

# ANNALI DELLA SCUOLA NORMALE SUPERIORE DI PISA *Classe di Scienze*

IACOPO BARSOTTI

## **Moduli canonici e gruppi analitici commutativi**

*Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3<sup>e</sup> série, tome 13, n° 3 (1959), p. 303-372*

[http://www.numdam.org/item?id=ASNSP\\_1959\\_3\\_13\\_3\\_303\\_0](http://www.numdam.org/item?id=ASNSP_1959_3_13_3_303_0)

© Scuola Normale Superiore, Pisa, 1959, tous droits réservés.

L'accès aux archives de la revue « Annali della Scuola Normale Superiore di Pisa, Classe di Scienze » (<http://www.sns.it/it/edizioni/riviste/annaliscienze/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

# MODULI CANONICI E GRUPPI ANALITICI COMMUTATIVI

di IACOPO BARSOTTI <sup>(1)</sup>

**Introduzione.** I gruppi analitici (commutativi), recentemente introdotti da J. Dieudonné, si sono dimostrati utilissimi nella investigazione delle varietà gruppali commutative (cfr. per esempio il [14] della bibliografia posta alla fine di questa memoria); manca però una trattazione organica dei gruppi analitici, ed è questa lacuna che ci proponiamo qui di colmare. Il metodo seguito, che ora descriveremo brevemente, antepone ai gruppi stessi certi moduli su un anello  $T$  definito al § 1, che già in [15] hanno dimostrato di essere lo strumento più efficace per lo studio dei gruppi analitici; per inciso, la parola « modulo » significherà sempre « modulo unitario, sinistro » salvo esplicita avvertenza in contrario.

Nel § 1 si trova la struttura di tutti i  $T^*$ -moduli finiti a torsione (1.12); il metodo è, con pochissime semplificazioni, quello di [7], ed i risultati di questo paragrafo sono tutti noti; principali fra essi sono l'1.11 e l'1.12.

Nel § 2 vengono introdotti i  $T$ -moduli canonici per mezzo delle 2.1 e 2.2; quasi tutto ciò che si riferisce ai  $T$ -moduli canonici è qui presentato per la prima volta, benchè varie loro proprietà, e principalmente il teorema di struttura 2.11, siano già state usate nello studio dei gruppi analitici. La proprietà che serve a definirli nei lavori di Dieudonné è qui presentata come un teorema, precisamente il 2.8; i risultati più usati, fra quelli del § 2, sono il 2.8, il 2.5, e il 2.11; nel 2.12, ove si descrive l'anello degli endomorfismi di un  $T$ -modulo canonico indecomponibile  $M$ , sono anche stabilite esplicitamente le condizioni sotto le quali tale anello è una schiera

---

\* Entrato in redazione il 18-5-1959.

<sup>(1)</sup> Dell'Università di Pittsburgh, e docente Fulbright presso la Scuola Normale Superiore di Pisa.

massima della propria algebra quoziente: oltre alla condizione  $\dim M=1$ , già nota, si trova la condizione  $\text{codim } M=1$ , che apparentemente era sfuggita fino ad ora.

Il § 3 tratta di un argomento nuovo: anzitutto, nel 3.1 si dimostra che un  $T$ -modulo canonico  $M$  che sia equidimensionale (ossia tale che  $\dim pM = \dim M$ ) è anche un  $K$ -modulo libero finito; tale proprietà era stata enunciata senza dimostrazione in [16], ma limitatamente a quei  $T$ -moduli che sono legati a varietà gruppali equidimensionali (cfr. anche 7.2 e 7.4 di [14]); il 3.1 mostra invece che l'algebricità non ha nulla a che fare con la proprietà in questione. L'essere  $M$  un  $K$ -modulo libero finito suggerisce immediatamente una dualità  $\bullet$  (rispetto a  $K$ ) fra  $M$  ed un opportuno  $II$ -modulo canonico equidimensionale ( $II$  essendo l'antiisomorfo di  $T$ ), dualità che viene definita e studiata nei 3.2, 3.3, 3.4; essa è utilissima nelle applicazioni alle varietà abeliane (cfr. [14]), ma non è nè la più naturale nè la più generale; la dualità più generale (qui chiamata trasposizione e denotata con  $\circ$ ) richiede l'introduzione di un  $T$ -bimodulo sinistro e destro  $\mathcal{K}$ ; per una teoria generale di tali dualità vedasi [17] (la cui conoscenza non è però presupposta per la comprensione del presente lavoro). La trasposizione  $\circ$  vale per tutti i  $T$ -moduli canonici, e la relazione di  $\circ$  con  $\bullet$  è assai semplice, ed è descritta nel 3.10.

Il § 4 introduce le iperalgebre, gli ipercampi, e i gruppi analitici (commutativi); gran parte dei risultati di questo paragrafo sono sparsi nella letteratura (benchè la locuzione « ipercampo » sia nuova); si noti che i gruppi analitici vengono definiti effettivamente (come nei miei precedenti lavori) come insiemi di punti, e non come insiemi di leggi e coordinate. Nel § 4 si insiste sul fatto che tanto le iperalgebre, quanto i gruppi analitici, sono dei duali, opportunamente costruiti, degli ipercampi. Il 4.13, infine, non è altro che una definizione, ridotta ai minimi termini, delle iperalgebre.

Nel § 5 si affronta il problema della rappresentazione dei  $T$ -moduli canonici per mezzo di vettori di Witt « canonici », a componenti in iperalgebre; l'utilità di tali vettori canonici di Witt è stata menzionata nell'introduzione del [18], e qualche loro proprietà è stata descritta, senza dimostrazione, nel [16]; si veda a tal proposito anche il [14]. I risultati principali del § 5 sono i 5.2, 5.3, 5.7, 5.8. Nelle ultime pagine di questo paragrafo si ritrovano, in maniera semplicissima, le ben note descrizioni dei gruppi vettoriali, logaritmici, e di Witt (talvolta usate come definizioni).

Il § 6 interrompe la trattazione, e prepara uno strumento per il § 7, con l'introduzione di tre nuovi algoritmi sul tema dei vettori di Witt; l'ultimo fra questi ha applicazione diretta al § 7, ma il più importante per future applicazioni è l'operazione  $x \log \zeta$ , ove  $x$  è un vettore canonico di

Witt di iperderivazioni, e  $\zeta$  è un vettore di Witt (che nelle applicazioni sarà del tipo  $(\xi, 0, 0, \dots)$ ): come infatti è brevissimamente spiegato nel § 7 di [14], l'operazione  $x \log \zeta$  permette di considerare ogni ciclo  $X$  di dimensione massima su una varietà abeliana  $A$  come un omomorfismo  $d_\infty X$  del  $T$ -modulo dei vettori canonici di iperderivazioni invarianti su  $A$ , sul  $T$ -modulo canonico delle iperclassi chiuse di ripartizioni su  $A$ , modulo iperclassi esatte; la prima approssimazione  $dX$  (del tipo  $\xi^{-1} d\xi$ ) di  $d_\infty X$  è studiata in [18], e la possibilità di costruire  $d_\infty X$  è accennata nell'introduzione di [18]. La  $d_\infty X$ , oltre a rendere possibile l'enunciato di Picard-Severi (sulle singolarità logaritmiche di un differenziale di terza specie) in caratteristica  $p$ , dà una relazione funzionale fra una varietà abeliana e la propria varietà di Picard, relazione una cui prima approssimazione (e precisamente la  $dX$ ) ha permesso a Cartier di dimostrare il teorema di dualità [19]; cfr. anche il § 6 di [14]; e la stessa relazione funzionale permette di verificare l'identità (o meglio, la dualità) del trattamento di Serre [20] della coomologia su varietà abeliane (trattamento una cui prima approssimazione è quella di [18], rielaborata in [21]), con quello che si può ottenere usando le iperalgebre di Lie. Queste applicazioni, comunque, non vengono perseguite nella presente memoria.

Il § 7 descrive, per i  $\Pi$ -moduli canonici, una teoria della rappresentazione analoga a quella svolta nel § 5 per i  $T$ -moduli canonici; il metodo è però più rapido, potendosi esso avvalere della trasposizione introdotta al § 3; essenzialmente, si riescono ad isolare nell'ipercampo  $R = k\{G\}$  legato al gruppo analitico  $G$ , degli « elementi canonici » che si combinano in maniera preassegnata (ossia mediante i covettori di Witt introdotti alla fine del § 6). Una indicazione schematica delle relazioni fra  $T$ -moduli canonici,  $\Pi$ -moduli canonici, iperalgebre, ipercampi, e gruppi analitici, può essere la seguente:

$$\begin{array}{ccc} M & \overset{\circ}{\longleftarrow} & N \\ \sigma \downarrow & & \downarrow \tau \\ A & \overset{\circ}{\longleftarrow} & R \longleftrightarrow G; \end{array}$$

qui,  $M$  (risp.  $N$ ) è un  $T$ -modulo (risp.  $\Pi$ -modulo) canonico;  $A$  è un'iperalgebra,  $R$  un ipercampo,  $G$  un gruppo analitico; le frecce orizzontali rappresentano relazioni di dualità;  $\sigma$  (risp.  $\tau$ ) è un isomorfismo di  $M$  (risp. di  $N$ ) sul  $T$ -modulo (risp.  $\Pi$ -modulo) canonico di tutti i vettori (risp. covettori o anche elementi) canonici di Witt a componenti in  $A$  (risp. in  $R$ ).

Nell'indice delle definizioni che segue, accanto ad ogni termine o simbolo usato consistentemente in questa memoria, indichiamo la pagina in cui esso è definito; in tal modo possiamo evitare, nel corso delle dimostrazioni, eccessivi richiami alle definizioni.

## INDICE DELLE DEFINIZIONI E DEI SIMBOLI.

Algebra involupante libera	347	$G_{r,s}$	359
alt $h$	345	$G(R, \Omega)$	340
$A_r$	343, 344	$H$	348
$A_{r,s}$	359	$h(a)$	308
$A^+$	338	$h_i$	348
$A^*$	338	$In$	338
base strutturale	338	indecomponibile ( $T$ -modulo)	325
base strutturale iperesponen- ziale	350	inseparabilità	327, 354
$\mathcal{C}(A)$	351	invariante (iperderivazione)	342
campo involupante libero	368	inversione	344
codimensione (di iperalgebra o ipercampi)	359	iperalgebra	338
codimensione di un $T$ -modulo	325	ipercampo	339
concomitanti	352	iperderivazione	342
connullità	327, 354	isomorfismo analitico	340
covettore canonico di Witt	368	isomorfismo strutturale	338
covettore di Witt	366	isogene (iperalgebra)	354
$\mathcal{C}(R)$	368	isogeni (ipercampi)	359
$C'$	333	isogeni ( $T$ -moduli)	325
derivazione	342	$j(x)$	311
dimensione di un gruppo	340	$k$	308
dimensione di un'iperalgebra	338	$K$	308
dimensione di un ipercampo	339	$\mathcal{K}$	333
dimensione di un $T$ -modulo ca- nonico	317	$K'$	308
dimensione di un $T$ -modulo	310	$k\{G\}$	340
$\mathcal{D}(R)$	342	$k_n$	333
duale (di iperalgebra o iper- campo)	342	legati (omomorfismi)	340, 351
duale (di un $T$ -modulo)	330	legge di un ipercampo	339
$\mathcal{D}^+(R)$	342	legge su un gruppo	340
$e$	308	logaritmico	325, 359
$E_i$	348	lunghezza	320
elemento canonico di Witt	368, 371	$M_{r,q}$	323
equidimensionale	324, 359	$M_{-1}$ (dualità)	332
$F_{p,e,s}$	314	$M_{-1}$ (trasposizione)	336
$F_{p,s}$	315	nocciolo	358
gruppo analitico	340	$N_{r,s}$	336
		nullità	327, 354
		$O$	340
		omomorfismo analitico	340
		ordine (di iperalgebra o iper- campo)	359

ordine di un $T$ -modulo canonico	324	vettore canonico iperesponen-	351
ordine di un $T^*$ -modulo	310	ziale	
$p$	308	vettoriale (gruppo)	359
$P$ (di un'iper-algebra)	338	$W$	348
$P$ (di un ipercampo)	339	$\mathcal{O} \setminus \mathcal{O}'(A)$	347
periodico	325, 359	$w_i$	348
periodo	325	Witt (gruppo di)	360
$p$ -base	338	$w_n(x_0, \dots, x_n; \zeta_0, \dots, \zeta_n)$	366
$p$ -dipendenza	338	$\mathcal{O} \setminus \mathcal{O}'(R^+)$	366
punto di un gruppo	340	$x \log \zeta$	363
$R^+$	339	$x\zeta$	365
radicale	325, 359	$\gamma$	333
rappresentazioni	354	$\varepsilon(i)$	338
$R_{r,s}$	359	$\zeta(P)$	340
$r(x)$	311	$\varkappa$	308
semiomorfismo canonico di iperalgebra o ipercampi	340	$\mu$ (omomorfismo di un $T$ -modulo)	318
semiomorfismo canonico di $T$ -moduli	318	$\mu$ (per la trasposizione)	334
semplice ( $T$ -modulo)	325	$\pi$	317
separabile	358	$\pi$	347, 351, 368
simile	310	$\Pi$	329
somma di omomorfismi di gruppi	351	$\pi_0$	351, 352
sottogruppo analitico	341	$\Pi^*$	329
$s(x)$	311	$\Pi$ -modulo canonico	329
$t$	308	$\rho$	333
$t$	347, 351, 368	$\rho$	347
$T$	308	$\sigma_{-1}$ (dualità)	332
$T$ -modulo canonico	317	$\sigma_{-1}$ (trasposizione)	336
trasposto	336	$\tau$	333
$t_0$	351, 352	$\Phi$	366
$T^*$	308	$\omega$	308
$v(a)$	308	$\Omega$	339
vettore canonico di Witt	350	$\Omega^+$	339
vettore canonico di Witt di iperderivazioni	364	$\overline{\times}$	338
		$\times$	371
		$\bullet$	330
		$\circ$	334, 342, 369
		$\cdot$	371

**1. I  $T^*$ -moduli.** Sia  $p$  un numero primo (positivo), e sia  $K'$  un corpo avente le seguenti proprietà:

- 1)  $K'$  ha caratteristica 0;
- 2)  $K'$  è completo rispetto ad una valutazione discreta  $v$  di rango 1, che supporremo normalizzata, tale che  $v(p) = e > 0$ ;
- 3) il corpo residuo  $k$  di  $K'$  rispetto a  $v$ , che ha certa caratteristica  $p$ , è algebricamente chiuso;
- 4) esiste un elemento  $\omega \in K'$  tale che  $\omega^e = p$ , onde  $v(\omega) = 1$ .

Un  $K'$  con tali proprietà è completamente individuato, a meno di isomorfismi, quando siano dati  $k, p, e$ ; indicheremo con  $K$  la schiera valutante di  $v$ ; un  $K$  siffatto sarà detto una *schiera valutante  $p$ -adica, di ramificazione  $e$  (o non ramificata se  $e = 1$ )*, con corpo residuo  $k$ .

È noto che esiste un solo endomorfismo (di Frobenius)  $a \mapsto a^\times$  di  $K$  tale che  $\omega^\times = \omega$ , e che  $\mu(a^\times) = (\mu a)^p$ , se  $\mu$  indica l'omomorfismo naturale di  $K$  su  $k$ ; inoltre  $\kappa$  è un automorfismo di  $K$ . Detta  $t$  una indeterminata, costruiremo i  $K$ -moduli destri  $K\{t\} = T$  e  $K\{t\} = T^*$  delle serie formali di potenze in  $t$ , a coefficienti (a destra) in  $K$ , ad esponenti interi  $\geq 0$  nel primo caso, o soltanto interi nel secondo, con la convenzione però che in ogni elemento di  $T^*$  compaia solo un numero finito di potenze di  $t$  ad esponente negativo. I  $K$ -moduli  $T$  e  $T^*$  saranno trasformati in campi d'integrità (non commutativi) col porre  $at = ta^\times$  se  $a \in K$ ; l'automorfismo  $\kappa$  sarà esteso a  $T$  e  $T^*$  col porre  $(\sum_i t^i a_i)^\times = \sum_i t^i a_i^\times$ . In questo paragrafo studieremo i  $T^*$ -moduli (sinistri unitari) a torsione, seguendo da vicino la trattazione datane in [1].

Se  $0 \neq a = \sum_n t^n a_n \in T^*$ , con  $a_i \in K$  ed  $a_n \neq 0$ , porremo  $v(a) = v(a_n)$ ; porremo poi  $v(0) = \infty$ ; si constata subito che  $a$  è una unità di  $T^*$  se e solo se  $v(a) = 0$ ; invece  $a$  è una unità di  $T$  se e solo se  $v(a) = n = 0$ ; si ha poi sempre  $v(ab) = v(a) + v(b)$ . Definiremo anche l'intero  $h(a) \geq 0$  come il minimo  $i$  tale che  $v(a_{n+i}) \leq v(a_j)$  per ogni  $j$ ; e porremo di nuovo  $h(0) = \infty$ ; è  $h(a) = 0$  se e solo se  $a$  è divisibile, in  $T^*$ , per  $\omega^{v(a)}$ ; si ha inoltre  $h(ab) = h(a) + h(b)$ .

**1.1 LEMMA.** *Sia  $\mu$  l'omomorfismo naturale di  $K$  su  $k$ ; sia  $f_0(X_0, \dots, X_n)$  un polinomio, a coefficienti in  $K$ , lineare nelle indeterminate  $X_i$ , e pongasi  $\varphi_0(X) = \mu f_0(X)$ . Allora per ogni  $\xi_0 \in k$  tale che  $\varphi_0(\xi_0, \xi_0^p, \dots, \xi_0^{p^n}) = 0$ , esiste almeno un  $x \in K$  tale che  $\mu x = \xi_0$  e che  $f_0(x, x^\times, \dots, x^{\times^n}) = 0$ .*

DIM. Supporremo  $f_0(X) \neq 0$ , chè altrimenti il risultato è banale. Se  $x_0 \in K$  è tale che  $\mu x_0 = \xi_0$ , si ha  $f_0(x_0, x_0^*, \dots, x_0^{*n}) \equiv 0 \pmod{\omega K}$ ; quindi  $f_0(x_0 + \omega X_0, x_0^* + \omega X_1, \dots, x_0^{*n} + \omega X_n) = \omega f_1(X)$ , con  $f_1(X) \in K[X]$  lineare non costante, ovvero nullo; se  $\varphi_1(X) = \mu f_1(X) \in k[X]$ , esiste allora un  $x_1 \in K$  tale che, posto  $\xi_1 = \mu x_1$ , si abbia  $\varphi_1(\xi_1, \xi_1^*, \dots, \xi_1^{*n}) = 0$ , ossia  $f_1(x_1, x_1^*, \dots, x_1^{*n}) \in \omega K$ , o infine  $f_0(x_0 + \omega x_1, (x_0 + \omega x_1)^*, \dots, (x_0 + \omega x_1)^{*n}) \equiv 0 \pmod{\omega^2 K}$ . Così proseguendo, si ottiene un  $x = \sum_0^{\infty} \omega^i x_i$  tale che  $f_0(x, x^*, \dots, x^{*n}) \equiv 0 \pmod{\omega^r K}$  per ogni  $r$ , C. V. D.

1.2 LEMMA. *L'anello  $T^*$ , con l'applicazione  $a \rightarrow v(a)$ , è euclideo, ossia :*

1)  $v(ab) = v(a) + v(b)$ ;

2) se  $a, b \in T^*$ , con  $b \neq 0$ , esistono elementi  $q_i, r_i \in T^*$  tali che  $a = bq_1 + r_1 = q_2 b + r_2$ , ove o  $r_i = 0$ , o  $v(r_i) < v(b)$ .

*Come conseguenza, ogni ideale sinistro (risp. destro) di  $T^*$  è principale.*

DIM. La 1) è palese. Per dimostrare la 2), se  $a = \sum_0^{\infty} t^i A_i, A_i \in K, A_r \neq 0$ , e se  $v(a) = n$ , sia  $\omega^n t^r \alpha$  la somma di tutti i  $t^i A_i$  tali che  $v(A_i) \geq n$ ; allora  $\alpha$  è una unità di  $T$ , e  $a = \omega^n t^r \alpha + t^{r+1} a'$ , ove  $a' \in T$  e ogni termine  $t^i A'_i$  della serie di potenze  $a'$  è tale che  $v(A'_i) < n$ . Analogamente, se  $v(b) = m$ , si scriva  $b = \omega^m t^s \beta + t^{s+1} b'$ . Se  $m > n$ , o se  $a = 0$ , gli elementi  $q_2 = 0, r_2 = a$  soddisfano la condizione 2); altrimenti, pongasi  $a_1 = a - \omega^{n-m} t^{r-s} (\alpha \beta^{-1})^{*s} b$ . Si ha  $v(a_1) < n$  ovvero  $a_1 = 0$ ; nel primò caso, il processo si può ripetere su  $a_1$ , ecc., fino a trovare appunto  $a = q_2 b + r_2$ ; analogamente per  $q_1$  ed  $r_1$ , C. V. D.

Dati ancora  $a$  e  $b$  come in 1.2, con  $a \neq 0 \neq b$ , esistono un massimo comun divisore destro  $d$  di  $a, b$  tale che  $T^*a + T^*b = T^*d$ , ed un loro minimo comune multiplo sinistro  $c$  tale che  $T^*a \cap T^*b = T^*c$ ; come indicato in [2],  $d$  si trova col processo di divisioni successive

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\dots \\ r_n &= q_{n+2} d, \end{aligned}$$

e  $c$  può essere scelto nel modo seguente :

$$c = r_n d^{-1} r_{n-1} r_n^{-1} r_{n-2} r_{n-1}^{-1} \dots r_0 r_1^{-1} b r_0^{-1} a; \text{ pertanto}$$

1.3 LEMMA. Se  $a, b$  sono elementi non nulli di  $T^*$ , e  $T^*a + T^*b = T^*d$ ,  $T^*a \cap T^*b = T^*c$ , allora  $v(a) + v(b) = v(c) + v(d)$ , e  $h(a) + h(b) = h(c) + h(d)$ .

Si consideri un  $T^*$ -modulo (sinistro unitario) ciclico  $M$ , generato da un elemento  $\xi$ ; è ben noto che se  $T^*a$ , supposto  $\neq 0$ , è l'annullatore di  $\xi$ , allora  $M \cong T^*/T^*a$ ; inoltre è anche  $M \cong T^*/T^*b$  se e solo se  $b$  è simile ad  $a$  [3, Cap. 3, § 4], ossia se e solo se esiste un  $x \in T^*$  tale che  $T^*ax = T^*b \cap T^*x$  e  $T^*b + T^*x = T^*$ ; allora, per 1.3,  $v(a) = v(b)$  ed  $h(a) = h(b)$ , cosicchè gli interi positivi o nulli  $v(a), h(a)$  sono degli invarianti di  $M$ , detti rispettivamente la sua *dimensione* e il suo *ordine*. Se invece  $M$  è un qualsiasi  $T^*$ -modulo finito a torsione (ossia ogni cui elemento abbia annullatore non nullo), per la teoria dei divisori elementari [3, Cap. 3, § 8]  $M$  è somma diretta di un numero finito di  $T^*$ -moduli ciclici a torsione, che per il teorema di Krull-Schmidt possono essere supposti indecomponibili e unicamente determinati a meno di isomorfismi; pertanto la somma delle loro dimensioni (risp. ordini) è un invariante di  $M$ , detto ancora la *dimensione* (risp. l'*ordine*) di  $M$ ; si vede subito che la definizione è consistente (cfr. 1.5).

1.4 LEMMA. Il  $T^*$ -modulo sinistro  $M = T^*/T^*(\omega^r - ta)$ , ove  $r$  è un intero positivo ed  $a$  è una unità di  $T$ , è semplice (ossia privo di sotto- $T^*$ -moduli propri non nulli), e isomorfo al  $T^*$ -modulo  $T^*/T^*(\omega^r - t)$ .

DIM. Un sotto- $T^*$ -modulo di  $M$  è del tipo  $T^*x/T^*(\omega^r - ta)$ , ove  $\omega^r - ta = yx$  per un  $y \in T^*$ . Allora  $1 = h(\omega^r - ta) = h(y) + h(x)$ , onde o  $x$  o  $y$  è una unità di  $T^*$ ; quindi  $M$  è semplice. Si cerchi poi una unità  $x = \sum_0^\infty t^i X_i$  di  $T$ , con  $X_i \in K$ , tale che  $x(\omega^r - ta) = (\omega^r - t)x$ . Se  $a = \sum_0^\infty t^i A_i$ , tale  $x$  esiste se si possono trovare delle  $X_i \in K$ , con  $X_0 \notin K$ , tali che  $\sum_0^{i-1} X_{i-j-1}^{j+1} A_j = X_{i-1}$  ( $i = 1, 2, \dots$ ); e ciò è effettivamente possibile per 1.1. Allora l'applicazione  $z \rightarrow xzx^{-1}$  è un automorfismo di  $T^*$ , che trasforma  $T^*(\omega^r - ta)$  in  $T^*(\omega^r - t)$ . Pertanto  $M \cong T^*/T^*(\omega^r - t)$ , C. V. D..

Per comodità del lettore, dimostriamo il seguente risultato ben noto:

1.5 LEMMA. Se  $b, c$  sono elementi non nulli di  $T^*$ , il  $T^*$ -modulo  $M = T^*/T^*bc$  è somma diretta di  $N = T^*c/T^*bc \cong T^*/T^*b$  e di un'altro  $T^*$ -modulo  $P$  se e solo se esistono elementi  $x, y \in T^*$  tali che  $xb + cy = 1$ ; e in tal caso  $P \cong T^*(1 - yc)/T^*bc \cong T^*/T^*c$ .

DIM. Sia  $\xi$  l'immagine di 1 in  $M$ ; allora l'annullatore di  $\xi$  è  $T^*bc$ , e  $M = T^*\xi, N = T^*c\xi$ ; l'annullatore di  $c\xi$  è  $T^*b$ , onde  $N \cong T^*/T^*b$ . Se

$M = N \oplus P$ , è  $\xi = \xi_N + \xi_P$ , con  $\xi_N \in N$ ,  $\xi_P \in P$  perfettamente determinati, e  $\xi_P = d\xi$  per qualche  $d \in T^*$ ; si vede subito che  $\xi_P$  genera  $P$ , e che inoltre  $a\xi_P = 0$ , con  $a \in T^*$ , se e solo se  $a\xi \in N$ , ossia se e solo se  $a \in T^*c$ ; quindi  $P \cong T^*/T^*c$ . Da  $\xi = \xi_N + \xi_P$  si ricava che esiste un  $y \in T^*$  tale che  $1 - yc - d \in T^*bc$ ; ma  $d$  è determinato a meno di un elemento di  $T^*bc$ , onde si può supporre  $d = 1 - yc$ ; ed allora  $c(1 - yc)\xi = 0$ ,  $c(1 - yc) = xbc$ ,  $1 - cy = xb$ . Il ragionamento è invertibile, ossia: se  $xb + cy = 1$ , posto  $d = 1 - yc$ , si ha intanto  $N + T^*d\xi = M$ ; poi, se  $zc\xi = vd\xi \in N \cap T^*d\xi$ , è  $zc - vd = wbc$ ,  $zc - v + vyc = wbc$ ,  $v \in T^*c$ , onde  $vd \in T^*cd = T^*(c - cye) = T^*abc$ , e  $vd\xi = 0$ , ossia  $N \cap T^*d\xi = 0$ , C.V.D..

Sia ora  $x = X_0 + tX_1 + t^2X_2 + \dots$  ( $X_i \in K$ ) un elemento non nullo di  $T$ , con  $X_0 \neq 0$ ; se  $h(x) > 0$ , definiremo gli interi  $r = r(x) > 0$ ,  $s = s(x) > 0$ ,  $j = j(x) \geq 0$  nel modo seguente:

$r$  ed  $s$  sono primi fra loro e  $\leq h$ ;  $j < h$ ;

$$v(X_i) > (h - i)r/s \quad \text{se } i < j;$$

$$v(X_j) = (h - j)r/s;$$

$$v(X_i) \geq (h - i)r/s \quad \text{se } j < i < h.$$

**1.6 LEMMA.** *Sia  $a$  un elemento di  $T$  non divisibile (in  $T$ ) nè per  $\omega$  nè per  $t$ , e tale che  $h(a) > 0$  ed  $s(a) = 1$ . Allora esistono unità  $\alpha, \beta$  di  $T$  tali che  $a$  sia divisibile, in  $T$ , a sinistra per  $\omega^r - t\alpha$  e a destra per  $\omega^r - t\beta$ , avendo posto  $r = r(a)$ .*

**DIM.** Posto  $h(a) = h$ , sia  $j(a) = j$ , ed  $a = A_0 + tA_1 + \dots$ , con  $A_i \in K$ ; per  $i = 0, 1, \dots, h - 1$  esiste un  $B_i$  tale che  $A_i = \omega^{r(h-i)} B_i$ ; posto allora  $c = A_h + tA_{h+1} + \dots$ , per 1.1 esiste una unità  $x$  di  $T$  tale che

$$1.7 \quad xB_0 + x^r B_1 + \dots + x^{r(h-1)} B_{h-1} + x^{rh} c = 0,$$

dato che  $v(B_j) = v(c) = 0$ . Posto ancora  $y_0 = xB_0$ ,  $y_1 = y_0 + x^r B_1, \dots$ ,  $y_{h-1} = y_{h-2} + x^{r(h-1)} B_{h-1}$ , risulta  $y_{h-1} = -x^{rh} c$ , onde, se  $y = \omega^{r(h-1)} y_0 + \omega^{r(h-2)} t y_1 + \dots + t^{h-1} y_{h-1}$ , si ha  $(\omega^r - t)y = xa$ , e pertanto  $a = (\omega^r - t\alpha)b$ , con  $\alpha = x^{-r} x$  e  $b = x^{-1} y$ . In modo analogo si opera a destra, C.V.D..

**1.8 COROLLARIO.** *L'elemento  $a = (\omega^r - t\alpha)(\omega^s - t\beta)$ , con  $\alpha, \beta$  unità di  $T$ , è divisibile a destra, in  $T$ , per un elemento  $(\omega^r - t\gamma) \neq (\omega^s - t\beta)$ , con  $\gamma$  unità di  $T$ ; qui,  $r, s$  sono interi positivi.*

**DIM.** Si ha  $a = \omega^{r+s} - t(\omega^s \alpha + \omega^r \beta) + t^2 \alpha \beta$ , onde  $h(a) = 2$ ; inoltre,  $s(a) = 1$ , ed è applicabile l'1.6. Se  $r < s$ , è  $r(a) = r$ , ed  $a$  è divisibile a

destra per un  $\omega^r - t\gamma$ , certo diverso da  $\omega^s - t\beta$ . Se invece  $r > s$ , è  $r(a) = s$ , onde  $a$  è divisibile a sinistra per un  $\omega^s - tx$ , con  $x$  unità di  $T$ ; allora  $a = (\omega^s - tx)(\omega^r - t\gamma)$ , con  $\gamma$  unità di  $T$ , e certo  $\omega^r - t\gamma \neq \omega^s - t\beta$ . Sia infine  $s = r$ ; allora si può trovare un divisore destro  $\omega^r - t\gamma$  di  $a$ , diverso da  $\omega^r - t\beta$ , se la 1.7, applicata ad  $a$ , ha almeno due soluzioni  $x, x_1$  tali che  $\mu(x^{-1}x) \neq \mu(x_1^{-1}x_1)$ , ove  $\mu$  indica riduzione di  $T \bmod \omega T + tT$ . Ora, nelle notazioni di 1.7, e nel caso presente, si ha  $\mu B_0 = 1$ ,  $\mu B_1 = -\mu(\alpha + \beta)$ ,  $\mu\alpha = (\mu\alpha)^p \mu\beta$ ; il polinomio (nell'indeterminata  $X$ )

$$X - \mu(\alpha + \beta)X^p + (\mu\alpha)^p(\mu\beta)X^{p^2}$$

ha la derivata 1, onde non ha radici multiple, e possiede quindi  $p^2 > p$  radici tutte distinte; se  $X \neq 0$  è una di esse, ve ne è quindi un'altra,  $X_1$ , del tipo  $X\xi$  con  $\xi \in k$  ma  $\xi^p \neq \xi$ . Pertanto  $X_1^{-p}X_1 = \xi^{-p}\xi X^{-p}X \neq X^{-p}X$ ; l'1.1 completa la dimostrazione, C.V.D..

