $\exists$: formiamo dapprima

$$V'(A) =: \{(x,y,s,t) \in A^4 \mid tx + sy = 1\}$$

come $\varprojlim$ finito con la tecnica appena descritta e definiamo

$$V^{1,2}(A) =: \mathrm{Im}\,(V'(A) \rightarrowtail A^4 \xrightarrow{\langle \pi_1,\pi_2 \rangle} A^2) \rightarrowtail A^2.$$

Se consideriamo in particolare $\mathscr{C} = \mathscr{S}^{\mathbb{A}}$ e $A = \mathbb{A}$, risulta $S^1(\mathbb{A}) = S^{\hat{1}}$ e $V^{1,2}(\mathbb{A}) = V^{\hat{1},\hat{2}}$. Il nostro anello $\mathbb{A}$ in $\mathscr{S}^{\mathbb{A}}$ collega dunque questi due punti di vista, facendo apparire il secondo come una generalizzazione del primo. Cercheremo nel seguito di comprendere meglio questa funzione generalizzante di $\mathbb{A}$, dando un senso preciso alle affermazioni

- $\mathbb{A} \in \mathscr{S}^{\mathbb{A}}$ è l'anello <u>generico</u>;
- $\mathbb{A} \in \mathscr{X}$ è l'anello locale <u>generico</u>;

si serviremo a questo scopo della nozione di <u>topos classificante</u>. Queste proprietà di $\mathbb{A}$, messe in evidenza da M.Hakim [H], significano naturalmente che le costruzioni geometriche che si effettuano su $\mathbb{A}$ hanno un'importanza particolare.

Le costruzioni che, partendo da un anello A in una cate-

goria $\mathscr{C}$, ci hanno portato ai sotto-oggetti $S^1(A)$ e $V^{1,2}(A)$ di A^2 si possono inquadrare in una semantica categoriale: possiamo concepirle come **interpretazioni di** formule. Indicheremo nel seguito un metodo che permette di interpretare ogni formula Φ espressa per esempio nel linguaggio della teoria degli anelli un sottooggetto $[\![\Phi]\!]$ **di** A^n (se in Φ occorrono non più di n variabili libere); si noti però che la logica classica non è generalmente valida in categorie come $\mathscr{S}^{\mathscr{A}}$ o $\mathscr{X}$; lo è invece la logica intuizionista nel senso che, date due formule Φ e Ψ , non è generalmente sufficiente che Φ implica Ψ nella teoria classica degli anelli perchè si abbia $[\![\Phi]\!] \leqslant [\![\Psi]\!]$: occorre che l'implicazione $\Phi \to \Psi$ si possa dimostrare con i mezzi della logica intuizionista. Tuttavia, dimostreremo un metateorema:

> finchè si considerano soltanto formule coerenti (cioè costruite usando come simboli logici solo $\wedge$, $\vee$, $\exists$ e $\uparrow$ (il vero)), la logica intuizionista coincide con quella classica.

Un modo particolarmente fruttuoso di lavorare con l'anello generico o con l'anello locale generico consiste quindi nel trasportare tutte le costruzioni e nozioni in un contesto di logica coerente.

La geometria algebrica classica si basa su campi, o addirittura su campi algebricamente chiusi, idealizzando così la situazione per avere un ambiente abbastanza vasto da consentire tutte le costruzioni algebriche. Considerare il funtore $\mathbb{A} \in \mathscr{S}^{\mathscr{A}}$ è per certi versi un punto di vista analogo: si prendono tutti gli anelli finitamente presentati contemporaneamente. Tuttavia, in un anello che è semplicemente commutativo, molte costruzioni presentano delle difficoltà, come per esempio le varietà grassmanniane: non disponiamo infatti di abbastanza elementi invertibili. Esiste

però una tecnica con la quale $\mathbb{A}$ può venir "forzato" ad essere

- un campo
- un campo algebricamente chiuso
- un anello locale;

di ciò parleremo nel seguito.

Osserviamo intanto che un modo di descrivere assiomaticamente un anello locale consiste nell'aggiungere agli assiomi di anello i seguenti assiomi:

a) $\neg(1=0)$,

b) $\forall x$, x è invertibile oppure $1-x$ lo è;

(si veda [K 77] p.62). La nozione di anello locale comporta quindi l'esistenza di almeno un certo numero di elementi invertibili, anche se non tanti quanti ne comporta la nozione di campo. Abbiamo però delle ragioni molto valide per non "forzare" $\mathbb{A}$ ad essere un campo : in tal caso, non avremmo infatti elementi nilpotenti, ed è nota l'importanza di questi elementi nella geometria algebrica. Forse è proprio questa la ragione per la quale il topos di Zariski è stato inventato. Infatti, se guardiamo al nostro funtore $\mathbb{A}$ in $\mathcal{X}$, esso è un anello locale.

Un'ultima osservazione: se la nozione di campo non è "buona", lo è però quella di chiusura algebrica; cercheremo quindi nel seguito di elaborare una nozione di

"anello locale algebricamente chiuso"

(o più precisamente, separatamente chiuso). Questa nozione esiste e possiede un ben noto topos classificante: è quello che Grothendieck chiama "topos étale" $\mathcal{E}t$.

2. L'anello generico e l'anello locale generico

2.1. La nozione di genericità

Premettiamo le seguenti definizioni:

Definizione 1. Un funtore $f: \mathscr{C} \longrightarrow \mathscr{D}$ si dice geometrico se possiede un aggiunto a sinistra

$$f^* \dashv f$$

che è esatto a sinistra (cioè conserva i $\varprojlim$ finiti; si ricordi che un aggiunto a sinistra conserva sempre i colimiti).

Definizione 2. Una sottocategoria piena $\mathscr{C}$ di una categoria $\mathscr{D}$ si dice geometrica se il funtore $\mathscr{C} \hookrightarrow \mathscr{D}$ è geometrico, cioè se $\mathscr{C}$ è una sottocategoria riflessiva di $\mathscr{D}$ per la quale il funtore di riflessione $r: \mathscr{D} \longrightarrow \mathscr{C}$ conserva i $\varprojlim$ finiti.

Definizione 3. Un topos di Grothendieck (o brevemente topos) è una categoria $\mathscr{E}$ che è (o può venir trasformata in) una sottocategoria geometrica di una categoria del tipo $\mathscr{S}^{\mathscr{C}^{dp}}$ con $\mathscr{C}$ piccola (*). In particolare quindi $\mathscr{S} \cong \mathscr{S}^{\{*\}}$ è un topos ($\{*\}$ è la categoria con un solo oggetto e un solo morfismo), e di questo topos, i topos di Grothendieck ereditano quasi tutte le proprietà, in particolare le proprietà di esattezza, poichè, come in ogni categoria di funtori a valori in $\mathscr{S}$, i limiti si calcolano "punto per punto".

La nozione adeguata di funtore tra due topos è la seguente:

(*) Questa definizione è equivalente a quella che richiede l'equivalenza con una categoria di fasci su un sito: il funtore r di riflessione induce una topologia di Grothendieck su $\mathscr{C}$ tale che $\mathscr{E} \cong$ Fasci ($\mathscr{C}$), ved. 2.3.

Definizione 4. Dati due topos $\mathscr{E}$ e $\mathscr{F}$, poniamo

$\mathrm{Top}(\mathscr{E},\mathscr{F})$ =: l'insieme dei funtori geometrici da $\mathscr{E}$ in $\mathscr{F}$.

Vorremmo parlare della categoria $\mathrm{Top}(\mathscr{E},\mathscr{F})$; osserviamo però che, per due funtori geometrici

$$\mathscr{E} \underset{f}{\overset{g}{\rightrightarrows}} \mathscr{F},$$

abbiamo (ved.[ML]) una corrispondenza biunivoca tra le trasformazioni naturali da f a g e quelle da g^* a f^*. Quali sceglieremo come morfismi di $\mathrm{Top}(\mathscr{E},\mathscr{F})$? Optiamo per la seguente

Definizione 5. Un morfismo tra due morfismi geometrici $f,g \in \mathrm{Top}(\mathscr{E},\mathscr{F})$ è una trasformazione naturale da f^* a g^*, (o, equivalentemente, da g a f).

Questa definizione è conveniente, perchè i morfismi del tipo f^*, conservando tutti i $\varprojlim$ finiti e tutti i colimiti, conservano molte cose, come, per esempio, la nozione di anello: un anello in $\mathscr{F}$ fornisce un anello in $\mathscr{E}$; l'esattezza a destra fa sì che anche la nozione di anello locale si conserva poichè, come ora vedremo, essa è formulabile(*) in termini di limiti e colimiti. Adottando come sopra le notazioni insiemistiche, dato un anello A in un topos $\mathscr{E}$, si consideri il composto

$$\{(a,b) \in A^2 \mid a\cdot b = 1\} \rightarrowtail A \times A \xrightarrow{\pi_1} A.$$

Definiamo U(A), l'"oggetto delle unità di A" come l'immagine di questo morfismo composto. Analogamente, definiamo $\tilde{U}(A)$ come l'immagine di

$$\{(a,b) \mid (1-a)\cdot b = 1\} \rightarrowtail A^2 \xrightarrow{\pi_1} A.$$

Possiamo ora dare la seguente:

(*) Daremo più avanti una semantica più sistematica; la definizione che diamo qui ha quindi un carattere "ad hoc".

Definizione 6: Un anello A in un topos è locale sse
- $U(A) \cup \tilde{U}(A) = A$ (*);
- $\neg(1=0)$, cioè l'oggetto iniziale $\emptyset$ è l'egualizzatore dei morfismi $1 \rightrightarrows A$ $\ulcorner 1 \urcorner$, $\ulcorner 0 \urcorner$.

f^* conserva tutti gli elementi di questa definizione:
- i sotto-oggetti di A^2 individuate dalle equazioni polinomiali per l'esattezza a sinistra;
- le immagini poichè conserva i monomorfismi e gli epimorfismi visto che si tratta di limiti rispettivamente di colimiti;
- l'unione che è un colimite;

e quindi f^* conserva gli anelli locali.

Questa nostra definizione "ad hoc" degli anelli locali è basata sull'assioma

$\forall x$ x è invertibile oppure $1-x$ lo è.

Si tratta di un enunciato del primo ordine logicamente equivalente all'usuale definizione degli anelli locali nella quale si richiede l'esistenza di un unico ideale massimale, e che rinchiude per ciò un enunciato di secondo ordine. Quando lavoriamo nei topos, dobbiamo sempre fare appello alla nostra abilità di trasformare enunciati di ordine superiore in un certo tipo di enunciati positivi di primo ordine. Vedremo più avanti quale è la logica più adatta per lavorare nei topos - la logica "coerente" - che in un primo momento possiamo caratterizzare come

> "la logica che viene conservata dai funtori f^* che provengono da funtori geometrici tra due topos".

Anche quando esporremo nel seguito alcuni lavori recenti di G.Wraith su una teoria di Galois intuizionista, il nostro interesse per

---

(*) Con il simbolo $\cup$ indichiamo l'unione, cioè il più grande sotto-oggetto contenente entrambi.

la logica intuizionista non è dovuta a motivi di"sicurezza", bensì al fatto che questa logica è applicabile in un topos ed ha pertanto una utilità per la matematica concreta. In questo modo si trova, per esempio, che la teoria di Galois intuizionista è la teoria degli anelli locali henseliani con un campo dei residui separatamente chiuso, o più precisamente, si vede che nell'ambito della logica intuizionista, questa teoria costituisce una buona traduzione della teoria classica dei campi algebricamente chiusi. Ma la teoria classica di questi anelli henseliani è di ordine superiore, e quindi occorre effettivamente riformularla all'interno della logica coerente.

Daremo ora, in prima approssimazione, una definizione del concetto di genericità; la diamo solo per gli anelli locali, poichè è chiaro come vada applicata ad altre nozioni che, come questa, coinvolgono soltanto $\varprojlim$ o $\varinjlim$, immagini e così via:

Definizione 7'. Un anello locale A in un topos $\mathscr{E}$ è generico se per ogni topos $\mathscr{F}$ e ogni anello locale B in $\mathscr{F}$ esiste un funtore geometrico

$$g: \mathscr{F} \longrightarrow \mathscr{E}$$

(essenzialmente) unico tale che $g^*(A)$ sia isomorfo a B.

Una definizione sostanzialmente identica ma formalmente più corretta è la seguente:

Definizione 7. Un anello locale A in un topos $\mathscr{E}$ è generico, sse per ogni topos $\mathscr{F}$, la categoria $\mathscr{L}(\mathscr{F})$ degli anelli locali in $\mathscr{F}$ è equivalente alla categoria $\mathrm{Top}(\mathscr{F}, \mathscr{E})$ in virtù della corrispondenza

$$g \longmapsto g^*(A).$$

Si dirà allora che il topos $\mathscr{E}$, o meglio, la coppia $(A, \mathscr{E})$, è il

topos classificante della nozione di anello locale.(*)
Per far vedere che una nozione, come quella di anello locale, possiede un topos classificante, occorre in realtà descrivere la categoria $\mathscr{L}(\mathscr{F})$, e in particolare i suoi morfismi; si noti che, in questo caso, i morfismi saranno tutti gli omomorfismi di anelli - non solo quelli locali. Più in generale, data una teoria T, la categoria dei modelli di T in un topos $\mathscr{F}$ ha per morfismi tutti i morfismi di $\mathscr{F}$ che conservano le operazioni e le nozioni primitive.

2.2. L'anello generico

Per dimostrare che $\mathbb{A} \in \mathscr{S}^{\mathscr{A}}$ è l'anello generico, dobbiamo mostrare che $\mathbb{A}$ induce per ogni topos $\mathscr{F}$ una equivalenza

$$\mathrm{Top}(\mathscr{F}, \mathscr{S}^{\mathscr{A}}) \simeq \mathscr{A}n(\mathscr{F}).$$

(Indichiamo con $\mathscr{A}n(\mathscr{F})$ la categoria degli anelli commutativi di $\mathscr{F}$; quando scriveremo semplicemente $\mathscr{A}n$, intendiamo $\mathscr{A}n(\mathscr{S})$). A questo scopo dimostriamo dapprima un teorema che rientra in una semantica funtoriale, analoga alla semantica di Lawvere che considera i modelli di una teoria algebrica $\mathscr{T}$ in una categoria $\mathscr{C}$ come funtori da $\mathscr{T}$ a $\mathscr{C}$ che conservano i prodotti finiti:

Teorema 1. Per ogni topos $\mathscr{F}$, la categoria $\mathscr{A}n(\mathscr{F})$ è equivalente alla categoria $\mathrm{Lex}(\mathscr{A}^{op}, \mathscr{F})$ dei funtori esatti a sinistra da $\mathscr{A}^{op}$ a $\mathscr{F}$(**)

(*) Diciamo il (e non un) topos classificante, visto che si tratta di un concetto definito tramite una proprietà universale.

(**) Si noti che $\mathscr{A}^{op}$ ha lim finiti, cioè $\mathscr{A}$ ha lim finiti: un lim finito di anelli finitamente presentati è ancora un anello finitamente presentato; ha perciò senso parlare di funtori esatti a sinistra da $\mathscr{A}^{op}$ a $\mathscr{F}$.

Per dimostrare questo teorema, ci serviamo di due lemmi:

Lemma 1. $\mathbb{A} \in \mathscr{S}^{\mathscr{A}n}$ è un funtore rappresentabile :

$$\mathbb{A} \cong h^{\mathbb{Z}[X]}.$$

Questo lemma risulta dal fatto che, definendo per ogni $B \in \mathscr{A}n$

$$i_B : \mathbb{A}(B) = B \longrightarrow h^{\mathbb{Z}[X]}(B)$$

$$b \in B \longmapsto \left[\lambda_b : \mathbb{Z}[X] \longrightarrow B, \text{ l'omomorfismo di anelli univocamente determinato dal fatto che } \lambda_b(X) = b\right],$$

si ottiene nella famiglia $(i_B)_{B \in \mathscr{A}n}$ un isomorfismo naturale

$$i : \mathbb{A} \xrightarrow{\cong} h^{\mathbb{Z}[X]}.$$

Lemma 2. $\mathbb{Z}[X]$ è un co-anello, cioè un anello in $\mathscr{A}^{op}$.

Visto che $\mathscr{A}^{op} \hookrightarrow \mathscr{A}n^{op}$ conserva i $\varprojlim$ finiti (gli anelli finitamente presentati sono stabili rispetto alla formazione dei lim in $\mathscr{A}n$), affinchè $\mathbb{Z}[X]$ sia un anello in $\mathscr{A}^{op}$, basta che lo sia in $\mathscr{A}n^{op}$. Ora, un oggetto A di una categoria $\mathscr{C}$ è un anello in $\mathscr{C}$ sse $h_A : \mathscr{C}^{op} \longrightarrow \mathscr{S}$ si fattorizza attraverso il funtore distratto da $\mathscr{A}n$ in $\mathscr{S}$ (cfr. [ML], III,6); nel nostro caso, si tratta perciò di stabilire che $h^{\mathbb{Z}[X]} : (\mathscr{A}n^{op})^{op} = \mathscr{A}n \longrightarrow \mathscr{S}$ si fattorizza attraverso $\mathbb{A} : \mathscr{A}n \longrightarrow \mathscr{S}$ - ma ciò discende immediatamente dal lemma 1.

Dimostrazione del teorema 1. In base al lemma 2, possiamo associare ad un dato $f \in \mathrm{Lex}(\mathscr{A}^{op}, \mathscr{F})$ l'anello $f(\mathbb{Z}[X])$ in $\mathscr{F}$. Viceversa, dato $R \in \mathscr{A}n(\mathscr{F})$, dobbiamo definire $f_R : \mathscr{A}^{op} \longrightarrow \mathscr{F}$, cioè occorre associare ad ogni $B \in \mathscr{A}^{op}$ un oggetto di $\mathscr{F}$. Per avere $\mathscr{A}n(\mathscr{F}) \simeq \mathrm{Lex}(\mathscr{A}^{op}, \mathscr{F})$, occorre intanto porre $f_R(\mathbb{Z}[X]) = R$; d'altra parte,

per definizione di $\mathscr{A}$, ogni $B \in \mathscr{A}$ è un colimite finito di varie copie di $\mathbb{Z}[X]$, e $B \in \mathscr{A}^{op}$ è pertanto il corrispondente limite; perciò, se f_R dev'essere esatto a sinistra, esso è completamente determinato dalla sua azione su $\mathbb{Z}[X]$. ◆

Teorema 2. $\mathbb{A} \in \mathscr{S}^{\mathscr{A}}$ è l'anello generico.