Nel seguito occorrerà considerare prolungamenti puramente ramificati di  $K$ ; più precisamente, se  $\varphi$  è elemento di una chiusura algebrica di  $K$ , tale che  $\varphi^s = \omega$  ( $s$  intero positivo), e se  $K' = K[\varphi]$ , anche  $K'$  è una schiera valutante  $p$ -adica con corpo residuo  $k$ , e su  $K'$  si possono costruire  $T' = T[\varphi]$  e  $T'^* = T^*[\varphi]$ , con la condizione  $\varphi^s = \omega$ . Indicheremo un  $\varphi$  siffatto semplicemente con  $\omega^{1/s}$ .

1.9 LEMMA. Sia  $a = x(\omega^{r_1} - t\alpha_1) \dots (\omega^{r_h} - t\alpha_h)$ , ove  $x, \alpha_1, \dots, \alpha_h$  sono unità di  $T$ , e gli  $r_i$  sono interi positivi; allora  $T^*/T^*a$  è isomorfo alla somma diretta dei  $T^*/T^*(\omega^{r_i} - t)$ .

DIM. Dimostriamo che  $M = T^*/T^*a$  è totalmente decomponibile, ossia somma diretta di un numero finito di  $T^*$ -moduli semplici; ciò equivale a dire che, per ogni sotto- $T^*$ -modulo  $N$  di  $M$ ,  $M$  è somma diretta di  $N$  e di un altro  $T^*$ -modulo [3, Cap. 1, § 6]. Ora, tale asserzione è vera se  $h = 1$ , per 1.4; suppostala vera per  $h - 1$ , sia, a norma dell'1.8,  $\omega^a - t\gamma$  un divisore destro di  $a$ , diverso da  $\omega^{r_h} - t\alpha_h$ . Posto  $a = b(\omega^a - t\gamma) = c(\omega^{r_h} - t\alpha_h)$ ,  $M$  contiene  $T^*(\omega^a - t\gamma)/T^*a \cong T^*/T^*b$  e  $T^*(\omega^{r_h} - t\alpha_h)/T^*a \cong T^*/T^*c$ , e ne è la somma perchè  $T^*(\omega^a - t\gamma)$  e  $T^*(\omega^{r_h} - t\alpha_h)$  sono ideali massimali sinistri (1.4) distinti. Poichè  $b$  e  $c$  sono fattorizzabili nello stesso modo di  $a$ , ma con  $h - 1$  fattori del tipo  $\omega^r - t\alpha$ ,  $T^*/T^*b$  e  $T^*/T^*c$  sono totalmente decomponibili, e quindi tale è  $T^*/T^*a$ . Una serie di fattori di una serie di composizione di  $M$  è data dai  $T^*/T^*(\omega^{r_i} - t\alpha_i) \cong T^*/T^*(\omega^{r_i} - t)$  (cfr. 1.4), e perciò il teorema di Krull-Schmidt dice appunto che gli addendi diretti di  $M$  sono isomorfi ai  $T^*/T^*(\omega^{r_i} - t)$ , C.V.D.

1.10 LEMMA. Il  $T^*$ -modulo  $T^*/T^*a$ , ove  $a \in T^*$  ma  $a \notin T^*\omega$ , è completamente decomponibile.

DIM. Si può supporre anche  $a \in T$ ,  $a \notin tT$ ,  $a \notin \omega T$ , ed escludere il caso banale in cui  $h(a) = 0$ , ossia in cui  $a$  è un'unità; sia  $s_1 = s(a)$ ; se  $a$  viene considerato come elemento di  $T[\omega^{1/s_1}]$ , è  $s(a) = 1$ , onde, per 1.6,  $a = a_1(\omega^{r_1/s_1} - t\alpha_1)$ , ed  $h(a_1) = h(a) - 1$  (computato in  $T$  o  $T[\omega^{1/s_1}]$ , chè non fa differenza); il processo può essere ripetuto su  $a_1$ , e così via; dopo  $h(a)$  volte,  $a$  assume, in  $T[\omega^{1/s}]$  per un  $s$  opportuno, la forma dell'1.9, e quindi  $T^*[\omega^{1/s}]/T^*[\omega^{1/s}]a$ , che è l'estensione su  $T^*[\omega^{1/s}]$  di  $M = T^*/T^*a$ , è completamente decomponibile. Per dimostrare che tale è anche  $M$ , a norma dell'1.5 basta dimostrare che se  $a = bc$ , con  $b, c \in T^*$ , esistono elementi  $x, y \in T^*$  tali che  $xb + cy = 1$ . Ora, tali  $x, y$  esistono certamente in  $T^*[\omega^{1/s}]$ , per esempio  $x = \sum_0^{s-1} \omega^{i/s} x_i, y = \sum_0^{s-1} \omega^{i/s} y_i, x_i, y_i \in T^*$ . Ma allora  $x_0 b + cy_0 = 1$ , C.V.D..

1.11 TEOREMA. Siano  $m, r, s$  interi positivi,  $r$  ed  $s$  essendo primi fra loro. Allora  $T^*/T^*\omega^m$  e  $T^*/T^*(\omega^r - t^s)$  sono  $T^*$ -moduli indecomponibili; il secondo è semplice, mentre l'unica serie di composizione del primo è data dai  $T^*\omega^i/T^*\omega^m \cong T^*/T^*\omega^{m-i}$  per  $i = 0, \dots, m$ . Viceversa, ogni  $T^*$ -modulo indecomponibile finito non libero e non nullo è isomorfo ad uno dei tipi descritti.

DIM. I sotto- $T^*$ -moduli di  $T^*/T^*\omega^m$  sono in corrispondenza biunivoca cogli ideali sinistri di  $T^*$  che contengono  $\omega^m$ ; se  $T^*x$  è uno di questi, sarà  $\omega^m = yx$ ; allora  $0 = h(\omega^m) = h(y) + h(x)$ , cosicchè  $x, y$  sono prodotti di potenze di  $\omega$  per unità di  $T^*$ ; ciò prova che ogni sotto- $T^*$ -modulo di  $T^*/T^*\omega^m$  è del tipo  $T^*\omega^i/T^*\omega^m$ , e prova anche che  $T^*/T^*\omega^m$  è indecomponibile.

Passando a considerare  $\omega^r - t^s$ , si ha intanto  $h(\omega^r - t^s) = s(\omega^r - t^s) = s, r(\omega^r - t^s) = r, j(\omega^r - t^s) = 0$ , onde, in  $T[\omega^{1/s}]$ ,  $\omega^r - t^s = a_1(\omega^{r/s} - t\alpha_1)$ , con  $\alpha_1$  unità di  $T[\omega^{1/s}]$  e  $a_1 \in T[\omega^{1/s}]$  (per 1.6); è ora  $h(a_1) = s - 1, j(a_1) = 0, s(a_1) = 1, r(a_1) = r$ , onde  $a_1 = a_2(\omega^{r/s} - t\alpha_2)$ , e così via; in conclusione, e per 1.9, l'estensione su  $T^*[\omega^{1/s}]$  di  $T^*/T^*(\omega^r - t^s)$  è somma diretta di  $s$   $T^*[\omega^{1/s}]$ -moduli indecomponibili isomorfi a  $T^*[\omega^{1/s}]/T^*[\omega^{1/s}](\omega^{r/s} - t)$ . Se  $T^*/T^*(\omega^r - t^s)$  non fosse semplice, si avrebbe per esempio  $\omega^r - t^s = bc$ , con  $b, c \in T$  e  $h(b), h(c)$  non nulli; allora  $h = s(c) < h(\omega^r - t^s) = s$ ; se  $l = r(c), c$  è divisibile a destra, in  $T[\omega^{1/h}]$ , per qualche  $\omega^{l/h} - t\beta$ , onde un elemento di una serie di fattori di una serie di composizione di  $T^*[\omega^{1/h}]/T^*[\omega^{1/h}](\omega^r - t^s)$  è isomorfo a  $T^*[\omega^{1/h}]/T^*[\omega^{1/h}](\omega^{l/h} - t)$ . Per quanto visto sopra, questo deve quindi essere isomorfo a  $T^*[\omega^{1/h}]/T^*[\omega^{1/h}](\omega^{r/s} - t)$ ; quindi  $\omega^{l/h} - t$  e  $\omega^{r/s} - t$  sono simili. Ciò comporta, per l'osservazione che segue l'1.3,  $l/h = r/s, ls = rh$ , impossibile perchè  $h < s$  ed  $r$  è primo con  $s$ ; ciò prova appunto che  $T^*/T^*(\omega^r - t^s)$  è semplice, e quindi indecomponibile.

Sia infine  $M \neq 0$  un  $T^*$ -modulo indecomponibile finito non libero; per la teoria dei divisori elementari, deve essere  $M \cong T^*/T^*a$ , con  $0 \neq a \in T^*$ , e si può supporre senz'altro  $a \in T$  ed  $a \notin tT$ . Se  $a \in \omega T$ , l'endomorfismo  $\xi \rightarrow \omega\xi$  di  $M$  non è un isomorfismo, onde, per il lemma di Fitting, per un opportuno  $n$  deve essere  $\omega^n M = 0$ , ossia  $\omega^n \in Ta$ ; ciò prova, come al principio di questa dimostrazione, che in tal caso  $a = \omega^m x$  ( $x$  unità di  $T$ ), e che perciò  $M \cong T^*/T^*\omega^m$ .

Sia dunque  $a \notin \omega T$ , e  $v(a) > 0$  (altrimenti  $M = 0$ ); se  $h = h(a)$ ,  $r = r(a)$ ,  $s = s(a)$ ,  $j = j(a)$ , è  $h > 0$ , e l'estensione  $M'$  di  $M$  su  $T^*[\omega^{1/s}]$ , considerata come  $T^*$ -modulo, è somma diretta degli  $s$   $T^*$ -moduli indecomponibili  $\omega^{i/s}M$  ( $i = 0, \dots, s-1$ ). D'altra parte, per 1.10 e 1.6,  $M'$ , come  $T^*[\omega^{1/s}]$ -modulo, è somma diretta di  $T^*[\omega^{1/s}]$ -moduli, uno dei quali è isomorfo a  $T^*[\omega^{1/s}]/T^*[\omega^{1/s}](\omega^{r/s} - t)$ . Nel caso particolare in cui  $a = \omega^r - t^s$ , ciò resta vero, ed il teorema di Krull-Schmidt applicato a questo caso ci dice che  $T^*[\omega^{1/s}]/T^*[\omega^{1/s}](\omega^{r/s} - t)$  è isomorfo, come  $T^*$ -modulo, a  $T^*/T^*(\omega^r - t^s)$ , ed è quindi semplice. Tornando allora al caso di  $a$  arbitrario, e sfruttando questo fatto, di nuovo il teorema di Krull-Schmidt implica che ogni  $\omega^{i/s}M$ , e in particolare  $M$ , è isomorfo, come  $T^*$ -modulo, a  $T^*/T^*(\omega^r - t^s)$ , C.V.D..

**1.12 COROLLARIO.** *Sia  $M$  un  $T^*$ -modulo finito a torsione; allora  $M$  è somma diretta di un numero finito di  $T^*$ -moduli dei tipi  $T^*/T^*\omega^m$  e  $T^*/T^*(\omega^r - t^s)$ , con  $m, r, s$  interi positivi, ed  $r, s$  primi fra loro. È poi  $T^*/T^*(\omega^r - t^s) \cong T^*/T^*(\omega^h - t^l)$ , con  $r, s, h, l$  interi positivi, se e solo se  $r = h$  ed  $s = l$ .*

**DIM.** La prima asserzione è conseguenza di 1.11 e della teoria dei divisori elementari; l'ultima asserzione discende dal fatto che se  $a, b$  sono elementi simili di  $T^*$ , allora, per 1.3,  $v(a) = v(b)$  ed  $h(a) = h(b)$ , C.V.D..

Ricordiamo che, dati l'intero  $e$  (tale che  $\omega^e = p$ ), ed un intero  $s > 0$ , esiste un solo corpo  $F = F_{p,e,s}$  (a meno di isomorfismi) che goda delle seguenti proprietà:  $F$  ha caratteristica 0, è completo rispetto ad una valutazione  $v$  discreta normalizzata di rango 1, e contiene un elemento  $\omega$  tale che  $\omega^e = p$  e  $v(\omega) = 1$ ; inoltre  $[F : K_p] = es$ , ove  $K_p$  indica il completamento del corpo razionale  $K$  secondo la valutazione  $p$ -adica. Il corpo  $F_{p,e,s}$  coincide con  $K_p[\zeta_s, \omega]$ , ove  $\zeta_s$  è una radice primitiva  $(p^s - 1)$ -esima dell'unità (in caratteristica 0); il corpo residuo di  $F_{p,e,s}$ , modulo la valutazione  $v$ , è  $C_p[\zeta'_s]$ , ove  $C_p$  è il corpo fondamentale di caratteristica  $p$ , e  $\zeta'_s$  è una radice primitiva  $(p^s - 1)$ -esima dell'unità (in caratteristica  $p$ );  $C_p[\zeta'_s]$  è caratterizzato dal fatto che  $x^{p^s} = x$  per ogni suo elemento  $x$ , ma  $x^{p^{s-1}} \neq x$  per qualche suo elemento  $x$ . Il corpo  $F_{p,e,s}$  possiede un solo endomorfismo  $\kappa$  (di Frobenius) su  $K_p[\omega]$ , tale che  $\zeta_s^\kappa = \zeta_s^p$ ; l'endomorfismo  $\kappa$  è un automorfismo, e genera il

gruppo di Galois di  $F_{p,e,s}$  su  $R_p[\omega]$ . Il corpo  $F_{p,1,s}$  si indicherà semplicemente con  $F_{p,s}$ .

Si consideri poi l' $F_{p,e,s}$ -modulo libero  $A$  generato da  $s$  elementi  $\tau^0, \tau = \tau^1, \tau^2, \dots, \tau^{s-1}$ ;  $A$  diviene un'algebra su  $R_p[\omega]$ , contenente  $F_{p,e,s}$  come sottoalgebra, se si identifica  $x\tau^0$  con  $x$  ( $x \in F_{p,e,s}$ ), e si definisce  $\tau^i\tau = \tau\tau^i = \tau^{i+1}$  se  $0 \leq i < s-1$ ,  $\tau^{s-1}\tau = \tau\tau^{s-1} = \omega^r$  ( $r$  intero positivo),  $\tau x = x^r\tau$  se  $x \in F_{p,e,s}$ ; l'algebra  $A$  non è altro che l'algebra ciclica  $(F_{p,e,s}, \tau, \omega^r)$ , che è semplice normale (= centrale) su  $R_p[\omega] = F_{p,e,1}$ , di grado  $s$  (e ordine  $s^2$ ). Essa è un'algebra divisoria se e solo se  $r$  è primo con  $s$  (cfr. [4, 5]).

Ciò premesso, si ha:

1.13 TEOREMA. *Sia  $M \neq 0$  un  $T^*$ -modulo ciclico a torsione, generato da un suo elemento  $\xi$  di annullatore  $T^*\omega^m$ , ovvero  $T^*(\omega^r - t^s)$ , a seconda dei casi ( $m, r, s$  interi positivi). Nel primo caso, l'anello degli endomorfismi di  $M$  è isomorfo a  $K''\{\tau\}$ , ove  $K'' = K/K\omega^m$  e  $\tau$  è una indeterminata su  $K''$  tale che  $\tau x = x^r\tau$  se  $x \in K''$ ; si ha precisamente  $\tau\xi = t\xi$ , e  $x\xi = y\xi$  se  $x \in K''$  e  $y$  è un elemento di  $K$  la cui immagine è  $x$ . Nel secondo caso, l'anello degli endomorfismi di  $M$  è isomorfo all'algebra  $(F_{p,e,s}, \tau, \omega^r) = F_{p,e,s}[\tau]$ , ove  $\tau^s = \omega^r$ ,  $\tau x = x^r\tau$  se  $x \in F_{p,e,s}$ ; si ha precisamente  $\tau\xi = t\xi$ ,  $x\xi = x\xi$  se  $x \in F_{p,e,s} \cap K$ .*

DIM. Sia  $A$  l'anello degli endomorfismi in questione; per ogni  $z \in A$ ,  $z\xi$  è elemento di  $M$ , ed è quindi della forma  $x\xi$ ; si consideri dapprima il caso dell'annullatore  $T^*\omega^m$ : in tal caso ad ogni  $x \in T^*$  corrisponde uno  $z \in A$  tale che, per ogni  $a \in T^*$ , si abbia  $z(a\xi) = ax\xi$ ; l'applicazione  $x \rightarrow z$  è un omomorfismo di gruppi addittivi, di nucleo  $T^*\omega^m$ , ed è tale che se  $x \rightarrow z$  e  $x' \rightarrow z'$ , allora  $zz'(a\xi) = z(ax'\xi) = ax'x\xi$ , ossia  $x'x \rightarrow zz'$ ; se perciò  $t \rightarrow \tau$ , si ha  $A \cong (K/K^m)\{\tau\}$ , con  $\tau x = x^r\tau$  quando  $x \in K/K\omega^m$ .

Si consideri ora il caso dell'annullatore  $T^*(\omega^r - t^s)$ ; se nuovamente  $z \in A$ , e se  $z\xi = x\xi$ , si deve avere  $x^{rs}t^s\xi = t^sx\xi = t^sz\xi = zt^s\xi = z\omega^r\xi = \omega^rz\xi = \omega^rx\xi = x\omega^r\xi = xt^s\xi$ , e pertanto  $(x^{rs} - x)t^s$ , e quindi  $x^{rs} - x$ , è elemento di  $T^*(\omega^r - t^s)$ , per esempio  $x^{rs} - x = a(\omega^r - t^s)$ ; ma è certo  $a = y^{rs} - y$  per un opportuno  $y \in T^*$  (per 1.1), onde, posto  $x' = x - y(\omega^r - t^s)$ , si ha  $x'^{rs} - x' = 0$ , e  $x'\xi = x\xi = z\xi$ . Quindi ad ogni  $z \in A$  corrisponde almeno un  $x \in T^*$  tale che  $z\xi = x\xi$ , e che  $x^{rs} = x$ ; se  $I_{p,e,s}$  è l'anello degli interi di  $F_{p,e,s}$ , considerato come sottoanello di  $K$ , l'ultima condizione indica che  $x \in I_{p,e,s}\{t\}$ . Viceversa, dato un  $x \in I_{p,e,s}\{t\}$ , ad esso corrisponde lo  $z \in A$  tale che  $z(a\xi) = ax\xi$ , ed è  $z = 0$  se e solo se  $x$  appartiene all'ideale bilatero  $I_{p,e,s}\{t\}(\omega^r - t^s)$  di  $I_{p,e,s}\{t\}$ . L'applicazione  $x \rightarrow z$  è di nuovo un omomorfismo di gruppi addittivi, e se  $x \rightarrow z$  e  $x' \rightarrow z'$ , si ha ancora che  $x'x \rightarrow zz'$ ; pertanto  $A$  è isomorfo ad  $I_{p,e,s}\{\tau\}$ , ove  $\tau$  soddisfa la  $\tau x = x^r\tau$  se  $x \in I_{p,e,s}$ . D'altra parte, le  $\tau^0 = 1, \tau, \tau^2, \dots, \tau^{s-1}$  sono linearmente indipendenti su

$I_{p,e,s}$ , mentre  $\tau^s = \omega^r$ ; quindi ogni potenza ad esponente negativo di  $\tau$  è combinazione lineare delle  $1, \tau, \dots, \tau^{s-1}$  a coefficienti in  $F_{p,e,s}$ , ed è anzi  $F_{p,e,s} \subseteq I_{p,e,s} \{\tau\}$ ; quindi  $A \cong I_{p,e,s} \{\tau\} = F_{p,e,s} [\tau] = (F_{p,e,s}, \alpha, \omega^r)$ , C.V.D.

In vista delle applicazioni è utile il risultato seguente:

**1.14 TEOREMA.**  $T^*/T^*(\omega^r - t^{2r})$  è isomorfo alla somma diretta di  $r$   $T^*$ -moduli isomorfi a  $T^*/T^*(\omega - t^2)$ .

**DIM.** Posto  $\omega^r - t^{2r} = \bar{a}$ , è  $h(a) = 2r, s(a) = r, r(a) = 1, j(a) = 0$ ; pertanto, come nella dimostrazione di 1.11,  $T^*[\omega^{1/2}]/T^*[\omega^{1/2}]a$  è isomorfo alla somma diretta di  $2r$   $T^*[\omega^{1/2}]$ -moduli isomorfi a  $T^*[\omega^{1/2}]/T^*[\omega^{1/2}](\omega^{1/2} - t)$ ; questo, a sua volta, si è visto (nella dimostrazione dell'1.11) essere isomorfo, come  $T^*$ -modulo, a  $T^*/T^*(\omega - t^2)$ , che è indecomponibile. Quindi ogni sotto- $T^*$ -modulo indecomponibile della estensione su  $T^*[\omega^{1/2}]$  di  $T^*/T^*(\omega^r - t^{2r})$  è isomorfo a  $T^*/T^*(\omega - t^2)$ , C.V.D..

**2. T-moduli canonici.** In questo paragrafo,  $K, T, T^*$ , ecc. manterranno gli stessi significati che hanno nel § 1. Un  $T$ -modulo finito  $M$  dicesi *canonico* se:

$$2.1 \quad \omega M \subseteq tM;$$

$$2.2 \quad \text{se } x \in M \text{ e } tx = 0, \text{ allora } x = 0.$$

Il minimo intero  $n$  tale che  $M$  sia generato da  $n$  suoi elementi dicesi la *dimensione* di  $M$ .

**2.3 LEMMA.** *Un  $T$ -modulo finito  $M$  è canonico se e solo se esso è un sotto- $T$ -modulo di un  $T^*$ -modulo, e soddisfa la 2.1; ed in tal caso il  $T^*$ -modulo  $T^*M$  è a torsione, ed  $M$  soddisfa la  $\bigcap_1^\infty t^i M = 0$ .*

**DIM.** Si noti che con la notazione  $T^*M$  si indica l'estensione di  $M$  su  $T^*$ , ossia il prodotto tensoriale  $T^* \otimes M$  di  $T$ -moduli, considerato come  $T^*$ -modulo. Se  $M$  è canonico, la 2.2 implica che l'estensione  $T^*M$ , considerata come  $T$ -modulo, contiene un sotto- $T$ -modulo isomorfo ad  $M$ . Viceversa se  $M$  è sotto- $T$ -modulo di un  $T^*$ -modulo  $M^*$ , esso soddisfa la 2.2, ed è quindi canonico se soddisfa la 2.1.

Posto  $\pi = t^{-1}\omega \in T^*$  (notazione che manterremo sempre nel seguito), ed,  $M^* = T^*M$ , la 2.1 implica che  $\pi$  è un semiendomorfismo di  $M$ , e che  $M$  è un  $T[\pi]$ -modulo; se  $M^*$  non fosse a torsione,  $M$  conterrebbe un elemento  $x$  con annullatore nullo; detto  $H$  l'insieme degli  $a \in T^*$  tali che  $ax \in M$ ,  $H$  è un  $T$ -modulo sinistro, finito perchè l'applicazione  $a \rightarrow ax$  è un isomorfismo di  $H$  su  $M$ , e contenente  $T[\pi]$ . Quindi  $\pi$  è «intero su  $T$ », ossia: per un opportuno  $n > 0$  si ha  $\pi^n = \sum_0^{n-1} a_i \pi^i, a_i \in T$ ; ma allora  $\omega^n = t^n \pi^n \in tT$ , assurdo. Ciò prova che  $M^*$  è a torsione.

Sia infine  $x$  un elemento di  $\bigcap_1^\infty t^i M$ ; allora la catena ascendente  $Tx \subseteq \subseteq Tt^{-1}x \subseteq Tt^{-2}x \subseteq \dots \subseteq M$  deve essere tale che il segno  $=$  vale da un certo punto in poi:  $t^{-r}x = t^{-r+1}ax$ , con  $a \in T$ . Pertanto  $(1 - ta)x = 0$ , e quindi  $x = 0$  perchè  $1 - ta$  è unità di  $T$ , C.V.D..

2.4 LEMMA. *Sia  $M$  un  $T$ -modulo canonico, e sia  $\mu$  il semiomomorfismo naturale di  $M$  su tutto il  $k$ -modulo  $M/tM$ ; allora gli  $x_1, \dots, x_r \in M$  generano  $M$  se e solo se i  $\mu x_i$  generano  $\mu M$ .*

DIM. Se gli  $x_i$  generano  $M$ , i  $\mu x_i$  certamente generano  $\mu M$ . Viceversa, suppongasi che i  $\mu x_i$  generino  $\mu M$ , e sia  $y \in M$ ; per opportuni  $a_i \in K$  è  $\mu y = \sum_i (\mu a_i) (\mu x_i)$ , ove  $\mu$  è stato interpretato anche come l'omomorfismo naturale di  $K$  su  $k$ . Allora  $y - \sum_i a_i x_i \in tM$ , e per esempio  $y = \sum_i a_i x_i + t y_1$ ; lo stesso ragionamento, applicato ad  $y_1$ , dà  $y - \sum_i (a_i + t b_i) x_i \in t^2 M$  per opportuni  $b_i \in K$ . Così proseguendo, si ottiene un elemento  $y' = \sum_i (a_i + t b_i + t^2 c_i + \dots) x_i$  tale che  $y - y' \in t^r M$  per ogni  $r$ ; quindi, per 2.3,  $y = y'$ , C.V.D.

Da 2.4 segue che la dimensione di  $M$  coincide con l'ordine del  $k$ -modulo libero  $M/tM$  («ordine» di un modulo libero significa, al solito, la potenza di un suo insieme libero di generatori).

Un semiomomorfismo  $\sigma$  di un  $T$ -modulo  $M$ , tale che  $\sigma(ax) = a^\sigma \sigma x$  ( $a \in T, x \in M$ ), dicesi *canonico* se l'applicazione  $a \rightarrow a^\sigma$  è un automorfismo di  $T$  che lascia  $\omega$  e  $t$  invariati; si ha:

2.5 TEOREMA. *Sia  $M$  un  $T$ -modulo canonico di dimensione  $n$ , e sia  $\sigma$  un semiomomorfismo canonico di  $M$ , di nucleo  $N$ ; allora:*

1)  $\sigma M$  è canonico se e solo se  $N \cap tM = tN$ , nel qual caso  $N$  è canonico;

2) se la 1) è soddisfatta, allora  $\dim N + \dim \sigma M = n$ .

Se invece  $N$  è un qualsiasi sotto- $T$ -modulo di  $M$ , tale che  $\omega N \subseteq tN$ ,  $N$  è canonico di dimensione  $\leq n$ ,  $l'$  = valendo se e solo se  $t^r M \subseteq N$  per qualche intero positivo  $r$ .

DIM. Se  $\sigma M$  è canonico, e se  $x \in N \cap tM$ , e per esempio  $x = ty$  con  $y \in M$ , si ha  $t\sigma y = t^\sigma \sigma y = \sigma(ty) = \sigma x = 0$ , onde  $\sigma y = 0$ ,  $y \in N$ ; perciò  $N \cap tM = tN$ , donde segue (per 2.1) che  $N$  è canonico. Viceversa, se  $N \cap tM = tN$ , intanto  $N$  è canonico; se poi  $x \in M$ , è  $\omega \sigma x = \omega^\sigma \sigma x = \sigma(\omega x) \in \sigma tM = t\sigma M$ , che è la 2.1 per  $\sigma M$ ; poi, se  $t\sigma x = 0$ , è  $\sigma(tx) = 0$ ,  $tx \in N \cap tM = tN$ ,  $x \in N$ ,  $\sigma x = 0$ , che è la 2.2 per  $\sigma M$ . Quindi  $\sigma M$  è canonico, e la 1) è dimostrata.

Supposta verificata la 1), sia  $n = \dim N$ , e sia  $\{x_1, \dots, x_n\}$  un insieme di generatori di  $N$ ; se  $\mu$  ha (per  $M$ ) il significato del 2.4, dico intanto che i  $\mu x_i$  sono linearmente indipendenti su  $k$ . Se così non fosse, e se per esempio  $\mu x_n = \sum_1^{n-1} (\mu a_i) (\mu x_i)$ ,  $a_i \in T$ , si avrebbe  $x_n = \sum_1^{n-1} a_i x_i + x'$ ,  $x' \in tN$ ; allora  $x' = \sum_1^{n-1} b_i t x_i + b_n t x_n$ ,  $b_i \in T$ . Posto  $a_i + b_i t = c_i$ , sarebbe  $x_n = \sum_1^{n-1} c_i x_i + b_n t x_n$ ,  $x_n = (1 - b_n t)^{-1} \sum_1^{n-1} c_i x_i$ , contro l'ipotesi che  $n = \dim N$ .

Visto allora che i  $\mu x_i$  sono linearmente indipendenti su  $k$ , ne segue, per 2.4, che l'insieme  $\{x_1, \dots, x_n\}$  può essere completato in un insieme  $\{x_1, \dots, x_m\}$  di generatori di  $M$ ; allora i  $\sigma x_{n+1}, \dots, \sigma x_m$  generano  $\sigma M$ , dal che si deduce che  $h = \dim \sigma M \leq m - n$ . D'altra parte, se i  $\sigma y_i$  ( $i = 1, \dots, h$ ) generano  $\sigma M$ , gli  $x_1, \dots, x_n, y_1, \dots, y_h$  generano  $M$ , onde  $n + h \geq m$ , e infine  $n + h = m$ , che è la 2).

Sia infine  $N$  un sotto- $T$ -modulo di  $M$  tale che  $\omega N \subseteq tN$ ; esso è canonico per 2.1; posto  $N' = M \cap T^*N$ , si ha  $N' \cap tM = tM \cap T^*N = tN'$ , onde, per 1) e 2),  $N'$  è canonico di dimensione  $n' \leq m$ . Se dimostriamo che  $n' = \dim N$ , l'ultima asserzione dell'enunciato resta dimostrata. Possiamo quindi porci senz'altro nel caso speciale in cui  $N' = M$ , ossia  $t^r M \subseteq N$  per qualche  $r$ ; sia anzi  $r$  il minimo per cui ciò vale. Sia poi  $s$  il massimo intero tale che  $N \subseteq t^s M$ , cosicchè  $s \leq r$ ; pongasi  $S_0 = \mu t^{-s} N$ ,  $S_1 = \mu t^{-s-1} (N \cap t^{s+1} M)$ ,  $\dots$ ,  $S_h = \mu t^{-r} (N \cap t^r M) = \mu M$ , se  $h = r - s$ . È  $S_0 \subseteq S_1 \subseteq \dots \subseteq S_h$ ; se  $d_0 = \text{ord } S_0$ , e  $d_i = \text{ord } S_i - \text{ord } S_{i-1}$  ( $i = 1, \dots, h$ ), siano  $t^s x_{01}, \dots, t^s x_{0d_0}$  elementi di  $N$  tali che i  $\mu x_{0j}$  formino una base di  $S_0$ ; siano poi, per  $0 < i \leq h$ ,  $t^{s+i} x_{i1}, \dots, t^{s+i} x_{id_i}$  elementi di  $N$  tali che i  $\mu x_{ij}$ ,  $\mu x_{1j}, \dots, \mu x_{ij}$  formino una base di  $S_i$ . Dico che i  $t^s x_{0j}, t^{s+1} x_{1j}, \dots, t^r x_{hj}$  (in numero di  $m$ ) formano un insieme di generatori di  $N$ , il che proverà che  $n \leq m$ , e che quindi  $m \leq n$  dato che  $t^q N \subseteq t^r M$  per qualche  $q$ .

Se dunque  $y$  è un elemento di  $N$ , ed  $y \in t^r M$ ,  $y$  è certo combinazione lineare, a coefficienti in  $T$ , dei  $t^r x_{0j}, \dots, t^r x_{hj}$ , dato che questi, per 2.4, generano  $t^r M$ . Se invece  $y$  appartiene ad  $N \cap t^{s+l} M$  ma non a  $t^{s+l+1} M$  (ove  $0 \leq l < h$ ),  $y$  è combinazione lineare dei  $t^{s+l} x_{0j}, \dots, t^{s+l} x_{lj}$  e dei  $t^{s+l+1} x_{l+1,j}, \dots, t^{s+l+1} x_{hj}$ , ed è quindi somma di una combinazione lineare dei  $t^{s+l} x_{0j}, \dots, t^{s+l} x_{lj}$  e di un elemento di  $N \cap t^{s+l+1} M$ ; la conclusione segue quindi per ricorrenza su  $l$  (cominciando da  $l = h$ ), C.V.D..

Si noti che quest'ultima parte della dimostrazione implica il

**2.6 TEOREMA.** *Sia  $M$  un  $T$ -modulo canonico di dimensione  $m$ , e sia  $N$  un suo sotto- $T$ -modulo canonico di dimensione  $n$ . Esistono allora degli insiemi di generatori  $\{x_1, \dots, x_m\}$ ,  $\{y_1, \dots, y_n\}$  di  $M, N$  rispettivamente, tali che, in notazioni matriciali,  $y = Vx$ , ove  $V$  è una matrice di tipo  $n \times m$  della forma*

$$V = \left( \begin{array}{ccc|c} t^{s_1} I_1 & & & 0 \\ & t^{s_2} I_2 & & \\ & & \ddots & \\ & & & t^{s_\nu} I_\nu \end{array} \right),$$

ove  $0 \leq s_1 < s_2 < \dots < s_\nu$ , e ove  $I_j$  è la matrice identica di un certo ordine  $d_j$ . Gli interi  $s_j, d_j, \nu$  sono unicamente determinati, e si ha  $\sum_j d_j = n$ .

Nelle notazioni di 2.6, se  $\dim N = \dim M$ , l'intero  $\sum_i s_i d_i$  si chiamerà la *lunghezza* di  $M/N$ .

**2.7 TEOREMA.** *Sia  $N$  un sotto- $T$ -modulo canonico del  $T$ -modulo canonico  $M$ , e suppongasi  $\dim N = \dim M = m$ . Sia  $l$  la lunghezza di  $M/N$ ; allora ogni catena  $N = H_0 \subset H_1 \subset \dots \subset H_r = M$  di  $T$ -moduli può essere raffinata in una per la quale  $r = l$ ; ma nessuna catena può essere raffinata in una per cui  $r > l$ . E se la data catena è tutta costituita di  $T$ -moduli canonici, fra i suoi raffinamenti non raffinabili ve n'è almeno uno tutto costituito da  $T$ -moduli canonici.*

**DIM.** Basta dimostrare che se  $l = 1$  non vi è nessun  $T$ -modulo  $P$  tale che  $N \subset P \subset M$ , e che se  $l > 1$  vi è un  $T$ -modulo canonico  $P$ , con  $N \subset P \subset M$ , tale che  $\text{lung} M/P < l$ ,  $\text{lung} P/N < l$ , e  $\text{lung} P/N + \text{lung} M/P = l$ .

Sia dunque  $l = 1$ , sicchè si può trovare un insieme  $\{x_1, \dots, x_m\}$  di generatori di  $M$  tale che  $\{tx_1, x_2, \dots, x_m\}$  generi  $N$ ; allora  $M/N$  è un  $K$ -modulo, dato che  $tx \in N$  per ogni  $x \in M$ , ed è anzi un  $k$ -modulo, dato che  $\omega M \subseteq tM \subseteq N$ ; esso è quindi un  $k$ -modulo libero generato dall'immagine di  $x_1$ , che non è nulla. Perciò non vi è nessun  $P$  tale che  $N \subset P \subset M$ .

Sia ora  $l > 1$ , e sia  $\{x_1, \dots, x_m\}$  un insieme di generatori di  $M$  tale che un insieme di generatori di  $N$  sia dato da  $t^{s_1}x_1, t^{s_2}x_2, \dots, t^{s_m}x_m$ , con  $s_1 \geq s_2 \geq \dots \geq s_m \geq 0$ ; sia, per esempio,  $s_1 = s_2 = \dots = s_h = s$ , mentre  $s_{h+1} < s_h$ . Essendo  $l > 1$ , si deve avere o  $s > 1$ , ovvero  $s = 1$  ed  $h > 1$ ; nel primo caso il  $T$ -modulo  $P$  generato da  $t^{s-1}x_1, \dots, t^{s-1}x_h, t^{s_h+1}x_{h+1}, \dots, t^{s_m}x_m$  è certamente canonico, e si ha  $N \subset P \subset M$ ,  $\text{lung} P/N = h < l$ ,  $\text{lung} M/P = l - h < l$ , come richiesto.

Resta il caso in cui  $s = 1$ , nel qual caso  $s_{h+1} = \dots = s_m = 0$  ed  $l = h$ ; posto allora  $S = M/N$ , e detto  $\sigma$  il semiomomorfismo naturale di  $M$  sul  $k$ -modulo  $S$ , definiremo  $\pi\sigma x = \sigma x$  per  $x \in M$ , e distingueremo due sottocasi:

*Sottocaso 1:* il semiendomorfismo  $\pi$  di  $S$  non è un semiautomorfismo; allora, per il lemma di Fitting, esiste un  $x \in M$  tale che  $\sigma x \neq 0$  ma  $\pi\sigma x = 0$ , e tale  $x$  può essere supposto combinazione lineare di  $x_1, \dots, x_h$  a coefficienti ciascuno dei quali è o 0, o una unità di  $K$ . Non vi è quindi perdita di generalità nel supporre  $x = x_1$ ; ed allora, il  $P$  generato da  $x_1, tx_2, \dots, tx_h, x_{h+1}, \dots, x_m$  è canonico, e soddisfa le  $N \subset P \subset M$ ,  $\text{lung} P/N = 1 < l$ ,  $\text{lung} M/P = h - 1 < l$ .

*Sottocaso 2:* il semiendomorfismo  $\pi$  di  $S$  è un semiautomorfismo; scelta una combinazione lineare  $y_1$  delle  $x_1, \dots, x_h$  tale che  $\eta_1 = \sigma y_1 \neq 0$ , siano le  $\eta_i = \pi^{i-1} \eta_1$  ( $i = 1, \dots, r$ ) linearmente indipendenti su  $k$ , e sia invece

$\pi\eta_r = \sum_1^r a_i \eta_i$ ,  $a_i \in k$ , ove certo  $a_i \neq 0$  per qualche  $i$ . Scelto un  $b_r \in k$  non nullo, tale che  $b_r = b_r^{p^r} a_1^{p^{r-1}} + b_r^{p^{r-1}} a_2^{p^{r-2}} + \dots + b_r^p a_r$ , e posto  $b_i = b_r^{p^i} a_1^{p^{i-1}} + b_r^{p^{i-1}} a_2^{p^{i-2}} + \dots + b_r^p a_i$  ( $i = 1, \dots, r-1$ ),  $\eta' = \sum_1^r b_i \eta_i$ , si ha  $\pi\eta' = \sum_1^r b_i^p \pi\eta_i = \sum_1^{r-1} b_i^p \eta_{i+1} + b_r^p \sum_1^r a_i \eta_i = b_r^p a_1 \eta_1 + \sum_2^r (b_{i-1}^p + b_r^p a_i) \eta_i = b_1 \eta_1 + \sum_2^r b_i \eta_i = \eta'$ . Esiste quindi una combinazione lineare  $y$  delle  $x_1, \dots, x_n$ , a coefficienti o nulli o unità di  $K$ , tale che  $\sigma\pi y = \sigma y \neq 0$ ; supposto che  $x_1$  abbia già tale proprietà, il  $P$  generato da  $x_1, tx_2, \dots, tx_n, x_{h+1}, \dots, x_m$  è canonico, e gode delle proprietà  $N \subset P \subset M$ ,  $\text{lung} P/N = 1 < l$ ,  $\text{lung} M/P = h-1 < l$ , C. V. D..

Si ha la seguente ulteriore caratterizzazione dei  $T$ -moduli canonici:

**2.8 TEOREMA.** *Sia  $M$  un  $T$ -modulo finito, e suppongasì che esistano un suo insieme di generatori  $\{x_1, \dots, x_n\}$ , ed una matrice  $C$ , quadrata di ordine  $n$  ad elementi in  $T$ , tali che: posto  $x = (x_1 \dots x_n)_{-1}$ , è  $ax = 0$  ( $a = (a_1 \dots a_n)$ ;  $a_i \in T$ ) se e solo se  $a = b(tC - \omega)$  per un opportuno  $b = (b_1 \dots b_n)$ ,  $b_i \in T$ . Allora  $M$  è canonico di dimensione  $n$ , e si ha  $\pi x = Cx$ .*

*Reciprocamente, se  $M$  è canonico di dimensione  $n$ , la proprietà descritta vale per ogni suo insieme di generatori  $\{x_1, \dots, x_n\}$  e per ogni  $C$  tale che  $\pi x = Cx$ .*

**DIM. I** — Siano  $x$  e  $C$  come detto; allora  $\omega x = tCx$ , onde  $\omega M \subseteq tM$ , che è la 2.1. Poi, se  $y \in M$ , per esempio  $y = ax$  con  $a$  ad elementi in  $T$ , e se  $ty = 0$ , si ha  $tax = 0$ , onde, per un opportuno  $b$ ,  $ta = b(tC - \omega)$ ; quindi  $b = tb'$ , con  $b'$  ad elementi in  $T$ , e  $a = b'(tC - \omega)$ , e perciò  $y = ax = 0$ ; ciò dimostra la 2.2 e prova che  $M$  è canonico di dimensione  $\leq n$ . Se  $\mu$  ha lo stesso significato come nel 2.4, per dimostrare che  $\dim M = n$  basta dimostrare che le  $\mu x_i$  sono linearmente indipendenti su  $k$ . Ora, se  $(\mu a)(\mu x) = 0$ , è anche  $ax = tdx$  per qualche  $d = (d_1 \dots d_n)$  con  $d_i \in T$ ; allora  $(a - td)x = 0$ ,  $a - td = b(tC - \omega)$ ,  $a_i \in tT + \omega T$ ,  $\mu a_i = 0$ , come annunciato.

**II** — Sia ora  $M$  canonico di dimensione  $n$ , e sia  $\{x_1, \dots, x_n\}$  un suo insieme di generatori; allora  $\{x_1, \dots, x_n\}$  è un insieme di generatori di  $M^* = T^*M$ ; e poichè  $T^*$  è a ideali sinistri principali, esiste una matrice  $A$ , ad elementi in  $T^*$ , tale che  $ax = 0$  se e solo se  $a = bA$  ( $a, b$  ad elementi in  $T^*$ ); la  $A$  può essere scelta ad elementi in  $T$ , e precisamente del tipo  $A = A_0 + tA_1 + t^2A_2 + \dots$ , con  $A_i$  ad elementi in  $K$  ed  $A_0 \neq 0$ . La  $A'$  ottenuta da  $A$  dividendo a sinistra una riga per  $t^r$  ( $r$  intero non

negativo), se ciò è possibile in  $T$ , gode della stessa proprietà; una tale  $A'$  si dirà *dedotta da*  $A$ ; della stessa proprietà di  $A$  gode anche una  $A'$  del tipo  $UA$ , con  $U$  matrice invertibile in  $T$ ; una tale  $A'$  si dirà *equivalente a sinistra ad*  $A$  in  $T$ ; infine, della stessa proprietà di  $A$ , ma rispetto ad un altro insieme di generatori di  $M$ , gode  $A' = AU$ , con  $U$  come sopra; una tale  $A'$  si dirà *equivalente a destra ad*  $A$  in  $T$ .

Indicheremó con  $S_0$  l'insieme delle matrici ottenute da  $A$  mediante applicazioni successive di deduzioni ed equivalenze in  $T$ ; per ogni  $A' \in S_0$  esiste una  $B = B_0 + tB_1 + \dots$ , equivalente ad  $A'$  in  $T$ , tale che

$$B_0 = \begin{pmatrix} \omega^{s_1} & & & & \\ & \omega^{s_2} & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \omega^{s_n} \end{pmatrix}, \text{ ove } 0 \leq s_1 \leq s_2 \leq \dots \leq s_n \leq \infty, \text{ intendendosi che}$$

$\omega^\infty$  significhi 0; gli  $s_i$  sono univocamente determinati da  $A'$ , e saranno quindi indicati con  $s_i(A')$ . Sia allora  $A^1 \in S_0$  tale che  $s_1(A^1) \leq s_1(A')$  per ogni  $A' \in S_0$ ; se  $S_1$  è l'insieme di tali  $A^1$ , sia  $A^2 \in S_1$  tale che  $s_2(A^2) \leq s_2(A')$  per ogni  $A' \in S_1$ , ecc.. La matrice  $A^n$  sarà indicata ancora con  $A$ , e la si supporrà già tale che

$$2.9 \quad A_0 = \begin{pmatrix} \omega^{s_1} & & & & \\ & \omega^{s_2} & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \omega^{s_n} \end{pmatrix}, \quad s_i = s_i(A^i).$$

Vogliamo dimostrare che  $s_n < \infty$ ; supposto ciò falso, sia  $r$  il minimo  $j$  tale che  $s_j = \infty$ , e sia  $\{a_1, \dots, a_r\}$  l' $r$ -esima riga di  $A_1$ . Vi è una  $B$  dedotta da  $A$  tale che

$$B_0 = \begin{pmatrix} \omega^{s_1} & & & & & & \\ & \cdot & & & & & \\ & & \cdot & & & & \\ & & & \omega^{s_{r-1}} & & & \\ a_1 & \dots & a_{r-1} & a_r & \dots & a_n & \\ & & & & 0 & & \\ & & & & & \cdot & \\ & & & & & & 0 \end{pmatrix};$$

per la proprietà di cui gode  $A$ , deve essere  $s_i \leq v(a_i)$  ( $i = 1, \dots, r-1$ ), ed  $a_r = \dots = a_n = 0$ , cosicchè esiste una  $U_1$ , invertibile in  $K$ , tale che  $B_0 = U_1 A_0$ ; pertanto l' $r$ -esima riga di  $A_1 - B_0 = A_1 - U_1 A_0$  è nulla, ed  $A$  è equivalente a sinistra, in  $T$ , alla  $(1 - tU_1)A = A_0 + t(A_1 - U_1 A_0) + \dots$ ,

nella quale ogni elemento dell' $r$ -esima riga è divisibile a sinistra, in  $T$ , per  $t^2$ . Operando su  $(1 - tU_1)A$  come si è fatto su  $A$  (ma usando  $A_2$  in luogo di  $A_1$ ), e così via, si ottiene una  $D = \dots(1 - t^3U_3)(1 - t^2U_2)(1 - tU_1)A$  equivalente a sinistra ad  $A$ , e la cui  $r$ -esima riga è nulla. Ma  $D$  è equivalente, in  $T^*$ , ad  $A$ , e quindi fra i divisori elementari di  $A$  (come matrice ad elementi in  $T^*$ ) ve ne è almeno uno che è nullo; ciò comporta che  $M^*$  possiede un elemento ad annullatore nullo, il che è impossibile per 2.3. Resta così provato che, per opportuna scelta di  $\{x_1, \dots, x_n\}$ , si può supporre che  $A$  sia tale che valga la 2.9, con  $s_n < \infty$ .

Poichè, per la 2.1,  $\omega x = tCx$ , con  $C$  matrice ad elementi in  $T$ , si ha  $(tC - \omega)x = 0$ , onde  $tC - \omega = BA$ , con  $B$  ad elementi in  $T^*$ . Ma allora, per la proprietà di  $A$  testè dimostrata, si deve avere  $B = B_0 + tB_1 + \dots$ , con  $B_i$  ad elementi in  $K$  e  $B_0A_0 = -\omega$ , donde  $s_n \leq 1$ . Se fosse  $s_1 = 0$ , la relazione  $(1 \ 0 \ \dots \ 0)Ax = 0$  implicherebbe

$(1 + t\alpha_1 + t^2\alpha_2 + \dots)x_1 \in \sum_2^n tTx_i$  ( $\alpha_i \in K$ ), e  $\{x_2, \dots, x_n\}$  sarebbe un insieme di generatori di  $M$ , assurdo. Quindi  $s_1 = \dots = s_n = 1$ ,  $A_0 = \omega$ , ed  $A = \omega + tA'$ . Si è così dimostrato che se  $M$  è canonico di dimensione  $n$ , esistono un suo insieme di generatori  $\{x_1, \dots, x_n\}$ , ed una matrice  $B$ , tali che  $ax = 0$  se e solo se  $a = b(tB - \omega)$  ( $a, b, B$  ad elementi in  $T$ ).

III — Sia, nelle notazioni precedenti,  $\{y_1, \dots, y_n\}$  un qualsiasi insieme di generatori di  $M$  (di potenza  $n$ ), e sia  $C$  una qualsiasi matrice tale che  $\pi y = Cy$ ; è  $y = Vx$ ,  $x = Uy$ , onde  $x = UVx$ ,  $1 - UV = Z(tB - \omega)$ , cosicchè  $U_0V_0 \equiv 1 \pmod{\omega K}$ , e  $V$  è invertibile in  $T$ ; perciò  $y = Vx$  ed  $x = V^{-1}y$ . Se  $ay = 0$ , è  $aVx = 0$ ,  $aV = b(tB - \omega)$ ,  $a = b'(tB' - \omega)$ , ove  $b' = bV^{-1}$ , e  $B' = V^*BV^{-1}$ , e reciprocamente. Poi,  $Cy = \pi y = B'y$ ,  $C - B' = Z(tB' - \omega)$ ,  $tC - \omega = (1 + tZ)(tB' - \omega)$ ; essendo  $1 + tZ$  invertibile in  $T$ , ciò comporta che  $ay = 0$  se e solo se  $a = d(tC - \omega)$  per qualche  $d$ , C.V.D..

Indicheremo con  $M_{r,q}$  ( $r$  intero positivo,  $q$  intero non negativo oppure  $q = \infty$ ) il  $T$ -modulo canonico di dimensione  $r$  la cui matrice  $C$  (nelle notazioni del 2.8) è

$$C = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ t^q & 0 & 0 & \dots & 0 \end{pmatrix}$$

(tipo  $r \times r$ , con  $C = t^q$  se  $r = 1$ ), ove  $t^0 = 1$  e  $t^\infty = 0$ . La  $tC - \omega$  è

equivalente, in  $T^*$ , a

$$\begin{pmatrix} t & 0 & 0 & \dots & 0 & -\omega \\ -\omega & t & 0 & \dots & 0 & 0 \\ 0 & -\omega & t & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & t & 0 \\ 0 & 0 & 0 & \dots & -\omega & t^{q+1} \end{pmatrix},$$

ed a

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 & -\omega t^{-1} \\ 0 & 1 & 0 & \dots & 0 & -\omega^2 t^{-2} \\ 0 & 0 & 1 & \dots & 0 & -\omega^3 t^{-3} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & -\omega^{r-1} t^{-r+1} \\ 0 & 0 & 0 & \dots & 0 & t^q - \omega^r t^{-r} \end{pmatrix},$$

e finalmente a

$$\begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & 1 & & \\ & & & & & \omega^r - t^{r+q} \end{pmatrix},$$

il che dimostra che

$$T^*M_{r,q} \cong T^*/T^*(\omega^r - t^{r+q}).$$

Sia  $M$  un qualsiasi  $T$ -modulo canonico; posto, in 2.6,  $N = \omega M$ , l'intero  $\sum_i s_i d_i$  se  $\dim M = \dim N$ , ovvero  $\infty$  se  $\dim M > \dim N$ , sarà chiamato l'ordine di  $M$  ( $= 0$  per definizione se  $M = 0$ );  $M$  dicesi *equidimensionale* se  $\dim M = \dim N$ , ossia se ha ordine finito. Si vede allora da quanto precede che  $\dim M_{r,q} = r = \dim T^*M_{r,q}$ , e che  $\text{ord } M_{r,q} = r + q = \text{ord } T^*M_{r,q}$  se  $q \neq \infty$ , mentre  $\text{ord } M_{r,q} = \infty = r + q$  se  $q = \infty$ , ossia se  $\text{ord } T^*M_{r,q} = 0$ .

**2.10 TEOREMA.** *Sia  $M^*$  un  $T^*$ -modulo finito a torsione; condizione necessaria e sufficiente acchè esista un  $T$ -modulo canonico  $M$  tale che  $M^* = T^*M$  è che per ogni sotto- $T^*$ -modulo semplice  $N^*$  di  $M^*$  valga una delle condizioni  $\text{ord } N^* = 0$  ovvero  $\text{ord } N^* \geq \dim N^*$ . E se è così, si ha  $\dim M = \dim M^*$ ,  $\text{ord } M = \infty$  se  $M^*$  possiede sotto- $T^*$ -moduli non nulli di ordine 0, ed  $\text{ord } M = \text{ord } M^*$  altrimenti. Se poi  $M$  è canonico, e  $\sigma$  è un suo semiomomorfismo canonico di nucleo  $N$  sul  $T$ -modulo canonico  $\sigma M$ , è  $\text{ord } M = \text{ord } N + \text{ord } \sigma M$ ; se infine  $N$  è un qualsiasi sotto- $T$ -modulo canonico di  $M$ , è  $\text{ord } N \leq \text{ord } M$ ,  $l' =$  valendo se e solo se  $trM \subseteq N$  per qualche intero positivo  $r$ .*

**Dim.** Escluderemo il caso  $M^* = 0$ , per il quale tutte le asserzioni sono immediatamente verificabili. Sia  $M^* = T^*M$  con  $M$  canonico, e sia  $x$  un elemento di  $M$  che generi un sotto- $T$ modulo semplice non nullo  $N^*$  di  $M^*$ ; per 1.11, si può supporre che l'annullatore di  $x$  sia o  $T^*\omega$ , nel qual caso  $\text{ord } N^* = 0$ , ovvero  $T^*(\omega^r - t^s)$ , con  $r, s$  primi fra loro. Nel secondo caso è  $t^{s-r}x = t^{-r}\omega^r x = \pi^r x \in M$ , onde  $t^{i(s-r)}x \in M$  per ogni intero positivo  $i$ ; quindi, per 2.3,  $s \geq r$ , ossia  $\text{ord } M^* \geq \dim M^*$ , come richiesto.

Suppongasi ora che  $M^*$  soddisfi la condizione enunciata; allora, per 1.11 e 1.12,  $M^*$  è somma diretta di  $T^*$ -moduli indecomponibili dei tipi  $T^*M_{r,\infty}$ ,  $T^*M_{r,q}$  ( $r, q$  primi fra loro),  $T^*M_{1,0}$ ; pertanto  $M^* = T^*M$ , ove  $M$  è somma diretta di  $T$ -moduli canonici dei tipi  $M_{r,\infty}$ ,  $M_{r,q}$ ,  $M_{1,0}$ .

Se  $M^* = T^*M$ , per 2.5 la dimensione di  $M$  dipende solo da  $M^*$ , e coincide quindi con  $\dim M^*$  perchè ciò è vero quando  $M$  è somma diretta di  $T$ -moduli dei tipi  $M_{r,q}$ . Lo stesso ragionamento vale per  $\text{ord } M$  se si dimostra che  $\text{ord } M$  dipende solo da  $M^*$ . Sia quindi  $N$  un sotto- $T$ modulo canonico di  $M$ , tale che  $T^*N = M^* = T^*M$ ; se  $\dim \omega M < \dim M$ , da  $\omega N \subseteq \omega M$  segue  $\dim \omega N < \dim N = \dim M$ ; quindi  $\text{ord } M = \infty$  implica  $\text{ord } N = \infty$ , e reciprocamente. Se invece  $M$  è equidimensionale, è  $t^r M \subseteq N$ ,  $t^r \omega M \subseteq \omega N$ , onde  $N$  è equidimensionale; poi, per 2.7,  $\text{lungh } M/N + \text{ord } N = \text{lungh } M/\omega N = \text{ord } M + \text{lungh } \omega M/\omega N = \text{ord } M + \text{lungh } M/N$ , onde  $\text{ord } N = \text{ord } M$ . Questo dimostra tutte le asserzioni dell'enunciato, C.V.D..

L'espressione  $\text{ord } M - \dim M$  si dirà la *codimensione di  $M$* ; essa è  $\infty$  se  $M$  non è equidimensionale, mentre se  $M$  è equidimensionale la sua codimensione coincide con  $\text{lungh } M/\pi M$ , ed è finita; in particolare,  $\text{codim } M_{r,q} = q$ ;  $M$  dicesi *periodico* se  $\omega^r M = 0$ , o, il che è lo stesso,  $\pi^r M = 0$  per qualche intero non negativo  $r$ ; se  $s$  è il minimo tale  $r$ ,  $\omega^s$  è il *periodo di  $M$* ;  $M$  dicesi *logaritmico* se  $\text{codim } M = 0$ , ossia se  $\pi M = M$ ; dicesi *radicale* se  $\pi^r M \subseteq tM$  per qualche intero positivo  $r$ ; dicesi *semplice* se non possiede sotto- $T$ -moduli canonici non nulli di dimensione  $< \dim M$ ; dicesi *indecomponibile* se tale è  $T^*M$ . Due  $T$ -moduli canonici  $M, N$  sono *isogeni* se ciascuno di essi è isomorfo ad un sotto- $T$ modulo dell'altro; per 2.5,  $M$  ed  $N$  sono isogeni se e solo se  $\dim M = \dim N$ , ed  $N$  è isomorfo ad un sotto- $T$ modulo di  $M$ .

**2.11 TEOREMA.** 1) Ogni  $T$ -modulo canonico è somma diretta di uno logaritmico ed uno radicale, unicamente determinati;

2) un  $T$ -modulo canonico di dimensione  $r > 0$  è logaritmico se e solo se è isomorfo ad  $M_{r,0}$ ; in tal caso esso è somma diretta di  $r$   $T$ -moduli isomorfi ad  $M_{1,0}$ ;

3) sia  $M$  un  $T$ -modulo canonico radicale; dette  $E, P$  le unioni di tutti i sotto- $T$ -moduli rispettivamente equidimensionali e periodici di  $M$ ,  $E$  è equidimensionale e  $P$  è periodico; inoltre  $M$  è isogeno ad  $E \oplus P$ ;

4) ogni  $T$ -modulo equidimensionale radicale non nullo è isogeno alla somma diretta di  $T$ -moduli radicali equidimensionali semplici non nulli; ciascuno di questi è isogeno ad un  $M_{r,q}$ , con  $r, q$  primi fra loro;

5) ogni  $T$ -modulo periodico non nullo è isogeno alla somma diretta di  $T$ -moduli del tipo  $M_{r,\infty}$ .

**DIM.** Per 1.12, 1.11 e 2.10,  $M$  è isogeno alla somma diretta di  $T$ -moduli dei tipi  $M_{r,q}$ , ove  $r, q$  soddisfano ad una delle condizioni seguenti: a)  $r = 1, q = 0$ ; b)  $r, q$  interi primi fra loro; c)  $r$  intero positivo,  $q = \infty$ . Se indichiamo con  $L, R$  le somme dirette degli  $M_{r,q}$  dei tipi a), e b) o c) rispettivamente, si può supporre  $M \subseteq L \oplus R$ . Pongasi  $L' = L \cap M, R' = R \cap M$ ; allora  $\text{codim } L' = \text{codim } L = 0$ , onde  $L'$  è logaritmico; invece, per  $r$  elevato,  $\pi^r R' \subseteq \pi^r R \subseteq tR'$ , onde  $R'$  è radicale. Un  $x \in M$  appartiene ad  $R'$  se e solo se per ogni  $s > 0$  esiste un  $r$  tale che  $\pi^r x \in t^s M$ ; invece  $L' = \bigcap_0^\infty \pi^r M$ ; infine, se  $x \in M$ , ed  $x = x_L + x_R$  con  $x_L \in L, x_R \in R$ , per  $s$  elevato si ha  $\pi^s x_R \in R'$ , onde  $\pi^s x_L = \pi^s x - \pi^s x_R \in M \cap L = L'$ ; quindi  $x_L \in L', x_R \in R'$ , ed  $M = L' \oplus R'$ , che dimostra la 1).

Se  $M$  è logaritmico, ossia se, nelle notazioni precedenti,  $M = L'$ , e se  $\mu$  ha, per  $M$ , il significato attribuitogli nel 2.4, si può, come nella dimostrazione del sottocaso 2 del 2.7, trovare un insieme minimo di generatori  $\{x_1, \dots, x_n\}$  di  $M$  tali che  $\pi \mu x_1 = \mu x_1$ ; poi si possono trovare facilmente degli  $x'_i = x_i + a_i x_1$  ( $a_i \in K; i = 2, \dots, n$ ) tali che  $\pi \mu x'_i \in \sum_2^n k \mu x'_j$ , cosicchè il  $k$ -modulo  $S$  generato dalle  $\mu x'_i$  soddisfa ancora (come  $\mu M$ ) la relazione  $\pi S = S$ , e si può trovare un  $x'_2$  con la proprietà  $0 \neq \pi \mu x'_2 = \mu x'_2 \in S$ , ecc.. In conclusione, si può trovare un insieme di generatori  $\{y_1, \dots, y_n\}$  di  $M$  tale che  $\pi y_i \equiv y_i \pmod{tM}$ ; ed allora si può applicare l'1.1 per trovare delle combinazioni lineari  $z_i$  degli  $y_j$ , a coefficienti in  $K$ , tali che  $\pi(y_i + tz_i) \equiv y_i + tz_i \pmod{t^2 M}$ , ecc.; infine, si giunge a costruire un insieme di generatori  $(u_1, \dots, u_n)$  di  $M$  con la proprietà  $\pi u_i = u_i$ , ed allora  $M = Tu_1 \oplus \dots \oplus Tu_n$ , con  $Tu_i = M_{1,0}$ ; questo si applica in particolare ad  $M = M_{r,0}$ , e dimostra la 2).