Dimostrazione. Grazie al teorema 1, è ora sufficiente dimostrare che, per ogni topos $\mathscr{F}$, $\mathbb{A}$ induce un'equivalenza

$$\mathbf{Top}(\mathscr{F}, \mathscr{S}^{\mathscr{A}}) \simeq \mathbf{Lex}(\mathscr{A}^{op}, \mathscr{F})$$

Dato $f \in \mathbf{Lex}(\mathscr{A}^{op}, \mathscr{F})$, consideriamo il diagramma

$$\begin{array}{ccc} \mathscr{A}^{op} & \xrightarrow{\text{Yoneda}} & \mathscr{S}^{\mathscr{A}} \\ & \searrow^{f} & \\ & & \mathscr{F} \end{array}$$

Sia $\overline{f}: \mathscr{S}^{\mathscr{A}} \longrightarrow \mathscr{F}$ l'estensione di Kan di f lungo il funtore di Yoneda. Essendo $\mathscr{F}$ un topos, $\mathscr{A}^{op}$ piccola con $\varprojlim$ finiti e f esatto a sinistra, possiamo applicare un teorema di Ulmer che stabilisce che, in queste condizioni, $\overline{f}$ è ancora esatto a sinistra e si vede facilmente che, in quanto estensione di Kan lungo il funtore di Yoneda, $\overline{f}$ possiede un aggiunto a destra $k: \mathscr{F} \longrightarrow \mathscr{S}^{\mathscr{A}}$, e precisamente il funtore che, ad un oggetto X di $\mathscr{F}$, associa $\hom_{\mathscr{F}}[f(-), X]$. k è quindi geometrico. ◆

Se consideriamo quest'ultimo risultato dal punto di vista della semantica funtoriale, possiamo concepire il funtore di Yoneda come l'anello generico, ossia come il generico funtore esatto a sinistra da $\mathscr{A}^{op}$ in un topos.

2.3. L'anello locale generico

Per dimostrare che $(\mathbb{A}, \mathscr{L})$ è l'anello locale generico, richiamiamo la nozione di topologia per un topos:
I seguenti dati per un topos $\mathscr{E}$ sono equivalenti e ognuno di essi si chiama una topologia τ per $\mathscr{E}$:

a) una sotto-categoria geometrica $\mathscr{E}_\tau$ di $\mathscr{E}$ (anche $\mathscr{E}_\tau$ sarà allora un topos);
b) un operatore di chiusura esatto a sinistra e naturale per i prodotti fibrati su tutti i reticoli dei sotto-oggetti (questo approccio è quello adottato in [KW]: ad ogni $X' \rightarrowtail X$ si associa $\overline{X'} \rightarrowtail X$, la chiusura di X' in X);
c) un morfismo $\Omega \xrightarrow{j} \Omega$ tale che $j^2 = j$, ecc. (cfr. [T]);
d) se $\mathscr{E} = \mathscr{S}^{\mathscr{C}^{op}}$, una topologia di Grothendieck su $\mathscr{C}$, o, più in generale - poichè ogni topos è del tipo Fasci $(\mathscr{C}_\gamma)$, dove $\mathscr{C}_\gamma$ è $\mathscr{C}$ munita di una topologia γ di Grothendieck - una topologia γ' di Grothendieck su $\mathscr{C}$ che sia più fine di γ .

L'equivalenza dei dati (a) e (d) che è quella che ci interessa maggiormente nel nostro contesto, riposa sul fatto che, data una sotto-categoria geometrica $\mathscr{E}_\tau \overset{r}{\hookleftarrow} \mathscr{E}$ di un topos $\mathscr{E}$, si ottiene una topologia di Grothendieck γ' su $\mathscr{C}$ ponendo, per ogni famiglia $(f_i : X_i \longrightarrow X)_{i \in I}$ di morfismi in $\mathscr{C}$,

$$(f_i)_{i \in I} \in \mathrm{Cop}_{\gamma'} X \quad \text{sse} \quad \big(r(f_i) : r(X_i) \longrightarrow r(X)\big)_{i \in I} \text{ è unitamente epi,}$$

(identifichiamo f_i con h_{f_i} in virtù dell'immersione di Yoneda $\mathscr{C} \hookrightarrow \mathscr{S}^{\mathscr{C}^{op}}$), e allora $\mathscr{E}_\tau \cong \mathrm{Fasci}\,(\mathscr{C}_{\gamma'})$; il legame con le topologie nel senso di (b) sta nel fatto che $(f_i)_{i \in I}$ è un ricoprimento di X sse $\mathrm{Im}\,(\coprod f_i) \rightarrowtail X$ è denso in X, cioè la sua chiusura coincide con X; ciò si esprime anche dicendo $\coprod f_i$ è quasi epi.

Possiamo ordinare le topologie su $\mathscr{E}$ dicendo che τ è più fine di τ' - ($\tau \leqslant \tau'$) se $\mathscr{E}_\tau \subseteq \mathscr{E}_{\tau'}$. Visto che una topologia di Grothendieck su una categoria $\mathscr{C}$ con $\varprojlim$ finiti si può costruire determinando dapprima una qualunque classe di morfismi di codominio X per ogni oggetto X di $\mathscr{C}$ e completando poi queste classi includendo i morfismi identici e chiudendo rispetto ai prodotti fibrati e alla composizione, si può stabilire abbastanza facilmente il seguente lemma che ci dà quasi immediatamente l'esistenza di un topos classificante per la teoria degli anelli locali:

Lemma: Data una famiglia $(X_i \longrightarrow X)_{i\in I}$ di morfismi in un topos $\mathscr{E}$, esiste una topologia τ univocamente determinata su $\mathscr{E}$ che è la meno fine con la seguente proprietà: il funtore di riflessione

$$\mathscr{E} \xrightarrow{r} \mathscr{E}_\tau$$

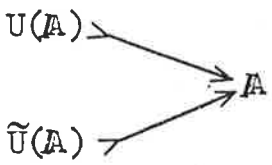
porta $(f_i)_{i\in I}$ in una famiglia unitamente epi; $\mathscr{E}_\tau$ possiede inoltre la seguente proprietà universale: un funtore geometrico $g:\mathscr{F}\longrightarrow\mathscr{E}$ si fattorizza attraverso $\mathscr{E}_\tau$ sse la famiglia $g^*(f_i)_{i\in I}$ è unitamente epi.

Se $(f_i)_{i\in I}$ consiste in particolare di un solo mono: $X' \xrightarrow{m} X$, r(m) sarà sia mono che epi, cioè iso, e Im(m)=m sarà denso; $\mathscr{E}_\tau$ si potrebbe allora chiamare $\mathscr{E}[m^{-1}]$, la "categoria delle frazioni" ma non in $\mathscr{CAT}$, bensì nella categoria dei topos!

Applichiamo ora questo lemma per rendere iso il morfismo

$$m: U(\mathbb{A}) \cup \tilde{U}(\mathbb{A}) \longrightarrow \mathbb{A}$$

ovvero, equivalentemente, per rendere unitamente "quasi epi" la famiglia



Definizione 8. Il topos di Zariski $\mathscr{Z} \hookrightarrow \mathscr{S}^{\mathscr{A}}$ è il topos che risolve il problema universale di invertire il morfismo

. $U(\mathbb{A}) \cup \tilde{U}(\mathbb{A}) \xrightarrow{m} \mathbb{A}$.

Il funtore di riflessione $r: \mathscr{S}^{\mathscr{A}} \longrightarrow \mathscr{Z}$ è esatto a sinistra, nonchè co-continuo (*) e conserva quindi la nozione di anello, U(A), $\tilde{U}$(A) e l'unione di questi due: risulta quindi

$$r\left(U(\mathbb{A}) \cup \tilde{U}(\mathbb{A})\right) = U\left(r(\mathbb{A})\right) \cup \tilde{U}\left(r(\mathbb{A})\right) \cong r(\mathbb{A});$$

ciò significa che r(𝔸) è un anello locale secondo la nostra definizione degli anelli locali in un topos. Ma possiamo stabilire anche subito il

Teorema 3: $r(\mathbb{A}) \in \mathscr{Z}$ è l'anello locale generico.

Dimostrazione: E' sufficiente riformulare la proprietà universale per la topologia che genera $\mathscr{Z}$: dato un funtore geometrico $g: \mathscr{F} \longrightarrow \mathscr{S}^{\mathscr{A}}$, $g^{*}(m)$ è iso, cioè $g^{*}(\mathbb{A})$ è locale, sse g si fattorizza attraverso $\mathscr{Z}$.◆

Risulta dunque Top $(\mathscr{F},\mathscr{Z}) \simeq \mathscr{L}(\mathscr{F})$ per ogni topos $\mathscr{F}$; si tratta però di $\mathscr{L}(\mathscr{F})$ considerata come sottocategoria piena di $\mathscr{A}n(\mathscr{F})$ - questa è la ragione per la quale la nozione di anello locale assieme alla nozione di omomorfismo di anello (non necessariamente locale) ammette un topos classificante.

(*) conserva tutti i colimiti.

Fin qui, sapendo solo dell'esistenza dell'anello locale generico, abbiamo in realtà solo una informazione parziale: vorremmo sapere com'è fatto questo topos. Daremo nel prossimo paragrafo una descrizione precisa del topos di Zariski, e risulterà $r(\mathbb{A}) \cong \mathbb{A} \in \mathscr{X}$ (*). Questo fatto che può sembrare paradossale, che cioè uno stesso oggetto possa fungere come oggetto generico per le due nozioni di anello commutativo e di anello locale, a secondo il topos ambiente, sta a dimostrare che

> la logica dipende dal topos nel quale si trova un oggetto, e non dall'oggetto visto isolatamente.

2.4. Descrizione esplicita del topos di Zariski.

Cercheremo di trovare effettivamente la topologia che genera $\mathscr{X}$ secondo il lemma di 2.3. descrivendo una topologia di Grothendieck su $\mathscr{A}^{op}$ per la quale $\mathscr{X}$ è la categoria dei fasci; dobbiamo cioè ricoprire gli oggetti di $\mathscr{A}^{op}$ "il meno possibile" per ottenere un sotto-topos di $\mathscr{S}^{\mathscr{A}} = \mathscr{S}^{[\mathscr{A}^{op}]^{op}}$ che sia il più grande possibile. Sappiamo già che il funtore distratto $\mathbb{A}: \mathscr{A} \to \mathscr{S}$ è rappresentabile in virtù dell'isomorfismo $\mathbb{A} \xrightarrow[1]{} h^{\mathbb{Z}[X]}$ (cfr. lemma 1). Ma anche $U(\mathbb{A})$ e $\tilde{U}(\mathbb{A})$ sono rappresentabili: si osservi infatti che:

a) il diagramma $U(\mathbb{A}) \rightarrowtail \mathbb{A} \times \mathbb{A} \underset{1}{\overset{\cdot}{\rightrightarrows}} \mathbb{A}$ è esatto in $\mathscr{S}^{\mathscr{A}}$: poichè i $\varprojlim$ nelle categorie di funtori a valori in $\mathscr{S}$ si calcolano

---

(*) Abbiamo qui usata la tecnica cui si accennata nell'introduzione: abbiamo "forzato" $\mathbb{A}$ ad essere un anello locale, prendendo una topologia tale che $r(m)$ sia iso.

"punto per punto", ciò discende dal fatto che, per ogni B in $\mathscr{A}$, il diagramma

$$\begin{array}{ccccc} U(\mathbb{A})(B) & \rightarrowtail & (\mathbb{A}\times\mathbb{A})(B) & \overset{\cdot}{\underset{1}{\rightrightarrows}} & \mathbb{A}(B) \\ \| & & \| & & \| \\ U(B) & & B\times B & & B \end{array}$$

è esatto in $\mathscr{S}$, giacchè, per l'unicità degli inversi, abbiamo: $U(B) = \{ r \mid r \text{ è invertibile} \}$

$$= \{ r \in B \mid \exists\, r' \in B \quad r \cdot r' = 1 \}$$

$$\cong \{ (r,r') \in B^2 \mid r \cdot r' = 1 \}$$

Ciò significa del resto che, nella nostra prima definizione di U(A), potevamo evitare di interpretare il quantificatore esistenziale.

b) L'immersione di Yoneda $\mathscr{A}^{op} \hookrightarrow \mathscr{S}^{\mathscr{A}}$ è esatta a sinistra. Quindi di $\mathbb{A}\times\mathbb{A}$, prodotto di rappresentabili, è rappresentato dal prodotto in $\mathscr{A}^{op}$ - cioè dalla somma in $\mathscr{A}$ - dei rispettivi rappresentanti; ma $\mathbb{Z}[X] \longrightarrow \mathbb{Z}[X,Y] \longleftarrow \mathbb{Z}[X]$ chiaramente è la somma in $\mathscr{A}$, perciò $\mathbb{A}\times\mathbb{A} \cong \hom_{\mathscr{A}}(\mathbb{Z}[X,Y], -)$. Il corrispondente isomorfismo naturale $j: \mathbb{A}\times\mathbb{A} \cong h^{\mathbb{Z}[X,Y]}$ associa ad ogni $B \in \mathscr{A}$ la biezione $j_B: (\mathbb{A}\times\mathbb{A})(B) = B\times B \xrightarrow{\sim} h^{\mathbb{Z}[X,Y]}(B)$.

$$(b,b') \longmapsto \left(\lambda_{b,b'} : \begin{array}{c} X \longmapsto b \\ Y \longmapsto b' \end{array} \right)$$

Anche $\mathbb{A}\times\mathbb{A} \xrightarrow{\cdot} \mathbb{A}$ e $\mathbb{A}\times\mathbb{A} \xrightarrow{1} \mathbb{A}$, morfismi tra rappresentabili, debbono essere rappresentabili, cioè essi debbono provenire ognuno da un morfismo (in $\mathscr{A}^{op}$) tra i rispettivi rappresentanti, e quindi da due morfismi, chiamiamoli f. e f_1; da $\mathbb{Z}[T]$ a $\mathbb{Z}[X,Y]$ in $\mathscr{A}$. Determiniamo $f.: h^{f.}$ è per definizione l'unico morfismo che rende commutativo il seguente diagramma

$$\begin{array}{ccc} \mathbb{A}\times\mathbb{A} & \xrightarrow{\cdot} & \mathbb{A} \\ {\scriptstyle j}\downarrow\wr & & \wr\downarrow{\scriptstyle i} \\ h^{\mathbb{Z}[X,Y]} & \xrightarrow{h^{f.}} & h^{\mathbb{Z}[T]} \end{array}$$

e dal lemma di Yoneda risulta $f_\cdot = h^{f\cdot}(id)$, dove indichiamo per brevità con id il morfismo identico di $\mathbb{Z}[X,Y]$; perchè il diagramma di sopra sia commutativo, dovrà essere $f_\cdot = i(\cdot(j^{-1}(id)))$; ora, $id = \lambda_{X,Y}: (X,Y) \longmapsto (X,Y)$; perciò, $j^{-1}(id)=(X,Y)$, cosicchè $\cdot(j^{-1}(id))=X\cdot Y$, e $f_\cdot = i(X\cdot Y)= \lambda_{X\cdot Y}: T \longmapsto X\cdot Y$. Analogamente si vede $f_1 = \lambda_1 : T \longmapsto 1$.

Se dunque $U(\mathbb{A})$ è l'egualizzatore del diagramma

$$\mathbb{A}\times\mathbb{A} \rightrightarrows \mathbb{A} \text{ in } \mathcal{S}^{\mathcal{A}},$$

$U(\mathbb{A})$ sarà rappresentato dall'egualizzatore del diagramma tra i rappresentanti in $\mathcal{A}^{op}$, e dunque, in $\mathcal{A}$, dal coegualizzatore del diagramma

$$\mathbb{Z}[T] \rightrightarrows \mathbb{Z}[X,Y] \quad (f_\cdot,\ f_1).$$

Questo coegualizzatore è l'anello $\mathbb{Z}[X,X^{-1}] = \mathbb{Z}[X,Y]/I$, I essendo l'ideale generato dal polinomio $X\cdot Y - 1$.
Analogamente si vede che $\tilde{U}(\mathbb{A})$ è rappresentato da $\mathbb{Z}[X,(1-X)^{-1}]$.

Ora, cerchiamo la topologia più scarsa per la quale la famiglia

$$U(\mathbb{A}),\ \tilde{U}(\mathbb{A}) \longrightarrow \mathbb{A}$$

venga portata in una famiglia unitamente epi. Con riguardo all'immersione di Yoneda $\mathcal{A}^{op} \hookrightarrow \mathcal{S}^{\mathcal{A}}$, questa famiglia sta già in $\mathcal{A}^{op}$ e poichè preferiamo lavorare in $\mathcal{A}$, occorre considerare la famiglia

$$\mathbb{Z}[X] \longrightarrow \mathbb{Z}[X,\ X^{-1}],\quad \mathbb{Z}[X,\ (1-X)^{-1}].$$

che dobbiamo dunque trasformare in un "co-ricoprimento" nella struttura di "co-sito" che ci proponiamo di descrivere per $\mathcal{A}$.
In base agli assiomi per un sito, dobbiamo fare soltanto due cose:

1) chiudere i ricoprimenti rispetto ai prodotti fibrati (cioè chiudere i nostri co-ricoprimenti rispetto ai push-out);
2) chiudere i ricoprimenti rispetto alla composizione.

ad 1) Abbiamo già visto che, dato $B \in \mathscr{A}$ e un elemento b di B, esiste uno ed un solo omomorfismo λ_b da $\mathbb{Z}[X]$ a B, che porta X in b. Come minimo, dovremo quindi "co-ricoprire" ogni B in $\mathscr{A}$ con la famiglia dei due push-out che risultano dai diagrammi

$$\begin{array}{ccc} \mathbb{Z}[X] & \xrightarrow{\lambda_b} & B \\ \downarrow & & \vdots \\ \mathbb{Z}[X, X^{-1}] & \dashrightarrow & \end{array} \qquad \begin{array}{ccc} \mathbb{Z}[X] & \xrightarrow{\lambda_b} & B \\ \downarrow & & \vdots \\ \mathbb{Z}[X,(1-X)^{-1}] & \dashrightarrow & \end{array} .$$

Ora, il push-out del primo diagramma deve essere l'anello nel quale b è "forzato" ad essere invertibile, cioè $B[b^{-1}]$, poichè in tale anello deve esistere un elemento c che ha per controimmagini: nell'omomorfismo proveniente da B, l'elemento b e nell'omomorfismo proveniente da $\mathbb{Z}[X,X^{-1}]$, l'elemento X, e c deve essere invertibile, poichè X lo è in $\mathbb{Z}[X,X^{-1}]$. Analogamente si vede che il push-out del secondo diagramma è $B[(1-b)^{-1}]$. La famiglia

$$B \rightrightarrows B[b^{-1}],\ B[(1-b)^{-1}]$$

dovrà quindi co-ricoprire ogni $B \in \mathscr{A}$, per ogni $b \in B$.

ad 2) Se si chiude poi anche rispetto alla composizione, si trova che le famiglie che "co-ricoprono" un oggetto B di $\mathscr{A}$ sono precisamente del tipo:

$$B \rightrightarrows B[b_1^{-1}], \ldots, B[b_n^{-1}]$$

tali che gli elementi $b_1,\ldots.b_n$ generano tutto l'anello B.