Le 3), 4), 5) si dimostrano analogamente, ma in maniera così semplice che non vale la pena di esporla, C.V.D.

**2.12 TEOREMA.** *Nelle notazioni di 1.13, l'anello degli endomorfismi di  $M_{r,\infty}$  è isomorfo a  $K''[\tau][\tau^{-1}\omega]$ ; invece l'anello degli endomorfismi di  $M_{r,q}$  ( $q$  finito) è isomorfo alla schiera di  $A = (F_{p,e,r+q}, \nu, \omega^r)$  generata, sulla schiera  $S$  degli interi di  $F_{p,e,r+q}$ , da  $\tau$  e  $\tau^{-1}\omega$ . Se  $r, q$  sono primi fra loro, oppure se  $r = 1$  e  $q = 0$ , questa è contenuta nella schiera massima  $R$  di  $A$  su  $S$ ,*

e coincide con  $R$  se e solo se o  $r = 1$ , ovvero  $q = 1$ ; nel primo caso è  $R = S[\tau]$ , e nel secondo caso è  $R = S[\tau^{-1}\omega]$ .

**DIM.** Eccetto le asserzioni contenute nell'ultima frase, è tutto conseguenza di 1.13, e del fatto che  $M_{r,q}$  e  $M_{r,\infty}$  sono  $T[\pi]$ -moduli ciclici; basta quindi dimostrare le asserzioni contenute nell'ultima frase.

Posto  $F = F_{p,e,r+q}$ , è noto [4, 5] che  $R$  è totalmente ramificata su  $S$  (essendo  $A$  divisoria), cosicchè se  $w$  è la valutazione normalizzata di  $A$  che estende la  $v$  di  $F$ , è  $w(\omega) = r + q$ , e perciò  $w(\tau) = r$ . Si scelgano i minimi interi non negativi  $\alpha, \beta$  tali che  $\alpha(r + q) = \beta r + 1$ ; allora un elemento di  $w$ -valore 1 è  $\omega^\alpha \tau^{-\beta}$ , e quindi  $R = S[\omega^\alpha \tau^{-\beta}]$ . Possono ora darsi tre casi:

1.  $r = 1$ , nel qual caso  $\alpha = 1$  e  $\beta = q$ ; allora  $R = S[\omega \tau^{-q}] = S[\omega \tau \omega^{-1}] = S[\tau]$ , e quindi  $R = S[\tau, \tau^{-1}\omega]$ ;

2.  $q = 1$ , nel qual caso  $\alpha = \beta = 1$ ; allora  $R = S[\omega \tau^{-1}]$ , che uguaglia appunto  $S[\tau, \tau^{-1}\omega]$ ;

3.  $r > 1$  e  $q > 1$ ; in tal caso si constata subito che  $\alpha < r$ ,  $\alpha < \beta < r + q$ ; dico allora che  $S[\tau, \tau^{-1}\omega]$  non contiene  $\omega^\alpha \tau^{-\beta}$ ; chè se infatti  $\omega^\alpha \tau^{-\beta} = \omega^{-(r-\alpha)} \tau^{r+q-\beta-1}$  fosse combinazione lineare, a coefficienti in  $S$ , di  $1, \tau, \tau^2, \dots, \tau^{r+q-1}, \tau^{-1}\omega, (\tau^{-1}\omega)^2, \dots, (\tau^{-1}\omega)^{r+q-1}$ , esso dovrebbe essere combinazione lineare di  $\tau^{r+q-\beta-1}$  e di  $(\tau^{-1}\omega)^\beta = \omega^{\beta-r} \tau^{r+q-\beta-1}$ ; essendo  $r - \alpha > 0$ , ciò comporterebbe  $r - \alpha \leq r - \beta$ ,  $\alpha \geq \beta$ , che si è visto essere falso, C.V.D..

Da 1.14 si ha subito:

**2.13 TEOREMA.**  $M_{r,r}$  è isogeno alla somma diretta di  $r$   $T$ -moduli canonici isomorfi ad  $M_{1,1}$ .

Vi sono alcuni invarianti che sono collegati ad un semiomorfismo canonico  $\sigma$  di un  $T$ -modulo canonico  $M$  su un  $T$ -modulo canonico  $P$ ; intanto, per 2.5, il nucleo  $N$  di  $\sigma$ , e il  $T$ -modulo  $\sigma M$  sono canonici; è canonico anche il  $T$ -modulo  $Q = P \cap T^*(\sigma M)$ . La  $\dim N = \dim M - \dim \sigma M$  sarà chiamata la *nullità di  $\sigma$* ; poi,  $\dim Q = \dim \sigma M$ , e quindi esiste l'intero  $l = \text{lungh } Q/\sigma M$ ; l'elemento  $\omega^l \in K$  sarà detto l'*inseparabilità di  $\sigma$* ; esso è 1 se e solo se  $Q = \sigma M$ , ossia, per 2.5, se e solo se  $P/\sigma M$  è canonico. L'intero  $\dim P - \dim M$  si dirà la *conullità di  $\sigma$* . Se  $\text{conull } \sigma = 0$ , e  $\tau$  è un semiomorfismo canonico di  $P$ , si ha  $\text{null } \tau \sigma = \text{null } \tau + \text{null } \sigma$ ; se invece  $\sigma$  è arbitrario, e  $\tau$  è tale che  $\text{null } \tau = 0$ , si ha  $\text{conull } \tau \sigma = \text{conull } \tau + \text{conull } \sigma$ ; se infine entrambe le condizioni sono verificate, ossia se  $\text{conull } \sigma = \text{null } \tau = 0$ , si ha  $\text{ins } \tau \sigma = (\text{ins } \tau)(\text{ins } \sigma)$ . In generale, e per 2.7,  $\sigma$  può essere decomposto nel modo seguente:

$$2.14 \quad M \xrightarrow{\varphi} M/N = H \xrightarrow{\varepsilon} Q_0 = \sigma M \xrightarrow{e_1} Q_1 \xrightarrow{e_2} \dots \xrightarrow{e_l} Q_l = Q \xrightarrow{\tau} P,$$

ove :

$\varphi, \varrho_i, \tau$  sono omomorfismi ;  $\varepsilon$  è un semiomomorfismo ;  
null  $\varphi =$  null  $\sigma$  , conull  $\varphi = 0$  , ins  $\varphi = 1$  ;  
null  $\varepsilon =$  conull  $\varepsilon = 0$  , ins  $\varepsilon = 1$  ;  
null  $\varrho_i =$  conull  $\varrho_i = 0$  , ins  $\varrho_i = \omega$  ;  
null  $\tau = 0$  , conull  $\tau =$  conull  $\sigma$  , ins  $\tau = 1$  .

**3. Dualità.** A questo punto è utile fare un'osservazione: ricordiamo che nel § 2 si è definito  $\pi = t^{-1} \omega$ ;  $\pi$  soddisfa la relazione  $\pi a = a^* \pi$  se  $a \in K$ . Si può quindi dare una traduzione di tutto ciò che si è fatto fin qui dopo aver cambiato  $t$  in  $\pi$ ,  $\pi$  in  $t$ , e  $\kappa$  in  $\kappa^{-1}$ ; esiste perciò una teoria dei  $\Pi^*$ -moduli e dei  $\Pi$ -moduli canonici (sinistri) analoga a quella dei  $T^*$ -moduli e dei  $T$ -moduli canonici; qui, si è posto  $\Pi^* = K\{\pi\}$ ,  $\Pi = K\{\pi\}$ ; ci proponiamo di sviluppare in questo paragrafo dei legami fra le due teorie.

**3.1 TEOREMA.** *Sia  $M$  un  $T$ -modulo canonico di dimensione  $m$  e codimensione  $n$ ; allora:*

1) *se  $n = \infty$ , ossia se  $M$  non è equidimensionale,  $M$ , considerato come  $K$ -modulo od anche come  $K[t]$ -modulo, non è nè libero nè finito;*

2) *se  $M$  è equidimensionale, siano  $x_1, \dots, x_{m+n}$  elementi di  $M$  (certo esistenti) le cui immagini, in  $M/\omega M$ , generano il  $k$ -modulo  $M/\omega M$ ; allora  $M$  è un  $K$ -modulo un cui insieme libero di generatori è  $\{x_1, \dots, x_{m+n}\}$ ;*

3) *nelle ipotesi di 2),  $M$  è generato da  $m$  elementi anche come  $K[t]$ -modulo;*

4)  *$M$  è anche, in modo naturale, un  $\Pi$ -modulo canonico, se e solo se è radicale equidimensionale; ed in tal caso esso è radicale equidimensionale, ma di dimensione  $n$  e codimensione  $m$ , anche come  $\Pi$ -modulo canonico.*

**DIM.** Se  $n = \infty$ ,  $M$  contiene un elemento  $x \neq 0$  tale che  $\omega x = 0$ ; quindi  $M$  non è libero, come  $K$  modulo o come  $K[t]$ -modulo, perchè  $\omega x = 0$ ; poi,  $Tx$  è, come  $K$ -modulo, e quindi come  $k$ -modulo, la somma diretta completa dei  $T^r x$  ( $r = 0, 1, \dots$ ), e non è quindi finito nè come  $K$ -modulo, nè come  $K[t]$ -modulo; ciò dimostra la 1).

Si consideri ora la 2); poichè  $n + m = \text{lungh } M/\omega M$ , per 2.6 esistono un insieme  $\{y_1, \dots, y_m\}$  di generatori di  $M$ , e degli interi  $s_1 \leq s_2 \leq \dots \leq s_m$  tali che un insieme di generatori di  $\omega M$  sia  $\{t^{s_1} y_1, \dots, t^{s_m} y_m\}$ ; e si ha inoltre  $m + n = \sum_i s_i$ . Allora il  $k$ -modulo  $M/\omega M$  è generato dalle immagini dei  $t^j y_i$  ( $j = 0, \dots, s_i - 1$ ), e queste ne formano anzi una base, perchè altrimenti  $M/\omega M$ , come  $k$ -modulo, avrebbe lunghezza  $< m + n$ , il che contraddirebbe il 2.7. Visto così che gli  $x_1, \dots, x_{m+n}$  con la proprietà richiesta esistono, e sono anzi linearmente indipendenti su  $K$ , mod  $\omega K$ , per un dato  $z \in M$  si trovino gli  $a_1, \dots, a_{m+n} \in K$  tali che  $z - \sum_i a_i x_i = \omega z_1 \in \omega M$ ; si operi poi su  $z_1$  nello stesso modo, ecc., col solito metodo di approssimazioni successive. Il risultato è che  $z$  è combinazione lineare degli  $x_i$  a coefficienti, unicamente determinati, in  $K$ ; ciò dimostra la 2). Il fatto poi che si pos-

sano scegliere le  $t^j y_i$  in luogo delle  $x_h$  mostra che le  $y_i$  generano  $M$  come  $K[t]$ -modulo, e prova la 3).

Per dimostrare la 4), osserviamo anzitutto che  $M$  è certamente un  $K[\pi]$ -modulo; l'essere esso un  $\Pi$ -modulo « in modo naturale » significa che per  $x \in M$  ed  $a_i \in K$  ha significato l'espressione  $\sum_0^\infty \pi^i a_i x$ , ossia che la successione dei  $\sum_0^r \pi^i a_i x$  ( $r = 0, 1, 2, \dots$ ) converge nella topologia naturale di  $M$ , che è quella in cui i  $t^i M$  sono gli intorni dello 0. Significa quindi che, dato  $j$ , è  $\pi^i x \in t^j M$  per  $i$  elevato; e ciò vuol dire che  $M$  è radicale. Se poi  $M$  deve essere non solo un  $\Pi$ -modulo, ma addirittura un  $\Pi$ -modulo canonico, per 2.2 si vede che  $\pi x = 0$  deve implicare  $x = 0$ , e che quindi  $M$  deve essere equidimensionale (come  $T$ -modulo). Se tutto ciò è verificato, si vede subito che allora  $M$  è radicale equidimensionale anche come  $\Pi$ -modulo. Quanto alla dimensione di  $M$  come  $\Pi$ -modulo canonico, per il 2.4 essa coincide con l'ordine del  $k$ -modulo libero  $M/\pi M$ , ossia con la lunghezza di  $M/\pi M$ , che è appunto  $n$ ; ciò prova la 4), C.V.D. .

Siano  $M, N$  rispettivamente un  $T$ -modulo canonico ed un  $\Pi$ -modulo canonico, e sia  $(x, y) \rightarrow x \bullet y$  ( $x \in M, y \in N$ ) un'applicazione dell'insieme prodotto  $M \times N$  su  $K$ , bilineare quando  $M, N$  vengono considerati come  $K$ -moduli; suppongasì inoltre che tale applicazione soddisfi le relazioni  $x \bullet \pi y = (tx \bullet y)^*$ ,  $(x \bullet ty)^* = \pi x \bullet y$ . Se queste condizioni sono soddisfatte, e se inoltre è vero che, dato un  $y \in N$  (rispettivamente un  $x \in M$ ), si ha  $x \bullet y = 0$  per ogni  $x \in M$  (rispettivamente per ogni  $y \in N$ ) se e solo se  $y = 0$  (rispettivamente  $x = 0$ ), allora l'applicazione «  $\bullet$  » dicesi una *dualità fra  $M$  ed  $N$* , e ciascuno di questi dicesi *duale dell'altro*. Noi ci occuperemo esclusivamente del caso dei  $T$ -moduli canonici equidimensionali; si ha :

**3.2 TEOREMA.** *Sia  $M$  un  $T$ -modulo canonico equidimensionale, di dimensione  $m$  e ordine  $q$ ; sia  $N$  il  $K$ -modulo duale del  $K$ -modulo  $M$  (ossia sia  $N$  il  $K$ -modulo degli omomorfismi del  $K$ -modulo  $M$  su  $K$ ); allora, con ovvie definizioni,  $N$  è un  $\Pi$ -modulo canonico duale di  $M$ , ed ha dimensione  $m$  ed ordine  $q$ . Ogni  $\Pi$ -modulo canonico duale di  $M$  è isomorfo ad  $N$ ; infine, la dualità è continua, nel senso che per ogni intero  $s > 0$  esiste un intero  $r > 0$  tale che  $x \bullet y \in \omega^s K$  ogniqualvolta  $x \in t^r M$  o  $y \in \pi^r N$ .*

**DIM.** È  $(x + z) \bullet \pi y = x \bullet \pi y + z \bullet \pi y$ ; poi, se  $a \in K$ , è  $(ax) \bullet \pi y = (tax \bullet y)^* = a (tx \bullet y)^* = a (x \bullet \pi y)$ , onde  $\pi y \in N$ , ed analogamente  $ty \in N$ .

Per 2.6, esistono un insieme  $\{x_1, \dots, x_m\}$  di generatori di  $M$ , e degli interi positivi  $s_1 \leq s_2 \leq \dots \leq s_m$ , tali che un insieme minimo di generatori di  $\omega M$  sia dato da  $\{t^{s_1} x_1, \dots, t^{s_m} x_m\}$ ; ed allora, per 3.1, un insieme libero di

generatori del  $K$ -modulo  $M$  è dato dai  $t^i x_j$ , con  $0 \leq i < s_j$ . Sia  $y_i$  l'elemento di  $N$  tale che  $t^{s_j-s} x_j \bullet y_i = \delta_{ji} \delta_{s1}$  ( $0 < s \leq s_j$ ), e si considerino gli elementi  $\pi^{i-1} y_j$  ove, per ogni  $j$ ,  $i$  assume i valori  $1, \dots, s_j$ ; dico che i  $\pi^{i-1} y_j$  formano un insieme libero di generatori del  $K$ -modulo  $N$ . Si consideri infatti la matrice  $H$  dei  $t^{s_h-s} x_h \bullet \pi^{i-1} y_j$ , ove gli  $s, h$  restano fissi in ogni riga, e ove  $h, j$  variano fra 1 ed  $m$ , mentre  $s, i$  variano fra 1 ed  $s_h$ , e 1 ed  $s_j$  rispettivamente; in tale matrice, si ordinino le righe e le colonne secondo l'ordine lessicografico di  $(s, h)$  e di  $(i, j)$  rispettivamente. Allora basta dimostrare che  $H$  è una matrice invertibile in  $K$ .

Ora, gli elementi diagonali di  $H$  sono i

$$t^{s_h-s} x_h \bullet \pi^{s-1} y_h = (t^{s_h-1} x_h \bullet y_h)^{\pi^{s-1}} = 1,$$

mentre quelli al di sotto della diagonale sono tutti nulli, in quanto o  $s > i$ , ed allora  $t^{s_h-s} x_h \bullet \pi^{i-1} y_j = (t^{s_h-(s-i)-1} x_h \bullet y_j)^{\pi^{i-1}} = 0$ , ovvero  $s = i$  ed  $h > j$ , nel qual caso  $t^{s_h-s} x_h \bullet \pi^{s-1} y_j = (t^{s_h-1} x_h \bullet y_j)^{\pi^{s-1}} = 0$ . Pertanto  $H$  è invertibile in  $K$ , onde i  $\pi^{i-1} y_j$  formano un insieme libero di generatori del  $K$ -modulo  $N$ .

Dato l'intero  $s > 0$ , esiste un  $r$  tale che  $t^r M \subseteq \omega^s M$ , onde  $t^r M \bullet y \subseteq \omega^r M \bullet y \subseteq \omega^r K$  se  $y \in N$ ; perciò  $y$  è continuo, come annunciato. Se allora  $a = \sum_0^\infty a_i \pi^i \in \Pi$ , con  $a_i \in K$ , e se  $y \in N$ , sia  $z$  l'elemento di  $N$  tale che, per  $x \in M$ ,  $x \bullet z = \sum_0^\infty a_i (t^i x \bullet y)^{\pi^i}$ ; tale  $z$  esiste per quanto precede; se si pone, per definizione,  $z = ay$ , si vede che  $N$  diviene un  $\Pi$ -modulo; siccome poi i  $\pi^r y_i$  generano  $N$  come  $K$ -modulo, si conclude che gli  $y_i$  generano  $N$  come  $\Pi$ -modulo, anzi, addirittura come  $K[\pi]$ -modulo (cfr. 3.1).

Per dimostrare che  $N$  è canonico occorre verificare le analoghe di 2.1, 2.2; ora, da  $tN \subseteq N$  e dall'ovvia relazione  $t(\pi y) = \pi(ty) = \omega y$  se  $y \in N$ , segue  $\omega N \subseteq \pi N$ , che è la 2.1. Se poi  $\pi y = 0$ , è anche  $\omega y = 0$ ,  $\bar{\omega}(x \bullet y) = 0$  per ogni  $x \in M$ , onde  $x \bullet y = 0$ ,  $y = 0$ , che è la 2.2.

La dimensione di  $N$  si è visto essere  $\leq m$ ; poichè  $M$  è ottenuto da  $N$  come  $N$  da  $M$  (previo scambio di  $t$  con  $\pi$ ), si deve avere  $m = \dim M \leq \dim N \leq m$ , dal che si conclude che  $\dim N = m$ , C.V.D..

Con dimostrazione ovvia si ottiene:

**3.3 COROLLARIO.** *Notazioni come al 3.2; se  $M = L \oplus R$ , con  $L$  logaritmico ed  $R$  radicale, allora  $N = P \oplus Q$ , ove  $P$  (risp.  $Q$ ) è l'insieme degli  $y \in N$  tali che  $x \bullet y = 0$  pe ogni  $x \in R$  (risp.  $x \in L$ ); allora  $P$  è logaritmico, ed è duale di  $L$ , mentre  $Q$  è radicale ed è duale di  $R$ . Inoltre, il duale di  $M_{r,s}$  ( $0 < s < \infty$ ) è  $M_{s,r}$ , quando quest'ultimo venga considerato come un  $\Pi$ -modulo canonico.*

Nel seguito, se  $M$  è un  $T$ -modulo canonico equidimensionale, il  $\Pi$ -modulo canonico duale di  $M$  sarà indicato con  $M_{-1}$ ; se  $\sigma$  è un semiomomorfismo canonico di  $M$  sul  $T$ -modulo canonico equidimensionale  $P$ , indicheremo con  $\sigma_{-1}$  il duale di  $\sigma$ , ossia il semiomomorfismo canonico di  $P_{-1}$  su  $M_{-1}$  definito da  $(x \bullet \sigma_{-1} y)^\sigma = \sigma x \bullet y$ , se  $x \in M$  ed  $y \in P_{-1}$ . Si ha:

**3.4 TEOREMA.** *Sia  $\sigma$  un semiomomorfismo canonico del  $T$ -modulo canonico equidimensionale  $M$  sul  $T$ -modulo canonico equidimensionale  $P$ ; allora  $\text{conull } \sigma = \text{null } \sigma_{-1}$ , e  $\text{ins } \sigma = \text{ins } \sigma_{-1}$ ; in particolare,  $\sigma_{-1}$  è un semiisomorfismo se e solo se  $\text{conull } \sigma = 0$ .*

**DIM.** Si decomponga  $\sigma$  come al 2.14, ma scrivendo  $\varrho^i, Q^i$  in luogo di  $\varrho_i, Q_i$ ; la corrispondente decomposizione di  $\sigma_{-1}$  è

$$P_{-1} \rightarrow Q_{-1} = \begin{array}{ccccccc} Q_{-1}^1 & \rightarrow & Q_{-1}^{l-1} & \rightarrow & \dots & \rightarrow & Q_{-1}^0 \rightarrow H_{-1} \rightarrow M_{-1}, \\ \tau_{-1} & & \varrho_{-1}^1 & & \varrho_{-1}^{l-1} & & \varrho_{-1}^1 & & \varepsilon_{-1} & & \varphi_{-1} \end{array}$$

ove  $\varphi_{-1}, \varrho_{-1}^i, \tau_{-1}$  sono omomorfismi, mentre  $\varepsilon_{-1}$  è semiomomorfismo; per dimostrare l'asserzione sulle nullità e conullità, occorre dimostrare che:

$$\text{conull } \tau_{-1} = 0, \text{ null } \tau_{-1} = \text{conull } \tau;$$

$$\text{conull } \varrho_{-1}^i = \text{null } \varrho_{-1}^i = 0;$$

$$\text{conull } \varepsilon_{-1} = \text{null } \varepsilon_{-1} = 0;$$

$$\text{null } \varphi_{-1} = 0, \text{ conull } \varphi_{-1} = \text{null } \varphi;$$

da queste seguirà anche  $\text{null } \tau_{-1} = \text{null } \sigma_{-1}$ ,  $\text{conull } \varphi_{-1} = \text{conull } \sigma_{-1}$ ,  $\text{conull } \sigma_{-1} = \text{null } \sigma$ ,  $\text{null } \sigma_{-1} = \text{conull } \sigma$ .

Ora, le asserzioni riguardanti  $\varepsilon_{-1}$  e  $\varphi_{-1}$  sono palesi; la seconda asserzione riguardante  $\varrho_{-1}^i$  (per esempio  $\varrho_{-1}^1$ ) si dimostra osservando che se  $0 \neq y \in Q_{-1}^1$ ,  $\varrho_{-1}^1 y$  è certo non nullo perchè se fosse nullo si avrebbe  $x \bullet y = 0$  per ogni  $x \in \varrho^1 Q^0$ , e quindi per ogni  $x \in Q^1$ , dato che  $t^r Q^1 \subseteq \varrho^1 Q^0$  per  $r$  elevato. Per dimostrare la prima asserzione riguardante  $\varrho_{-1}^1$ , si osservi che se  $y \in Q_{-1}^0$ , per  $r$  elevato si ha  $x \bullet \pi^r y \in \omega^s K$  con  $s$  elevato; quindi  $\pi^r y$  è estensibile a tutto  $Q^1 \supseteq \varrho^1 Q^0$ , ossia  $\pi^r y \in \varrho_{-1}^1 Q_{-1}^1$ .

Le asserzioni riguardanti  $\tau_{-1}$  si dimostrano osservando che per 3.1 esiste un insieme libero  $X$  di generatori di  $Q$  (come  $K$ -modulo) tale che  $\tau X$  può essere completato in un insieme libero di generatori di  $P$ ; quindi  $\tau_{-1}$  è su tutto  $Q_{-1}$ , e perciò  $\text{conull } \tau_{-1} = 0$ ,  $\text{null } \tau_{-1} = \text{conull } \tau$ , ed anche  $\text{ins } \tau_{-1} = 0$ .

Pertanto, per dimostrare che  $\text{ins } \sigma = \text{ins } \sigma_{-1}$ , basta dimostrare le seguenti asserzioni:

- a)  $\text{ins } \tau_{-1} = 1$ ;
- b)  $\text{ins } \varrho_{-1}^i = \omega$ ;
- c)  $\text{ins } \varepsilon_{-1} = 1$ ;
- d)  $\text{ins } \varphi_{-1} = 1$ .

Ora,  $\varepsilon$  è un semiisomorfismo di  $H$  su tutto  $Q^0$ , onde la c) è palese; la a) è già stata dimostrata. Per dimostrare la d), si considerino un  $y \in H_{-1}$  ed uno  $z \in M_{-1}$  tali che  $\pi z = \varphi_{-1}y$ ; si ha, per  $x \in M$ ,  $\pi\varphi x \bullet y = \pi x \bullet \varphi_{-1}y = = \pi x \bullet \pi z = (\omega x \bullet z)^\pi$ , onde  $\pi H \bullet y \subseteq \omega K$ ,  $H \bullet ty \subseteq \omega K$ ,  $ty \in \omega H_{-1}$ ,  $y \in \pi H_{-1}$ ; pertanto  $z \in \varphi_{-1}H_{-1}$ , il che prova che  $M_{-1} \cap \Pi^*(\varphi_{-1}H_{-1}) = \varphi_{-1}H_{-1}$ , e che perciò  $\text{ins } \varphi_{-1} = 1$ , che è la d).

La b) sarà dimostrata, per esempio, nel caso  $i = 1$ ; essendo  $\varrho^1$  l'isomorfismo di immersione di  $Q^0$  in  $Q^1$ , ed avendosi lungi  $Q^1/Q^0 = 1$ , per 2.7 è  $Q^1 = Q^0 + Tv$  per un opportuno  $v \notin Q^0$  tale che  $tv \in Q^0$ . Un  $y \in Q_{-1}^0$  appartiene a  $\varrho_{-1}^1 Q_{-1}^1$  se e solo se  $\pi(tv) \bullet y \in \omega K$ ; quindi  $Q_{-1}^0/\varrho_{-1}^1 Q_{-1}^1$  è isomorfo, come  $K$ -modulo, a  $K/\omega K \cong k$ ; ne segue lungi  $Q_{-1}^0/\varrho_{-1}^1 Q_{-1}^1 = 1$ , o  $\text{ins } \varrho_{-1}^1 = \omega$ , che è la b), C.V.D..

La dualità « $\bullet$ » precedentemente introdotta, pur essendo la più naturale per i  $T$ -moduli canonici equidimensionali, ha il difetto di non essere estensibile a quelli non equidimensionali; introdurremo pertanto un altro tipo di dualità. Si osservi prima di tutto che ogni  $T$ -modulo canonico (sinistro)  $M$  può essere considerato, in modo naturale, come un  $\Pi$ -modulo canonico destro, qualora si definisca, per  $x \in M$  ed  $a \in \Pi$ ,  $xa = a^\pi x$ ; qui,  $\gamma$  indica la reciprocità (= antiisomorfismo) di  $\Pi$  su  $T$ , od anche di  $T$  su  $\Pi$ , che a  $\sum_i a_i \pi^i$  ( $a_i \in K$ ) fa corrispondere  $\sum_i t^i a_i$ ; si noti, a tal proposito, che per  $a \in T$ ,  $b \in \Pi$ ,  $x \in M$  è in generale  $(ax)b \neq a(xb)$ . Se  $M$  ha l'insieme minimo di generatori  $\{x_1, \dots, x_m\}$ , e se, a norma del 2.8,  $\pi x_{-1} = Cx_{-1}$ , con  $x = (x_1 \dots x_m)$ , allora  $xt = xC^r$ , ove  $C^r$  è la trasposta della matrice ottenuta applicando  $\gamma$  ad ogni elemento di  $C$ . Lo stesso dicasi riguardo ai  $\Pi$ -moduli sinistri e  $T$ -moduli destri.

Per  $n = 0, 1, \dots$ , si indichi con  $k_n$  l'algebra (bilatera)  $K/K\omega^{n+1}$  su  $K$ ; in  $k_n$  è definito in modo naturale il semiendomorfismo  $\kappa$  (di algebre); vi è poi un omomorfismo naturale (di algebre)  $\varrho$  di  $k_{n+1}$  su tutto  $k_n$ , con  $k_0^e = 0$  per definizione; e vi è infine l'operatore  $\tau$  che ad un elemento di  $k_n$ , immagine di  $a \in K$ , fa corrispondere l'immagine, in  $k_{n+1}$ , di  $\omega a^{\kappa^{-1}}$ ; esso è un semiomomorfismo di  $K$ -moduli; se  $a \in k_n$  e  $b \in K$ , valgono le regole:  $(ba)^\kappa = = b^\kappa a^\kappa$ ,  $(ba)^\varrho = ba^e$ ,  $(ba)^\tau = b^{\kappa^{-1}} a^\tau$ .

Indicheremo con  $\mathcal{K}$  l'insieme delle successioni  $u = [u_0, u_1, u_2, \dots]$ ,  $u_i \in k_i$ ; se  $b \in K$ , definiremo  $bu = [bu_0, bu_1, \dots]$ ,  $ub = [bu_0, b^{\kappa^{-1}}u_1, b^{\kappa^{-2}}u_2, \dots]$ ,  $u^\kappa = [u_0^\kappa, u_1^\kappa, \dots]$ ,  $tu = [0, u_0^\tau, u_1^\tau, \dots]$ ,  $\pi u = [u_1^{\varrho^\kappa}, u_2^{\varrho^\kappa}, \dots]$ ,  $ut = [0, u_0^{\tau^\kappa}, u_1^{\tau^\kappa}, \dots]$ ,

$u\pi = [u_1^e, u_2^e, \dots]$ . Allora  $\mathcal{K}$  diviene, in modo naturale, un  $T[\pi]$ -modulo sinistro e destro; le  $u_i$  diconsi le *componenti di  $u$* , e la somma viene definita sulle componenti; si ha inoltre  $\pi u = \pi t u = u t \pi = u \pi t = \omega u = u \omega$ ,  $u t = (t u)^* = t u^*$ ,  $\pi u = (u \pi)^* = u^* \pi$ ,  $(b u) c = b(u c)$  se  $b, c \in T[\pi]$ . Infine,  $\delta t u = 0$  (risp.  $u t = 0$ ) se e solo se  $u = 0$ ; porremo, per  $u \in \mathcal{K}$ ,  $\mu u = u_0 \in k_0 = k$ .