Definizione 9. La topologia di Zariski è la seguente topologia di Grothendieck su $\mathscr{A}^{op}$: per ogni $B \in \mathscr{A}^{op}$

$$Cop\ B =: \{(B[b_i^{-1}] \longrightarrow B)_i \mid b_1,\ldots,b_n \text{ generano } B\},$$

In termini di geometria algebrica, si pensi agli anelli B come schemi affini, ai morfismi $B \longrightarrow B[b_i^{-1}]$ come sottoschemi affini aperti; la condizione che i b_i generano l'anello, corrisponde allora al fatto che, come insieme di punti ($\approx$ ideali primi), queste famiglie di applicazioni saranno in Spec B famiglie ricoprenti.

Teorema 4. Il topos di Zariski $\mathscr{Z}$, cioè la più grande sottocategoria geometrica nella quale $U(\mathbb{A}) \cup \tilde{U}(\mathbb{A}) \longrightarrow \mathbb{A}$ viene riflesso come un isomorfismo, è la categoria dei fasci per la topologia di Zariski su $\mathscr{A}^{op}$.

Ora, i funtori rappresentabili in $\mathscr{S}^{\mathscr{A}}$ sono fasci per la topologia di Zariski (una dimostrazione dettagliata di questo teorema si trova in [K 77], § 5.18. Così come la stessa nozione del topos di Zariski, questo teorema risale a Grothendieck). Risulta perciò

Teorema 5. $\mathbb{A} \in \mathscr{Z}$ è l'anello locale generico.

3. La semantica di Kripke-Joyal e la logica coerente

Una condizione necessaria perchè una teoria possegga un topos classificante è evidentemente la seguente:

> la nozione in questione deve essere conservata dai funtori f^* ~~e, quindi deve essere stabile ri-~~ ~~spetto a $\varprojlim$ finiti e colimiti arbitrari.~~

Non sempre possiamo dare definizioni "ad hoc" come abbiamo fatto finora, specie quando si tratta di nozioni più complicate. Per questa ragione è stata elaborata una tecnica precisa per descrivere queste nozioni: essa è basata sul fatto che possiamo interpretare la logica nei topos. Vi sono molti modi per introdurre questa interpretazione: infatti, in logica abbiamo due alternative:

1) tutte le proposizioni parlano di elementi;
2) tutte le proposizioni determinano un sotto-oggetto (l'estensione globale).

Nella teoria dei topos, si insiste per lo più sul secondo punto di vista, perchè nelle categorie non si lavora mai con elementi. Ma penso che è effettivamente più immediato lavorare con elementi, purchè si prenda questa nozione in un senso generalizzato. Vorremo comunque sottolineare che questa semantica, che va sotto il nome di semantica di Kripke-Joyal, risale anch'essa essenzialmente a Grothendieck.

Osserviamo anzitutto che un oggetto A in una categoria $\mathscr{C}$ è un oggetto anello

- sse $h_A: \mathscr{C}^{op} \longrightarrow \mathscr{S}$ si fattorizza attraverso la categoria degli anelli
- sse per ogni X in $\mathscr{C}$, hom(X,A) possiede una struttura di anello che è naturale in X.

Adottiamo quest'ultimo punto di vista, vale a dire:

> ogni volta che abbiamo <u>elementi</u> in A intendiamo ora per un elemento di A un qualunque morfismo da un oggetto arbitrario X a A, e chiameremo un tale $X \longrightarrow A$ un <u>elemento di A "definito sopra X"</u>, o "<u>allo stadio X</u>" - ogni volta che abbiamo questi elementi con dominio arbitrario (ma uguale per tutti), possiamo moltiplicare, addizionare ecc.

In altri termini, possiamo sempre stabilire quando una certa equazione polinomiale $g(x_1,\ldots,x_n)=f(x_1,\ldots x_n)$ è verificata per $(a_i : X \longrightarrow A)_{i=1,\ldots,n}$ (*). Negli enunciati della teoria degli anelli, le equazioni polinomiali rappresentano precisamente le formule atomiche, cosicchè siamo in possesso di una base di induzione per la nostra semantica. Supporremo ora, per fissare le idee, di avere un anello A in un topos $\mathscr{E}$. Scriveremo

$$\vdash_X \Phi(a_1,\ldots a_n)$$

e diremo "Φ vale per $a_1,\ldots,a_n$) allo stadio X" per esprimere la validità semantica di una formula Φ per gli elementi $(X \xrightarrow{a_i} A)_{i=1,\ldots,n}$ di A.

Proseguiamo nella nostra induzione: se per tutti gli $X\in\mathscr{E}$ e per tutti gli $X \xrightarrow{a} A$ sappiamo cosa significa

$$\vdash_X \Phi(a) \quad \text{e} \quad \vdash_X \Psi(a),$$

diremo

$$\vdash_X (\Phi \vee \Psi)(a) \qquad \text{sse}$$

esiste una famiglia $(X_i \xrightarrow{f_i} X)_{i\in I}$ unitamente epi tale che per ogni $i\in I$, $\vdash_{X_i} \Phi(f_i\cdot a)$, oppure $\vdash_{X_i} \Psi(f_i\cdot a)$.

Il punto decisivo di questa semantica è infatti questo: il pas

(*) Si confronti questa tecnica di interpretazione delle equazioni polinomiali con quella data nella sezione 1, ben più pesante.

so di induzione comporta spesso un cambiamento dello "stadio"; (non così per la congiunzione: diremo $\Vdash_X (\Phi \wedge \Psi)(a)$ sse $\Vdash_X \Phi(a)$ e $\Vdash_X \Psi(a)$).

Per illustrare come si interpreta il quantificatore esistenziale, consideriamo, per esempio, una formula in due variabili libere, $\Phi(x,y)$ e supponiamo di aver stabilito per ogni coppia $X \xrightarrow{(a,b)} A^2$, quando sia $\Vdash_X \Phi(a,b)$. Diremo allora

$$\Vdash_X (\exists x\ \Phi)(x,b),$$

sse esistono una famiglia $(X_i \xrightarrow{f_i} X)_{i\in I}$ unitamente epi e degli elementi $(X_i \xrightarrow{a_i} A)_{i\in I}$ tali che

$$\Vdash_{X_i} \Phi(a_i, f_i \cdot b) \text{ per ogni } i\in I.$$

Non occorre quindi necessariamente trovare un elemento allo stadio X; anche qui possiamo cambiare stadio.

Per ulteriori definizioni, ad esempio di $\forall$, nella semantica di Kripke-Joyal, rimandiamo a [K 77].

In realtà, ciò che ci interessa, non è tanto di lavorare in un topos, ma in un sito. Il fatto è che, in un topos, abbiamo sempre una soluzione canonica per i ricoprimenti: è sufficiente prendere le famiglie unitamente epi.

Supponiamo ora che $\Phi(x_1 \ldots x_n)$ sia una formula che si riferisce ad elementi di A.

Definizione 1. L'estensione di Φ (se esiste) è un sotto-oggetto di A^n che si indica con $[\![(x_1,\ldots,x_n)\in A^n \mid \Phi]\!]$ che gode della seguente proprietà universale: una n-pla $X \xrightarrow{(a_1,\ldots,a_n)} A^n$ si fattorizza attraverso esso sse $\Vdash_X \Phi(a_1,\ldots,a_n)$.

Non entriamo nei dettagli della costruzione esplicita delle esten-

sioni; si confronti l'articolo di Osius [O] dove si mostra che la nostra nozione di estensione è equivalente a quella che si dà di solito.

Quindi, se le estensioni esistono, esse sono univocamente determinate, poichè godono di una proprietà universale. La loro importanza è questa: una volta che disponiamo di questi oggetti, possiamo chiederci:

dato un morfismo geometrico $g: \mathscr{E} \longrightarrow \mathscr{F}$ tra due topos, ed un anello A in $\mathscr{F}$, quali sono le formule Ψ tali che

$$g^*([\![(x_1,\ldots,x_n)\in A^n \mid \Psi]\!] = [\![(x_1\ldots x_n)\in g^*(A^n) \mid \Psi]\!] ?$$

Una condizione sufficiente (e in qualche senso anche necessaria) è: Ψ è una <u>formula coerente</u> nel senso della seguente

<u>Definizione 2</u>. Una formula si dice <u>coerente</u> se è costruita a partire dalle formule atomiche (nel nostro caso le equazioni polinomiali) con l'aiuto dei soli simboli $\wedge, \vee, \exists$.

Infatti, dal modo in cui costruiamo le estensioni, risulta che

$$\mathrm{Ext}\ (\Psi_1 \wedge \Psi_2) = \mathrm{Ext}\ (\Psi_1) \wedge \mathrm{Ext}\ (\Psi_2);$$
$$\mathrm{Ext}\ (\Psi_1 \vee \Psi_2) = \mathrm{Ext}\ (\Psi_1) \vee \mathrm{Ext}\ (\Psi_2);$$
$$\mathrm{Ext}\ (\exists x\, \Psi(a,x)) = \exists_x\ (\mathrm{Ext}\ \Psi(a,x)),$$

e g^* conserva tutto ciò.

Per esempio, possiamo ora definire correttamente $V^{1,2}(A) =: [\![(x,y)\in A^2 \mid \exists s,t \quad sx+ty=1]\!]$; e avremo $V^{1,2}(g^*(A)) = g^*(V^{1,2}(A))$.

<u>Definizione 3.</u> Un <u>"sequent" coerente</u> è una formula chiusa del tipo

$$\forall \vec{x}\ (\Phi(\vec{x}) \Longrightarrow \Psi(\vec{x})),$$

dove e sono formule coerenti ($\vec{x}$ stà per $(x_1,\ldots,x_n)$).

Definiamo anche $\uparrow$ (il vero) e $\downarrow$ (il falso) come formule coerenti, con

$$\left.\begin{array}{l} \text{Ext}\,(\downarrow) = \emptyset \\ \text{Ext}\,(\uparrow) = \mathbb{1} \end{array}\right\} \text{ entrambi conservate da } g^*.$$

Vediamo così, per esempio, che $\forall x\ (\neg\Psi(x))$ è un sequent coerente: prendiamo $\neg\Psi$ come abbreviazione per $\Psi \Rightarrow \downarrow$; anche $\forall x\ \Psi(x)$ è un sequent coerente: lo trasformiamo in $\forall x\ (\uparrow \Rightarrow \Psi)$.

L'importanza dei sequent coerenti consiste nel fatto che se un anello A in un topos soddisfa $\forall x \left(\Phi(x) \Rightarrow \Psi(x)\right)$, il che significa semplicemente $[\![\Phi]\!] \leqslant [\![\Psi]\!]$, anche $g^*(A)$ lo soddisfa, cosicchè la validità dei sequent coerenti viene conservata dai funtori g^*. Ma abbiamo anzitutto un teorema fondamentale:

Teorema 1. (Reyes e Joyal): Ogni teoria coerente T, cioè ogni teoria che ammette dei sequent coerenti come assiomi, possiede un topos classificante $\mathscr{E}(T)$ che è un topos coerente, cioè $\mathscr{E}(T)$ è del tipo Fasci ($\mathscr{C}$), dove $\mathscr{C}$ è un sito nel quale tutti i ricoprimenti sono famiglie finite.
Questa nozione di coerenza è già in [SGA 4], Exp.6 .

Il modo in cui $\mathscr{E}(T)$ si costruisce a partire da T è descritto dettagliatamente in [C] e si articola approssimativamente come segue:

1) a T si associa una teoria T_0 i cui assiomi sono validi in T e consistono esclusivamente in sequent coerenti formati a partire da formule espresse in un linguaggio L_0 che possiede, come simboli logici, soltanto $\wedge$ e $\uparrow$ (il vero). Ad esempio, se T è la teoria degli anelli locali, T_0 è la teoria degli a-

nelli. Ora, le teorie del tipo T_0 ammettono tutte un topos classificante del tipo $\mathscr{S}^{\mathscr{C}^{op}}$, (dove $\mathscr{C}$ è una categoria che ammette $\varprojlim$ finiti), cioè una categoria di prefasci, che è certamente un topos coerente. (Se T_0 è una teoria algebrica, cioè monosorte e avente come unica relazione l'uguaglianza, come appunto la teoria degli anelli, $\mathscr{C}$ è l'opposto della categoria delle T_0-algebre finitamente presentabili; lo abbiamo visto nel caso T_0 = teoria degli anelli).

2) Per "forzare" gli assiomi di T ad essere veri in $\mathscr{E}(T)$, si munisce $\mathscr{C}$ di un'opportuna topologia di Grothendieck, di modo che risulti $\mathscr{E}(T)$ = Fasci ($\mathscr{C}$) - e, perchè $\mathscr{E}(T)$ goda della proprietà universale dei topos classificanti si prenderà la topologia la meno fine possibile, come abbiamo fatto nella costruzione del topos di Zariski. A questo scopo si osserva che:

a) per una formula φ di L_0, cioè per una congiunzione finita di formule atomiche (o per la formula $\varphi = \top$), $[\![\varphi]\!]$ è un oggetto rappresentabile di $\mathscr{S}^{\mathscr{C}^{op}}$: $[\![\top]\!]$ è rappresentato da $\mathbb{1}$, e, per esempio, nel caso della teoria degli anelli, dove φ è del tipo $F_1=G_1 \wedge \ldots\ldots \wedge F_r=G_r$, con F_i, G_i espressioni polinomiali, in, poniamo n variabili, $[\![\varphi]\!]$ sarà rappresentato da $\mathbb{Z}[X_1 \ldots\ldots X_n]/I$, dove I è l'ideale generato dai polinomi $F_i - G_i$;

b) ogni sequent coerente è equivalente (nella logica coerente) ad un insieme finito di sequent del tipo

$\forall x_1 \ldots x_n \exists y_1 \ldots y_m (\varphi \Longrightarrow \bigvee_{i=1}^{n} \psi_i)$, con $\varphi, \psi_i \in L_0$; ma

$\top \vdash \varphi \Longrightarrow \bigvee \psi_i$ significa $[\![\varphi]\!] \leq \bigvee [\![\psi_i]\!]$, cioè

$[\![\varphi]\!] \wedge \bigvee [\![\psi_i]\!] = [\![\varphi]\!]$ ovvero

$\bigvee [\![\varphi \wedge \psi_i]\!] = [\![\varphi]\!]$; dunque, se $[\![\psi_i \wedge \varphi]\!]$ è rappresentato da X_i e $[\![\varphi]\!]$ da X, si tratta in definitiva

di fare della famiglia $(X_i \longrightarrow X)_{i \in I}$ di $\mathscr{C}$ un ricoprimento di X.

Descriviamo ora brevemente la dimostrazione del seguente Metateorema di cui si è fatto cenno già nell'introduzione.

Teorema 2. Data una teoria coerente T e un sequent coerente σ, si ha:

$T \vdash \sigma$ in ogni topos

$\Longleftrightarrow$

$T \vdash \sigma$ nel topos degli insiemi $\mathscr{S}$.

"La logica dei topos coincide con quella classica se ci si limita alla logica coerente".

Questo teorema si basa essenzialmente su un teorema di Deligne (cfr. [SGA 4] II, App. all'Exp. 6) il cui significato come metateorema è stato riconosciuto da Lawvere e Reyes. Il teorema di Deligne dice:

Ogni topos coerente possiede "abbastanza punti" nel senso delle seguenti definizioni:

Definizione 4. Un punto di un topos $\mathscr{E}$ è un funtore geometrico

$$p: \mathscr{S} \longrightarrow \mathscr{E} .$$

Definizione 5. Un topos $\mathscr{E}$ ha abbastanza punti, se, per ogni $X \in \mathscr{E}$ e per ogni coppia $X' \rightarrowtail X$, $X'' \rightarrowtail X$ di sotto-oggetti di X,

$X' \leqslant X''$ equivale a:

per ogni punto p di $\mathscr{E}$, $p^*(X') \leqslant p^*(X'')$ in $\mathscr{S}$.

("con i punti possiamo discriminare le relazioni d'ordine tra sotto-oggetti se ci sono abbastanza").

Per dimostrare ora il teorema 2. ($\Longleftarrow$ è banale) , si supponga che σ sia il sequent $\forall \vec{x}\left(\Phi(\vec{x}) \Longrightarrow \Psi(\vec{x})\right)$, con Φ e Ψ formule coerenti; (scriviamo $\vec{x}$ per $x_1,\ldots,x_n$).