**3.5 TEOREMA.** *Sia  $M$  un  $T$ -modulo canonico (sinistro) di dimensione  $n$ , e sia  $N$  l'insieme degli omomorfismi  $\zeta$  (ossia  $x \rightarrow x \circ \zeta$  per  $x \in M$ ) di  $M$  sul  $T$ -modulo sinistro  $\mathcal{K}$ ; con la definizione  $x \circ \zeta a = (x \circ \zeta) a$  ( $a \in T$ ),  $N$  è un  $T$ -modulo canonico destro di dimensione  $n$ . Si ha  $x = 0$  se e solo se  $x \circ \zeta = 0$  per ogni  $\zeta \in N$ ; inoltre  $M$  è isomorfo al  $T$ -modulo sinistro degli omomorfismi del  $T$ -modulo destro  $N$  su  $K$ . Sia  $x$  (matrice ad una colonna) un insieme minimo di generatori di  $M$ , e sia  $C$  una matrice quadrata ad elementi in  $T$  tale che  $\pi x = Cx$ ; allora esiste un insieme minimo  $\zeta$  (matrice ad una riga) di generatori di  $N$  tale che  $\mu(x \circ \zeta) = 1$  e che  $\zeta \pi = \zeta C^{-1}$ . Infine, gli elementi  $\xi_i \in N$  ( $i = 1, \dots, n$ ) generano  $N$  se e solo se  $\det \mu(x_i \circ \xi_j) \neq 0$ , mentre  $\delta \eta \in Nt$  se e solo se  $\mu(y \circ \eta) = 0$  per ogni  $y \in M$ .*

**DIM.** Se  $\zeta \in N$ , si ha, per  $x \in M$ ,  $x \circ \zeta \omega = (x \circ \zeta) \omega = \omega(x \circ \zeta) = \omega x \circ \zeta = t y \circ \zeta$  per un opportuno  $y \in M$ , onde  $x \circ \zeta \omega \in t\mathcal{K} = \mathcal{K}t$ ; quindi  $N$  contiene la  $\eta$  tale che  $x \circ \eta = (x \circ \zeta \omega) t^{-1}$ , e ciò prova la 2.1. Poi, se  $\zeta t = 0$ , da  $(x \circ \zeta) t = 0$  segue  $x \circ \zeta = 0$ ,  $\zeta = 0$ , che è la 2.2. Pertanto  $N$  è un  $T$ -modulo canonico se è finito; si noti che  $(x \circ \zeta \pi) = (x \circ \zeta) \pi$ .

Si indichi con  $\omega_m^s$  ( $s, m = 0, 1, \dots; s \leq m$ ) l'immagine di  $\omega^s$  in  $k_m$ ; se  $x, C$  sono legate come all'enunciato, sia  $C = C_0 + tC_1 + t^2C_2 + \dots$ , con  $C_i$  matrice ad elementi in  $K$ . Pongasi  $U_0 = \omega_0^0$  (matrice identità di ordine  $n$  ad elementi in  $k$ ), e, per  $m > 0$ , si indichi con  $U_m$  la matrice che è somma di tutte le espressioni

$$C_{i_1}^{x-l_1} \dots C_{i_r}^{x-l_r} \omega_m^s$$

che soddisfano le condizioni seguenti:

$$l_1 = i_1 + 1, l_2 = i_1 + i_2 + 2, \dots, l_r = i_1 + i_2 + \dots + i_r + r = m; \\ i_1 + \dots + i_r = s.$$

Con verifica diretta, e tenendo presente che  $(\omega_m^s)^x = \omega_m^s$ ,  $(\omega_m^s)^{x^i} = \omega_{m+i}^{s+i}$ ,  $(\omega_m^s)^e = \omega_{m-1}^s$  ( $= 0$  se  $s = m$ ), si trova che le  $U_m$  soddisfano le relazioni ricorrenti seguenti:

$$3.6 \quad U_{m+1}^{e^x} = \sum_0^m C_i^{x-i} U_{m-1}^{x^i}; \quad U_{m+1}^e = \sum_0^m U_{m-i}^{x^i} C_i^{x-m-1};$$

se si pone  $U = [U_0, U_1, \dots]$  (scrivendo una successione di matrici anzichè una matrice i cui elementi siano successioni appartenenti a  $\mathcal{K}$ ), le 3.6 significano rispettivamente  $\pi U = CU$ ,  $U\pi = UC^{\kappa-1}$ ; esistono quindi delle  $\zeta_1, \dots, \zeta_n \in N$  tali che  $x \circ \zeta = U$ , ed è  $\mu(x \circ \zeta) = \mu U = U_0 = 1$ , e  $x \circ \zeta\pi = U\pi = UC^{\kappa-1} = x \circ \zeta C^{\kappa-1}$ , ossia  $\zeta\pi = \zeta C^{\kappa-1}$ , come richiesto.

Dico ora che le  $\zeta_1, \dots, \zeta_n$  generano il  $T$ -modulo destro  $N$ : sia infatti  $\xi \in N$ , e pongasi  $x \circ \xi = w$  (matrice ad una colonna); è  $\pi w = Cw$ , ossia, per ogni  $m \geq 0$ ,

$$3.7 \quad w_{m+1}^{e\kappa} = \sum_0^m C_i^{\kappa-i} w_{m-i}^{\kappa^i}.$$

Dobbiamo trovare un  $a = a_0 + ta_1 + \dots$ , con  $a_i$  matrice ad una colonna con elementi in  $K$ , tale che  $\xi = \zeta a$ , ossia tale che  $w = x \circ \zeta a = Ua$ ; ciò significa trovare le  $a_i$  in modo che, per  $m = 0, 1, \dots$ , sia

$$3.8 \quad w_m = \sum_0^m U_{m-i}^{\kappa^i} a_i^{\kappa^{-m}}.$$

Ora, per  $m = 0$  la  $a_0$  esiste certamente, poichè  $U_0 = \omega_0^0$ ; supposto quindi che  $a_i$  sia stato trovato per  $i = 0, \dots, m-1$ , si potrà trovare una  $a_m$  che soddisfi la 3.8 se e solo se

$$w_m^{e\kappa} - \sum_0^{m-1} U_{m-i}^{\kappa^{i+1}e} a_i^{\kappa^{-m+1}} = 0,$$

ossia, per 3.7, se e solo se

$$\sum_0^{m-1} C_i^{\kappa-i} w_{m-i-1}^{\kappa^i} - U_{m-i}^{\kappa^{i+1}e} a_i^{\kappa^{-m+1}} = 0.$$

Ma, di nuovo per la 3.8, il primo membro di quest'ultima diviene:

$$\begin{aligned} & \sum_0^{m-1} C_i^{\kappa-i} \sum_0^{m-i-1} U_{m-i-1-j}^{\kappa^{i+j}} a_j^{\kappa^{-m+1}} - U_{m-i}^{\kappa^{i+1}e} a_i^{\kappa^{-m+1}} = \\ & = \sum_0^{m-1} \left( \sum_0^{m-i-1} C_j^{\kappa-j} U_{m-i-j-1}^{\kappa^{i+j}} - U_{m-i}^{\kappa^{i+1}e} \right) a_i^{\kappa^{-m+1}} = 0 \end{aligned}$$

per la prima delle 3.6. Pertanto le  $a_i$  esistono, e le  $\zeta_1, \dots, \zeta_n$  generano  $N$ .

Le  $\xi_1, \dots, \xi_n$  generano  $N$  se e solo se  $\xi = \zeta A$  per una matrice  $A$  ad elementi in  $T$  ed invertibile in  $T$ ; e cioè se e solo se, fra le matrici  $A$  (certo esistenti) tali che  $x \circ \xi = UA$  ve n'è una invertibile; ciò accade appunto se e solo se  $\det \mu(x \circ \xi) \neq 0$ , come richiesto.

Se  $y \in M$  è tale che  $y \circ \eta = 0$  per ogni  $\eta \in N$ , da  $\mu(y \circ \zeta) = 0$  segue ora  $y \in tM$ , e per esempio  $y = tz$ ; allora, da  $tz \circ \zeta = 0$  segue  $z \circ \zeta = 0$ , onde  $z \in tM$ ,  $y \in t^2M$ , ecc.; infine,  $y = 0$ , come richiesto. Invertendo il ruolo di  $M$  ed  $N$  si constata subito che  $M$  è isomorfo al  $T$ -modulo sinistro degli omomorfismi del  $T$ -modulo destro  $N$  su  $\mathcal{K}$ , C.V.D..

Se si considera  $tN$  del 3.5 come un  $II$ -modulo canonico (sinistro), e se  $\zeta$  è ora la matrice ad una colonna degli  $\zeta_i$ , si ha  $t\zeta = C^{\gamma\kappa-1}\zeta$ , e la matrice  $\pi C^{\gamma\kappa-1} - \omega = (tC - \omega)^\gamma$  è legata a  $\zeta$  come la  $tC - \omega$  è legata alla  $x$  (cfr. 2.8). Per questo motivo, il  $II$ -modulo canonico  $N$  sarà detto il *trasposto di  $M$*  e indicato con  $M_{-1}$  (cosicchè  $M_{-1}$  avrà, a seconda dei casi, il significato di duale o di trasposto); in particolare, il trasposto di  $M_{r,s}$  sarà indicato con  $N_{r,s}$ ; per elementi  $y \in M$ ,  $\eta \in N$ , continueremo a scrivere  $y \circ \eta$ ; questa operazione bilineare gode delle seguenti proprietà (ove  $a \in K$ ):  $ay \circ \eta = a(y \circ \eta)$ ,  $y \circ a\eta = (y \circ \eta)a$ ,  $\pi y \circ \eta = (y \circ t\eta)^\pi$ ,  $(ty \circ \eta)^\pi = y \circ \pi\eta$ .

Se  $\sigma$  è un semiomomorfismo canonico del  $T$ -modulo canonico  $M$  sul  $T$ -modulo canonico  $P$ , il *trasposto di  $\sigma$* , indicato ancora con  $\sigma_{-1}$ , è il semiomomorfismo canonico di  $P_{-1}$  su  $M_{-1}$  definito da  $(x \circ \sigma_{-1}\zeta)^\sigma = \sigma x \circ \zeta$ ; qui, se  $u = [u_0, u_1, \dots] \in \mathcal{K}$ ,  $u^\sigma$  significa  $[u_0^\sigma, u_1^\sigma, \dots]$ .

**3.9 TEOREMA.** *Il 3.4 vale anche per  $M$  e  $P$   $T$ -moduli canonici qualsiasi, purchè  $\sigma_{-1}$  indichi il trasposto di  $\sigma$  anzichè il suo duale.*

**DIM.** La dimostrazione del 3.4 può essere ripetuta quasi parola per parola; le modificazioni meno evidenti da apportare sono le seguenti:

1. Per dimostrare le asserzioni riguardanti  $\tau_{-1}$ , si completi un insieme minimo di generatori  $\{x_1, \dots, x_m\}$  del  $T$ -modulo  $\tau Q$ , in un insieme minimo di generatori  $\{x_1, \dots, x_n\}$  di  $P$ ; se le  $\zeta_i$  sono legate alle  $x_1, \dots, x_n$  come al 3.5, le  $\tau_{-1}\zeta_1, \dots, \tau_{-1}\zeta_m$  generano  $Q_{-1}$  per 3.5, donde  $Q_{-1} = \tau_{-1}P_{-1}$ ;

2. Nella dimostrazione di *d*), sostituire la formula  $\pi\varphi x \bullet y = \dots = (\omega x \bullet z)^\pi$  con  $\varphi x \circ y = x \circ zt$ ;

3. Nella dimostrazione di *b*), sostituire la  $\pi(tv) \bullet y \in \omega K$  con la  $(tv) \circ y \in t\mathcal{K}$ , C.V.D..

Nel caso in cui  $M$  sia equidimensionale, abbiamo così definito un suo duale (con l'operazione  $\bullet$ ), ed un suo trasposto (con l'operazione  $\circ$ ); essi sono legati nel modo seguente:

**3.10 TEOREMA.** *Sia  $M$  un  $T$ -modulo canonico equidimensionale; sia  $N$  il suo duale, e sia  $P$  il suo trasposto; allora esiste un unico isomorfismo  $\sigma$  di  $tN$  su tutto  $P$  tale che, per  $\zeta \in tN$  ed  $x \in M$ ,  $(x \circ \sigma\zeta)_r$  sia l'immagine, in  $k_r$ , di  $x \bullet t^r\zeta$  ( $r = 0, 1, \dots$ ).*

DIM. Il  $\sigma$  così definito associa ad ogni  $\zeta \in tN$  una applicazione  $\sigma\zeta$  di  $M$  su  $\mathcal{K}$ ; occorre anzitutto dimostrare che  $\sigma\zeta$  è un omomorfismo di  $T$ -moduli sinistri. E infatti, è intanto  $((x + y) \circ \sigma\zeta)_r = (x \circ \sigma\zeta)_r + (y \circ \sigma\zeta)_r$ , e  $(ax \circ \sigma\zeta)_r = a(x \circ \sigma\zeta)_r$  per  $a \in K$ . Poi,  $(tx \circ \sigma\zeta)_r$ , per  $r > 0$ , è l'immagine, in  $k_r$ , di  $tx \bullet t^r\zeta = \omega(x \bullet t^{r-1}\zeta)^{r-1}$ , e questa non è altro che  $(x \circ \sigma\zeta)_{r-1}^r$ ; se invece  $r = 0$ ,  $(tx \circ \sigma\zeta)_0$  è l'immagine, in  $k_0$ , di  $tx \circ \zeta$ ; essendo  $\zeta$  elemento di  $tN$ , ossia  $\zeta = t\zeta'$  per uno  $\zeta' \in N$ , è  $tx \bullet \zeta = tx \bullet t\zeta' \in \omega K$ , onde  $(tx \circ \sigma\zeta)_0 = 0$ ; quindi  $tx \circ \sigma\zeta = t(x \circ \sigma\zeta)$ . Pertanto  $\sigma\zeta \in P$ ; è ovviamente  $\sigma(\zeta + \eta) = \sigma\zeta + \sigma\eta$ ,  $\sigma(a\zeta) = a\sigma\zeta$  se  $a \in K$ ; inoltre,  $(x \circ \sigma\pi\zeta)_r$  è l'immagine, in  $k_r$ , di  $x \bullet t^r\pi\zeta = \omega x \bullet t^{r-1}\zeta$ , e questa non è altro che  $(x \circ \sigma\zeta)_{r-1}^{rx}$  (valido, come prima, anche se  $r = 0$ ); quindi  $\sigma\pi\zeta = \pi\sigma\zeta$ , e  $\sigma$  è un omomorfismo di  $\Pi$ -moduli.

Se  $\sigma\zeta = 0$ , ossia se  $x \bullet t^r\zeta \in \omega^{r+1}K$  per ogni  $x$  ed ogni  $r$ , si ha intanto  $x \bullet \zeta \in \omega K$  per ogni  $x$ , onde  $\zeta \in \omega N \subseteq \pi N$ , e per esempio  $\zeta = \pi\zeta'$ ; poi,  $x \bullet t\pi\zeta' \in \omega^2 K$ ,  $x \bullet \zeta' \in \omega K$ ,  $\zeta' \in \omega N \subseteq \pi N$ ,  $\zeta \in \pi^2 N$ , ecc.; quindi  $\zeta = 0$ , e ciò prova che  $\sigma$  è un isomorfismo di  $tN$  su  $P$ . Infine, come si è visto nella dimostrazione del 3.2, esistono un insieme minimo di generatori  $\{x_1, \dots, x_n\}$  di  $M$ , ed uno  $\{\zeta_1, \dots, \zeta_n\}$  di  $N$ , tali che  $\pi x_i \bullet \zeta_j = \delta_{ij}$ , od anche  $x_i \bullet t\zeta_j = \delta_{ij}$ ; ed allora, per 3.5, i  $\sigma t\zeta_j$  generano  $P$ , C.V.D..

**4. Iperalgebre, ipercampi, gruppi analitici.** In questo paragrafo riassumeremo, con dimostrazioni schematiche, alcuni risultati che sono ormai ben noti ai cultori di teoria dei gruppi algebrici. Il corpo  $k$  continuerà ad essere algebricamente chiuso e di caratteristica  $p \neq 0$ ; indicheremo con  $I^n$  il semigruppino additivo dei vettori  $h = (h_1, \dots, h_n)$  a componenti  $h_i$  interi non negativi; porremo  $h < l$  se  $h_i \leq l_i$  per ogni  $i$ , il  $<$  valendo per almeno un valore di  $i$ ; porremo anche  $\varepsilon(i) = (\delta_{i1}, \dots, \delta_{in})$ . Se  $A$  è un'algebra commutativa con identità su  $k$ , una  $p$ -base di  $A$  significherà un insieme  $X$  di elementi di  $A$  tale che ogni elemento di  $A$  sia esprimibile in un sol modo come polinomio, a coefficienti in  $k$ , negli elementi di  $X$ , di grado  $< p$  in ogni argomento; la  $p$ -dipendenza è allora definita in maniera consistente con la precedente definizione. Se  $A^+$  è un'algebra su  $k$ , indicheremo con  $k \oplus A^+$  l'algebra (con identità) su  $k$  che, come  $k$ -modulo, è somma diretta di  $k$  ed  $A^+$ , e in cui l'operazione di prodotto è definita mediante la  $(c + a)(c' + a') = cc' + ca' + c'a + aa'$ , ove  $c, c' \in k$  ed  $a, a' \in A^+$ ; in tal modo  $A^+$  diviene un ideale bilatero di  $k \oplus A^+$ . Siano  $R, S$  algebre commutative su  $k$ , dotate di metriche determinate da successioni di ideali  $\{R_i\}, \{S_j\}$ , con  $R_0 = R, S_0 = S, R_{i+1} \subseteq R_i, S_{j+1} \subseteq S_j, \bigcap_i R_i = \bigcap_j S_j = 0$ , e complete rispetto a tali metriche; indicheremo con  $R \overline{\otimes} S$  il completamento del prodotto tensoriale  $R \otimes S$  (di algebre su  $k$ ) rispetto alla metrica determinata in  $R \otimes S$  dalla successione di ideali  $\{ \sum_{i+j=r} R_i \otimes S_j \}$ .

Una *iperalgebra (commutativa)* su  $k$  è un'algebra commutativa  $A$  su  $k$ , possedente un omomorfismo  $P$  (di algebre) sull'algebra  $A \overline{\otimes} A$ , tale che:

4.1 esistono un intero positivo  $n$ , ed una base  $\{x_h\}$  di  $A$ , con  $h$  percorrente  $I^n$ , tali che  $x_0 = 1$ , e che le  $x_h$  con  $h > 0$  formino una base (come  $k$  modulo) di un ideale  $A^+$  di  $A$ , che soddisferà pertanto la relazione  $A = k \oplus A^+$ ;

4.2 fra le basi  $\{x_h\}$  introdotte al 4.1 ve n'è almeno una tale che  $Px_h = \sum_{r+s=h} x_r \otimes x_s$ , per ogni  $h \in I^n$ .

Il  $P$  (che si vede subito essere un isomorfismo) si dirà *isomorfismo strutturale* di  $A$ , ed ogni base  $\{x_h\}$  che soddisfi le 4.1, 4.2 si dirà una *base strutturale* di  $A$ ; si vede subito che  $A^+$  è indipendente dalla scelta della base strutturale, e che è quindi unicamente determinato; lo stesso dicasi del sotto- $k$ -modulo  $A^*$  di  $A$  generato dalle  $x_{\varepsilon(i)}$  ( $i = 1, \dots, n$ ): un elemento  $y$  appartiene ad  $A^*$  se e solo se  $P_y = y \otimes 1 + 1 \otimes y$ ; l'ordine di  $A^*$  è  $n$ , il che mostra che  $n$  è un invariante di  $A$ , detto la sua *dimensione*.

Un *ipercampo* su  $k$  è un campo d'integrità locale regolare completo  $R$  di dimensione finita positiva  $n$  e caratteristica  $p$ , con corpo residuo  $k$ , tale che se  $R^+$  è il suo ideale primo massimo (onde  $R = k \oplus R^+$ ), esista un omomorfismo  $P$  di  $R$  sul campo locale completo  $R \overline{\times} R$ , tale che:

4.3 *commutatività*: se  $\eta \in R$ ,  $P\eta$  è invariante rispetto allo scambio del primo col secondo fattore di  $R \overline{\times} R$ ;

4.4 *associatività*: se  $\iota$  indica l'isomorfismo identico, allora

$$(\iota \overline{\times} P) P = (P \overline{\times} \iota) P;$$

4.5 sia  $\sigma$  l'omomorfismo naturale di  $R$  su  $R/R^+ \cong k \subset R$ ; sia  $\mu$  la chiusura (in  $R \overline{\times} R$ ) dell'applicazione  $(\xi, \eta) \rightarrow \xi\eta$  di  $R \otimes R$  su  $R$ ; allora

$$\mu(\iota \overline{\times} \sigma) P = \mu(\sigma \overline{\times} \iota) P = \iota.$$

Le 4.3, 4.4, 4.5 possono essere scritte, in modo più familiare, come segue: intanto,  $R$  è un anello formale di potenze  $R = k \langle \xi_1, \dots, \xi_n \rangle$ , mentre  $R^+$  è l'ideale generato da  $\xi_1, \dots, \xi_n$ ; se si pone

$$P\xi_i = g_i(\xi_1 \overline{\times} 1, \dots, \xi_n \overline{\times} 1; 1 \overline{\times} \xi_1, \dots, 1 \overline{\times} \xi_n) \in k \langle \xi \overline{\times} 1; 1 \overline{\times} \xi \rangle = R \overline{\times} R,$$

le 4.3, 4.4, 4.5 divengono:

$$4.6 \quad g_i(\xi; \eta) = g_i(\eta; \xi); \quad g_i(\xi; g(\zeta; \eta)) = g_i(g(\xi; \zeta); \eta); \quad g_i(\xi; 0) = g_i(0; \xi) = \xi_i,$$

le  $\xi_i, \zeta_i, \eta_i$  essendo indeterminate. La 4.5 mostra che  $PR$  ha la stessa dimensione di  $R$ , e che pertanto  $P$  è un isomorfismo; esso dicesi la *legge* di  $R$ .

Indicheremo nel seguito con  $\Omega$  un campo d'integrità contenente  $k$  ed avente le seguenti proprietà:

1)  $\Omega$  è completo rispetto ad una valutazione  $v$  su  $k$ , di rango 1, tale che  $v(\alpha) \geq 0$  per ogni  $\alpha \in \Omega$ ;

2) se  $\Omega^+$  è l'ideale legato a  $v$  (ossia l'insieme degli  $\alpha \in \Omega$  tali che  $v(\alpha) > 0$ ), è  $\Omega = k \oplus \Omega^+$ ;

3) il corpo quoziente  $\Omega^*$  di  $\Omega$  è algebricamente chiuso, e  $\Omega$  è aritmeticamente chiuso in  $\Omega^*$ ;

4)  $\Omega^+$  contiene una infinità di elementi analiticamente indipendenti su  $k$ , rispetto alla topologia indotta da  $v$ .

La  $v$  risulterà necessariamente non discreta; un tale  $\Omega$  si può ottenere nel modo seguente:  $\Omega_0 = k \langle z_1, z_2, \dots \rangle$ , le  $z_i$  essendo una infinità di indeter-

minate;  $\Omega^*$  = chiusura algebrica di  $\Omega_0$ ;  $\Omega$  = chiusura aritmetica di  $\Omega_0$  in  $\Omega^*$ ;  $v$  = una qualsiasi delle estensioni ad  $\Omega$  (o  $\Omega^*$ ) della valutazione  $v_0$  di  $\Omega_0$  tale che, per  $z \in \Omega_0$ ,  $v_0(z)$  = grado della forma iniziale di  $z$  nelle  $z_i$ .

Se  $R$  è un ipercampo di dimensione  $n$ , sia  $G$  l'insieme degli omomorfismi dell'algebra  $R^+$  (su  $k$ ) sull'algebra  $\Omega^+$ , ciascuno di essi potendo essere considerato anche come omomorfismo di  $R$  su  $\Omega$ ; gli elementi di  $G$  si diranno i suoi punti. Se  $P$  è un punto di  $G$ ,  $PR$  è necessariamente un sottoanello locale completo di  $\Omega$ , e perciò  $P$  è un omomorfismo continuo rispetto alle topologie naturali di  $R$  e  $PR$ ; ora, se  $h = \min(v(P\zeta)) > 0$  quando  $\zeta$  varia in  $R^+$ ,  $PR$  possiede anche la topologia determinata dalla successione di ideali  $\{Q_r\}$ , ove  $Q_0 = PR$ ,  $Q_1 = PR^+$ , e  $Q_r$  = insieme dei  $P\zeta$ ,  $\zeta \in R^+$ , tali che  $v(P\zeta) \geq rh$ ; tale topologia è quella indotta in  $PR$  dalla topologia  $v$  di  $\Omega$ , ed è ovviamente  $\supseteq$  della topologia naturale di  $PR$ , in quanto  $(PR^+)^r \subseteq Q_r$ ; d'altra parte la topologia naturale di  $PR$  si sa essere  $\supseteq$  di ogni altra topologia; quindi  $P$  è continuo rispetto alla topologia naturale di  $R$  ed a quella di  $PR$  indotta dalla  $v$  di  $\Omega$ ; d'ora in poi, se  $P \in G$  e  $\zeta \in R$ , si scriverà  $\zeta(P)$  in luogo di  $P\zeta$ .

L'insieme  $G$  è un gruppo commutativo rispetto all'operazione di somma che ai punti  $P, Q \in G$  associa il punto  $P + Q$  tale che (nelle notazioni di 4.5)  $\zeta(P + Q) = \mu[(P\zeta)(Q\zeta)]$ , ossia  $\xi_i(P + Q) = g_i(\xi(P); \xi(Q))$ . Infatti le 4.6 dicono che  $P + Q = Q + P$ ,  $P + (Q + R) = (P + Q) + R$ , e che  $P + O = O + P$ , se  $O$  è il punto tale che  $\xi_i(O) = 0$  per ogni  $i$ ; l'esistenza, per ogni  $P \in G$ , del  $-P$  tale che  $-P + P = O$  discende facilmente dalle 4.6 (cfr. [6, 7], e cfr. anche le considerazioni che precedono il 4.11). Ogni tale  $G$  si dirà un gruppo analitico (commutativo) di dimensione  $n$  su  $(k, \Omega)$ ; dato  $G$ , l'ipercampo  $R$  che lo determina si indicherà con  $k\{G\}$ ; viceversa, dato l'ipercampo  $R$  con la legge  $P$ , il gruppo analitico legato ad esso si indicherà con  $G(R, \Omega)$ , e  $P$  si dirà la legge su  $G(R, \Omega)$ .

Gli omomorfismi e semiomomorfismi (come algebre su  $k$ ) delle iperalgebre e degli ipercampi sono definiti in modo ovvio (sono quelli che commutano con  $P$ , e quelli degli ipercampi sono necessariamente continui); un tale semiomorfismo è canonico se induce un automorfismo di  $k$ ; quanto ai gruppi analitici, se  $G, F$  sono due di essi (con lo stesso  $\Omega$ ), e  $\tau$  è una applicazione di  $G$  su  $F$ ,  $\tau$  è un omomorfismo (analitico) di  $G$  su  $F$  se, posto  $R = k\{G\}$ ,  $S = k\{F\}$ , esiste un omomorfismo  $\sigma$  di  $S$  su  $R$  (detto legato a  $\tau$ ) tale che  $\zeta(\tau P) = (\sigma\zeta)(P)$  per ogni  $\zeta \in S$  ed ogni  $P \in G$ ; ogni tale  $\sigma$  determina un  $\tau$ , e ne è determinato; il nome di « omomorfismo » dato a  $\tau$  è giustificato dal fatto che  $\tau(P + Q) = \tau P + \tau Q$ , come si verifica subito. Se  $\sigma$  è su tutto  $R$ ,  $\tau$  dicesi un isomorfismo (analitico), nome giustificato dal fatto che in tal caso il nucleo di  $\tau$  si riduce all'elemento  $O$  di  $G$ ; questa ultima condizione non è però sufficiente per asserire che  $\tau$  sia un isomorfi-

smo di gruppi analitici (benchè esso risulti certo un isomorfismo di gruppi). Dico invece che  $\tau$  è su tutto  $F$  se e solo se  $\sigma$  è un isomorfismo; e infatti, se  $\tau$  è su tutto  $F$ , si vede subito che da  $\sigma\zeta = 0$  segue  $\zeta(Q) = 0$  per ogni  $Q \in F$ , e quindi  $\zeta = 0$ . Viceversa, sia  $\sigma$  un isomorfismo, e sia  $Q \in F$ ; se  $S = k\{\eta_1, \dots, \eta_m\}$ , con gli  $\eta_i$  analiticamente indipendenti, è  $S(Q) = k\{\eta(Q)\} \subset \Omega$ ; esistono elementi  $\xi_{m+1}, \dots, \xi_n \in R$  tali che l'insieme  $\{\sigma\eta_1, \dots, \sigma\eta_m, \xi_{m+1}, \dots, \xi_n\}$  sia un insieme di parametri di  $R$ ; se quindi  $\{\zeta_1, \dots, \zeta_n\}$  è un insieme regolare di parametri di  $R$ , ogni  $\zeta_i$  è intero su  $k\{\sigma\eta, \xi\}$ ; per la proprietà di  $\Omega$ , esistono allora elementi  $\zeta'_i \in \Omega$  tali che l'applicazione  $\zeta_i \rightarrow \zeta'_i$  induca un omomorfismo di  $R$  su tutto  $k\{\zeta'_i\} \subset \Omega$ , ossia un punto  $P \in G$ , con la proprietà  $(\sigma\eta_i)(P) = \eta_i(Q)$ ,  $\xi_j(P) = 0$ ; ed allora  $Q = \tau P$ , come richiesto.

Sia  $J$  un ideale primo di  $S$ , tale che

$$4.7 \quad PJ \subseteq J \overline{\times} S + S \overline{\times} J,$$

e che  $S/J$  sia locale regolare; perchè l'ultima condizione sia soddisfatta è noto che occorre e basta che esista un insieme regolare  $\{\zeta_1, \dots, \zeta_m\}$  di parametri di  $S$  tale che  $J$  sia generato da, per esempio,  $\zeta_{n+1}, \dots, \zeta_m$ ; sia  $\sigma$  l'omomorfismo naturale di  $S$  su tutto  $R = S/J$ ; se si definisce, per  $\zeta \in S$ ,  $P\sigma\zeta = (\sigma \overline{\times} \sigma)P\zeta$ ,  $R$  diviene un ipercampo; se  $G = G(R, \Omega)$ , l'omomorfismo  $\tau$  di  $G$  su  $F$ , legato a  $\sigma$ , è un isomorfismo, ed è tale che, per  $P \in G$ ,  $\tau P$  è il punto di  $F$  per il quale  $\zeta_i(\tau P) = (\sigma \zeta_i)(P)$  ( $i = 1, \dots, n$ ), mentre  $\zeta_i(\tau P) = 0$  ( $i = n + 1, \dots, m$ ); esso può essere identificato con  $P$ , cosicchè  $G$  diviene il sottoinsieme di  $F$  costituito dai  $P \in F$  tali che  $J(P) = 0$ ; un siffatto insieme dicesi un *sottogruppo analitico di  $F$* . Dimostriamo, reciprocamente, il seguente risultato parziale: se  $J$  è un ideale di  $S$ , e se l'insieme  $G$  dei  $P \in F$  tali che  $J(P) = 0$  è un gruppo (formale) rispetto alla legge su  $F$ , allora il radicale di  $J$  è un ideale primo che soddisfa la 4.7. Intanto, è  $J(P) = 0$  se e solo se  $(\text{rad } J)(P) = 0$ , onde si può supporre  $J = \text{rad } J$ , e dimostrare che  $J$  è primo; ora, se  $\{\zeta_1, \dots, \zeta_m\}$  è un insieme regolare di parametri di  $S$ , e se  $J_1, J_2$  sono primi minimali distinti di  $\overline{J}$ , detto  $P_1$  l'omomorfismo naturale di  $S$  su  $S/J_1$  si può supporre  $S/J_1 \subset \Omega$ , il che è quanto dire che  $P_1$  è un punto di  $G$ ; definito analagamente  $P_2$  mediante  $J_2$ , ma in modo che le  $\zeta_i(P_2)$  siano analiticamente indipendenti dalle  $\zeta_j(P_1)$  (il che vuol dire che  $k\{\zeta(P_1), \zeta(P_2)\}$  ha dimensione uguale alla somma delle dimensioni delle  $k\{\zeta(P_i)\}$ ), si consideri  $Q = P_1 + P_2$ , ove  $Q$  è un punto di  $G$  tale che  $\zeta_i(Q) = \nu \zeta_i(P_1)$ , essendo  $\nu$  un isomorfismo di  $S(P_1)$  su  $\Omega$  applicante le  $\zeta_i(P_1)$  su elementi analiticamente indipendenti dall'insieme delle  $\zeta_j(P_j)$  ( $j = 1, 2$ ); se si considera  $\nu^{-1}$  esteso a tutto  $k\{\zeta(Q), \zeta(P_1), \zeta(P_2)\}$ , in modo da applicare ogni elemento di  $k\{\zeta(P_1), \zeta(P_2)\}$  in sè, è  $\nu^{-1}[\zeta_i(Q - P_1 + P_2)] = \zeta_i(P_1 - P_1 + P_2) = \zeta_i(P_2)$ ; ora,

$Q - P_1 + P_2$  è un punto di  $G$ , il cui nucleo  $N$  contiene quindi qualche primo minimale  $J'$  di  $J$ ; la relazione precedente dice allora che  $J' \subseteq N \subseteq J_2$ , onde  $N = J_2$ ; ma se il nucleo di  $Q - P_1 + P_2$  è  $J_2$ , quello di  $Q = Q - O + O$ , che è  $J_1$ , contiene  $J_2$ , assurdo. L'asserzione resta pertanto dimostrata, dato che  $J$  soddisfa evidentemente la 4.7. Questi risultati verranno completati più avanti.