$T \vdash \sigma$ in un topos $\mathscr{F}$ significa: per ogni modello M di T in $\mathscr{F}$,

$$[\![\vec{x} \in M^n \mid \Phi]\!] \leqslant [\![\vec{x} \in M^n \mid \Psi]\!] \quad .$$

Consideriamo ora il topos classificante $\mathscr{E}(T)$ di T e il modello generico G di T in $\mathscr{E}(T)$. Un modello di T in $\mathscr{F}$ è del tipo $g^*(G)$ con $g \in \mathrm{Top}(\mathscr{F}, \mathscr{E}(T))$; in particolare, un modello di T in $\mathscr{S}$ è del tipo $p^*(G)$, dove p è un punto di $\mathscr{E}(T)$. Quindi $T \vdash \sigma$ in <u>ogni</u> topos $\mathscr{F}$ equivale a:

(*) $[\![\vec{x} \in G^n \mid \Phi]\!] \leqslant [\![\vec{x} \in G^n \mid \Psi]\!]$

poichè se $M \in \mathscr{F}$ è del tipo $g^*(G)$,

$$[\![\vec{x} \in M^n \mid \Phi]\!] = [\![\vec{x} \in (g^*(G))^n \mid \Phi]\!] = g^*\left([\![\vec{x} \in G^n \mid \Phi]\!]\right)$$

e analogamente per Ψ (g^* conserva le estensioni delle formule coerenti e evidentemente anche le inclusioni). D'altra parte, $T \vdash \sigma$ in $\mathscr{S}$ equivale a:

(**) $p^*\left([\![\vec{x} \in G^n \mid \Phi]\!]\right) \leqslant p^*\left([\![\vec{x} \in G^n \mid \Psi]\!]\right)$ per ogni punto p di $\mathscr{E}(T)$.

(**) $\Longrightarrow$ (*) discende ora immediatamente dal teorema di Deligne.◆

Si noti che il teorema di Deligne significa: ogni teoria coerente possiede abbastanza modelli in $\mathscr{S}$; del resto, non solo ogni teoria coerente possiede un topos classificante che è coerente, ma anche viceversa ogni topos coerente classifica una teoria coerente.

4. Una teoria di Galois intuizionista

Considereremo ora particolarmente quegli aspetti dell'algebra che riguardano le soluzioni di equazioni polinomiali; elaboreremo quindi, in un certo senso, una teoria di Galois. Il nostro preciso problema è: trovare un buon concetto di

campo algebricamente chiuso

nella logica coerente. Vedremo che il modello generico di questa nozione è ancora il nostro funtore $\mathbb{A}$, questa volta come oggetto del topos étale $\mathscr{E}t \hookrightarrow \mathscr{X}$.

Possiamo definire un campo prendendo ad esempio l'assioma (*)

C1: $\forall x \quad x=0 \vee x$ è invertibile,

che è un sequent coerente ma troppo forte: vi sono pochi modelli per questa nozione nei topos, oppure

C2: $\forall x \quad \neg(x=0) \vee x$ è invertibile,

ma questa formula non è un sequent coerente: nell'antecedente compare una negazione, cioè una formula non coerente.

Poichè le nozioni di campo e di chiusura algebrica sono troppo forti, le sostituiremo rispettivamente con quella di anello locale e di chiusura separabile. Per la nozione di chiusura algebrica, consideriamo per ogni $n \geqslant 1$ l'assioma

$$A_n: \forall a_0, \ldots, a_{n-1} \quad \exists x \, (x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0).$$

La famiglia (A_n) esprime la chisura algebrica nel senso che richiede una radice per ogni polinominio con coefficiente direttore 1. Poichè quindi (A_n) non implica l'esistenza di elementi invertibili, possiamo anche considerare, invece dell'assioma di campo C1, l'assioma per gli anelli locali :

(*) Gli assiomi che daremo dovranno intendersi come aggiunti a quelli di anello, i quali, in quanto puramente equazionali, sono evidentemente coerenti.

$\forall x$ x è invertibile $\vee$ 1-x è invertibile.

Ma anche gli assiomi (A_n) sono ancora molto forti; in realtà siamo interessati piuttosto alle chiusure separabili. Ecco la definizione classica:

Definizione 1. Un campo k è separabilmente chiuso se ogni polinomio $P(X) \in k[X]$ che possiede una radice semplice nella chiusura algebrica $\bar{k}$ di k, possiede già una radice semplice in k.

Questa definizione non è né coerente né del 1° ordine - la chiusura algebrica $\bar{k}$ di un campo k non è definibile nella logida del 1° ordine. Ma perchè A_n è troppo forte? Ecco un

Esempio: l'anello G dei germi di funzione $\mathbb{C}^n \longrightarrow \mathbb{C}$ analitiche in un punto P di $\mathbb{C}^n$.

Prendiamo n=1, P=0. Questo anello contiene l'identità $\mathbb{C} \xrightarrow{id} \mathbb{C}$, ma il polinomio X^2-id non ammette una radice: altrimenti, potremo definire una funzione f tale che f^2=id, cioè per ogni x in un opportuno intorno di 0, si avrebbe $(f(x))^2$=x. G non è quindi algebricamente chiuso; ma G risulterà separabilmente chiuso, e ciò non è in contraddizione con il fatto che X^2-id non ammette una radice: la derivata 2X di X^2-id si annulla nel punto 0 per una tale funzione f; X^2-id non possiede pertanto una radice semplice.

Ricordiamo ora un'altra nozione classica dell'algebra commutativa: dato un anello locale B, indichiamo con:

- k = B/m il suo campo dei residui (se m è l'ideale massimale di B);

- $\bar{b} \in k$ l'immagine di un elemento b di B nell'omomorfismo canonico $B \longrightarrow\!\!\!\!\!\rightarrow k$;
- $\bar{P} \in k[X]$ l'immagine di un polinomio $P \in B[X]$ nell'omomorfismo $B[X] \longrightarrow\!\!\!\!\!\rightarrow k[X]$;
- $\bar{k}$ la chiusura algebrica di k.

Definizione 2. Un anello locale B è henseliano se per ogni polinomio $P = X^n + a_{n-1}X^{n-1} + \ldots + a_o \in B[X]$, ogni radice semplice di $\bar{P}$ in k proviene da una radice di P in B, cioè per ogni $x \in k$ che è radice semplice di $\bar{P}$ esiste $b \in B$ tale che $P(b)=0$ e $x=\bar{b}$.

Definizione 3. Un anello locale si dice strettamente henseliano se è henseliano e se il suo campo dei residui è separabilmente chiuso.

Per trasformare la teoria degli anelli locali strettamente henseliani in una teoria coerente, ci serviremo di certi polinomi, i cosidetti "iperdiscriminanti" che sono stati studiati almeno 300 anni fa, e che furono riscoperti da A.Joyal e G.Wraith in questo contesto.
Sia $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_o$ un polinomio su un campo k; sia $\bar{k}$ la chiusura algebrica di k; quindi, esistono $x_1, \ldots, x_n$ in $\bar{k}$ tali che

$$P(X) = \prod_{j=1}^{n}(X-x_j);$$

differenziamo P:

$$P'(X) = \sum_{i=1}^{n}\Big(\prod_{j\neq i}(X-x_j)\Big)$$ secondo la regola di Leibniz, e sostituiamo a X uno degli x_i:

$$P'(x_i) = \prod_{j\neq i}(x_i-x_j);$$

x_i è una radice semplice di P sse $P'(x_i)$ è invertibile (è questa la versione positiva di $P'(x_i) \neq 0$).

Studiamo ora l'enunciato

σ : esiste almeno una radice semplice di P in $\bar{k}$.

Vogliamo trasformare σ in un enunciato coerente nel quale non si parli più di $\bar{k}$. Intanto, per quanto sopra, abbiamo

(1) $\quad \sigma \Longleftrightarrow \left(P'(x_1),\ldots\ldots,P'(x_n)\right) \neq \underline{0} \in k^n.$

Ricordiamo ora che i polinomi simmetrici elementari (ved. [W] § 33)

$$C_1 = X_1+X_2+\ldots+X_n$$
$$C_2 = X_1X_2+X_1X_3+\ldots+X_2X_3+\ldots+X_{n-1}X_n$$
$$\vdots$$
$$C_n = X_1X_2\ldots X_n$$

che verificano $(Z-X_1)\cdot(Z-X_2)\cdot\ldots\cdot(Z-X_n)=Z^n-C_1Z^{n-1}+\ldots+(-1)^nC_n$, hanno la seguente proprietà:

l'applicazione da k^n in k^n che porta

$$(y_1,\ldots y_n) \text{ in } \left(C_1(y_1,\ldots,y_n),\ldots,C_n(y_1,\ldots,y_n)\right),$$

conserva e riflette $\underline{0} \in k^n$. Abbiamo dunque:

(2) $\quad \sigma \Longleftrightarrow \Big(C_1\left(P'(x_1),P'(x_2),\ldots P'(x_n)\right),\ldots\ldots,$
$$C_n\left(P'(x_1),\ldots,P'(x_n)\right)\Big) \neq \underline{0}.$$

Ora, ogni $C_j(P'(x_1),\ldots,P'(x_n))$ è una funzione <u>simmetrica</u> in $x_1,\ldots,x_n$ poichè, permutando gli x_i, si permutano i $P'(x_i)$, mentre i C_j non cambiano; perciò possiamo applicare il <u>teorema di Newton</u> per i polinomi simmetrici: ogni polinomio simmetrico in $X_1,\ldots,X_n$ si può scrivere in un unico modo come polinomio in $C_1,\ldots C_n$; quindi, per ogni $j=1,\ldots,n$, esiste uno ed <u>un solo polinomio</u> $D_j(Y_1,\ldots,Y_n)$ tale che

$$C_i(P'(x_1),\ldots,P'(x_n)) =$$
$$= D_j\left(C_1(x_1,\ldots,x_n),\ldots,C_n(x_1,\ldots,x_n)\right)$$
$$= D_j(-a_{n-1}, a_{n-2},-\ldots,(-1)^n a_o) = :D_j(P).$$

Disponiamo ora di una condizione che non si riferisce più a $\bar{k}$, ma solo ai coefficienti del polinomio iniziale.
Chiamiamo i polinomi $D_j(P)$ gli iper discriminanti di P; per ogni n, esistono n polinomi di questo tipo che si possono associare in modo canonico alla n-pla dei coefficienti di un polinomio di grado n. Per esempio, per n=2, $P(X)=X^2+a_1X+a_o$, si trova $D_1(a_1,a_o)=0$; $D_2(a_1,a_o)=a_1^2-4a_o$: D_2 è dunque il discriminante abituale; (in generale, $D_n^{(n)}$ è il discriminante abituale, se indichiamo con $D_j^{(n)}$ il j-esimo iperdiscriminante di un polinomio di grado n).
Abbiamo dunque:

(3) $\sigma \iff (D_1(P),\ldots,D_n(P)) \neq \underline{0}$

$\iff$ almeno uno degli $D_j(P)$ è invertibile

$\iff$ la n-pla $(D_1(P),\ldots,D_n(P))$ genera tutto k.

Ora, dato un polinomio P di grado n, possiamo identificarlo con la n-pla dei suoi coefficienti $a_o,\ldots,a_{n-1}$; se dunque, dato un anello B in un topos, indichiamo con

$$\sigma_n(P) = \sigma_n(a_o,\ldots,a_{n-1})$$

la formula corrispondente all'enunciato: "gli n iperdiscriminanti di P generano tutto B", σ_n è certamente una formula coerente. Definiamo ora:

Definizione 4. Un anello B in un topos si dice separabilmente chiuso se per ogni n, B verifica il sequent coerente

$$\vdash \forall P \left(\sigma_n(P) \Longrightarrow \exists b\ P(b)=0 \right).$$

In questo contesto ci interessano tre teoremi dovuti risp. a

- Wraith: un anello locale separabilmente chiuso in $\mathcal{S}$ è un anello locale strettamente henseliano.

- Hakim : Esiste un topos $\mathscr{E}t \hookrightarrow \mathscr{X}$ (il "topos étale") tale che la categoria Top ($\mathscr{S}$, $\mathscr{E}t$) è equivalente alla categoria degli anelli locali strettamente henseliani (in $\mathscr{S}$);
- Makkai-Reyes : se per una teoria coerente T esiste un topos $\mathscr{E}$ tale che Top ($\mathscr{S}$, $\mathscr{E}$) è equivalente alla categoria dei modelli di T in $\mathscr{S}$, allora $\mathscr{E}$ è il topos classificante di T. (+ further assumptions)

Sulla base di questi teoremi possiamo perciò affermare:
il topos $\mathscr{E}t$ classifica la nozione di anello locale separabilmente chiuso (sempre con $\mathbb{A}$ come modello generico).

Di questi teoremi dimostreremo in seguito solo il primo (teorema 1). Intanto, l'analisi degli iperdiscriminanti permette di dedurre molto facilmente il seguente .

Lemma : Se B è un anello in $\mathscr{S}$, allora $\sigma_n(P)$ vale per un polinomio di grado n sse per qualche campo algebricamente chiuso k' che sia una B-algebra (cioè esiste un omomorfismo di anelli $B \longrightarrow k'$), P possiede una radice semplice in k'.

(Avevamo considerato soltanto $B = k \hookrightarrow \bar{k}$).
Il teorema di Wraith è precisamente questo:

Teorema 1. Per un anello locale B in $\mathscr{S}$, le condizioni seguenti sono equivalenti:
1) B è strettamente henseliano;
2) B verifica per ogni n, $\forall P\left(\sigma_n(P) \longrightarrow \exists b\ P(b)=0\right)$,
cioè B è un anello locale separabilmente chiuso in $\mathscr{S}$;

3) B verifica per ogni n:

$\forall P\ (\sigma_n(P) \Longrightarrow \exists b\ P(b) = 0 \wedge P'(b)$ è invertibile).

Premettiamo due osservazioni su σ_n

- poichè σ_n è coerente, σ_n è conservato dagli omomorfismi di anello, cioè, se $f: B \longrightarrow C$ è un omomorfismo di anello (che si estende a $B[X] \longrightarrow C[X]$), e $P \in B[X]$ verifica σ_n, allora anche $f(P)$ verifica σ_n;
- se B e C sono anelli <u>locali</u> e f è un omomorfismo <u>locale</u>, cioè se f riflette l'invertibilità, allora abbiamo anche che

$$\sigma_n(f(P)) \text{ implica } \sigma_n(P);$$

procediamo ora alla

<u>Dimostrazione</u> del Teorema 1. (usiamo le notazioni adottate nella Definizione 2.)

1) $\Longrightarrow$ 3): sia $P=X^n+\ldots+a_o$ e supponiamo $\sigma_n(P)$; vale allora $\sigma_n(\overline{P})$ e quindi, per la nostra precedente analisi dell'enunciato σ, $\overline{P}$ possiede una radice semplice in k; ma k è separabilmente chiuso per ipotesi: $\overline{P}$ ha quindi una radice semplice x in k. Poichè B è henseliano, x proveiene da una radice b di P in B; P'(b) è certamente invertibile in B: x è radice semplice di $\overline{P} \Longleftrightarrow \overline{P'(b)} = \overline{P}'(x) \neq 0$ in k; $\overline{P'(b)}$ è perciò invertibile in k; ma $B \longrightarrow k$ riflette l'invertibilità.

3) $\Longrightarrow$ 2): è evidente.

2) $\Longrightarrow$ 1): bisogna dimostrare che, dati $P \in B[X]$ di grado n, $x \in k$ radice semplice di $\overline{P}$, (cioè $\sigma_n(\overline{P})$ e $\overline{P}'(x) \neq 0$), esiste $b \in B$ tale che $x=\overline{b}$ e P'(b) invertibile in B. Poichè $B \longrightarrow k$ è locale, sappiamo che P verifi-

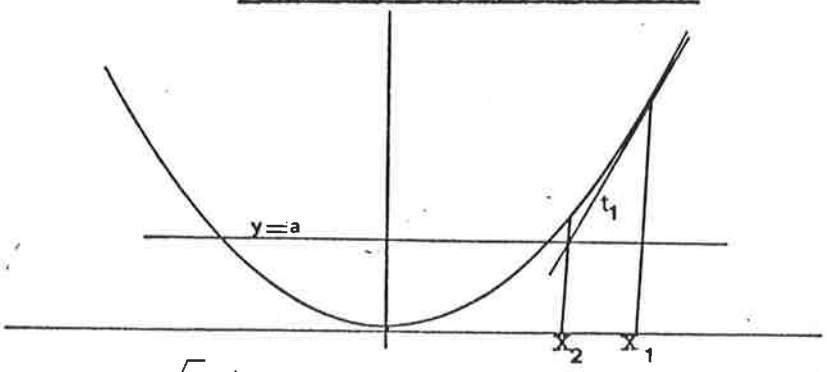
ca σ_n, e che, trovato $b \in B$ con $P(b)=0$, se b verifica $x=\bar{b}$, anche $P'(b)$ sarà invertibile, poichè $\bar{P}'(x)$ lo è. Ma $\sigma_n(P)$ implica, per 2), che esiste $b \in B$ tale che $P(b)=0$; se $\bar{b}=x$, abbiamo finito. Altrimenti sarà $P = (X-b)\cdot Q$, e essendo $\bar{b} \neq x$, x sarà radice semplice di $\bar{Q}$; abbiamo quindi $\sigma_{n-1}(\bar{Q})$ e pertanto $\sigma_{n-1}(Q)$; in questo modo, possiamo procedere per induzione: per i polinomi di grado 1, il tutto è evidente. Il fatto che k è separabilmente chiuso risulta sempre dal fatto che ogni $P \in k[X]$ è del tipo $\bar{Q}$ per qualche $Q \in B[X]$: P possiede una radice semplice in $\bar{k}$ equivale a $\sigma_n(P)$ e ciò equivale a sua volta a $\sigma_n(Q)$ ($B \longrightarrow k$ è locale) e, per ipotesi, $\sigma_n(Q)$ implica che esiste $b \in B$ con $Q(b)=0$.◆

Esempio di un anello locale separabilmente chiuso in un topos: riprendendo l'esempio citato all'inizio di questo paragrafo, consideriamo il fascio dei germi di funzioni analitiche da $\mathbb{C}^n$ in $\mathbb{C}$ nel topos dei fasci su $\mathbb{C}^n$. Questo fascio è un anello in Fasci ($\mathbb{C}^n$), e le sue fibre sono anelli locali strettamente henseliani (per dimostrarlo si usa il teorema delle funzioni implicite); poichè la nozione di anello locale separabilmente chiuso è coerente, ciò implica che il fascio stesso è un anello locale separabilmente chiuso in Fasci ($\mathbb{C}^n$).