Passiamo ora a considerare le relazioni fra iperalgebre e ipercampi; anzitutto, è noto [6,7] che se  $R$  è un campo d'integrità (commutativo) di caratteristica  $p$ , e se  $r$  è un intero positivo, si chiama *iperderivazione  $r$ -speciale di  $R$*  ogni endomorfismo  $x$  dell' $R^{p^r}$ -modulo  $R$  tale che  $x1 = 0$  (ove  $1 \in R$ ); l'insieme delle iperderivazioni  $r$ -speciali di  $R$  è un'algebra su  $R^{p^r}$ , ed è anche un  $R$ -modulo sinistro; appartengono ad esso, per ogni  $r$ , le *derivazioni*, che sono quelle iperderivazioni  $x$  che soddisfano la  $x(\eta\zeta) = \eta x\zeta + \zeta x\eta$  per  $\eta, \zeta \in R$ . Se in particolare  $R$  è un ipercampo di dimensione  $n$ , una iperderivazione  $r$ -speciale  $x$  di  $R$  dicesi *invariante* se  $P(x\eta) = (\iota \overline{x}) P\eta = (x \overline{\iota}) P\eta$  per ogni  $\eta \in R$ ; se  $\{\zeta_1, \dots, \zeta_n\}$  è un insieme regolare di parametri di  $R$ , e se si pone, per brevità,  $\zeta^h = \zeta_1^{h_1} \dots \zeta_n^{h_n}$  quando  $h = (h_1, \dots, h_n) \in I^n$ , si può esprimere, in un sol modo, la legge  $P$  di  $R$  nella forma

$$4.8 \quad P\eta = \sum_{h \in I^n} \zeta^h (\otimes) x_h \eta \quad (\zeta \in R),$$

le  $x_h$  essendo endomorfismi del  $k$ -modulo  $R$ ; si dimostra allora facilmente (cfr. [6, 7, 8]) che le  $x_h$  con  $0 < h \leq (p^r - 1, \dots, p^r - 1)$  formano una base dell'algebra  $\mathcal{D}_r^+(R)$ , su  $k$ , delle iperderivazioni  $r$ -speciali invarianti di  $R$ ; è poi  $x_0 = 1$ , e si porrà  $\mathcal{D}_r(R) = k \oplus \mathcal{D}_r^+(R)$ ,  $\mathcal{D}^+(R) = \bigcup_r \mathcal{D}_r^+(R)$ ,  $\mathcal{D}(R) = \bigcup_r \mathcal{D}_r(R) = k \oplus \mathcal{D}^+(R)$ . Le  $x_{\varepsilon(i)}$  formano invece una base del  $k$ -modulo delle derivazioni invarianti di  $R$ , indicato con  $\mathcal{D}^*(R)$ .

Se  $R$  è un ipercampo, chiameremo suo *duale (debole)* il  $k$ -modulo degli omomorfismi  $x$  del  $k$ -modulo  $R$  su  $k$ , per ciascuno dei quali esiste un  $i$  tale che  $x \circ (R^+)^i = 0$ ; se invece  $A$  è un'iperalgebra, chiameremo suo *duale (forte)* il  $k$ -modulo degli omomorfismi del  $k$ -modulo  $A$  su  $k$ .

**4.9 TEOREMA.** *Sia  $R$  un ipercampo di dimensione  $n$ , e sia  $A = \mathcal{D}(R)$ ,  $A^+ = \mathcal{D}^+(R)$ ; sia  $\{\zeta_1, \dots, \zeta_n\}$  un insieme regolare di parametri di  $R$ , e sia  $\{x_h\}$  la base di  $A$  definita da 4.8. Allora  $A$  è duale di  $R$ , con legge di dualità  $x \circ \eta = (x\eta)(O)$ , ove  $x \in A$ ,  $\eta \in R$ , e  $O$  è il punto  $O$  del gruppo analitico  $G(R, \Omega)$ . L'algebra  $A$  è un'iperalgebra di dimensione  $n$ , con base strutturale  $\{x_h\}$ ; l'isomorfismo strutturale  $P$  di  $A$  è il trasposto dell'applicazione bilineare  $(\xi, \eta) \rightarrow \xi\eta$  di  $R \otimes R$  su  $R$ , mentre l'applicazione  $(x, y) \rightarrow xy$  di  $A \otimes A$  su  $A$  è il trasposto della legge  $P$  di  $R$ . Il duale di  $A$  è isomorfo ad  $R$ .*

**4.10 TEOREMA.** *Sia  $A$  un'iperalgebra di dimensione  $n$ , con base strutturale  $\{x_h\}$ ; allora il duale di  $A$  è un ipercampo  $R$  di dimensione  $n$ , un cui insieme regolare di parametri è costituito dalle  $\zeta_i$  definite da  $x_h \circ \zeta_i = \delta_{h, s(i)}$ . La legge  $P$  di  $R$  è il completamento del trasposto dell'applicazione  $(x, y) \rightarrow xy$  di  $A \otimes A$  su  $A$ , mentre l'applicazione  $(\xi, \eta) \rightarrow \xi\eta$  di  $R \overline{\times} R$  su  $R$  è il completamento del trasposto dell'isomorfismo strutturale  $P$  di  $A$ . Il duale di  $R$ , costruito come indicato nel 4.9, è isomorfo ad  $A$ , ed anzi, vi è un sol modo di definire l'applicazione bilineare  $(x, \eta) \rightarrow x\eta$  di  $A \times R$  su  $R$  in modo che sia soddisfatta la relazione  $x \circ y\eta = xy \circ \eta$ .*

**DIM. (schizzo).** Le dimostrazioni di 4.9 e 4.10 si trovano, in maniera concisa ma chiara, nelle prime pagine di [9]; comunque si tratta di un esercizio sulla dualità, nn cui schizzo è il seguente: dato  $R$ , e costruita  $A$  come al 4.9, dalla 4.8 segue subito che  $x_h \circ \zeta^l = \delta_{hl}$  ( $h, l \in I^n$ ); poi,  $A$  è l'unione delle  $A_r = \mathcal{D}_r(R)$ ; la  $A_r$  è caratterizzata dall'essere  $x \in A_r$  se e solo se  $x \circ \zeta^h = 0$  ogniqualvolta  $h \leq (p^r - 1, \dots, p^r - 1)$ , ed ha per base (come algebra su  $k$ ) l'insieme delle  $x_h$  con  $h \leq (p^r - 1, \dots, p^r - 1)$ . D'altra parte, il duale di  $R$  è il limite diretto dei duali degli  $R/(R^+)^{p^r}$ , ciascuno dei quali è isomorfo al corrispondente  $A_r$ , avendo lo stesso ordine. Quindi  $A$  è tutto il duale di  $R$ . L'isomorfismo strutturale  $P$  di  $A$  si ottiene osservando che la 4.8 dà appunto  $x_h (\eta\xi) = \sum_{r+s=h} (x_r \eta) (x_s \xi)$ . Osservando poi che  $xy \circ \eta = x \circ y\eta$  (il che servirà anche per il 4.10), la relazione  $xy \circ \eta = (x \otimes y) \circ P\eta$  è conseguenza dell'invarianza di  $x$  e  $y$ .

Data invece  $A$ , il suo duale  $R$  è certo somma diretta completa dei duali dei  $kx_h$ ; se  $\zeta^h$  è appunto definito da  $x_i \circ \zeta^h = \delta_{ih}$ , e se si definisce il prodotto di elementi di  $R$  mediante la relazione  $x \circ \eta\xi = Px \circ (\eta \otimes \xi)$ , si verifica direttamente che  $\zeta^h = \zeta_1^{h_1} \dots \zeta_n^{h_n}$ , ove  $\zeta_i$  sta per  $\zeta^{e(i)}$ . Pertanto  $R$  diviene un campo d'integrità, e quindi  $R = k[\zeta_1, \dots, \zeta_n]$ . La legge  $P$  di  $R$  si definisce mediante  $(x \otimes y) \circ P\eta = xy \circ \eta$ , e le 4.6 si verificano direttamente.

Infine, posto  $x_h x_l = \sum_s c_{hls} x_s$  ( $c_{hls} \in k$ , note), e  $x_i \zeta^m = \sum_s d_{ims} \zeta^s$  ( $d_{ims} \in k$ , incognite), si trova esservi un solo modo di determinare le  $d_{ims}$  in maniera che  $\sum_s c_{hls} x_s \circ \zeta^m = x_h \circ \sum_s d_{ims} \zeta^s$ , e precisamente  $d_{lmh} = c_{hlm}$ , C.V.D..

Siano  $A$  ed  $R$  legati come nei 4.9, 4.10, e sia  $G = G(R, \Omega)$ ; sia  $\{x_n\}$  una base strutturale di  $A$ , e si definiscano le  $y_l \in A$  col porre  $\sum_{r+s=h} x_r y_s = 0$ ; si vede subito che tali  $y_l$  sono unicamente determinate, e che  $\{y_l\}$  è una base strutturale di  $A$ ; inoltre esiste un solo isomorfismo  $\varrho$  (di iperalgebre) di  $A$  in  $A$  tale che  $\varrho(x) = x$  e  $\varrho(y) = y$ . Esiste pertanto un trasposto  $\varrho_{-1}$  di  $\varrho$ , che è un isomorfismo (di ipercampi) di  $R$  su tutto  $R$ , definito da  $x \circ \varrho_{-1} \eta = \varrho x \circ \eta$ ;  $\varrho_{-1}$  è continuo rispetto

alla topologia naturale di  $R$ , ed è l'unico tale isomorfismo che soddisfa la

$$\mu(\iota \overline{\times} \varrho_{-1}) P = \mu(\varrho_{-1} \overline{\times} \iota) P = 0,$$

ossia, nelle notazioni del 4.6,  $g_i(\xi; \varrho_{-1}\xi) = g_i(\varrho_{-1}\xi; \xi) = 0$ . Il  $\varrho_{-1}$  definisce un isomorfismo analitico  $\sigma$  di  $G$  su tutto  $G$ , che è precisamente il  $\sigma P = -P$  per  $P \in G$ ; pertanto  $\varrho$ ,  $\varrho_{-1}$ ,  $\sigma$  diconsi le *inversioni in*, rispettivamente,  $A$ ,  $R$ ,  $G$ .

**4.11 LEMMA.** *Sia  $A$  una iperalgebra di dimensione  $n$  e base strutturale  $\{x_h\}$ , e sia  $A_r$  ( $r = 1, 2, \dots$ ) il sotto- $k$ -modulo di  $A$  generato dalle  $x_h$  con  $0 \leq h \leq (p^r - 1, \dots, p^r - 1)$ ; allora  $A_r$  è una sottoalgebra di  $A$ , indipendente da  $\{x_h\}$ , una cui  $p$ -base è data dall'insieme delle  $x_{p^{i_\varepsilon(j)}}$  ( $j = 1, \dots, n$ ;  $i = 0, \dots, r - 1$ ).*

**DIM.** (cfr. Teor. 1 di [6] o (1.6) di [7]). Si è già visto nella dimostrazione dei 4.9 e 4.10 che  $A_r$  è un'algebra, indipendente da  $\{x_h\}$ ; posto

$$x_i^h = x_{p^{i_\varepsilon(1)}}^{h_1} \dots x_{p^{i_\varepsilon(n)}}^{h_n},$$

con  $0 \leq h \leq (p - 1, \dots, p - 1)$ , si vede facilmente che  $x_0^{h_0} \circ \zeta^l = (l_1!) \dots (l_n!) \delta_{hl} = l! \delta_{hl}$  (onde  $x_0^h = h! x_h$ ), cosicchè (per  $0 \leq l \leq (p - 1, \dots, p - 1)$ ) le  $x_{\varepsilon(j)}$  formano una  $p$ -base di  $A_1$ . Suppongasi il risultato vero per  $r \leq m$ ; per dimostrarlo nel caso  $r = m + 1$ , basta dimostrare che le  $x_0^{h_0} \dots x_m^{h_m}$ , con  $0 \leq h_i \leq (p - 1, \dots, p - 1)$ , sono linearmente indipendenti su  $k$ . Si indichino con  $y_1, \dots, y_{p^{mn}}$  le  $x_0^{h_0} \dots x_{m-1}^{h_{m-1}}$  distinte, e certo linearmente indipendenti su  $k$  per l'ipotesi di ricorrenza, e con  $\eta_1, \dots, \eta_{p^{mn}}$  le  $\zeta^h$  con  $0 \leq h \leq (p^m - 1, \dots, p^m - 1)$ ; per ipotesi, se  $H$  è la matrice  $(y_i \circ \eta_j)$ , è  $\det H \neq 0$ ; se  $L$  è la matrice degli  $y_i x_m^h \circ \eta_j \zeta^{lp^m}$  (con  $h$  ed  $l$  maggiori o uguali a 0, e  $\leq (p - 1, \dots, p - 1)$ ), ove  $i, h$  restano fissi in ciascuna riga, occorre dimostrare che è anche  $\det L \neq 0$ . Si considerino le  $h$  e le  $l$  ordinate lessicograficamente; è

$$y_i x_m^h \circ \eta_j \zeta^{lp^m} = x_m^h \circ (\zeta^{lp^m} y_i \eta_j) = \sum_{r+s=h} \binom{h}{r} (x_m^r \circ \zeta^{lp^m}) (x_m^s y_i \circ \eta_j) = \binom{h}{l} x_m^{h-l} y_i \circ \eta_j,$$

dato che le restrizioni delle  $x_m^h$  ad  $R^{p^m}$  formano una base di  $\mathcal{D}_i(R^{p^m})$ ; qui, si deve interpretare  $\binom{h}{l} = 0$  se  $h_i < l_i$  per qualche  $i$ , e in particolare se  $h$  precede  $l$  (nell'ordine lessicografico). Ed allora si vede che  $L$ , di ordine  $p^{(m+1)n}$ , consta di blocchi di matrici di ordine  $p^{mn}$ , con i blocchi diagonali tutti eguali ad  $H$ , ed i blocchi a destra della diagonale tutti nulli; pertanto  $\det L = \det H^{p^n} \neq 0$ , C.VD..

4.12 LEMMA. Nelle notazioni del 4.11, sia  $\{y_h\}$  ( $0 \leq h \leq (p^r - 1, \dots, p^r - 1)$ ) un insieme di elementi di  $A$ , tale che  $y_0 = 1$ , che gli  $y_{e(i)}$  siano linearmente indipendenti su  $k$ , e che  $P y_h = \sum_{i+j=h} y_i \otimes y_j$ . Allora  $\{y_h\}$  è una base di  $A_r$ , ed esistono degli  $y_i \in A$ , con  $(p^r - 1, \dots, p^r - 1) \ni l \leq (p^{r+1} - 1, \dots, p^{r+1} - 1)$ , che, insieme con i dati  $y_h$ , continuano a soddisfare le relazioni precedenti. L'insieme dei dati  $y_h$  e degli  $y_i$  trovati è una base dell'algebra  $A_{r+1}$ .

DIM. Per un dato  $h$ , pongasi  $\text{alt } h = \sum_i h_i$ ; vogliamo dimostrare anzitutto che i dati  $y_h$  sono linearmente indipendenti; se così non fosse, sia  $m$  il minimo intero tale che le  $y_h$  con  $\text{alt } h \leq m$  siano linearmente dipendenti; è certo  $m > 0$ . Se, per esempio,  $c_0 y_0 + \sum c_h y_h = 0$ , ove la  $\Sigma$  è estesa a tutte le  $h \leq (p^r - 1, \dots, p^r - 1)$ ,  $> 0$ , e per le quali  $\text{alt } h \leq m$ , e ove le  $c_h$  sono elementi, non tutti nulli, di  $k$ , si deve avere  $P c_0 y_0 + P \sum c_h y_h = 0$ , ossia  $(c_0 1 \otimes 1 + \sum c_h y_h \otimes 1) + (c_0 1 \otimes 1 + \sum c_h 1 \otimes y_h) + (-c_0 1 \otimes 1 + \sum_{\substack{q+s=h \\ q,s>0}} c_q \otimes y_s) = 0$ ; le prime due parentesi sono nulle, e si ha quindi  $-c_0 1 \otimes 1 + \sum_q y_q \otimes \sum_s c_{q+s} y_s = 0$ , ove  $\Sigma$  è estesa ai  $q > 0, < (p^r - 1, \dots, p^r - 1)$ , e pei quali  $\text{alt } q < m$  (se ne esistono), e la  $\Sigma$  è estesa a quegli  $s > 0$  tali che  $q + s$  sia  $\leq (p^r - 1, \dots, p^r - 1)$  e soddisfi la  $\text{alt } (q + s) \leq m$ . Quindi  $c_0 = c_{q+s} = 0$ , ossia  $c_h = 0$  se  $h = 0$  o se  $\text{alt } h > 1$ ; ma allora  $m = 1$  e  $c_0 = 0$ , onde  $c_h = 0$  per ogni  $h$  perchè le  $y_{e(i)}$  sono linearmente indipendenti. Pertanto le date  $y_h$  sono linearmente indipendenti.

Come conseguenza, se  $R$  è l'ipercampo duale di  $A$ , esistono elementi  $\xi_i \in R$  ( $i = 1, \dots, n$ ) tali che  $y_{e(j)} \circ \xi_i = \delta_{ij}$ , e che  $y_h \circ \xi_i = 0$  se  $0 \leq h \leq (p^r - 1, \dots, p^r - 1)$  e  $\text{alt } h \neq 1$ ; la prima relazione implica, come è noto, che  $\{\xi_1, \dots, \xi_n\}$  è un insieme regolare di parametri di  $R$ . Posto pertanto  $\xi^l = \xi_1^{l_1} \dots \xi_n^{l_n}$ , risulta  $y_h \circ \xi^l = \delta_{hl}$  per le date  $y_h$  e per ogni  $\xi^l$ ; queste relazioni dicono intanto che le  $y_h$  appartengono ad  $A_r$ , e che ne formano quindi una base, e servono inoltre a determinare le  $y_i$  con  $(p^r - 1, \dots, p^r - 1) \ni l \leq (p^{r+1} - 1, \dots, p^{r+1} - 1)$ ; come prima, ne segue che l'insieme delle date  $y_h$  e delle nuove  $y_i$  è una base di  $A_{r+1}$ ; inoltre, ogni nuovo insieme  $\{y_i\}$  è ottenibile in tal modo per mezzo di opportuni  $\xi_i$ , C.V.D.

Dal 4.12 si vede che la definizione di iperalgebra, data al principio di questo paragrafo, è fortemente sovrabbondante; si ha infatti:

4.13 COROLLARIO. Sia  $A$  un'algebra commutativa su  $k$ , generata, come  $k$  modulo, da un insieme  $\{y_h\}$  di suoi elementi, con  $h$  percorrente  $I^n$ ; suppongasi che le seguenti condizioni siano veri ca e:

- 1)  $y_0 = 1 =$  identità di  $A$ ;
- 2) le  $y_{e(i)}$  ( $i = 1, \dots, n$ ) sono linearmente indipendenti su  $k$ ;

3) esiste un omomorfismo  $P$  (di algebre) di  $A$  su  $A \otimes A$ , tale che, per ogni  $h$ ,  $P y_h = \sum_{r+s=h} y_r \otimes y_s$ .

Allora  $A$  è un'iper algebra di dimensione  $n$ , isomorfismo strutturale  $P$ , e base strutturale  $\{y_h\}$ .

DIM. La stessa dimostrazione data per il 4.12 mostra che le  $y_h$  sono linearmente indipendenti, e formano quindi una base di  $A$ ; l'iper campo  $R$  duale di  $A$  è allora costruibile, come nella dimostrazione dei 4.9 e 4.10, senza nessun intervento di  $A^+$ ; ne segue pertanto che l' $A^+$  generato dalle  $y_h$  con  $h > 0$  (come  $k$ -modulo) è un'algebra, e quindi un ideale di  $A$ , in quanto  $x \in A^+$  se e solo se  $x \circ 1 = 0$ , C.V.D..

4.14 LEMMA. Siano  $A, R$  rispettivamente un'iper algebra e un ipercampo duali l'uno dell'altro; se  $y_1, \dots, y_m$  sono elementi di  $A$ , linearmente indipendenti su  $k$ , gli  $y_i$ , interpretati come endomorfismi del  $k$ -modulo  $R$ , sono linearmente indipendenti su  $R$ .

DIM. Sia  $\{x_h\}$  ( $h \in I^n$ ) una base strutturale di  $A$ , e siano  $\zeta_1, \dots, \zeta_m$  elementi non tutti nulli di  $R$  tali che  $\sum_i \zeta_i y_i = 0$ , ossia tali che  $\sum_i \zeta_i (y_i \eta) = 0$  per ogni  $\eta \in R$ . Esiste un minimo intero  $r \geq 0$  tale che  $x_h \circ \zeta_i \neq 0$  per qualche valore di  $i$ , e per qualche  $h$  tale che  $\text{alt } h = r$  (cfr. la dimostrazione di 4.12 per la definizione di  $\text{alt}$ ); allora  $0 = \sum_i x_h \circ \zeta_i y_i \eta = \sum_i \sum_{u+v=h} (x_u \circ \zeta_i) (x_v \circ y_i \eta) = \sum_i (x_h \circ \zeta_i) y_i \eta$ , il che dice che le  $y_i$  sono linearmente dipendenti su  $k$ , C.V.D..

**5. Rappresentazioni dei  $T$ -moduli canonici.** In tutto questo paragrafo supporremo  $e = 1$ , ossia  $\omega = p$  (cfr. § 1); ricordiamo [10] che in tal caso  $K$  è isomorfo all'anello dei vettori infiniti di Witt a componenti in  $k$ ; identificheremo perciò  $K$  con tale anello. Ricordiamo anche che vi sono tre operatori fondamentali che si applicano ai vettori di Witt, e precisamente:

$$\begin{aligned} \mathfrak{t}(x_0, \dots, x_n) &= (0, x_0, \dots, x_n); \quad \pi(x_0, \dots, x_n) = (x_0^p, \dots, x_n^p); \\ \rho(x_0, \dots, x_n) &= (x_0, \dots, x_{n-1}); \end{aligned}$$

essi commutano a due a due, e si ha  $\mathfrak{t}\pi\rho = p =$  moltiplicazione per l'intero  $p$ ; se  $n = \infty$ ,  $\rho$  diviene l'identità.

Sia  $A$  un'algebra commutativa su  $k$ ; indicheremo con  $\mathcal{W}(A)$  l'anello dei vettori infiniti di Witt a componenti in  $A$ ; se  $x \in \mathcal{W}(A)$  ed  $a \in K$ , l'espressione  $ax$  (prodotto di vettori di Witt) ha significato, ed è un vettore di Witt a componenti in  $A$ ; nelle stesse notazioni, si ha  $\mathfrak{t}(ax) = (\pi a)\mathfrak{t}x = a^{\pi}x$ ; se allora  $b = \sum_0^{\infty} \mathfrak{t}^i b_i \in T$ , con  $b_i \in K$ , è lecito definire  $bx = \sum_0^{\infty} \mathfrak{t}^i (b_i x)$ ; valgono le relazioni  $b(cx) = (bc)x$ ,  $(b+c)x = bx + cx$ ,  $b(x+y) = bx + by$ ,  $1x = x$ . Queste definizioni saranno mantenute fisse nel seguito, cosicchè sarà lecito parlare di  $T$ -moduli di vettori di Witt; si noti che un sotto- $T$ -modulo finito  $M$  di  $\mathcal{W}(A)$  è canonico non appena esso soddisfa la 2.1, od anche non appena soddisfa la  $\pi M \subseteq M$ , in quanto la 2.2 è automaticamente soddisfatta. Se  $M$  è un sotto- $T$ -modulo di  $\mathcal{W}(A)$ , e se  $B^+$  è la minima sottoalgebra di  $A$  che contiene tutte le componenti di tutti gli elementi di  $M$ ,  $B = k + B^+$  (ovvero  $b = k \oplus B^+$  se  $A$  non ha identità) si dirà l'algebra involupante di  $M$ ; diremo poi che  $B$  involuppa  $M$  liberamente (od anche che è una sua algebra involupante libera) se esiste un opportuno insieme minimo  $\{x_1, \dots, x_m\}$  di generatori di  $M$ , con  $x_i = (x_{i0}, x_{i1}, \dots)$ , tale che le  $x_{ij}$  formino una  $p$ -base di  $B$ , naturalmente con la condizione  $x_{ij}^0 = 1 \in k$ .

**5.1 LEMMA.** Sia  $M$  un sotto- $T$ -modulo canonico di  $\mathcal{W}(A)$ , e sia  $A$  algebra involupante libera di  $M$ ; se allora  $\{y_1, \dots, y_m\}$  è un qualsiasi insieme minimo di generatori di  $M$ , con  $y_i = (y_{i0}, y_{i1}, \dots)$ , le  $y_{ij}$  formano una  $p$ -base di  $A$ .

**DIM.** Dalle relazioni  $\pi y_i = \sum_j a_{ij} y_j$  ( $a_{ij} \in T$ ) segue che ogni elemento di  $A$  è esprimibile in almeno un modo come polinomio nelle  $y_{ij}$ , di grado  $< p$  in ogni argomento, a coefficienti in  $k$ . Sia poi  $\{x_1, \dots, x_m\}$  un insieme mi-

nimo di generatori di  $M$  tale che le  $x_{ij}$  formino una  $p$ -base di  $A$ ; se le  $y_{ij}$  non formano una  $p$ -base di  $A$ , sia  $r$  il minimo intero tale che le  $y_{ij}$  ( $i = 1, \dots, m$ ;  $j = 0, \dots, r$ ) siano  $p$ -dipendenti; allora esiste un polinomio  $f(Y_{1r}, \dots, Y_{mr}) \neq 0$  nelle indeterminate  $Y_{ir}$ , a coefficienti in  $H = k[\dots y_{ij} \dots]$  ( $i = 1, \dots, m$ ;  $j = 0, \dots, r-1$ ), di grado  $< p$  in ogni argomento, e tale che  $f(\dots y_{ir} \dots) = 0$ . Esistono elementi  $c_{ij} \in k$ , tali che  $\det(c_{ij}) \neq 0$ , ed elementi  $b_i \in H$ , tali che  $y_{ir} = \sum_j c_{ij} x_{jr} + b^i$ ; posto allora  $g(\dots X_{ir} \dots) = f(\dots \sum_j c_{ij} X_{jr} + b_i \dots)$  (le  $X_{ir}$  essendo indeterminate),  $g$  ha grado  $< p$  in ogni argomento, ha coefficienti in  $H$ , è non nullo, ed è tale che  $g(\dots x_{ir} \dots) = 0$ , impossibile; quindi le  $y_{ij}$  formano una  $p$ -base di  $A$ , C.V.D.

Abbiamo usato fin'ora i vettori di Witt, ma si potrebbe usare qualsiasi tipo di « vettori » che si compongano secondo una legge ricorrente soddisfacente alle condizioni poste per la validità dell'(8) di [11]. Useremo nel seguito anche i vettori iperesponenziali, definiti in [12]; esistono dei polinomi  $E_i(x_0, \dots, x_j)$  ( $p^j \leq i < p^{j+1}$ ), a coefficienti nel corpo fondamentale  $C_p$  di caratteristica  $p$ , tali che i vettori iperesponenziali si compongono secondo la legge (ove si usa il segno di somma anzichè quello più solito di prodotto)  $(x_0, x_1, \dots) + (y_0, y_1, \dots) = (z_0, z_1, \dots)$ , con  $z_i = \sum_{r+s=p^i} E_r(x) E_s(y)$ ; si ha poi  $E_0(x) = 1$ ,  $E_{p^i}(x) = x_i$ ,  $E_i(z) = \sum_{r+s=i} E_r(x) E_s(y)$ ,  $E_i(0, x_0, x_1, \dots) = E_{i/p}(x_0, x_1, \dots)$ , da interpretare come 0 se  $i/p$  non è intero.

Il passaggio dai vettori di Witt agli iperesponenziali, e viceversa (cfr. [13], [22], o [11]), si fa per mezzo di certi polinomi  $w_i(x_0, \dots, x_i)$ ,  $h_i(y_0, \dots, y_i)$ , a coefficienti in  $C_p$ , tali che  $w_0(x) = h_0(x) = x_0$ . Più precisamente, se si ha la somma  $(x_0, x_1, \dots) + (y_0, y_1, \dots) = (z_0, z_1, \dots)$  di vettori di Witt (risp. di vettori iperesponenziali), allora la  $(h_0(x), h_1(x), \dots) + (h_0(y), h_1(y), \dots) = (h_0(z), h_1(z), \dots)$  (risp. la  $(w_0(x), w_1(x), \dots) + (w_0(y), w_1(y), \dots) = (w_0(z), w_1(z), \dots)$ ) è una somma di vettori iperesponenziali (risp. di Witt); i vettori  $(h_0(x), h_1(x), \dots)$ ,  $(w_0(x), w_1(x), \dots)$  saranno indicati rispettivamente con  $H(x_0, x_1, \dots)$  e  $W(x_0, x_1, \dots)$ . I  $w_i, h_i$  sono ricorrenti, vale a dire  $w_i(0, x_0, \dots, x_{i-1}) = w_{i-1}(x_0, \dots, x_{i-1})$ , e analogamente per le  $h_i$ .