Vorremmo ora formulare una congettura che, approssimativamente, significa che i numeri complessi costruttivi soddisfano la nostra teoria coerente degli anelli locali separabilmente chiusi; questa congettura non è - e non può essere - preci

sa: la nostra idea è che ciò è la migliore cosa che si possa fare dal punto di vista costruttivista, per il quale il campo dei residui di un anello locale non esiste.

Consideriamo per esempio un polinomio $P \equiv X^2 - a$; abbiamo visto che $D_1(P) = 0$, $D_2(P) = -4a$; in un campo separabilmente chiuso, P possiede una radice se a è invertibile - in un campo algebricamente chiuso invece, basta che a sia diverso da 0, e, intuizionisticamente, ciò non è affatto la stessa cosa. Bishop, con le sue successioni (arbitrarie) di scelta, trova che $\mathbb{C}$ è alg. chiuso, ma consideriamo un algoritmo senza scelte arbitrarie, come la regulae falsi di Newton:



per trovare $\sqrt{a}$ (a strettamente maggiore di 0 per esempio), si parte da un qualunque x_1 con $x_1^2 > a$ e si considera la tangente t_1 in x_1 alla parabola; dalla intersezione di t_1 con la retta $y = a$ si ottiene un valore x_2 che si avvicina già meglio a $\sqrt{a}$; iterando il processo con x_2, si trova x_3, ecc., e in questo modo, $\sqrt{a}$ si può approssimare a piacere. Tuttavia, questo metodo dà buoni valori solo quando non si è troppo vicini a 0, poiché allora la tangente viene ad essere parallela alla retta $y = a$; i calcoli diventano allora inesatti. Ciò significa: dobbiamo sapere che a è effettivamente invertibile - $a>0$ non è sufficiente.

Un altro argomento che potrà illustrare l'adeguatezza del concetto di anello locale separabilmente chiuso è basato sulla seguente costruzione che collega peraltro le due

partidel nostro seminario: la parte dedicata all'algebra commutativa è quella in cui parleremo di geometria differenziale. Vedremo che la nostra "teoria di Galois" è stabile rispetto a questa costruzione, mentre la teoria classica, che opera con campi algebricamente chiusi, non lo è.

Definizione 5. Dato un anello commutativo B in una categoria $\mathscr{C}$ con prodotti finiti, si definisce su BxB una struttura di anello che si indica con

$B[\varepsilon]$ =: anello dei numeri duali su B,

ponendo,

$$(b_1,b_2)\cdot(c_1,c_2) =: (b_1c_1,\ b_1c_2 + b_2c_1)$$

(l'addizione si definisce "componente per componente").

Con $(0,1) =: \varepsilon \in BxB$, risulta $\varepsilon^2 = 0$, mentre (1,0) è l'unità di $B[\varepsilon]$; identificando $b \in B$ con $(b,0) \in B[\varepsilon]$, ogni elemento (b_1,b_2) di $B[\varepsilon]$ si può scrivere come $b_1 + b_2\cdot\varepsilon$.

Possiamo anche definire $B[\varepsilon]$ come $B[X] / (X^2)$, cioè come il co-egualizzatore dei morfismi

$$B[X] \underset{X \longmapsto 0}{\overset{X \longmapsto X^2}{\rightrightarrows}} B[X],$$

ma per formare $B[\varepsilon]$ in una qualunque categoria con prodotti finiti, la costruzione sopra indicata è più adatta.

Si noti che $\mathbb{C}[\varepsilon]$ non è un campo né algebricamente chiuso; abbiamo invece il seguente

Teorema 2. Se B è un anello locale separabilmente chiuso in un topos $\mathscr{E}$, allora anche $B[\varepsilon]$ lo è.

Dimostrazione. La conclusione di questo teorema è, come si vede facilmente, un sequent coerente su coppie di "elementi"

di B - per il nostro metateorema, possiamo quindi limitarci a dimostrare la cosa in $\mathscr{S}$, il che è molto opportuno, poichè la manipolazione degli iperdiscriminanti in un topos è molto scomoda; basterà quindi dimostrare in $\mathscr{S}$:
se B è henseliano, allora $B[\varepsilon]$ lo è (il campo dei residui di $B[\varepsilon]$ coincide con quello di B).
Abbiamo i seguenti omomorfismi:

$$\begin{array}{ccccc} B[\varepsilon] & \longrightarrow\!\!\!\!\rightarrow & B & \longrightarrow\!\!\!\!\rightarrow & B/m = k \\ (b,b') & \longmapsto & b & \longmapsto & \bar{b} \end{array}$$

che inducono degli omomorfismi corrispondenti negli anelli polinomiali. Consideriamo un polinomio $P \in B[\varepsilon][X]$, cioè

$$\begin{aligned} P &= X^n + (a_{n-1} + \varepsilon \cdot b_{n-1})X^{n-1} + \ldots\ldots \\ &= X^n + a_{n-1}X^{n-1} + \ldots\ldots \\ &\quad + \varepsilon \cdot (b_{n-1}X^{n-1} + \ldots\ldots) \\ &=: Q + \varepsilon \cdot R, \end{aligned}$$

dove Q e R in $B[X]$, sono due polinomi, con R di grado n-1.
L'immagine di P in $k[X]$ è $\bar{Q}$, e per ipotesi esiste dunque x in k che è radice semplice di $\bar{Q}$; essendo B henseliano, x proviene da una radice semplice $b \in B$ di Q. Il problema si riduce quindi a trovare $c \in B$ tale che $(b,c) = b + c\cdot\varepsilon$ sia radice di P,
ma $P(b+\varepsilon c) = Q(b+\varepsilon c) + \varepsilon \cdot R(b+\varepsilon c) =$

$$= Q(b) + \varepsilon \cdot c \cdot Q'(b) + \varepsilon \cdot (R(b) + \varepsilon \cdot c \cdot R'(b))$$

(sviluppo in serie di Taylor, tenendo conto di $\varepsilon^2 = 0$).
Ora, $Q(b) = 0$ per ipotesi; d'altra parte $\varepsilon \cdot \varepsilon \cdot c \cdot R'(b) = 0$ poichè $\varepsilon^2 = 0$; si tratta quindi di risolvere

$$c \cdot Q'(b) + R(b) = 0 \text{ per } c,$$

ma, poichè $Q'(b)$ è invertibile ($b = x$ è una radice semplice di Q), basta prendere

$$c = -R(b) \cdot (Q'(b))^{-1}.$$

PARTE SECONDA: La geometria differenziale in un topos

1. Introduzione

Secondo una vecchia idea di Lawvere [L 67], si dovrebbe cercare di dare una forma più geometrica alla geometria e al calcolo differenziale, nel senso che tutti gli oggetti "lisci" (smooth) della geometria dovrebbero formare una categoria $\mathcal{G}$, e in $\mathcal{G}$ dovremmo avere per lo meno un oggetto terminale 1 ($\approx$ un punto), una retta A (il nostro anello A sarà un modello di questa geometria sia in $\mathcal{G}^A$ che in $\mathcal{X}$ e in $\mathcal{E}t$); la retta dovrebbe avere un'origine O, dovremmo avere cioè un morfismo

$$1 \xrightarrow{\ o\ } A$$

in $\mathcal{G}$; infine dovrebbe esistere un intorno molto piccolo di O che chiameremo D, il "germe della retta" che rappresenta gli infinitesimali.

Dato poi un oggetto V ($\approx$ una varietà) in $\mathcal{G}$, dovrebbe esistere l'oggetto V^D (l'oggetto dei vettori tangenti a V), cosicchè abbiamo il morfismo

$$V^D \xrightarrow{\ V^o\ } V^1 =: V^D \xrightarrow{\ p\ } V$$

("valutazione nel punto 0" : $t \in V^D \longmapsto t(0)$, il punto nel quale t è applicato). Vorremmo che V^D funga in quel modo da fibrato tangente di V. Ciò è ragionevole geometricamente, perchè un vettore tangente su una varietà V non è tutt'una retta, bensì un piccolo segmento di essa: l'idea è quindi di concepire D come

"il generico vettore tangente",

e un campo di vettori su V dovrebbe essere, sempre in questo ambito di idee che mirano a dare una formulazione più geometrica

di cose note, una sezione s del morfismo p di sopra; dovremmo avere cioè

$$V \xrightarrow{s} V^D \xrightarrow{p} V = V \xrightarrow{id} V.$$

Sfruttando l'aggiunzione esponenziale, s dà luogo a

$$V \times D \xrightarrow{\hat{s}} V \text{ (un'azione di D su V)},$$

o ancora, sempre per aggiunzione esponenziale, al morfismo

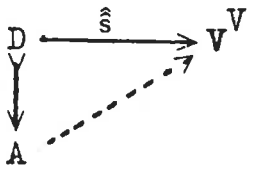
$$D \xrightarrow{\hat{\hat{s}}} V^V.$$

In altri termini, assimilando V^V all'oggetto delle trasformazioni da V in se stessa, $\hat{s}$ è una famiglia di trasformazioni $V \longrightarrow V$ parametrizzata da un segmento infinitesimale della retta. Il fatto che s è una sezione di p, cioè $s \circ p = id_V$, si traduce ora in:

$$1 \xrightarrow{'0'} D \xrightarrow{\hat{s}} V^V$$

proviene per aggiunzione esponenziale da $V \times 1 \xrightarrow{id} V$.

Se concepiamo un'equazione differenziale come un campo di vettori, integrare l'equazione significa in questa terminologia: estendere un flusso infinitesimale ad un flusso finito, ovvero, estendere l'azione infinitesimale ad un'azione di tutta la retta su V^V, ad una "dinamica su V", o ancora, in termini di diagrammi, completare il diagramma



Ciò che, assieme a Reyes e Wraith, ho cercato di fare è: trovare dei modelli dove queste cose avvengono, e descrivere assiomaticamente cosa occorre esattamente. A me premeva in particolare di introdurre delle coordinate in questa situazione, in modo da poter effettuare i calcoli elementari.

2. Anelli di tipo retta.

2.1. Un assioma che permette il calcolo differenziale in un topos.

Prendiamo dunque una categoria $\mathcal{G}$ con $\varprojlim$ finiti, e un anello A in $\mathcal{G}$ che assumerà il ruolo della retta. Definiamo poi un sotto-oggetto D di A, l'oggetto degli "infinitesimali" di A, nel modo seguente:

$$D =: [\![x \in A \mid x^2 = 0]\!]$$

che contiene perciò 0_A (più precisamente, $1 \xrightarrow{\ulcorner 0 \urcorner} A$ si fattorizza attraverso $D \rightarrowtail A$).

Assumiamo anche che in $\mathcal{G}$ esiste l'oggetto A^D, e consideriamo il morfismo

$$A \times A \xrightarrow{\alpha} A^D$$

così definito:

$$(a_0, a_1) \longmapsto [d \longmapsto a_0 + a_1 \cdot d].$$

La maggior parte delle nostre costruzioni sarà basata sul seguente

Assioma 1 : α è invertibile.

Definizione 1 Un anello A in $\mathcal{G}$ si dice di tipo retta ("ring of line-type") se verifica l'assioma 1.

Vedremo che l'anello generico $\mathbb{A} \in \mathcal{SA}$ e anche $\mathbb{A} \in \mathcal{L}$, l'anello locale generico, soddisfano il nostro assioma.

L'assioma 1 afferma sostanzialmente:

ogni applicazione $D \longrightarrow A$ è completamente determinata da un polinomio di grado 1.

Sviluppiamo intanto alcuni corollari puramente euristici del nostro assioma, in modo da motivare l'impostazione formale che poi daremo. Il fatto che α è mono significa: per ogni $t : D \longrightarrow A$, esiste al più una coppia $(a_0, a_1) \in A^2$ tale che sia

$$t(d) = a_0 + a_1 d \text{ per ogni } d \in D;$$

pertanto, se per ogni $d \in D$

$$a_0 + a_1 \cdot d = b_0 + b_1 \cdot d,$$

allora, $- a_0 = b_0$; e ciò vale anche senza ipotesi su α : basta porre $d = 0$;

$- a_1 = b_1$; e ciò è importante poichè implica :

se per ogni $d \in D$ $a \cdot d = b \cdot d$, allora $a = b$.

In altri termini, abbiamo risolto la contraddizione classica che consiste nella divisione per elementi infinitesimali (un elemento d di D è talmente piccolo che $d^2 = 0$; esso è pertanto addirittura un divisore dello zero). Si noti comunque che non possiamo dividere per un singolo d, bensì, per così dire, soltanto per un "d preceduto da un quantificatore universale".

Come imposteremo ora la differenziazione? Si tratta, dato $A \xrightarrow{f} A$, di trovare $A \xrightarrow{f'} A$, e vogliamo che sia, per ogni $a \in A$, $d \in D$

$$\frac{f(a + d) - f(a)}{d} = f'(a);$$

questo quoziente non è generalmente definito ma possiamo trasformare l'equazione in

$$f(a) + d \cdot f'(a) = f(a+d).$$

Sempre in termini puramente euristici, possiamo considerare la

funzione

$$\Delta f_a : d \longmapsto f(a+d)$$

da D in A : f'(a) dovrebbe essere il coefficiente della parte lineare del polinomio che corrisponde a Δf_a in virtù di α; e per trovare questo coefficiente, basterà applicare prima α^{-1}, poi la seconda proiezione a Δf_a, cioè

$$f'(a) = \pi_2(\alpha^{-1}(\Delta f_a)).$$

Di tutto ciò, possiamo ora dare una formulazione rigorosa:
dato $A \xrightarrow{f} A$, consideriamo

$$A \xrightarrow{\hat{+}} A^D \xrightarrow{f^D} A^D =: \Delta f$$

$$a \longmapsto (d \longmapsto a+d) \longmapsto (d \longmapsto f(a+d)) = \Delta f_a$$

($\hat{+}$ è l'aggiunto esponenziale del morfismo $AxD \xrightarrow{+} A$, che si ottiene restringendo a AxD l'addizione in A), e diamo la seguente

Definizione 2 $\quad f' =: A \xrightarrow{\Delta f} A^D \xrightarrow{\alpha^{-1}} AxA \xrightarrow{\pi_2} A.$

Possiamo ora dimostrare rigorosamente ciò che costituiva il nostro punto di partenza euristico:

Teorema 1 ("Taylor") : Per ogni $f : A \longrightarrow A$

$$\vdash_1 \forall (a,d) \qquad f(a+d) = f(a) + d \cdot f'(a).$$

Abbiamo quindi uno sviluppo in "serie" di Taylor per ogni $f: A \longrightarrow A$ ($d^2 = 0$!).

Dimostrazione: il teorema afferma che i due morfismi da AxD in A così descritti:

$$(a,d) \longmapsto f(a+d)$$

$$(a,d) \longmapsto f(a)+d \cdot f'(a)$$

coincidono, ovvero per aggiunzione esponenziale, che Δf coincide con il morfismo λ così definito

$$a \longmapsto (d \longmapsto f(a) + d\cdot f'(a));$$

in altri termini

$$\lambda = \langle f, f' \rangle \cdot \alpha \quad .$$

Essendo α un isomorfismo, $\Delta f = \lambda$ equivale a

$$\Delta f \cdot \alpha^{-1} = \langle f, f' \rangle \quad ,$$

ovvero $\Delta f \cdot \alpha^{-1}\pi_1 = f$, $\Delta f \cdot \alpha^{-1} \cdot \pi_2 = f'$;
la seconda uguaglianza vale per definizione di f'; rimane pertanto da verificare la prima; a questo scopo consideriamo Δf_a per un dato $a \in A$, e supponiamo che a Δf_a corrisponde, in virtù di α^{-1} la coppia (a_0, a_1): si tratta di dimostrare $a_0 = f(a)$. Per definizione di α , per ogni $d \in D$ è $\Delta f_a(d) = a_0 + a_1 d$, e quindi in particolare $\Delta f_a(0) = a_0$; ma $\Delta f_a(0) = f(a+0) = f(a)$. ◆

Prima di verificare che abbiamo ancora le solite regole per la differenziazione, enunciamo un lemma (che non dipende dalla invertibilità di α :

Lemma 1 : $A \times A \longrightarrow A^D$

$$(a_0, a_1) \longmapsto (d \longmapsto a_0 + a_1 \cdot d)$$

è un omomorfismo di anelli rispetto alla struttura $A[\varepsilon]$. (A^D è canonicamente munito di una struttura di anello : $(-)^D$ commuta con i $\varprojlim$ e porta quindi anelli in anelli).

La dimostrazione del lemma consiste essenzialmente in un uso sistematico delle aggiunzioni esponenziali, e la lasciamo come esercizio. Questo lemma ci fa vedere come il fatto di aver posto $D = \{ x \mid x^2 = 0 \}$ crea un legame tra questo calcolo infinitesimale e i numeri duali: se è iso, $(-)^D$ trasforma A nell'anello dei numeri duali di A, e ciò significa sostanzialmente che

> ogni funzione è lineare in un intorno sufficientemente piccolo (*).

(*) M. Galuzzi mi ha fatto notare che per l'anello generico, abbiamo: $\mathbb{A}^{\mathbb{A}} \cong \mathbb{A}[X]$, e ciò è un'estensione della nostra proposizione $A[\varepsilon] \cong A^D$ tramite α .

Disponendo delle nostre "serie" di Taylor, possiamo ora dimostrare varie regole del calcolo differenziale, e precisamente:

Teorema 2. Dati due morfismi f e g da A in A,

(1) $(f\cdot g)' = f'\cdot g + g'\cdot f$;

(2) $(g\circ f)' = (g\circ f')\cdot g'$;

(3) $(id)' = 1_A$.

Dimostrazione

ad (1): abbiamo $\forall(a,d)$

$(f\cdot g)(a+d) = (f\cdot g)(a)+d\cdot(f\cdot g)'(a)$ ("Taylor");

d'altra parte,

$$\begin{aligned}(f\cdot g)(a+d) &= f(a+d)\cdot g(a+d)\\ &= (f(a)+d\cdot f'(a))\cdot(g(a)+d\cdot g'(a))\\ &= f(a)\cdot g(a)+d\cdot[f'(a)\cdot g(a)+g'(a)\cdot f(a)] + d^2\cdot\ldots\\ &= (f\cdot g)(a)+ d\cdot[(f'g+g'\cdot f)(a)].\end{aligned}$$

Quindi, paragonando questi due sviluppi, viene:

$\forall(a,d)\quad d\cdot(f\cdot g)'(a) = d\cdot(f'\cdot g+g'\cdot f)(a)$

e, cancellando d (visto che la formula è preceduta da $\forall d$), rimane

$\forall a$: $(f\cdot g)'(a) = (f'\cdot g+g'\cdot f)(a)$, cioè

$(f\cdot g)' = f'\cdot g + g'\cdot f$.

ad (2): abbiamo

$$\begin{aligned}\forall(a,d)\ (g\circ f)\ (a+d) &=: f(g(a+d))\\ &= f(g(a)+d\cdot g'(a)) \quad \text{(Taylor per g)};\end{aligned}$$

poichè $d\cdot g'(a) \in D$ se $d \in D$, sviluppando f secondo Taylor,

il membro destro diventa

$$= f(g(a)) + d\cdot g'(a)\cdot f'(g(a));$$

d'altra parte,

$$(g\circ f)(a+d) = (g\circ f)(a)+d\cdot(g\circ f)'(a) \quad \text{(Taylor per } g\circ f\text{)}$$
$$= f(g(a)) + d\cdot(g\circ f)'(a);$$

sottraendo nei due casi $f(g(a))$ e cancellando d, rimane:

$$\forall a : (g\circ f)'(a) = g'(a)\cdot f'(g(a))$$
$$= [g'\cdot(g\circ f')](a),$$

cioè: $(g\circ f) = g'\cdot(g\circ f')$.

ad (3): id' è, per definizione,

$$A \xrightarrow{\hat{f}} A^D \xrightarrow{id^D} A^D \xrightarrow{\alpha^{-1}} AxA \xrightarrow{\pi_2} A$$
$$a \longmapsto (d \longmapsto a+d) \longmapsto (a,1) \longmapsto 1;$$

ciò risulta dal fatto che $\alpha:(a,1)\longmapsto(d\longmapsto a+1\cdot d=a+d)$. ◆

La differenziazione parziale.

Dato $A^n \xrightarrow{f} A$, $\frac{\partial f}{\partial x_1}$ può venir definito con tecniche analoghe a quelle cui sopra. Ma, quando siamo in un topos $\mathcal{E}$, possiamo ricondurci direttamente alla differenziazione semplice lavorando in $\mathcal{E}/A^{n-1}$, quella che Lawvere chiama la categoria degli oggetti "smoothly parametrized" dalle n-1 variabili, le quali non entrano nel processo di differenziazione parziale. In fatti, poichè il passaggio da $\mathcal{E}$ a $\mathcal{E}/X$ che porta un oggetto B in

$$B \times X \downarrow \pi_2 \; X =: B/X$$

conserva i $\varprojlim$ finiti e l'esponenziazione, un anello di tipo retta viene portato ancora in un anello di tipo retta; dato quindi

$A \in \mathcal{E}$ di tipo retta, anche A/A^{n-1} lo sarà.

Dato $A^n \xrightarrow{f} A$ in $\mathcal{E}$, associamo ad esso il morfismo

$$F: A/A^{n-1} \longrightarrow A/A^{n-1} \quad \text{in } \mathcal{E}/A^{n-1}$$

dato dal seguente diagramma commutativo in $\mathcal{E}$:

$$\begin{array}{ccc} A^n \cong A \times A^{n-1} & \longrightarrow & A \times A^{n-1} \\ & \searrow \quad \swarrow & \\ & A^{n-1} & \end{array}$$

$$(a,\vec{b}) \longmapsto (f(a,\vec{b}),\ \vec{b}).$$

Définizione 3.

$$\frac{\partial f}{\partial x_1} =: F' \circ \pi_1 : A^n \xrightarrow{F'} A^n \cong A \times A^{n-1} \longrightarrow A,$$

e analogamente si definisce la derivata parziale rispetto alle altre variabili.

In questo modo, la validità del Teorema 2. implica direttamente la validità delle regole analoghe per la differenziazione parziale .

La nozione di anello di tipo retta è stata introdotta in [K 76 a] ; il calcolo delle serie di Taylor (anche in più variabili per un anello di tipo retta è stato sviluppato ulteriormente in [K 76 b].

2.2. L'anello generico e la $\mathbb{T}$-algebra generica sono di tipo retta

Andiamo ora in cerca di modelli per il nostro assioma 1. In $\mathcal{S}$ non ne esistono - almeno non sembra; $\mathbb{R}$ non è certamente di tipo retta, altrimenti tutte le funzioni $\mathbb{R} \longrightarrow \mathbb{R}$ sarebbero differenziabili !

Teorema 3. $\mathbb{A} \in \mathcal{S}^{\mathcal{A}}$ è di tipo retta.

Dimostrazione

$\mathbb{A}$ è rappresentato da $\mathbb{Z}[X]$;

$D \rightarrowtail \mathbb{A}$ è rappresentato da $\mathbb{Z}[X]/(X^2) = \mathbb{Z}[\varepsilon]$

Per vedere che $\mathbb{A} \times \mathbb{A} \xrightarrow{\alpha} \mathbb{A}^D$ è iso, si tratta dunque di mostrare che, per ogni $B \in \mathcal{A}$,

$$(\mathbb{A} \times \mathbb{A})\,(B) \cong \mathbb{A}^D\,(B);$$

(tralasciamo di mostrare che è effettivamente α che induce questo isomorfismo). Per il lemma di Yoneda,

$$\mathbb{A}^D(B) \cong \hom(h^B, \mathbb{A}^D) \cong \hom(h^B \times D, \mathbb{A})$$
$$= \hom(h^B \times h^{\mathbb{Z}[\varepsilon]}, \mathbb{A}) = \hom(h^{B + \mathbb{Z}[\varepsilon]}, \mathbb{A})$$

(il funtore Yoneda $\mathcal{A}^{op} \longrightarrow \mathcal{S}^{\mathcal{A}}$ conserva $\varprojlim$, cioè porta $\varinjlim$ in $\mathcal{A}$ in $\varprojlim$ in $\mathcal{S}^{\mathcal{A}}$)

$$= \hom(h^{B[\varepsilon]}, \mathbb{A}) = \mathbb{A}(B[\varepsilon]) = B[\varepsilon] \approx B \times B = (\mathbb{A} \times \mathbb{A})\,(B).$$ ◆

Dal teorema 3. discende il

Corollario: ogni morfismo $f: \mathbb{A} \longrightarrow \mathbb{A}$ in $\mathcal{S}^{\mathcal{A}}$ è differenziabile.

Ciò non deve sorprendere: f, come morfismo tra funtori rappresentabili, è anch'esso rappresentabile, cioè proviene da un morfismo

$$\mathbb{Z}[X] \xleftarrow{\lambda} \mathbb{Z}[X] \in \mathcal{A}$$

che è univocamente determinato da $\lambda(X)$, immagine del generatore di $\mathbb{Z}[X]$; $\lambda(X)$ sarà un elemento di $\mathbb{Z}[X]$, cioè un polinomio, e i

polinomi sono evidentemente differnziabili (la differenziazione formale coincide con quella da noi definita). Che cioè $\mathbb{A}$ sia un anello di tipo retta in $\mathscr{SA}$, $\mathscr{Z}$, $\mathscr{E}t$ (lo si dimostra analogamente) riflette soltanto l'esistenza della differenziazione formale per i polinomi in $\mathbb{Z}[X]$, e non bisogna quindi aspettarsi di poter fare molte analisi in $\mathbb{A}$; abbiamo semplicemente inquadrato la differenziabilità dei polinomi in un'altra ottica, più geometrica. Anche la stessa genericità di $\mathbb{A}$ non conferisce tanta importanza al fatto che $\mathbb{A}$ sia di tipo retta: la genericità riguarda soltanto quelle strutture che vengono conservate dai funtori g^* (con g geometrico), ma l'essere di tipo retta non viene generalmente conservato da questi funtori poichè coinvolge l'esponenziazione.

Sarà dunque il caso di considerare altri modelli nei quali possiamo svolgere un po' più di analisi; vorremmo per esempio poter trovare soluzioni per equazioni differenziali come

$$y' = y, \quad y(0)=1.$$

$y'=y$ è verificato solo per il polinomio costante 0, che però non verifica $y(0)=1$. Volgiamoci dunque a modelli nei quali abbiamo non solo polinomi, ma anche funzioni analitiche, riprendendo, ancora una volta, delle idee di Lawvere: definiamo una teoria algebrica (nel senso di Lawvere):

Definizione 4. La teoria delle algebre analitiche è la teoria algebrica $\mathbb{T}$ nella quale, per ogni $n\in\mathbb{N}$,

$\mathbb{T}(n,1)$ =: insieme delle funzioni analitiche dovunque definite (*) $\mathbb{C}^n \longrightarrow \mathbb{C}$.

$\mathbb{T}(1,1)$ sarà dunque l'insieme delle serie di potenza che conver

(*) Se si prendessero per esempio le funzioni meromorfe, avremmo problemi con la sostituzione; la teoria delle categorie non è tutt'ora riuscita a fornire un quadro per funzioni non dovunque definite,o a valori multipli; che cos'è la teoria "categorica"dell superfici di Riemann ?

gono dovunque. Poichè in $\mathbb{T}(2,1)$ abbiamo naturalmente le funzioni

$$X_1 + X_2 \quad \text{e} \quad X_1 \cdot X_2 ,$$

$\mathbb{T}$ comprende la teoria degli anelli commutativi, delle $\mathbb{C}$-algebre etc.

Come per ogni teoria algebrica (in questo senso) l'oggetto iniziale nelle categorie delle $\mathbb{T}$-algebre coincide con $\mathbb{T}(0,1)$ che è l'insieme delle funzioni analitiche da $\mathbb{C}$ in $\mathbb{C}$, insieme isomorfo a $\mathbb{C}$, che è anche la $\mathbb{T}$-algebra con 0 generatori. Una $\mathbb{T}$-algebra è dunque anzitutto un anello commutativo, anzi una $\mathbb{C}$-algebra, dove possiamo valutare non solo i polinomi, ma anche le serie di potenza convergenti.

Teorema 4: $\mathbb{C}[\varepsilon]$ è una $\mathbb{T}$-algebra, e precisamente $\mathbb{C}\{X\}/\ X^2 \equiv 0$, cioè $\mathbb{C}[\varepsilon]$ è il coegualizzatore dei morfismi $\mathbb{C}\{X\} \underset{X \longmapsto 0}{\overset{X \longmapsto X^2}{\rightrightarrows}} \mathbb{C}\{X\}$ nella categoria delle $\mathbb{T}$-algebre

(indichiamo con $\mathbb{C}\{X\}$ la $\mathbb{T}$-algebra libera con 1 generatore).

Dimostrazione: prima di tutto, dobbiamo definire su $\mathbb{C}[\varepsilon]$ una struttura di $\mathbb{T}$-algebra. Il modo di farlo è canonico: prendiamo per esempio qualche $\omega \in \mathbb{T}(1,1)$ e consideriamo il composto

$$2 \xrightarrow{+} 1 \xrightarrow{\omega} 1$$

che indichiamo con $\omega(X+Y) \in \mathbb{T}(2,1)$.

Esiste allora $\varrho \in \mathbb{T}(2,1)$ tale che

$$\omega(X+Y) = \omega(X) + Y \cdot \omega'(X) + Y^2 \cdot \varrho ,$$

e questa è una legge di $\mathbb{T}$ (in termini di algebra universale), cioè ciò vale in tutte le $\mathbb{T}$-algebre. Dobbiamo quindi definire, per ogni $a + \varepsilon \cdot b \in \mathbb{C}[\varepsilon]$,

$$\omega(a + \varepsilon \cdot b) = \omega(a) + \varepsilon \cdot b \cdot \omega'(a) + \varepsilon^2 \cdot \ldots\ldots ,$$

e poichè $\varepsilon^2 = 0$, e che $a \in \mathbb{C}$ che è una $\mathbb{T}$-algebra, a destra abbiamo un ben definito elemento di $\mathbb{C}[\varepsilon]$.

Vediamo ora di dimostrare che $\mathbb{K}[\varepsilon]$ è effettivamente il coegualizzatore di cui sopra: per ogni $\mathbb{T}$-algebra B e ogni morfismo

$$\mathbb{K}\{X\} \xrightarrow{\beta} B$$

di $\mathbb{T}$-algebre che "co-egualizza" i due morfismi di cui sopra - ciò sarà il caso se e solo se β manda il generatore X di $\mathbb{K}\{X\}$ in un elemento b di B che verifica $b^2 = 0$ - esiste uno ed un solo morfismo di $\mathbb{T}$-algebre $\mathbb{K}[\varepsilon] \xrightarrow{\gamma} B$ tale che

$$\beta = \mathbb{K}\{X\} \longrightarrow \mathbb{K}[\varepsilon] \xrightarrow{\gamma} B .$$

Ora, possiamo anzitutto supporre $\mathbb{K} \subset B$: poichè $\mathbb{K}$ è la $\mathbb{T}$-algebra iniziale, esiste un $\mathbb{T}$-omomorfismo $\mathbb{K} \xrightarrow{\iota} B$ che sarà dunque in particolare un omomorfismo di anelli, e, poichè $\mathbb{K}$ è un campo, ι è necessariamente un <u>monomorfismo</u>.

Quindi, dovremo avere necessariamente

$$\gamma(a + \varepsilon \cdot a') = a + \gamma(\varepsilon) \cdot a'$$

e $\gamma(\varepsilon) = b$, cioè $\gamma : a + \varepsilon \cdot a' \longmapsto a + b \cdot a'$.

Resta da vedere che γ è un morfismo di $\mathbb{T}$-algebre, cioè che commuta con tutte le $\mathbb{T}$-operazioni: ciò si fa sfruttando, come sopra, le <u>leggi</u> della teoria $\mathbb{T}$. ◆

Abbiamo così visto che $\mathbb{K}[\varepsilon]$ è una $\mathbb{T}$-algebra e risolve nella categoria delle $\mathbb{T}$-algebre lo stesso problema universale che nella categoria degli anelli commutativi. Più in generale, per <u>ogni</u> $\mathbb{T}$-algebra B, l'<u>anello</u> $B[\varepsilon]$ ammette un'unica struttura come $\mathbb{T}$-algebra tale che sia

$$B[\varepsilon] = B + \mathbb{K}[\varepsilon] \quad \text{(coprodotto nella categoria delle } \mathbb{T}\text{-algebre).}$$

La dimostrazione di questo fatto è analoga a quella che stabilisce che $\mathbb{K}[\varepsilon]$ è una $\mathbb{T}$-algebra.

Sia ora $\mathcal{T}$ la categoria delle $\mathbb{T}$-algebre finitamente presentate, e consideriamo il funtore distratto $\mathcal{T} \longrightarrow \mathcal{S}$ che indicheremo ancora con $\mathbb{A}$ e che, come si dimostra nella semantica funtoriale, è ancora la generica $\mathbb{T}$-algebra.

Teorema 5. $\mathbb{A} \in \mathcal{S}^{\mathcal{T}}$ è un anello di tipo retta.

La dimostrazione si svolge esattamente come quella che stabilisce che $\mathbb{A} \in \mathcal{S}^{\mathcal{A}}$ è di tipo retta: basta sostituire $\mathbb{Z}$ con $\mathbb{C}$: $\mathbb{C}\{X\}$ rappresenta $\mathbb{A}$ in questo caso; analogamente, D è ora rappresentato da $\mathbb{C}[\varepsilon]$.◆

Il fatto analitico che ci ha permesso di ottenere questo risultato è questa volta la legge di $\mathbb{T}$: per ogni operazione $\omega \in \mathbb{T}(1,1)$ esiste ϱ tale che

$$\omega(X+Y) = \omega(X) + Y \cdot \omega'(X) + Y^2 \cdot \varrho$$

basata sullo sviluppo delle funzioni analitiche in serie di Taylor, che ci permetteva di sostituire $\mathbb{C}\{X\}/X^2 \equiv 0$ con $\mathbb{C}[\varepsilon]$ di cui sappiamo che, come spazio vettoriale su $\mathbb{C}$, ha soltanto dimensione 2, cosicchè, con $Y = b \cdot \varepsilon$, il termine $Y^2 \cdot \varrho$ si annulla sempre.

Vorrei infine considerare alcuni aspetti dell'analisi che si può svolgere nella $\mathbb{T}$-algebra generica $\mathbb{A}$: consideriamo il seguente enunciato su $\mathbb{A}^{\mathbb{A}}$:

$$\forall a \in \mathbb{A} \quad \exists ! \ f \in \mathbb{A}^{\mathbb{A}} \text{ tale che } f' + a \cdot f = 1 \text{ e } f(0) = 0.$$

Chiaramente, tra i morfismi $\mathbb{A} \longrightarrow \mathbb{A}$ abbiamo la funzione esponenziale exp, visto che $\mathbb{C} \xrightarrow{e^z} \mathbb{C}$ è analitica e dovunque definita, e si dimostra facilmente che $\exp(0) = 1$.

Si potrebbe pensare di dimostrare l'enunciato di sopra con il seguente argomento: si distinguono due casi:

- $a = 0$; $f(z) = z$ è allora una soluzione;
- $a \neq 0$; $\dfrac{1 - \exp(-az)}{a}$ è allora una soluzione.