Il prodotto  $(x_0, x_1, \dots)(y_0, y_1, \dots)$  è in generale definito solo fra vettori di Witt (benchè ciò che abbiamo chiamato « somma » di iperesponenziali sia comunemente chiamata « prodotto »); poichè a noi occorrerà anche il prodotto di vettori iperesponenziali, e quello di un vettore di Witt per uno iperesponenziale, daremo le seguenti definizioni: se  $x, y$  sono iperesponenziali, il loro prodotto è definito da  $xy = H[(Wx)(Wy)]$ , ed è un vettore iperesponenziale; se invece  $x$  è di Witt ed  $y$  è iperesponenziale, il loro prodotto sarà  $xy = H(xWy)$ , che è iperesponenziale. Vale la legge distributiva, e l'associativa quando ha senso; valgono poi le  $tW = Wt$ ,  $\pi W = W\pi$ ,  $tH = Ht$ ,  $\pi H = H\pi$ .

**5.2 TEOREMA.** *Sia  $M$  un  $T$ -modulo canonico; allora esiste un  $T$ -modulo canonico  $M'$  di vettori infiniti di Witt, isomorfo ad  $M$ , ad algebra invilupante libera.*

**DIM.** Sia  $\{y_1, \dots, y_m\}$  un insieme minimo di generatori di  $M$ , e sia  $C$  la matrice legata ad  $\{y\}$  nel senso di 2.8; è quindi  $\pi y = Cy$ . Siano  $X_{ij}$  ( $i = 1, \dots, m; j = 0, 1, \dots$ ) indeterminate su  $k$ , e pongasi  $X_i = (X_{i0}, X_{i1}, \dots)$  (vettore di Witt); previa la solita identificazione di  $t$  con  $\mathfrak{t}$  e  $\pi$  con  $\pi$ , le espressioni  $\pi X, CX$  (ove  $X$  è la matrice ad una colonna delle  $X_i$ ) hanno significato, ed ha significato la matrice  $\pi X - CX$ , i cui elementi sono vettori di Witt  $Z_i = (Z_{i0}, Z_{i1}, \dots)$ . Posto  $B = k[\dots X_{ij} \dots]$ , sia  $\sigma$  l'omomorfismo di  $B$  di nucleo  $N = \sum_{ij} BZ_{ij}$ ; se  $A = \sigma B$ ,  $x_{ij} = \sigma X_{ij}$ ,  $x_i = (x_{i0}, x_{i1}, \dots)$ , si constata facilmente che le  $x_{ij}$  formano una  $p$ -base di  $A$ , e che  $A$  è l'algebra invilupante del  $T$ -modulo  $M'$  generato dalle  $x_i$ . Essendo  $\pi x = Cx$ , ossia  $\pi x_i \in M'$ ,  $M'$  è un  $T$ -modulo canonico, di dimensione al massimo  $m$ ; ma tale dimensione è proprio  $m$ , per 2.4, dato che  $M'/tM'$  è isomorfo al  $k$ -modulo generato dalle  $x_{i0}, \dots, x_{m0}$ , che sono linearmente indipendenti su  $k$  in quanto  $X_{10}, \dots, X_{m0}$  sono linearmente indipendenti su  $k \bmod N$ . L'applicazione  $y_i \rightarrow x_i$  genera allora un omomorfismo  $\tau$  del  $T$ -modulo canonico  $M$  su tutto il  $T$ -modulo canonico  $M'$ ; poichè  $\tau$  ha nullità 0, esso è un isomorfismo, C.V.D..

Nel seguito, se  $x = (x_0, x_1, \dots)$  è un vettore di Witt, o iperesponenziale, a componenti in  $A$ , e se  $\sigma$  è un semiomomorfismo di  $A$ , si porrà  $\sigma x = (\sigma x_0, \sigma x_1, \dots)$ ; si indicherà poi con  $x \otimes 1$  il vettore  $(x_0 \otimes 1, x_1 \otimes 1, \dots)$  di  $A \otimes A$ .

**5.3 TEOREMA.** *Sia  $M$  un sotto- $T$ -modulo canonico di dimensione  $n$  di  $\mathcal{W}(A)$ , con algebra invilupante libera  $A$ . Esiste allora un solo omomorfismo  $P$  di  $A$  su  $A \otimes A$  (come algebra) tale che  $P1 = 1 \otimes 1$  e che*

$$5.4 \quad Px = x \otimes 1 + 1 \otimes x$$

per ogni  $x \in M$ . La  $A$ , con  $P$  come isomorfismo strutturale, diviene una iperalgebra di dimensione  $n$ .

Viceversa, sia  $A$  una iperalgebra di dimensione  $n$  e isomorfismo strutturale  $P$ , e sia  $M$  l'insieme di tutti gli elementi  $x \in \mathcal{W}(A)$  che soddisfano la 5.4. Allora  $M$  è un  $T$ -modulo canonico di dimensione  $n$ , ed è l'unico, fra i propri sotto- $T$ -moduli canonici, che abbia  $A$  come algebra invilupante libera.

**DIM.** Invece di usare  $M$ , useremo  $HM$ , che è un  $T$ -modulo canonico di vettori iperesponenziali, ad algebra invilupante libera  $A$ . Siano  $y_i = (y_{i0}, y_{i1}, \dots) = Hx_i$  gli elementi di un insieme minimo di generatori di  $HM$  ( $i = 1, \dots, n$ ); vogliamo dimostrare che le relazioni  $Px_i = x_i \otimes 1 +$

$+ 1 \otimes x_i$  definiscono effettivamente un omomorfismo di  $A$ . Essendo l'insieme delle  $x_{ij}$  una  $p$  base di  $A$ , per 5.1, ciò sarà vero se è vero che la relazione  $\pi x_i = \sum_j a_{ij} x_j$  ( $a_{ij} \in T$ ) implica  $\pi P x_i = \sum_j a_{ij} P x_j$ ; e la verifica della verità di questa asserzione è immediata. Pertanto  $P$  è effettivamente definito, ed è un omomorfismo di algebre; si ha quindi  $P y_i = P H x_i = H P x_i = H [x_i \otimes 1 + 1 \otimes x_i] = y_i \otimes 1 + 1 \otimes y_i$ . Posto, per  $h = (h_1, \dots, h_n) \in I_n$ ,  $E_h(y) = E_{h_1}(y_{10}, y_{11}, \dots) \dots E_{h_n}(y_{n0}, y_{n1}, \dots)$ , la precedente si può scrivere:  $P E_h(y) = \sum_{r+s=h} E_r(y) \otimes E_s(y)$ , che dimostra, per 4.13, che  $A$ , con l'isomorfismo strutturale  $P$ , è un'iper algebra di dimensione  $n$  e base strutturale  $\{E_h(y)\}$ . La prima parte del teorema risulta così dimostrata.

Per dimostrare la seconda parte, si consideri una base strutturale  $\{x_h\}$  di  $A$  ( $h \in I^n$ ); vogliamo trovare degli elementi  $y_{ij} \in A^+$  ( $i = 1, \dots, n; j = 0, 1, \dots$ ), tali che le  $E_h(y) = E_{h_1}(y_{10}, y_{11}, \dots) \dots E_{h_n}(y_{n0}, y_{n1}, \dots)$  siano un'altra base strutturale di  $A$ ; sceglieremo intanto  $y_{j0} = x_{e(j)}$ ; supposto poi che delle  $y_{ij}$  siano state trovate per  $j < r$ , in modo che siano soddisfatte le  $P E_h(y) = \sum_{r+s=h} E_r(y) \otimes E_s(y)$  per  $0 \leq h \leq (p^r - 1, \dots, p^r - 1)$  il 4.12 assicura l'esistenza di elementi  $y_{ir}$ , che rendono le precedenti soddisfatte per  $h \leq (p^r, \dots, p^r)$ ; ed allora esse saranno automaticamente soddisfatte per  $h \leq (p^{r+1} - 1, \dots, p^{r+1} - 1)$ . Pertanto, per 4.13, le  $E_h(y)$ , per  $h \in I^n$ , formano una base strutturale di  $A$ .

Sia allora  $M'$  il  $T$ -modulo dei vettori iperesponenziali  $z = (z_0, z_1, \dots)$ ,  $z_i \in A$ , tali che  $P z = z \otimes 1 + 1 \otimes z$ ; è evidentemente  $\pi M' \subseteq M'$ ; poi, i vettori  $y_i = (y_{i0}, y_{i1}, \dots)$  ( $i = 1, \dots, n$ ) appartengono ad  $M'$ ; se  $z \in M'$ , esistono certamente elementi  $a_{0i} \in T$  tali che  $z' = z - \sum_i a_{0i} y_i = t z_1 \in t M'$ ; poi, esistono degli  $a_{1i} \in T$  tali che  $z_1 - \sum_i a_{1i} y_i \in t M'$ , ecc.. Pertanto  $z = \sum_i (a_{0i} + t a_{1i} + \dots) y_i$ , onde  $M'$  è finito, di dimensione  $\leq n$ , ed è canonico. Esso ha dimensione  $n$  perchè le  $y_{i0}$  sono linearmente indipendenti su  $k$  (cfr. 2.4). Il secondo asserto dell'enunciato si dimostra allora subito applicando la trasformazione  $W$  agli elementi di  $M'$ , e ponendo  $W M' = M$ . Se poi  $N$  è un sotto- $T$ -modulo canonico di  $M$  avente  $A$  come algebra involupante libera, deve essere  $N \cap t M = t N$  (perchè le  $y_{i0}$  debbono figurare come prime componenti di elementi di  $N$ ); quindi, per 2.5, o  $N = M$ , o  $\dim N < n$ ; il secondo caso è impossibile, e perciò  $N = M$ , C.V.D..

Nel corso di questa dimostrazione si è anche provato il

**5.5 COROLLARIO.** *Sia  $A$  un'iper algebra di dimensione  $n$ ; allora esiste una base strutturale (detta iperesponenziale)  $\{y_h\}$  di  $A$  tale che  $y_h = E_{h_1}(z_{10}, z_{11}, \dots) \dots E_{h_n}(z_{n0}, z_{n1}, \dots)$ , ove  $z_{ji} = y_{p^i e(j)}$ .*

Sia ora  $A$  un'iper algebra, con isomorfismo strutturale  $P$ ; ogni  $x \in \mathcal{W}(A)$  tale che  $P x = x \otimes 1 + 1 \otimes x$  si dirà un *vettore canonico di Witt a componenti in  $A$* , od anche un *elemento canonico di  $\mathcal{W}(A)$* ; analogamente si defi-

niscono i *vettori canonici iperesponenziali*; l'insieme degli elementi canonici di  $\mathcal{W}(A)$  sarà indicato con  $\mathcal{C}(A)$ .

Siano  $A, B$  iperalgebre, e pongasi  $M = \mathcal{C}(A), P = \mathcal{C}(B)$ ; sia  $\sigma$  un semiomorfismo canonico dell'iperalgebra  $A$  sull'iperalgebra  $B$ ; allora l'applicazione  $(x_0, x_1, \dots) \rightarrow (\sigma x_0, \sigma x_1, \dots)$ , ove  $(x_0, x_1, \dots) \in M$ , è un semiomorfismo canonico  $\tau$  di  $M$  su  $P$ , che sarà detto *legato a  $\sigma$* . Viceversa, sia  $\tau$  un semiomorfismo canonico di  $M$  su  $P$ , e sia  $\{x_i\}$  ( $i = 1, \dots, n$ ), con  $x_i = (x_{i0}, x_{i1}, \dots)$ , un insieme minimo di generatori di  $M$ ; siano poi gli  $a_{ij}$  elementi di  $T$  tali che  $\pi x_i = \sum_j a_{ij} x_j$ . Posto  $\tau x_i = (y_{i0}, y_{i1}, \dots) \in P$ , è  $\pi \tau x_i = \pi \tau x_i = \sum_j a_{ij}^{\tau} \tau x_j$ , onde esiste un unico semiomorfismo  $\sigma$  (di algebre) di  $A$  su  $B$  tale che  $\sigma x_{ij} = y_{ij}$ ; tale  $\sigma$  risulta poi essere un semiomorfismo canonico di iperalgebre. Vi è pertanto una corrispondenza biunivoca fra semiomorfismi canonici di  $T$ -moduli canonici, e semiomorfismi canonici di iperalgebre. In particolare, esistono semiendomorfismi  $\pi, t$  di  $A$  (legati ai  $\pi = \pi, t = t$  di  $M$ ) tali che  $\pi x = x^p$  se  $x \in A$ , e che, nelle notazioni del 5.5,  $tz_{i0} = 0, tz_{ij} = z_{i,j-1}$  se  $j > 0$ ;  $t$  è sempre semiendomorfismo su tutto  $A$ , mentre  $\pi$  è su tutto  $A$  se e solo se  $M$  è equidimensionale; si noti che  $\pi t$ , legato a  $\pi t = p$ , non è l'omomorfismo nullo  $p = 0$  di  $A$ . Usando una base iperesponenziale di  $A$ , si vede che il duale del semiendomorfismo  $t$  di  $A$  è il semiendomorfismo  $\pi$ , dell'ipercampo  $R$  duale di  $A$  (4.9, 4.10), tale che  $\pi \zeta = \zeta^p$  per ogni  $\zeta \in R$ ; si ha cioè  $(tx \circ \zeta)^p = x \circ \zeta^p$ , e quindi anche  $[(tx) \zeta]^p = x(\zeta^p)$ . Ciò mostra, fra l'altro, che per qualsiasi base strutturale  $\{x_h\}$  di  $A$  si ha  $tx_h = x_{h/p}$ , da interpretare come 0 se  $h/p = p^{-1}h \notin I^n$ . Analogamente, il duale del  $\pi$  di  $A$  è il  $t$  di  $R$  tale che  $(x \circ t\zeta)^p = x^p \circ \zeta$ ; perciò  $xt\zeta = t(x^p\zeta)$ .

Consideriamo ora il gruppo analitico  $G = G(R, \Omega)$ ; se  $\tau, \tau'$  sono suoi endomorfismi, legati agli endomorfismi  $\sigma, \sigma'$  di  $R$ ,  $\tau + \tau'$  sarà l'endomorfismo di  $G$  legato al  $\mu(\sigma \overline{\times} \sigma')$   $P$  di  $R$  (nelle notazioni del 4.5), ossia:  $(\tau + \tau')P = \tau P + \tau'P$  se  $P \in G$ ; analogamente si definisce la somma di omomorfismi di  $G$  su un altro gruppo analitico. In tal modo, se  $n$  è un intero, è definito  $n\tau$  (che è  $= 0$  per definizione se  $n = 0$ ), ed è definito  $n1 = n$  nel caso particolare in cui  $\tau = 1 =$  *isomorfismo identico*; il  $-\tau$  è naturalmente definito da  $(-\tau)P = -(\tau P)$ .

Ora, i  $\pi, t$  di  $R$  sopra definiti non sono legati a omomorfismi di  $G$ , in quanto essi sono semiomorfismi ma non omomorfismi; per renderli interpretabili come omomorfismi, fisseremo una base strutturale  $\{x_h\}$  di  $A$ , e quindi un insieme regolare di parametri  $\{\xi_i\}$  di  $R$ ; indicheremo poi con  $B$  l'iperalgebra di base strutturale  $\{y_h\}$  tale che, se  $x_h x_l = \sum_r c_{hlr} x_r$ , sia  $y_h y_l = \sum_r c_{hlr}^{p-1} y_r$  ( $c_{hlr} \in k$ ); denoteremo con  $\pi_0$  l'omomorfismo di  $A$  su  $B$  tale che  $\pi_0 x_h = y_h^p$ . Il  $\pi_0$  ha un duale  $t_0$ , che è un omomorfismo su  $R$  dell'ipercampo  $S$  duale di  $B$ . Defuiremo invece un omomorfismo  $t_0$  di  $B$  su tutta

A col porre  $t_0 y_h = t x_h$ ; il duale di  $t_0$  è un isomorfismo  $\pi_0$  di  $R$  su  $S$ ; se  $\{\eta_i\}$  è l'insieme regolare di parametri di  $S$  che corrisponde ad  $\{y_h\}$ , si ha  $y_h \circ \pi_0 \zeta^l = t x_h \circ \zeta^l = \delta_{h,pl}$ , onde  $\pi_0 \zeta^i = \eta_i^p$ . Il  $\pi_0'$  definito mediante un'altra base strutturale di  $A$  è tale che  $\alpha \pi_0' = \pi_0$  per un opportuno isomorfismo  $\alpha$  su tutta  $B$ ; lo stesso dicasi per  $t_0$ .

Se  $G = G(R, \Omega)$ ,  $F = G(S, \Omega)$ , i  $\pi_0, t_0$  di  $R$  su  $S$  e di  $S$  su  $R$  (rispettivamente) sono legati, a norma del § 4, ad omomorfismi  $\pi_0, t_0$  di  $F$  su tutto  $G$ , e di  $G$  su  $F$ ; un rapido calcolo mostra allora che il prodotto  $\pi_0 t_0$  è l'endomorfismo  $p$  di  $G$ ; si deve però tener presente che ciò è vero solo se il  $t_0$  di  $B$  è costruito mediante la base  $\{y_h\}$  legata alla  $\{x_h\}$  usata per  $\pi_0$  nel modo detto; quando questo è il caso si dirà che  $\pi_0$  e  $t_0$  sono *concomitanti*. L'ordine di  $\pi_0, t_0$  può essere invertito, naturalmente con un'altra  $B$ , ottenendo ancora  $p = t_0 \pi_0$ .

**5.6 TEOREMA.** *Sia  $A$  un'iper algebra,  $\sigma$  un semiomorfismo canonico di  $A$  (come algebra) di nucleo  $C$ ; allora  $\sigma A$  è un'iper algebra (con la definizione naturale di  $P$ ) se e solo se  $PC \subseteq C \otimes A + A \otimes C$ . Se la condizione è verificata, e se  $\sigma$  indica anche il semiomorfismo canonico di  $\mathcal{C}(A)$  su  $\mathcal{C}(\sigma A)$ , indotto da  $\sigma$ , si ha:*

1.  $\text{conull } \sigma = 0$ ;

2. se  $x_i = (x_{i0}, x_{i1}, \dots)$  ( $i = 1, \dots, m$ ), e  $y_i = (y_{i0}, y_{i1}, \dots)$  ( $i = 1, \dots, n \leq m$ ) formano degli insiemi minimi di generatori di  $\mathcal{C}(A)$  e  $\mathcal{C}(\sigma A)$  rispettivamente, tali che, secondo il 2.6, esistano interi  $0 \leq s_1 \leq s_2 \leq \dots \leq s_n$  con la proprietà  $\sigma x_i = t^{s_i} y_i$  ( $i \leq n$ ),  $\sigma x_i = 0$  ( $i > n$ ), allora  $C$  è generato, come ideale, dagli  $x_{ij}$  con  $j < s_i$  se  $i \leq n$ , e  $j$  qualsiasi se  $i > n$ ;

3. se  $v_i = Hx_i$ , e  $z_h = E_{h_1}(v_{10}, v_{11}, \dots) \dots E_{h_m}(v_{m0}, v_{m1}, \dots)$  ( $h \in I^m$ ),  $C$  è generato, come  $k$  modulo, dalle  $z_h$  per le quali non ogni  $h_i$  è divisibile per il corrispondente  $p^{s_i}$  ( $i = 1, \dots, m$ ;  $s_i = \infty$  se  $i > n$ ;  $p^\infty = \infty$ ;  $0$  divisibile per  $\infty$ ).

**DM.** Se  $\sigma A$  è un'iper algebra, la condizione  $PC \subseteq C \otimes A + A \otimes C$  è certo verificata. Viceversa, suppongasi che la condizione sia verificata, e suppongasi anche che  $\sigma$  sia un omomorfismo, il caso più generale essendo una conseguenza immediata di questo più particolare; posto  $M = \mathcal{C}(A)$ ,  $M$  è un  $T$ -modulo canonico di dimensione  $m$ , e  $\sigma M$  è un  $T$ -modulo canonico, per esempio di dimensione  $n$ , ogni cui elemento  $\sigma x$  soddisfa la  $P\sigma x = (\sigma \otimes \sigma) Px = \sigma x \otimes 1 + 1 \otimes \sigma x$ . Se  $N$  è il nucleo dell'omomorfismo  $\sigma$  di  $M$ , per 2.5 esiste un insieme minimo di generatori  $\{x_i\}$ , con  $x_i = (x_{i0}, x_{i1}, \dots)$  ( $i = 1, \dots, m$ ), di  $M$  tale che gli  $x_{n+1}, \dots, x_m$  formino un insieme minimo di generatori di  $N$ . Sia  $s_1$  il minimo intero  $\nu$  tale che esistano elementi  $y' = (y'_0, y'_1, \dots)$  di  $\sigma M$ , ma non di  $\sigma tM = t\sigma M$ , con  $y'_0 = \dots = y'_{\nu-1} = 0$ ,

$y'_v \neq 0$ ; detto  $y_1 = (y_{10}, y_{11}, \dots)$  un elemento per il quale  $\nu = s_1$ , sia  $s_2$  (certo  $\geq s_1$  se esiste) il minimo intero  $\nu$  per il quale esistono degli  $z$  di  $\sigma M$ , ma non di  $t\sigma M$ , tali che  $z_0 = \dots = z_{\nu-1} = 0$ , e che  $z_\nu$  sia linearmente indipendente, su  $k$ , da  $y_{1s_1}$ ; detto  $y_2$  uno  $z$  con tale proprietà, si costruisca così una successione  $y_1, y_2, \dots$ . Dico che, se  $\mu$  è il semiomomorfismo di  $\sigma M$  di nucleo  $t\sigma M$  (il nucleo di  $\mu$  in  $T$  essendo l'ideale generato da  $p$  e  $t$ ), i  $\mu y_i$  sono linearmente indipendenti su  $k$ . Se infatti  $\sum_1^r \alpha_i \mu y_i = 0, \alpha_i \in k$ , esistono elementi  $a_i = (\alpha_i, \beta_i, \dots) \in K$  ( $\alpha_i, \beta_i, \dots \in k$ ) tali che  $\sum_1^r a_i y_i \in t\sigma M$ ; se  $s_1 = \dots = s_l < s_{l+1}$ , ciò dà intanto  $\alpha_1 = \dots = \alpha_l = 0$ ; allora  $\sum_{l+1}^r a_i y_i \in t\sigma M$ , il che dà  $\alpha_{l+1} = \dots = \alpha_n = 0$  se  $s_{l+1} = \dots = s_n < s_{n+1}$ , e così via. Essendo i  $\mu y_i$  linearmente indipendenti su  $k$ , il loro numero  $q$  è finito e  $\leq n = \dim \sigma M$ , per 2.4.

Dico ora che gli  $y_i$  generano  $\sigma M$ , per il che basta dimostrare (per 2.4) che i  $\mu y_i$  generano  $\mu\sigma M$ . Sia infatti  $\mu z$ , con  $z = (z_0, z_1, \dots) \in \sigma M$ , un elemento di  $\mu\sigma M$  che non sia combinazione lineare dei  $\mu y_i$ , e sia  $z_h$  la prima componente non nulla di  $z$ ; allora, per la costruzione degli  $y_i$ ,  $z_h$  è combinazione lineare, a coefficienti in  $k$ , degli  $y_{1s_1}, \dots, y_{qs_q}$ ; esistono quindi elementi  $a_1, \dots, a_q \in K$  tali che  $z' = z - \sum_1^q t^{h-s_i} a_i y_i$  (con  $a_i = 0$  se  $h < s_i$ ) abbia come prima componente non nulla (se ne esistono) la  $z'_h$ , con  $h' > h$ ; resta vero che  $\mu z'$  non è combinazione lineare dei  $\mu y_i$ , onde su  $z'$  si può ripetere lo stesso ragionamento, ottenendo uno  $z'' = z - \sum_1^q t^{h-s_i} a_i y_i - \sum_1^q t^{h'-s_i} a'_i y_i = z - \sum_1^q (t^{h-s_i} a_i + t^{h'-s_i} a'_i) y_i$  la cui prima componente non nulla è la  $z''_h$ , con  $h'' > h'$ , ecc.. Posto  $b_i = t^{h-s_i} a_i + t^{h'-s_i} a'_i + \dots \in T$ , è  $z = \sum_1^q b_i y_i$ ,  $\mu z = \sum_1^q (\mu b_i) \mu y_i$ , assurdo. Ciò prova che gli  $y_i$  generano  $\sigma M$ , e che di conseguenza  $q = n$ . Posto allora  $H y_i = (v_{i0}, v_{i1}, \dots)$ , gli

$$E_h(v) = E_{h_1}(v_{1s_1}, v_{1,s_1+1}, \dots) \dots E_{h_n}(v_{ns_n}, v_{n,s_n+1}, \dots) \quad (h \in I^n)$$

generano, come  $k$ -modulo, la  $\sigma A$ ; essendo i  $v_{is_i}$  linearmente indipendenti su  $k$ , la  $\sigma A$  è un'iperalgebra per 4.13. I vettori di Witt  $(y_{is_i}, y_{i,s_i+1}, \dots)$  generano tutto  $\mathcal{C}(\sigma A)$ , donde l'asserzione 1.

Si vede ora subito che gli  $s_i$  introdotti in questa dimostrazione coincidono con gli  $s_i$  dell'asserzione 2, e che quindi, nelle notazioni della 2, l'ideale  $C'$  generato dalle  $x_{ij}$  è  $\subseteq C$ . Se  $\tau$  indica l'omomorfismo di  $A$  di nucleo  $C'$ , essendo  $PC' \subseteq C' \otimes A + A \otimes C'$ ,  $\tau$  è un omomorfismo di iperalgebre, o di  $T$ -moduli canonici, e inoltre  $\sigma = \sigma'\tau$  per un  $\sigma'$  di nucleo  $\tau C$ . Poichè

null  $\tau \geq$  null  $\sigma$ , deve valere  $l' =$ ; poi, ins  $\tau \geq$  ins  $\sigma$ , onde ancora vale  $l' =$ , e  $\sigma'$  è un isomorfismo, ossia  $C = C'$ , che è la 2.

Infine, gli  $z_h$  indicati nella 3 sono certo elementi di  $C$ , poichè  $\sigma z_h = 0$  (per la proprietà di ricorrenza degli  $E_{h_i}$ ); invece, i rimanenti  $z_h$  sono linearmente indipendenti su  $k$ , mod  $C$ , poichè si è visto che i  $\sigma z_h$  formano una base strutturale di  $\sigma M$ ; ciò dimostra la 3, C.V.D..

Dal 5.6 segue, in particolare, che se  $\sigma$  è un semiomorfismo canonico dell'iper algebra  $A$  su un'iper algebra  $B$ ,  $\sigma A$  è certamente una sottoiper algebra di  $B$ ; e dalla dimostrazione del 5.6 si deduce che se  $l = \sum_i s_i$ ,  $p^l$  è l'inseparabilità del semiomorfismo canonico  $\sigma$  di  $M$  su  $\mathcal{C}(\sigma A)$ , o anche su  $\mathcal{C}(B)$  per ogni sopraiper algebra  $B$  di  $\sigma A$ ; tale  $p^l$  si chiamerà perciò *l'inseparabilità del semiomorfismo  $\sigma$  di  $A$* ; la *nullità di tale  $\sigma$*  è  $\dim A - \dim \sigma A$ , e la *conullità di tale  $\sigma$*  (quando  $B$  sia stata fissata) è  $\dim B - \dim \sigma A$ . Due iperalghebre  $A, B$  sono *isogene* se  $\mathcal{C}(A), \mathcal{C}(B)$  sono isogeni; ciò accade se e solo se  $\dim A = \dim B$ , ed esiste un omomorfismo di  $A$  su tutta  $B$ ; od anche se e solo se ciascuna di esse è immagine omomorfa dell'altra.

Se  $M$  è un  $T$ -modulo canonico, ogni isomorfismo  $\sigma$  di  $M$  su tutto un  $\mathcal{C}(A)$ , per qualche  $A$ , si dirà una *rappresentazione di  $M$* ; i 5.2, 5.3 assicurano che ogni  $M$  ha qualche rappresentazione; ed il 5.6 dice che due qualsiasi rappresentazioni  $\sigma, \tau$  di  $M$  sono *equivalenti*, nel senso che  $\tau = \tau' \sigma$  per un isomorfismo  $\tau'$  dell'iper algebra invilupante di  $\sigma M$  su tutta l'iper algebra invilupante di  $\tau M$ .

**5.7 TEOREMA.** *Siano  $A, R$  un'iper algebra e un ipercampo duali l'uno dell'altra; sia  $\sigma$  un semiomorfismo canonico di  $A$  su tutta l'iper algebra  $\sigma A$ , e sia  $\sigma_{-1}$  il semiisomorfismo canonico duale, su  $R$ , dell'ipercampo  $S$  duale di  $\sigma A$ ; sia  $C$  (ideale di  $A$ ) il nucleo di  $\sigma$ , e pongasi*

$$1. \quad J = (\sigma_{-1} S^+) R \text{ (ideale di } R \text{);}$$

nelle notazioni del 5.6, sia  $B$  la sottoalgebra di  $A$  generata, come algebra, dalle  $x_{ij}$  con  $i = 1, \dots, m$ , e  $j < s_i$ , cosicchè una base di  $B$  su  $k$  è data dall'insieme delle  $z_h$  con  $h \leq (p^{s_1} - 1, \dots, p^{s_m} - 1)$ ; allora:

$$2. \quad \sigma_{-1} S \text{ è l'insieme degli } \zeta \in R \text{ tali che } C \circ \zeta = 0;$$

$$3. \quad C \text{ è l'insieme degli } x \in A \text{ tali che } x \circ \sigma_{-1} S = 0;$$

$$4. \quad tB \subseteq B;$$

5. se l'insieme regolare  $\{\zeta_1, \dots, \zeta_m\}$  di parametri di  $R$  è legato a  $\{z_h\}$  dalle  $z_h \circ \zeta^l = \delta_{hl}$ , allora  $\{\zeta_1^{p^{s_1}}, \dots, \zeta_n^{p^{s_n}}\}$  è un insieme regolare di parametri di  $\sigma_{-1} S$ ;

6. se  $l = \sum_1^n s_i$ , onde  $p^l =$  ins  $\sigma$ ,  $J$  è primario di lunghezza  $p^l$  e dimensione  $m - n =$  null  $\sigma$ ;

7. se  $D$  è la sottoalgebra di  $A$  generata dalle  $x_{ij}$  con  $i > n$ ,  $D$  è anche la massima fra le sottoalgebre di  $B$  che sono sottoiper-algebre di  $A$ ; è  $\dim D = \text{null } \sigma$ ,  $D^+ = D \cap A^+$ ,  $D^+ A \cap B = D^+ B$  e  $B/D^+ B$  è un'algebra di ordine  $p^l$  su  $k$ ;

8.  $B$  è l'insieme degli  $x \in A$  tali che  $x \circ J = 0$ ;

9.  $B$  è l'insieme degli  $x \in A$  tali che  $x(\zeta\eta) = \zeta x\eta$  per  $\eta \in R$  e  $\zeta \in \sigma_{-1} S$ ;

10.  $J$  è l'insieme degli  $\zeta \in R$  tali che  $B \circ \zeta = 0$ ;

11.  $B$  è l'unica sottoalgebra  $H$  di  $A$  tale che  $PH \subseteq H \otimes H$  e che  $H^+ = H \cap A^+$  generi  $C$  (come ideale);

12.  $\sigma_{-1} S$  è l'insieme degli  $\zeta \in R$  tali che  $B^+ \zeta = 0$ , o anche tali che  $C\zeta = 0$ ;

13.  $C$  è l'insieme degli  $x \in A$  tali che  $x\sigma_{-1} S = 0$ ;

14.  $B$  è l'insieme degli  $x \in A$  tali che  $Px \in (k + C) \otimes (k + C)$ ;

15.  $\sigma_{-1} S$  è l'insieme degli  $\zeta \in R$  tali che  $P\zeta \in (k + J) \otimes (k + J)$ ;

16.  $\sigma_{-1} S$  è l'insieme degli  $\zeta \in R$  tali che  $x(\zeta\eta) = \zeta x\eta$  per  $x \in B$  ed  $\eta \in R$ ;

17.  $\sigma_{-1} S$  è l'unico sottoanello  $U$  di  $R$  tale che  $U^+ = U \cap R^+$  generi  $J$ , e che  $PU \subseteq U \otimes U$ ;

18.  $V = k\{\zeta_1, \dots, \zeta_n\}$  è la chiusura algebrica di  $\sigma_{-1} S$  in  $R$ ; esso è un sottoipercampo di  $R$ , puramente inseparabile su  $\sigma_{-1} S$ , e soddisfacente la  $V + R = \text{rad } J$ .