Ma ciò non dimostra l'enunciato internamente, poichè, internamente, la disgiunzione che si traduce nella distinzione dei due casi non è valida; oltretutto, non abbiamo $a \neq 0 \Longleftrightarrow a$ è invertibile, poichè $\mathbb{A}$ non è un oggetto-campo in $\mathcal{S}^{\mathcal{T}}$. Per dimostrare la validità dell'enunciato internamente, occorre esibire un morfismo $\mathbb{A} \longrightarrow \mathbb{A}^{\mathbb{A}}$ che associa ad ogni $a \in \mathbb{A}$ un $f_a \in \mathbb{A}^{\mathbb{A}}$ tale che $f_a' + a f_a = 1$ e $f_a(0)=0$; per l'aggiunzione esponenziale, ciò significa che occorre trovare

$$\mathbb{A} \times \mathbb{A} \xrightarrow{\varphi} \mathbb{A} \text{ tale che per ogni } a \in A$$

$$\varphi(a,z) = f_a(z) \text{ possiede le proprietà richieste, cioè}$$

$$\frac{\partial \varphi}{\partial z}(a,z) + a \cdot \varphi(a,z) = 1 \quad \text{e} \quad \varphi(a,0)=0.$$

Entra dunque in gioco la differenziazione parziale. Il fatto che l'argomentazione di sopra non costituisca una dimostrazione per la validità interna del nostro enunciato ha una controparte esterna; esso ha cioè una rilevanza per la matematica concreta: la soluzione $\frac{1-\exp(-az)}{a}$ fornisce infatti, per valori piccoli di a, dei valori numerici che sono poco precisi: al tendere di a verso 0, sia il numeratore che il denominatore tendono a zero, cosicchè il quoziente diventa inesatto. Un mio collega, il prof.Svejgaard, che si occupa di calcolatori elettronici e che si interessa di analisi costruttiva, mi ha indicato come si possono ottenere dei valori numerici migliori nel calcolo della soluzione: si può trovare precisamente una funzione $\varphi(a,z)$ che possiede i requisiti per la validità interna del nostro enunciato e che quindi, esternamente, dimostra un enunciato più generale.

A questo scopo si consideri la funzione

$$E(t) =: 1 + \frac{t}{2!} + \frac{t^2}{3!} + \frac{t^3}{4!} + \ldots \in \mathbb{T}(1,1);$$

ponendo $\varphi(a,z) = z \cdot E(-az)$, troviamo una soluzione nella quale

a interviene come parametro C-infinito. Il fatto che, come serie di potenza, $\frac{1-\exp(-az)}{a}$ e $z \cdot E(-az)$ coincidono, non deve ingannare: come morfismi composti della $\mathbb{T}$-algebra $\mathbb{A}$, il primo non è definito, il secondo lo è; e esternamente, ciò si traduce, per esempio, nel fatto che, in un calcolatore tascabile, calcolando E(t) a partire da exp, cioè come $\frac{\exp(t)-1}{t}$, si ottengono valori molto inesatti per valori piccoli di t, mentre al contrario, calcolando exp(t) come $t \cdot E(t)+1$, si ottengono valori buoni per exp.

3. La geometria differenziale in un topos

3.1. L'assioma di linearità infinitesimale e la struttura lineare dei fibrati tangente.

Anche in questo capitolo, il nostro approccio sarà ancora assiomatico: dati una categoria $\mathscr{C}$ con $\varprojlim$ finiti, un anello A in $\mathscr{C}$ e $D = [\![x \mid x^2=0]\!] \rightarrowtail A$, vorremmo trovare degli assiomi che garantiscono che, secondo l'idea "geometrizzante" di Lawvere, V^D funga da fibrato tangente per ogni oggetto V di $\mathscr{C}$ (supporremo che V^D e gli altri oggetti esponenziali che useremo in seguito esistono in $\mathscr{C}$). A questo scopo, converrà certamente richiedere che le fibre di V^D siano A-moduli (cioè che $V^D \xrightarrow{p} V^{(*)}$ sia un A-modulo in $\mathscr{C}/V$ il che, parlando in termini insiemistici, significa che per ogni $x \in V$, l'insieme $p^{-1}(x) = \{t: D \to V \mid t(0)=x\}$ che costituisce la fibra di x, ovvero l'insieme dei vettori tangenti su V che sono applicati in x, sia un A-modulo)$^{(**)}$. Se pensiamo ad A come, per esempio, ai numeri reali, ciò significa che V^D è un fibrato vettoriale su V.

(*) Si ricordi che $V^D \xrightarrow{p} V$ proviene da $\mathbb{1} \xrightarrow{\ulcorner 0 \urcorner} D$ tramite il funtore $V^{(\ )}$, cioè $p = V^{\ulcorner 0 \urcorner} : (t:D \to V) \longmapsto t(0)$.

(**) Più precisamente ancora, dovremmo parlare di $V^D \xrightarrow{p} V$ come di un $(A \times V \to V)$ - modulo in $\mathscr{C}/V$; si noti che tutti gli "abusi" insiemistici che facciamo qui e nel seguito parlando di "elementi" $x \in V$ e di $t \in V^D$ come "funzione" da D in V diventano formulazioni rigorose non appena si intende "elemento" in senso lato, cioè, $x \in V$ significa: $X \xrightarrow{x} V$, $t \in V^D$ significa $X \xrightarrow{t} V^D$, cioè $D \times X \xrightarrow{\tilde{t}} V$; in questo modo, lavoriamo automaticamente in $\mathscr{C}/V$.

Ora, consideriamo, oltre a D =: D(1), anche

$$D(2) =: \quad [\![(x,y) \in A^2 \mid x^2 = y^2 = xy = 0]\!]$$

e, analogamente

$$D(3) =: \quad [\![(x_1,x_2,x_3) \in A^3 \mid x_i x_j = 0]\!].$$

Chiaramente, risulta $D(2) \subset D \times D \subset A \times A$. Da D a D(2) abbiamo due morfismi i_1 e i_2 che possiamo descrivere così:

$$i_1 : d \longmapsto (d,0)$$

$$i_2 : d \longmapsto (0,d);$$

analogamente, abbiamo tre morfismi j_1, j_2, j_3 da D in D(3):

$$j_1 : d \longmapsto (d,0,0)$$

e così via. Componendo questi morfismi con $\mathbb{1} \xrightarrow{0} D$ e applicando il funtore $V^{(\ )}$, otteniamo allora due diagrammi:

$$(1) \quad V = V^{\mathbb{1}} \xleftarrow{V^0 = p} V^D \underset{V^{i_2}}{\overset{V^{i_1}}{\leftleftarrows}} V^{D(2)}$$

$$(2) \quad V = V^{\mathbb{1}} \xleftarrow{V^0 = p} V^D \underset{V^{j_3}}{\overset{V^{j_1}}{\leftleftarrows}} V^{D(3)}$$

Possiamo dimostrare che le fibre di V^D sono A-moduli se V è <u>infinitesimamente lineare</u>, nel senso che verifica il seguente

<u>Assioma 2.</u> I diagrammi (1) e (2) sono esatti a sinistra cioè $V^{D(2)} \cong V^D \underset{V}{\times} V^D$, e analogamente, $V^{D(3)} \cong V^D \underset{V}{\times} V^D \underset{V}{\times} V^D$.

La condizione essenziale è l'esattezza di (1); quella di (2) sarà usata solo per dimostrare l'associatività dell'addizione sulle fibre. Si noti che, se $D(2) \cong D \underset{\mathbb{1}}{+} D$ (cioè se

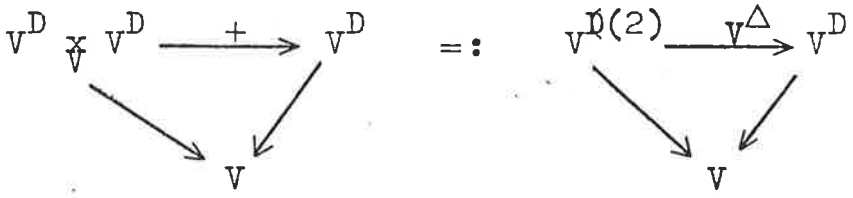
$$\begin{array}{ccc} \mathbb{1} & \xrightarrow{0} & D \\ {\scriptstyle 0}\downarrow & & \downarrow \\ D & \longrightarrow & D(2) \end{array}$$

è un push-out), e se $D(3) \cong D \underset{\mathbb{1}}{+} D \underset{\mathbb{1}}{+} D$, <u>tutti</u> gli oggetti di $\mathscr{C}$ sono infinitesimamente lineari, poichè il funtore $V^{(\ )}$ trasforma

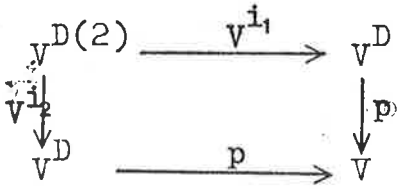
i push-out in prodotti fibrati.

Teorema 1. Se $V \in \mathscr{C}$ è infinitesimamente lineare, le fibre di V^D sono A-moduli.

Dimostrazione. Per definire l'addizione sulle fibre di V^D, consideriamo il morfismo diagonale $D \xrightarrow{\Delta} DxD$; chiaramente Δ si fattorizza attraverso D(2), indicheremo ancora con $D \xrightarrow{\Delta} D(2)$ tale morfismo, e definiamo l'addizione in $V^D \longrightarrow V$ come segue:



Per esplicitare questa definizione, vediamo anzitutto cosa dice l'assioma 2:



è un prodotto fibrato, sse, per ogni coppia (t_1,t_2) di elementi di V^D tali che $p(t_1)=p(t_2)$, cioè per ogni coppia di "vettori tangente" applicati in uno stesso punto $x=p(t_1)=p(t_2)$ di V, esiste uno ed un solo $f \in V^{D(2)}$ tale che $i_1 \circ f = t_1$ e $i_2 \circ f = t_2$, cioè tale che

$$f(d,0)=t_1(d) \text{ e } f(0,d) = t_2(d) \text{ per ogni } d \in D.$$

La nostra definizione dell'addizione in V^D significa perciò:

data una coppia $t_1,t_2 \in V^D$ in una stessa fibra di V^D, e associata ad essa la funzione $f \in V^{D(2)}$ come sopra, si pone $t_1+t_2 =: \Delta \circ f : D \xrightarrow{\Delta} D(2) \xrightarrow{f} V$,

ovvero, per ogni $d \in D$,

$(t_1+t_2)(d) = f(d,d)$;

poichè $(t_1+t_2)(0) = f(0,0) = t_1(0) = t_2(0)$, t_1+t_2 appartiene ancora alla stessa fibra.

Verificheremo in dettaglio soltanto che questa addizione ammette l'inversa: osserviamo anzitutto che il morfismo

$$A \longrightarrow A \qquad (a \longmapsto -a)$$

induce un morfismo $D \longrightarrow D$, poichè, se $d^2=0$, allora $(-d)^2=0$. Dato quindi $t \in V^D$ con $t(0)=x$ (*), anche $D \longrightarrow D \xrightarrow{t} V$ porta il punto 0 in x; possiamo quindi considerare $t+(-t)$ secondo l'addizione nella fibra di x sopra descritta; poichè la funzione $f: D(2) \longrightarrow V$ così definita:

$$(d_1,d_2) \longmapsto t(d_1-d_2)$$

verifica $f(d,0) = t(d)$

$f(0,d) = t(-d) = (-t)(d)$,

essa è l'(unico!) elemento di $V^{D(2)}$ corrispondente alla coppia $(t, -t)$ nell'isomorfismo $V^D \underset{V}{\times} V^D \cong V^{D(2)}$, e quindi, per ogni $d \in D$, risulta

$$(t+(-t))(d) = f(d,d) = t(d-d) = t(o) = x;$$

in altri termini, $t+(-t)$ coincide nella fibra di V^D su x con quella "funzione" che associa ad ogni $d \in D$ il punto base x della fibra; ora, questo è precisamente l'elemento neutro dell'addizione nella fibra su x.

Per definire infine la moltiplicazione con i scalari di A, dati $a \in A$ e $t: D \longrightarrow V$, poniamo

(*) Adoperiamo ora direttamente la terminologia insiemistica, visto che è facile tradurla in termini di diagrammi.

$$a\cdot t =: D \xrightarrow{\cdot a} D \xrightarrow{t} V$$
$$(d \longmapsto d\cdot a \longmapsto t(d\cdot a));$$

chiaramente, D è stabile rispetto alla moltiplicazione con scalari: $d^2=0$ implica $(a\cdot d)^2 = 0$ per ogni $a \in A$.◆

Abbiamo così definito una struttura di A-modulo per ogni $V \in \mathscr{C}$ che è infinitesimamente lineare; inoltre, si vede facilmente che questa definizione è naturale in V: dati due oggetti infinitesimamente lineari, V e V', e $V \xrightarrow{f} V'$, abbiamo il diagramma commutativo

$$\begin{array}{ccc} V & \xrightarrow{f} & V' \\ {\scriptstyle p}\uparrow & & \uparrow{\scriptstyle p'} \\ V^D & \xrightarrow{f^D} & V'^D \end{array}$$

e f^D è lineare sulle fibre, visto che abbiamo dato tutte le nostre definizioni funtorialmente.

Teorema 2 .(*) Se A è di tipo retta, allora per ogni n, A^n è infinitesimamente lineare.

(*) Questa proposizione non è perfettamente esatta: si dovrebbe prendere una nozione leggermente più generale degli anelli di tipo retta: dalla definizione originale discendeva che le funzioni da D in A si possono sviluppare in serie di Taylor con due termini; ciò che occorre qui è che le funzioni $D \times D \longrightarrow A$ si possono sviluppare in serie di Taylor naturalmente con quattro termini. ~~Comunque, se A è l'anello generico o l'anello locale generico, abbiamo $D(2)=D+D$, $D(3)=D+D+D$, e quindi ogni oggetto in $\mathscr{C}_0$ o in $\mathscr{C}_A$ infinitesimamente lineare.~~

Corollario. Se A è di tipo retta, $(A^n)^D \xrightarrow{p} A^n$ possiede una struttura lineare su ogni fibra.

Potremmo vedere direttamente che $(A^n)^D \xrightarrow{p} A^n$ è un fibrato vettoriale: abbiamo $A^D \cong AxA$ tramite α, e quindi

$$(A^n)^D \cong (A^D)^n \cong (AxA)^n = A^n x A^n \longrightarrow A^n,$$

e il morfismo p è in questo caso semplicemente la prima proiezione; si tratta cioè del fibrato tangente banale che deve ovviamente essere il fibrato tangente di questi "spazi vettoriali" canonici se tutta la nostra impostazione vuole avere un qualche senso.

Una delle scoperte fondamentali della geometria differenziale, dovuta a Lie, è che una varietà che porta una struttura di gruppo, cioè un gruppo di Lie, induce sullo spazio tangente sopra l'elemento neutro una struttura di algebra di Lie. Per ottenere anche per i nostri fibrati tangente una proprietà analoga, formuliamo lo

Assioma 3. Il funtore $V^{(\ )}$ porta il seguente diagramma in un diagramma esatto:

$$DxD \underset{h_2}{\overset{h_1}{\rightrightarrows}} DxD \longrightarrow D,$$

dove poniamo h_1: $(d_1,d_2) \longmapsto (d_1,0)$;

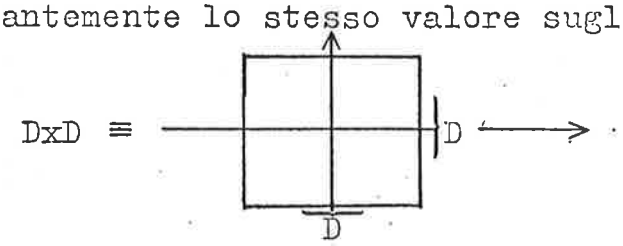
h_2: $(d_1,d_2) \longmapsto (0,d_2)$;

è la restrizione della moltiplicazione di A a D.

Questo assioma, secondo il quale dunque $V^D \xrightarrow{V^\bullet} V^{DxD}$ è l'egualizzatore di

$$V^{DxD} \underset{V^{h_2}}{\overset{V^{h_1}}{\rightrightarrows}} V^{DxD},$$

significa in termini geometrici che ogni "funzione" $f \in V^{D \times D}$ che assume costantemente lo stesso valore sugli assi



(per la quale si ha cioè $f(d,0)=f(0,d)$ per ogni $d \in D$), è del tipo $(d_1,d_2) \longmapsto g(d_1 \cdot d_2)$ con $g : D \longrightarrow V$; vivecersa, ogni funzione siffatta è ovviamente costante sugli assi:

$$f(d,0) = g(d \cdot 0) = g(0) = g(0 \cdot d) = f(0,d).$$

Se A è un anello di tipo retta, A^n verifica questo assioma 3, come si vede facilmente usando le "serie" di Taylor.

Possiamo ora effettivamente dimostrare il seguente

Teorema 3. Se V è un monoide in $\mathscr{C}$ (cioè un semigruppo con un elemento neutro $1 \xrightarrow{e} V$) che verifica gli assiomi 2 e 3, allora lo spazio tangente L di V nel punto e dato dal seguente prodotto fibrato

$$\begin{array}{ccc} L & \longrightarrow & V^D \\ \downarrow & & \downarrow p \\ 1 & \xrightarrow{e} & V \end{array}$$

è un'algebra di Lie in $\mathscr{C}$.

Non entriamo nei dettagli della dimostrazione (cfr. [RW]). Si vede intanto che se V è infinitesimamente lineare, L eredita da $V^D \xrightarrow{p} V$ la struttura di A-modulo. Indichiamo ancora come si definisce il prodotto di Lie su L usando, come al solito,

là notazione insiemistica: data una coppia di elementi di L, cioè $(t_1,t_2)\in V^D$ tali che $t_1(0)=t_2(0)=e$, consideriamo $\tau\in V^{DxD}$ così definito:

$$(d_1,d_2) \xrightarrow{\tau} (t_1(d_1))^{-1} \circ (t_2(d_2))^{-1} \circ t_1(d_1) \circ t_2(d_2)$$

($\circ$ indica l'operazione che munisce V della struttura di semi gruppo; la formazione degli inversi in V, teoricamente non definita, può essere evitata con opportuni accorgimenti). Chiaramente, se $d_1=0$ oppure $d_2=0$, viene $(d_1,d_2)=e$ - in altri termini, τ egualizza V^{h_1} e V^{h_2}; ciò implica l'esistenza di un $t\in V^D$ univocamente determinato tale che $\tau(d_1,d_2) = t(d_1\ d_2)$ per ogni $(d_1;d_2)\in DxD$. Definiamo dunque $[t_1,t_2] = t$.

3.2. I morfismi étale e la nozione di varietà

Non c'è da aspettarsi che tutti gli oggetti nei topos della geometria algebrica siano infinitesimamente lineari o che verifichino l'assioma 3(*). A nostro avviso, queste condizioni dovrebbero però essere verificate quando si costruisce un oggetto geometrico in un topos. La tecnica adatta per questa verifica è - coerentemente la nostra impostazione geometrica - quella che consiste nel definire una varietà come un oggetto che può venir ricoperto con degli "aperti omeomorfi allo spazio euclideo". Cerchiamo dunque anzitutto di definire nel nostro contesto una nozione di sotto-oggetto aperto di un oggetto dato. Poichè tutto il nostro discorso dipende da quegli

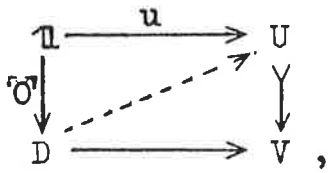
---

(*) Si noti che nell'assioma 3 non si fa nessun riferimento ad una eventuale struttura di semi-gruppo su V.

oggetti infinitesimali che sono D, D(2) ecc., un modo naturale di dare questa definizione potrebbe essere il seguente:

$U \rightarrowtail V$ è <u>aperto</u> (rispetto a D)

se è stabile rispetto alle estensioni mediante D, cioè: per ogni punto $\mathbb{1} \xrightarrow{u} U$ di U, e ogni elemento di V che è una estensione infinitesimale di u - in altri termini, per ogni quadrato commutativo

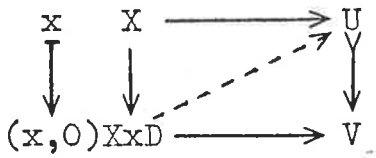


esiste uno (ed un solo) morfismo da D in U che rende commutativo il diagramma risultante. L'esistenza di questo morfismo sta a significare che quella estensione infinitesimale di u in V è già in U : "U contiene assieme ad ogni suo elemento anche un suo intorno infinitesimale".

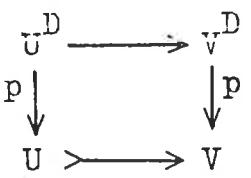
Per ragioni tecniche abbastanza ovvie, conviene considerare degli elementi più generali di quelli definiti su $\mathbb{1}$ e dire che

$U \rightarrowtail V$ è <u>aperto</u> (rispetto a D)

se per ogni diagramma commutativo



esiste una (e quindi una sola) fattorizzazione tramite U, o, equivalentemente, sse il diagramma



è un prodotto fibrato;

("ogni azion infinitesimale su un elemento di U si svolge

interamente in U".

Analogamente si definisce quando $U \rightarrowtail V$ è aperto rispetto a D(2), D(3), DxD ecc.

Definizione 1. $U \longrightarrow V$ (non necessariamente mono) è étale(*) sse

$$\begin{array}{ccc} U^D & \longrightarrow & V^D \\ \downarrow & & \downarrow \\ U & \longrightarrow & V \end{array}$$

e i diagrammi analoghi per D(2), DxD, ecc. sono prodotti fibrati.

In base alle nostre considerazioni precedenti, un monomorfismo étale potrà quindi venir concepito come un sotto-oggetto aperto. Un caso tipico di morfismo étale che non è un monomorfismo si presenta come

$$\amalg U_i \longrightarrow V$$

dove ogni U_i è aperto nel senso che l'immersione di U_i in V è étale. In questo modo possiamo assimilare un morfismo étale che sia un epimorfismo regolare ad un ricoprimento aperto del suo codominio. per definire poi le varietà come si fa classicamente, cioè come fibrati vettoriali le cui fibre siano spazi "euclidei"; ciò porta alla

Definizione 2. V è una varietà di dimensione n se esiste un oggetto V' infinitesimamente lineare e un epimorfismo regolare étale $V' \twoheadrightarrow V$ tale che l'A-modulo sopra V'

$$V'^D \longrightarrow V'$$

è isomorfo a $V' \times A^n \longrightarrow V'$ (consideriamo A^n come lo "spazio euclideo" canonico di dimensione n).

(*) cfr. la nozione di morfismo étale che si dà in [I].

Anche nei topos abbiamo un teorema di "descente étale":

Teorema 4. Se $V' \longrightarrow\!\!\!\!\!\rightarrow V$ è un epi regolare étale, e se V' è infinitesimamente lineare, anche V lo è.

Pensando a $V' \longrightarrow\!\!\!\!\!\rightarrow V$ come ad un ricoprimento aperto, questo teorema è geometricamente fondato: se V' ha degli spazi tangenti lineari, V' induce una struttura lineare anche sugli spazi tangente di V. In particolare, questo teorema fa sì che ogni varietà è infinitesimamente lineare.
Con il seguente

Assioma 4 : $(-)^D$ commuta con i colimiti

concludiamo la lista dei nostri assiomi e ci accingiamo ora a dimostrare che, per esempio, le varietà grassmanniane sono varietà nel senso da noi definito. La varietà grassmanniana più semplice è la retta proiettiva $\mathbb{P}^1$ così definita:

dato un anello A di tipo retta in un topos (*) $\mathcal{E}$, e posto
$V^{1,2} =: \{(x,y) \in A^2 \mid x \text{ è invertibile oppure lo è } y\}$
si definisce $\mathbb{P}^1 =: V^{1,2}/\equiv$, $\equiv$ essendo la relazione di proporzionalità (determinata dall'azione del gruppo lineare generale $GL(1,A)$);

Teorema 5. La retta proiettiva $\mathbb{P}^1$ è una varietà di dimensione 1.

(*) E' per ragioni di semplicità che supponiamo che la categoria ambiente sia un topos, anche se basterebbe prendere una categoria esatta con sup stabili e qualche oggetto esponenziale.

Dimostrazione. (scriviamo semplicemente V e $\mathbb{P}$ invece di $V^{1,2}$ e $\mathbb{P}^1$). In ogni topos si dimostra facilmente che $\mathbb{P}$ è l'unione di due coppie della retta affine A:

possiamo descrivere con $a \swarrow^{\overline{(1,a)}}_{\overline{(a,1)}}$ le immersioni di A in $\mathbb{P}$.

Per dimostrare ora il teorema ci serviamo di alcuni lemmi che discendono dall'assioma 4:

Lemma 1. Se $(X_i \rightarrowtail X)_{i\in I}$ è una famiglia di monomorfismi étale, allora anche $\amalg X_i \longrightarrow X$ è étale.

Lemma 2. Se ogni X_i è una varietà di dimensione n, anche $\amalg X_i$ lo è.

Questi lemmi discendono in parte dal fatto che i coprodotti sono disgiunti e universali in un topos, in parte dalla possibilità di analizzare $\amalg(X_i^D)$ in termini di $(\amalg X_i)^D$ in virtù dell'assioma 4.

Poichè sappiamo che $\mathbb{P} = A\amalg A$ e che A è ben inteso una varietà di dimensione 1 se è di tipo retta, la nostra dimostrazione si riduce in virtù di questi lemmi a mostrare che i due monomorfismi da A in $\mathbb{P}$ sono étale. Come vedremo, l'assioma 4 interviene in modo essenziale in questa argomentazione in quanto esso ci assicura che $(\ )^D$ conserva gli epimorfismi regolari.

Visto che $\mathbb{P}$ è definito come il quoziente $V/\equiv$, $V \longrightarrow \mathbb{P}$ è regolare. D'altra parte, consideriamo

$$U =: \{(x,y)\in A^2 \mid x \text{ è invertibile}\} \rightarrowtail V.$$

Si vede facilmente che U è stabile sotto l'azione di GL(1,A) e ciò permette di affermare che il diagramma

$$\begin{array}{ccc} (x,y) & U & \longrightarrow V \\ \downarrow & \downarrow & \downarrow \\ x^{-1}y & A & \longrightarrow \mathbb{P} \\ & a & \longmapsto (1,a) \end{array} \qquad (I)$$

è un prodotto fibrato, cosicchè anche $U \twoheadrightarrow A$ è regolare. Si dimostra peraltro facilmente che $U \hookrightarrow V$ è étale: ciò riposa sul fatto che, se $x \in A$ è invertibile, anche $x+d$ lo è:

$$(x+d)\cdot \frac{x-d}{x^2} = 1$$

Per mostrare ora che $A \hookrightarrow \mathbb{P}$ è étale, che cioè il quadrato

$$\begin{array}{ccc} A^D & \longrightarrow & \mathbb{P}^D \\ \downarrow & & \downarrow \\ A & \longrightarrow & \mathbb{P} \end{array} \qquad (II)$$

è un prodotto fibrato, consideriamo $a \in A$ e $t \in \mathbb{P}^D$ tali che $t(0) = \overline{(1,a)} \in \mathbb{P}$; occorre trovare $s \in A^D$ che si proietta su questi due "elementi"; un $s \in A^D$ siffatto è necessariamente unico, poichè $A^D \longrightarrow \mathbb{P}^D$ è un monomorfismo. Inoltre, se s si proietta su t lungo $A^D \longrightarrow \mathbb{P}^D$, s si proietterà certamente su a lungo $A^D \longrightarrow A$, cioè $s(0)=a$: il quadrato II è comunque commutativo; quindi, se in senso orario abbiamo

$$s \longmapsto t \longmapsto t(0)=\overline{(1,a)}$$

avremo in senso antiorario

$$s \longmapsto s(0) \longmapsto \overline{(1,s(0))};$$

ma $\overline{(1,a)}=\overline{(1,s(0))}$ vale se e solo se $a = s(0)$.

Per trovare $s \in A^D$ con le proprietà richieste, consideriamo i due quadrati (I) e

$$\begin{array}{ccc} V^D & \longrightarrow & V \\ \downarrow & & \downarrow \\ t\in\mathbb{P}^D & \longrightarrow & \mathbb{P} \end{array} \qquad \text{(III)}$$

In entrambi questi quadrati il lato sinistro è un epi regolare (per III ciò risulta dal fatto che $(\ )^D$ conserva gli epi regolari) e possiede quindi una sezione; siano $a'\in U$ e $t'\in V^D$ gli elementi che si ottengono "alzando" a e t lungo questi lati. Anche se generalmente sarà $t'(0)\neq a'$ in V, risulta comunque

$$t'(0)\equiv a';$$

infatti, per la commutatività di III è $\overline{t'(0)}=t(0)$; ma $t(0)=\overline{(1,a)}$ per ipotesi, e per la commutatività di I è $\overline{(1,a)} = \overline{a'}$.
Ora, U è stabile sotto l'azione di GL(1,A); pertanto $t'(0)\equiv a'\in U$ implica $t'(0)\in U$, e poichè $U \rightarrowtail V$ è étale, ciò significa che l'azione di t' si esaurisce in U, ossia $t'\in U^D$.
Si vede ora che l'elemento $s\in A^D$ che cerchiamo non è altro che l'immagine di t' in $U^D \twoheadrightarrow A^D$: per mostrarlo, consideriamo il quadrato I^D, cioè

$$\begin{array}{ccc} U^D & \rightarrowtail & V^D \\ \downarrow & & \downarrow \\ A^D & \rightarrowtail & \mathbb{P}^D \end{array}$$

in senso orario abbiamo $t' \longmapsto t' \longmapsto t$, e quindi anche in senso antiorario $t' \longmapsto s \longmapsto t$.◆

Con una nozione leggermente più generale di varietà e con una tecnica molto simile a quella che abbiamo usata nella precedente dimostrazione, si può dimostrare che tutte le grassmanniane sono varietà - cfr. [RK].

Teorema 6. L'anello generico e l'anello locale generico verificano l'assioma 4.

Dimostrazione:

- per $A \in \mathcal{S}^{\mathcal{A}}$, sappiamo che $D = h^{\mathbb{Z}[\varepsilon]}$. Ora, è un teorema generale della teoria delle categorie che, per ogni oggetto X di una categoria $\mathcal{C}$, $(-)^X$ commuta con i colimiti;
- per $A \in \mathcal{X}$ (dove il teorema riveste naturalmente un interesse maggiore, poichè la costruzione delle grassmanniane, per esempio, non ha molto senso per un anello che non è locale), ci serviamo di un

lemma: per ogni $X \in \mathcal{S}^{\mathcal{A}}$, $a(X^D) \cong (aX)^D$ (a il funtore di riflessione $\mathcal{S}^{\mathcal{A}} \longrightarrow \mathcal{X}$).

Questo lemma si dimostra considerando il modo in cui, in SGA4, si costruisce il funtore a come il composto $l \cdot l$; esso dipende essenzialmente dal fatto che, dato $B \in \mathcal{A}$, vi è una corrispondenza biunivoca tra i co-ricoprimenti di B e quelli di $B[\varepsilon]$: chiaramente, dato $(B \longrightarrow B_i)_{i \in I} \in \mathrm{Cocop}\ (B)$, per la stabilità dei co-ricoprimenti rispetto ai push-out, $B \longrightarrow B[\varepsilon]$ dà luogo ad un co-ricoprimento $(B[\varepsilon] \longrightarrow C_i)_{i \in I}$ di $B[\varepsilon]$;;il fatto che ogni co-ricoprimento di $B[\varepsilon]$ è di questa forma per un unico $(B \longrightarrow B_i)_{i \in I} \in$ Cocop B, dipende essenzialmente dal fatto che $b_1 + \varepsilon b_2$ è invertibile in $B[\varepsilon]$ sse b_1 è invertibile in B, cosicchè una famiglia $(b_i + \varepsilon c_i)$ genera $B[\varepsilon]$ sse (b_i) genera B.

Nella dimostrazione del teorema 6, possiamo sfruttare inoltre il fatto che a commuta con $\varinjlim$, cosidchè, data una famiglia $(X_i)_{i \in I}$ in $\mathcal{X}$, viene:
$\varinjlim_{\mathcal{X}}(X_i^D) = a\,(\varinjlim_{\mathcal{S}^{\mathcal{A}}}(X_i^D)) = a\,((\varinjlim_{\mathcal{S}^{\mathcal{A}}} X_i)^D)$ perchè il teorema vale in $\mathcal{S}^{\mathcal{A}}$

$= \left(a(\varinjlim_{\mathscr{A}} X_i)\right)^D$ per il lemma

$= \left(\varinjlim_{\mathscr{X}} (aX_i)\right)^D$ perchè a commuta con $\varinjlim$

$= \left(\varinjlim_{\mathscr{X}} X_i\right)^D$ poichè gli X_i erano già in $\mathscr{X}$.◆

Osservazioni finali

Già in [K74] ci eravamo proposti di trovare delle proprietà combinatorie del piano proiettivo in $\mathscr{X}$, come l'incidenza punti-retta per poter esprimere, per esempio, che ogni coppia di punti distinti determina una ed una sola retta, ecc.; è chiaro che questo genere di cose si può fare con l'aiuto delle varietà grassmanniane in $\mathscr{X}$, poichè si tratta di nozioni lineari, e $\mathscr{X}$ è il topos che classifica la nozione di anello locale che è la migliore approssimazione della nozione di campo in un topos; in un campo si può fare soltanto l'algebra lineare. Nel topos $\mathscr{E}t$ si possono esprimere delle proprietà combinatorie più complesse, cioè intersezioni di quadriche e altre intersezioni non lineari; ci possiamo domandare quali sono, per esempio, le proprietà delle varietà grassmanniane in $\mathscr{E}t$. Ma cosa bisogna intendere con proprietà combinatorie e perchè non vengono prese maggiormente in considerazione ? Il fatto è che questi problemi sono stati affrontati e la tecnica più adatta in questo contesto è quella della coomologia con i suoi cup-product ecc., che costituisce un approccio a tutta quella teoria delle intersezioni. Sembra quindi che ciò che abbiamo cercato di fare in $\mathscr{E}t$, dove, in realtà, sappiamo fare ben poche cose, è di pervenire ad una coomologia étale motivata dai semplici assiomi geometrici che abbiamo qui illustrati.

Potrebbe quindi darsi che, in ultima analisi, ciò che stiamo cercando non è che una motivazione per la coomologia étale, cioè per il titolo di SGA 4 ! Troveremmo perciò semplicemente un punto di vita diverso per una teoria classica.

B I B L I O G R A F I A

[C] Coste; M. e M.F.: Théories cohérentes et topos cohérents, Sém.de théorie des catégories dirigé par J.Bénabou,1975

[GD] P.Gabriel e M.Demazure: Groupes Algébriques I. North Holland, 1970

[H] M.Hakim: Topos annelés et schémas relatifs. Springer,1972.

[I] B.Iversen: Generic local structure of the morphisms in Commutative algebra, Springer Lecture Notes Vol.310,1973.

[K74] A.Kock: Linear algebra and projective geometry in the Zariski topos, Aarhus Preprint Series 1974/75 No.4.; versione rivista: Universal projective geometry via topos theory, Journ.Pure Appl.Alg.9 (1976),1-24

[K76a] A.Kock: A simple axiomatics for differentiation, Aarhus Preprint Series 1975/76 No.12 (da pubblicare in Math. Scand.)

K76b A.Kock: Taylor Series calculus for ring objects of line type, Aarhus Preprint Series 1976/77 No.4

[K77] A.Kock: Structured objects in categories, Aarhus Lecture notes, 1977

[KR] A.Kock e G.Reyes: Manifolds in formal differential geometry, manoscritto, aprile 1977

[KW] A.Kock e G.Wraith: Elementary toposes. Lecture Notes No. 30, Aarhus Universitet, 1971

[L67] F.W.Lawvere: Categorical dynamics, lecture Chicago 1967 (non pubblicato)

[L75] F.W.Lawvere: Introduction to Model theory and topoi, Springer Lecture Notes 445, 1975, 3-14

[ML] S.MacLane: Categories for the working mathematician, Graduate Texts in Mathematics Vol.5, Springer, 1971
Trad.it.: Categorie nella pratica matematica, Torino 1977

[MR] M.Makkai e G.Reyes: Model theoretic methods in the theory of topoi and related categories I, II, Bull.Acad.Polon. Sci.24, 1976, 385-392

[O] G.Osius: A Note on Kripke-Joyal Semantics for the internal language of topoi, in: Springer Lecture Notes, 445, 1975, 349-354

[RW] G.E.Reyes e G.Wraith: A note on tangent bundles in a category with a ring object, da pubblicare in Math.Scand.

[SGA 4] M.Artin, A.Grothendieck, J.L.Verdier: Théorie des topos et cohomologie étale des schémas (SGA 4), Springer Lecture Notes, vol.269,270,(1972), 305,(1973).

[T] M.Tierney: Axiomatic sheaf theory, some constructions and applications. Categories and commutative algebra, C.I.M.E. Varenna 1971, Edizioni Cremonese, Roma 1973, 249-236.

[W] B.L.Van der Waerden: Algebra, 7.ed., 2 voll., Springer 1966