DIM. Si può supporre, senza perdita di generalità, che  $\sigma$  sia un omomorfismo, e che quindi  $\sigma_{-1}$  sia l'isomorfismo di immersione di  $S$  in  $R$ , cosicchè  $\sigma_{-1} S = S \subseteq R$ .

I. Le 2, 3 discendono dalla teoria della dualità di  $k$ -moduli; la 4 è palesemente vera. La 5 discende subito, dualizzando, dalla 3 del 5.6. La 6 è conseguenza della 5.

II. Ogni sottoiper-algebra  $D'$  di  $B$  genera, a norma del 5.6, il nucleo  $D^+ A$  di un omomorfismo  $\tau$  di  $A$ , tale che  $\sigma = \sigma' \tau$  per un  $\sigma'$  opportuno; il nucleo di  $\tau$  come omomorfismo di  $\mathcal{C}(A)$  è  $\mathcal{C}(D')$ , ed è contenuto nel nucleo dell'omomorfismo  $\sigma$  di  $\mathcal{C}(A)$ ; quindi  $D' \subseteq D$ ; il resto del 7 è palese.

III. Se  $x, y$  sono elementi di  $A$  che soddisfano la condizione posta nel 9 per  $x$ , si vede subito che anche  $xy$  vi soddisfa; quindi la 9 definisce una algebra  $B'$ . Se  $x \in B'$ ,  $\zeta \in S^+$ , ed  $\eta \in R$ , e se  $O$  è il punto  $O$  di  $G(R, \Omega)$ , si ha  $x \circ \zeta\eta = (x(\zeta\eta))(O) = (\zeta x\eta)(O) = 0$ ; quindi, per 1,  $x \circ J = 0$ , che è la condizione 8. Viceversa, se  $x \circ J = 0$ , per ogni  $h \in I^m$  si ha  $z_h \circ x(\zeta\eta) = z_h x \circ \zeta\eta = x z_h \circ \zeta\eta = x \circ z_h(\zeta\eta) = x \circ \sum_{r+s=h} (z_r \zeta)(z_s \eta)$ ; ma da  $\zeta \in S$  segue  $O \circ \zeta = 0$  per 2, onde  $O \circ z_r \zeta = O z_r \circ \zeta \subseteq O \circ \zeta = \{0\}$ , e  $z_r \zeta \in S$ ; quindi  $z_r \zeta \equiv z_r \circ \zeta \pmod{S^+}$ , onde  $z_h \circ x(\zeta\eta) = x \circ \sum_{r+s=h} (z_r \circ \zeta)(z_s \eta) = \sum_{r+s=h} (z_r \circ \zeta)(z_s \circ x\eta) = z_h \circ (\zeta x\eta)$ , il che prova che  $x(\zeta\eta) = \zeta x\eta$ , ossia prova che la condizione

8 su  $x$  implica la 9. Pertanto le 8, 9 definiscono la stessa algebra  $B'$ , e si ha  $B \subseteq B'$  perchè da  $h \leq (p^{s_1}-1, \dots, p^{s_m}-1)$  segue  $z_h \circ \zeta \eta = \sum_{r+s=h} (z_r \circ \zeta)(z_s \circ \eta) = 0$  se  $\zeta \in S^+$ , ossia  $z_h \circ J = 0$ . Per ogni tale  $B'$  (in luogo di  $B$ ) vale evidentemente la 10.

IV. Essendo, per III,  $B \subseteq B'$ , e  $B'^+ \subseteq C$  per 8 e 3, la  $B'^+$  genera l'ideale  $C$ ; è poi  $P B' \subseteq B' \otimes B'$ , perchè da  $x \in B'$ ,  $\zeta \in J$ ,  $\eta \in R$  segue  $P x \circ (\zeta \overline{\times} \eta) = x \circ \zeta \eta = 0$  per 8, onde  $P x \circ (J \overline{\times} R + R \overline{\times} J) = 0$ ,  $P x \in B' \otimes B'$ . Quindi  $B'$  è una delle  $H$  che soddisfano la 11. Dico poi che ogni tale  $H$ , e in particolare  $B$ , è  $\subseteq B'$ : se infatti  $\zeta \in S$  ed  $\eta \in R$ ; da  $x \in H$  segue  $x(\eta \zeta) = \mu(P x)(\eta \overline{\times} \zeta)$  (nelle notazioni di 4.5), ossia  $x(\eta \zeta) = \eta x \zeta + \zeta x \eta + \mu w(\eta \overline{\times} \zeta)$ , con  $w \in H^+ \otimes H^+$ . Ma  $x \zeta = 0$  (perchè  $z_h x \circ \zeta = 0$  per 3), e analogamente  $w(\eta \overline{\times} \zeta) = 0$ , onde  $x(\eta \zeta) = \zeta x \eta$ , che per 9 dà appunto  $x \in B'$ , ossia  $H \subseteq B'$ . Si osservi infine che la 12, e di conseguenza la 13, vale per ogni  $H$  che soddisfi la 11, e in particolare per  $B$  e  $B'$ : se infatti  $\zeta \in R$  è tale che  $H^+ \zeta = 0$ , si ha, per  $x \in A$ ,  $x H^+ \circ \zeta = x \circ H^+ \zeta = 0$ ,  $C \circ \zeta = 0$ , e  $\zeta \in S$  per 2; viceversa, se  $\zeta \in S$  si ha  $H^+ \zeta \subseteq B'^+ \zeta = \{0\}$ , come si vede ponendo  $x \in B'^+$ ,  $\eta = 1$  nel 9.

V. Vogliamo dimostrare ora che se  $H$  soddisfa la 11, è necessariamente  $H = B'$ . Prima di tutto, una osservazione: il dire che  $P H \subseteq H \otimes H$  significa dire che l'insieme  $H^*$  degli  $\zeta \in R$  tali che  $H \circ \zeta = 0$  è un ideale di  $R$ ; analogamente, se  $A_{(r)}$  indica il  $k$ -modulo generato dagli  $z_h$  con  $\text{alt } h \leq r$  (cfr. la dimostrazione di 4.12 per la definizione di  $\text{alt}$ ), essendo  $P A_{(r)} \subseteq A_{(r)} \otimes A_{(r)}$ , anche  $A_{(r)}^*$  è un ideale. Ma allora tale è  $H^* + A_{(r)}^*$ , e quindi la  $H' = H \cap A_{(r)}$  soddisfa la  $P H' \subseteq H' \otimes H'$ .

Ciò premesso, si consideri dapprima il caso in cui  $n = m$ , e si supponga, per assurdo,  $H \subset B'$ ; per 5,  $R$  è in questo caso un  $S$ -modulo libero di ordine  $p^l$ , e di base, per esempio,  $\{\eta_1, \dots, \eta_{p^l}\}$ ; questa è anche una base del corpo quoziente  $Q$  di  $R$  su quello di  $S$ . L' $R$ -modulo  $Z$  degli endomorfismi dell' $S$ -modulo  $R$  ha una base (nel senso della dipendenza lineare su  $R$ ) di potenza  $p^l$ ; avendo  $B$  ordine  $p^l$ , per 4.14 una base di  $B$  (su  $k$ ) è anche una base di  $Z$  (su  $R$ ). Poichè, per 9,  $B' \subseteq Z$ , e  $B \subseteq B'$  per III, di nuovo per 4.14 si conclude che in questo caso è  $B = B'$ , e quindi  $H \subset B$ . Se allora  $\{x_1, \dots, x_q\}$ , con  $q < p^l$ , è una base di  $H$ , la matrice  $(x_i \eta_j)$  ha più colonne che righe, onde, per esempio, le sue prime  $u \leq q$  colonne sono linearmente indipendenti su  $R$ , mentre ogni altra è loro combinazione lineare a coefficienti in  $Q$ ; se  $u < v \leq p^l$ , siano  $c_1, \dots, c_u$  elementi di  $Q$  tali che  $\sum_1^u c_j x_i \eta_j + x_i \eta_v = 0$  per ogni  $i$ , e quindi anche  $\sum_j c_j x \eta_j + x \eta_v = 0$  per ogni  $x \in H$ . Se  $x \in H^+ \cap A_{(1)} = H^+ \cap A^*$ , l'applicazione di  $x$  alla precedente dà  $\sum_j (x c_j)(x_i \eta_j) + [\sum_j c_j (x x_i) \eta_j + x x_i \eta_v] = 0$ , ossia  $\sum_j (x c_j)(x_i \eta_j) = 0$ , e  $x c_j = 0$ , stante l'indipendenza delle prime  $u$  colonne; analogo risultato si ottiene, per

ricorrenza su  $r$ , quando  $x \in H^+ \cap A_{(r)}$ . Quindi  $H^+ c_j = 0$ , onde, per 12 (che si è visto al IV essere valida per  $H$ ),  $c_j$  deve appartenere al corpo quoziente di  $S$ ; questa essendo una contraddizione (perchè implica  $\sum_j c_j \eta_j + \eta_0 = 0$ ), si conclude che  $H = B = B'$  se  $n = m$ .

Si consideri ora il caso  $n \leq m$ ; posto  $B'_r = B' \cap A_r$ ,  $H_r = H \cap A_r$ ,  $B'_r$  è finita, e  $B'_r + \subseteq C = H^+ A = \bigcup_s H_s^+ A$ ; quindi, per qualche  $s$ , è  $B'_r + \subseteq H_s^+ A$ . Ora, per quanto precedentemente osservato, è  $P H_s \subseteq H_s \otimes H_s$ , onde  $H_s^+ A$  è, per 5.6, il nucleo di un omomorfismo  $\sigma_s$  di  $A$  su tutta l'iper algebra  $\sigma_s A$ ; l' $S_s$  legato a  $\sigma_s$  (come  $S$  a  $\sigma$ ) soddisfa la  $S_s \supseteq R^{p^s}$ , cosicchè null  $\sigma_s = 0$ ; quindi, per il caso precedente in cui  $n = m$ ,  $H_s$  è, a norma dell'11, unicamente determinato da  $H_s^+ A$ ; e se  $J_s = S_s^+ R$ ,  $H_s$  è legato a  $J_s$  dalla 8. Siano ora  $\sigma'_r, S'_r, J'_r$  similmente legati alla  $B'_r$ ; essendo  $B'_r + A \subseteq H_s^+ A$ , è anche  $S'_r \supseteq S_s$  (per 2),  $J'_r \supseteq J_s$  (per 1),  $B'_r \subseteq H_s$  (per 8); ma allora  $B' = \bigcup_r B'_r \subseteq \bigcup_s H_s = H$ , e pertanto  $H = B'$ , e in particolare  $B = B'$ . È così dimostrata (per III e IV) la verità delle tesi 8, 9, 10, 11, 12, 13.

VI. Ogni  $x \in B$  soddisfa la condizione 14; se poi  $x$  soddisfa tale condizione, per  $\zeta \in S^+$  ed  $\eta \in R$  si ha  $x \circ (\zeta \eta) = P x \circ (\zeta \overline{\eta}) = 0$  per 13, onde  $x \in B$  per 8; ciò dimostra la 14. Analogamente, se  $\zeta \in R$  soddisfa la 15, è  $B^+ A \circ \zeta = 0$  per 8, onde  $\zeta \in S$  per 2; ciò dimostra la 15. Se  $\zeta \in R$  soddisfa la 16, postovi  $\eta = 1$ ,  $x \in B^+$ , si ha  $x \zeta = 0$ , onde  $\zeta \in S$  per 12; ciò dimostra la 16.

VII. Per 15,  $S$  è il massimo  $U$  che soddisfa la 17; se poi  $U \subset S$  soddisfa la 17, e se a partire da  $U$  si costruiscono un  $C_U$  da 3, poi un  $B_U$  da 14, poi un  $J_U$  da 10, si ha  $C_U \supset C$ ,  $B_U \supset B$ ,  $J_U \subset J$ , e d'altra parte  $U^+ R = J_U$  per 1, contro l'ipotesi. Ciò dimostra la 17. Quanto alla 18,  $V$  è legato a  $D$  come  $S$  lo è a  $B$ ; quindi  $V$  è un ipercampo, e soddisfa la  $V^+ R = \sum_i^n \zeta_i R = \text{rad } J$ . Infine è ben noto che  $V$  è algebricamente chiuso in  $R$ , C.V.D..

5.8 TEOREMA. Siano  $R, A$  come al 5.7; si ha:

1. un sottoanello  $S$  di  $R$  è un sottoipercampo di  $R$  se e solo se  $PS \subseteq \subseteq S \overline{S}$ ;
2. un sottoanello  $S$  di  $R$  è un sottoipercampo di  $R$  se e solo se  $xS \subseteq S$  per ogni  $x \in A$ ; in tal caso il duale dell'isomorfismo di immersione di  $S$  in  $R$  è dato dalla restrizione ad  $S$  degli elementi di  $A$ ;
3. un ideale  $J$  di  $R$  è il nucleo di un omomorfismo  $\tau$  dell'ipercampo  $R$  su tutto un ipercampo, se e solo se  $PJ \subseteq J \overline{R} + R \overline{J}$  e  $J = \text{rad } J$ ; e in tal caso  $\tau_{-1}$  è l'isomorfismo di immersione in  $A$  della  $B$  legata a  $J$  dalla 8 del 5.7;
4. se  $J$  è un ideale di  $R$  tale che  $PJ \subseteq J \overline{R} + R \overline{J}$ , esiste un solo sottoanello  $U$  di  $R$  legato a  $J$  come al 17 di 5.7; tale  $U$  è un sottoipercampo di  $R$ .

DIM. Se  $S$  è sottoanello di  $R$  tale che  $PS \subseteq S \overline{\times} S$ , il  $C$  legato ad  $S$  dalla 3 del 5.7 è un ideale di  $A$ , e soddisfa la  $PC \subseteq C \otimes A + A \otimes C$  perchè  $S$  è un anello; allora, per 5.6,  $C$  è nucleo di un omomorfismo  $\sigma$  di  $A$  su tutta  $\sigma A$ , e dualizzando si ottiene che  $S$  è isomorfo all'ipercampo duale di  $\sigma A$ . Ciò dimostra la 1.

Se invece  $S$  è tale che  $xS \subseteq S$  per ogni  $x \in A$ , la definizione 4.8 delle  $x_n$  di  $A$  dà che  $PS \subseteq R \overline{\times} S$ , e quindi  $PS \subseteq S \overline{\times} S$ ; ciò, e la 1, dicono che  $S$  è un sottoipercampo di  $R$ ; il resto della 2 è palese.

Se  $PJ \subseteq J \overline{\times} R + R \overline{\times} J$ , per dualità si vede che il  $B$  legato a  $J$  dalla 8 di 5.7 è un'algebra, e soddisfa la  $PB \subseteq B \otimes B$ ; allora, per le 10, 1, e 5 di 5.7, le  $\zeta_i^{p^{s_i}}$  di 5 sono una base di  $J$  come ideale; se  $J = \text{rad } J$ ,  $J$  è generato dalle  $\zeta_1, \dots, \zeta_m$ , ed allora si sa già (cfr. la dimostrazione della 4.7) che  $R/J$  è un ipercampo. Nelle notazioni del 5.7, è anche  $B = D$ , e il resto del 3 è palese.

Infine, se si abbandona la condizione  $\text{rad } J = J$ , la 4 discende subito dalle 17, 1 di 5.7, C.V.D..

Nelle notazioni del 5.8, pongasi  $G = G(R, \Omega)$ ; se  $J$  è un ideale di  $R$ , ed  $F$  è l'insieme dei  $P \in G$  tali che  $J(P) = 0$ , la 3 dice che per assicurarsi che  $F$  sia un sottogruppo analitico di  $G$  basta sapere che  $P + Q \in F$  ogniqualvolta  $P, Q \in F$ ; questa è una forte precisazione di quanto si disse nella discussione del 4.7. La 3 dice pure che se  $\sigma$  è un semiomorfismo canonico di  $R$  su un ipercampo,  $\sigma R$  è un ipercampo. La 3 del 5.8, in congiunzione con la 1 del 5.7, implica che il nucleo di un omomorfismo (analitico) di  $G$  è un sottogruppo (analitico) di  $G$ ; infine, un caso particolare della 4 del 5.8 stabilisce che ogni sottogruppo analitico  $N$  di  $G$  è il nucleo di un omomorfismo analitico separabile (ossia di inseparabilità 1; cfr. più avanti) di  $G$ , unicamente determinato a meno di isomorfismi; l'immagine di  $G$  in tale omomorfismo sarà indicata, al solito, con  $G/N$ .

Per ricapitolare, siano  $A, A'$  iperalgebre,  $R, R'$  gli ipercampi loro duali; sia  $M = \mathcal{C}(A)$ ,  $M' = \mathcal{C}(A')$ ,  $G = G(R, \Omega)$ ,  $G' = G(R', \Omega)$ , e sia  $\sigma$  un semiomorfismo canonico di  $A$  su  $A'$ ; sia  $\sigma_{-1}$  (di  $R'$  su  $R$ ) il duale di  $\sigma$ , e sia  $\tau$  l'omomorfismo di  $G$  su  $G'$  legato a  $\sigma_{-1}$  se  $\sigma$  è un omomorfismo; sia poi  $\sigma^*$  il semiomorfismo canonico di  $M$  su  $M'$  definito da  $\sigma^*x = \sigma x$  per  $x \in M$ . L'algebra  $B$  definita dall'11 del 5.7 si dirà il nocciolo di  $\sigma$ , e l'ideale  $J$  definito dall'1 del 5.7 è il nocciolo di  $\sigma_{-1}$ ; la  $D$  definita dal 7 del 5.7 è il radicale di  $B$ , mentre  $D^+A$  è il radicale di  $C$ ; i 5.7, 5.8 dicono, fra l'altro, che il nocciolo e il nucleo di  $\sigma$  si determinano a vicenda, e che l'immagine e il nocciolo di  $\sigma_{-1}$  si determinano a vicenda; che il nucleo di  $\sigma^*$  è legato al nucleo di  $\tau$  come  $M$  a  $G$ ; che il nocciolo di  $\sigma_{-1}$  è nucleo di qualche  $\sigma'_{-1}$  se e solo se coincide col proprio radicale; che il nocciolo di  $\sigma$  è l'immagine di qualche  $\sigma'$  e solo se coincide col proprio radicale; che  $\tau$  è su tutto  $G'$  se e solo

se  $\text{conull } \sigma^* = 0$ ; che  $\tau$  è un isomorfismo se e solo se  $\sigma^*$  è un isomorfismo di inseparabilità 1. Definiremo quindi:

$\text{null } \sigma_{-1} = \text{conull } \sigma = \text{dimensione del nucleo di } \sigma_{-1} = \dim R' - \dim \sigma_{-1} R'$ ;

$\text{conull } \sigma_{-1} = \text{null } \sigma = \text{dimensione del nucleo di } \sigma_{-1} = \dim R - \dim \sigma_{-1} R'$ ;

$\text{ins } \sigma_{-1} = \text{ins } \sigma$ ;  $\text{null } \tau = \text{null } \sigma^* = \text{dimensione del nucleo di } \tau$ ;

$\text{conull } \tau = \text{conull } \sigma^* = \dim G' - \dim \tau G$ ;  $\text{ins } \tau = \text{ins } \sigma$ .

$R$  ed  $R'$  sono *isogeni*, e tali sono  $G, G'$ , se e solo se tali sono  $A, A'$ ;  $A, R$ , e  $G$  sono, di volta in volta, *logaritmici, radicali, periodici, equidimensionali*, se tale è  $M$ ; lo stesso dicasi per le nozioni di *codimensione* e *ordine*. L'intero  $p^l = \text{ins } \sigma = \text{ins } \tau = \text{ins } \sigma_{-1} = \text{ins } \sigma^*$ , che è legato a  $B$  dalla 7 del 5.7, è caratterizzato dall'essere  $l$  anche la lunghezza di una catena non raffiabile di nuclei fra il nucleo di  $\sigma$  e il proprio radicale, o di noccioli fra il nocciolo di  $\sigma$  e il proprio radicale.

In base ai risultati di questo paragrafo, le iperalgebre, gli ipercampi, i gruppi analitici possono essere classificati secondo la classificazione 2.11 dei  $T$ -moduli canonici; interessa pertanto sapere la struttura delle iperalgebre  $A$  tali che  $\mathcal{C}(A) = M_{r,s}$ , con  $r$  intero positivo ed  $s$  intero non negativo ovvero  $s = \infty$ ; una tale iperalgebra sarà indicata con  $A_{r,s}$ , e l'ipercampo duale di  $A_{r,s}$  con  $R_{r,s}$ , mentre si porrà  $G_{r,s} = G(R_{r,s}, \Omega)$ . Si vede allora subito che  $A_{r,s}$  è unicamente determinata, a meno di isomorfismi, dal possedere una base strutturale iperesponenziale  $\{z_h\}$ , con  $h \in I^r$ , tale che  $z_h^p = z_l$ , con  $l = (h_r p^{-s}, h_1, h_2, \dots, h_{r-1})$ , ove  $z_l = 0$  se  $h_r p^{-s}$  non è intero ( $h_r p^{-\infty}$  si considera intero, ed  $= 0$ , se e solo se  $h_r = 0$ ). Le formule corrispondenti per  $R_{r,s}$  sono di scrittura algebricamente complicata, e verranno studiate nel § 7.

Ed allora, si vede che  $G_{1,0}$  e  $R_{1,0}$  sono univocamente determinati dall'averne dimensione 1 e ordine 1; la seconda richiesta significa che l'endomorfismo  $p$  di  $G_{1,0}$  ha nullità 0 e inseparabilità  $p$ ; ciò è verificato ponendo  $R_{1,0} = k[\zeta]$ , e  $P\zeta = \zeta \overline{\times} 1 + 1 \overline{\times} \zeta + \zeta \overline{\times} \zeta$ , ossia  $(1 + \zeta)(P + Q) = [(1 + \zeta)(P)][(1 + \zeta)(Q)]$ ; quindi un gruppo analitico è *logaritmico di dimensione 1 se e solo se è, come gruppo astratto, isomorfo al gruppo moltiplicativo degli elementi di  $\Omega$  che sono  $\equiv 1 \pmod{\Omega^+}$* . Anche il gruppo analitico  $G_{1,\infty} \times \dots \times G_{1,\infty}$  (e i corrispondenti  $R_{1,\infty} \overline{\times} \dots \overline{\times} R_{1,\infty}$  e  $A_{1,\infty} (\otimes) \dots (\otimes) A_{1,\infty}$ ) sono univocamente determinati dalla dimensione  $r$  (= numero dei fattori diretti) e dal fatto che  $A^p = 0$ , ossia che l'endomorfismo  $p$  di  $G_{1,\infty} \times \dots \times G_{1,\infty}$  è l'endomorfismo nullo; pertanto  $R_{1,\infty} \overline{\times} \dots \overline{\times} R_{1,\infty} = k\{\zeta_1, \dots, \zeta_r\}$ , con  $P\zeta_i = \zeta_i \overline{\times} 1 + 1 \overline{\times} \zeta_i$ , ossia: *un gruppo analitico è isomorfo a  $G_{1,\infty}$  se e solo se è isomorfo, come gruppo astratto, al gruppo additivo  $\Omega^+$* . I  $G_{1,\infty} \times \dots \times G_{1,\infty}$ , ed i corrispondenti  $R$  ed  $A$ , diconsi *vettoriali*; essi sono tutti e soli i periodici di periodo  $p$ .

Nello stesso modo si vede che un gruppo analitico è *isogeno a  $G_{r,\infty}$  se e solo se, come gruppo astratto, è isomorfo al gruppo additivo dei vettori di*

Witt ad  $r$  componenti in  $\Omega^+$ ; si è qui usata la parola « isogeno », anzichè « isomorfo », perchè la proprietà di avere dimensione  $r$  e periodo  $p^r$  è caratteristica di tutti i  $T$ -moduli canonici isogeni ad  $M_{r,\infty}$ . Si ha però un risultato più preciso, ossia:  $R_{r,\infty} = k\{\zeta_1, \dots, \zeta_r\}$ , con  $\mathbf{P}$  determinato, in notazioni di vettori di Witt, da  $(\mathbf{P}\zeta_1, \dots, \mathbf{P}\zeta_r) = (\zeta_1 \overline{\times} 1, \dots, \zeta_r \overline{\times} 1) + (1 \overline{\times} \zeta_1, \dots, 1 \overline{\times} \zeta_r)$ ; questo risultato si dimostra subito osservando che  $M_{r,\infty}$  si distingue, fra i  $T$ -moduli canonici ad esso isogeni, per il fatto di essere generato, come  $T[\pi]$ -modulo, da un solo elemento; quindi  $A_{r,\infty}$  si distingue, fra le iperalgebre ad essa isogene, dal fatto che  $A_{r,\infty}^*$  ha una base (come  $k$ -modulo) del tipo  $x, x^p, x^{p^2}, \dots, x^{p^{r-1}}$ , con  $x^{p^r} = 0$ ; e l'iperalgebra duale dell' $R_{r,\infty}$  sopra descritto ha appunto tale proprietà,  $x$  essendo definito da  $x \circ \zeta^h = \delta_{h,\varepsilon(1)}$ . Per quanto esposto, gli  $M_{r,\infty}$ ,  $A_{r,\infty}$ ,  $R_{r,\infty}$  diconsi di Witt. Per lo stesso risultato, ma nell'ambiente algebrico, vedasi [11].

**5.9 TEOREMA.** *Sia  $A$  un'iperalgebra di dimensione  $r$ ; sia  $R$  l'ipercampo duale di  $A$ , e sia  $G = G(R, \Omega)$ ,  $M = \mathcal{C}(A)$ . Allora:*

1.  *$A$  è isomorfa ad  $A_{1,1} \overline{\otimes} \dots \overline{\otimes} A_{1,1}$  ( $r$  fattori) se e solo se  $A^{*p} = 0$  e  $\text{codim } A \leq r$ , nel qual caso  $\text{codim } A = r$ ;*

2.  *$M$  è isomorfo ad  $M_{1,1} \oplus \dots \oplus M_{1,1}$  ( $r$  addendi) se e solo se  $\pi M = tM$ ;*

3.  *$R$  è isomorfo ad  $R_{1,1} \overline{\times} \dots \overline{\times} R_{1,1}$  ( $r$  fattori) se e solo se, detto  $\sigma$  l'endomorfismo di  $R$  legato all'endomorfismo  $p$  di  $G$ , è  $\sigma R = R^{p^2}$ .*

**DIM.** Le condizioni poste sono evidentemente necessarie; esse sono, altrettanto evidentemente, equivalenti fra loro; basta quindi dimostrare la sufficienza della 2. Supposto allora  $\pi M = tM$ , si osservi che  $t^{-1}\pi$  è un semiomorfismo canonico di  $M$  su tutto  $M$ ; quindi  $M$  si comporta, rispetto a  $t^{-1}\pi$ , come un  $T$ -modulo logaritmico si comporta rispetto a  $\pi$ ; ed allora, come nella dimostrazione del 2) di 2.11, si possono trovare dei generatori  $u_1, \dots, u_r$  di  $M$  tali che  $t^{-1}\pi u_i = u_i$ . Ciò fatto, è  $M = Tu_1 \oplus \dots \oplus Tu_r$ , con  $Tu_i \cong M_{1,1}$ , C.V.D..

Chiudiamo questo paragrafo con una osservazione sul nocciolo  $B$  di un omomorfismo  $\sigma$  dell'iperalgebra  $A$ , quando  $B$  è di ordine finito, ossia quando  $\text{null } \sigma = 0$ ; se  $p^l$  è tale ordine, si vede che, per  $r$  abbastanza elevato,  $B$  è generato, come algebra, dalle componenti degli elementi di un insieme di generatori del  $T$ -modulo  $\Delta$  dei vettori di Witt  $x = (x_0, \dots, x_r)$ , a componenti in  $A$ , che soddisfano le relazioni  $\sigma x_i = 0$  e  $(\mathbf{P}x_0, \dots, \mathbf{P}x_r) = (x_0 \overline{\otimes} 1, \dots, x_r \overline{\otimes} 1) + (1 \overline{\otimes} x_0, \dots, 1 \overline{\otimes} x_r)$ ;  $\Delta$  è un  $T$ -modulo qualora si definisca  $ax = (a_0, \dots, a_r)(x_0, \dots, x_r)$  per  $a = (a_0, a_1, \dots) \in K$ , e  $tx = ptx$ ; se ciò vale già per  $r = 0$  (ossia se  $B \subseteq A_1$ ),  $\Delta$  si riduce al sotto- $k$ -modulo di  $A^*$  considerato nella teoria di Jacobson.

**6. Alcuni nuovi algoritmi.** Sia  $I$  l'anello degli interi, e siano  $x_0, x_1, \dots, \xi_0, \xi_1, \dots$  delle indeterminate su  $I$ ; posto  $L = I[\dots, x_i, \dots]$ , e fissato un primo  $p$ , si consideri il vettore di Witt  $x = (x_0, x_1, \dots)$  rispetto al primo  $p$ , e si indichino, al solito, con  $x^{(i)}$  le sue componenti fantasma. Siano  $h_0 = 1, h_1, h_2, \dots$  tutti i monomi monici nelle  $x_i$ ; si introducano nuove indeterminate come prodotti formali  $h_i \xi_j$  (con  $h_0 \xi_j = \xi_j$ ), e pongasi  $A = I[\dots, h_i \xi_j, \dots]$ . Vogliamo definire l'operazione di prodotto di un elemento di  $L$  (a sinistra) per uno di  $A$  (a destra); tale operazione sarà univocamente definita se porremo le condizioni che essa sia un'applicazione bilineare di  $L \times A$  su  $A$  ( $L$  e  $A$  considerati come  $I$ -moduli), e che soddisfi le relazioni

$$6.1 \quad \begin{cases} h_i (h_j \zeta) = (h_i h_j) \zeta \\ x^{(i)} (\zeta \zeta') = \zeta x^{(i)} \zeta' + \zeta' x^{(i)} \zeta \end{cases} \quad (\zeta, \zeta' \in A).$$

Ciò posto, si ha :

**6.2 LEMMA.** Sia  $\zeta$  un elemento di  $A$ , e sia  $\theta$  l'endomorfismo dell'algebra  $L$  (su  $I$ ) tale che  $\theta x_i = x_{i+1}$  ( $i = 0, 1, \dots$ ); si indichi con  $\theta$  anche un qualsiasi endomorfismo di  $A$  (come algebra su  $I$ ) tale che  $\theta \zeta \equiv \zeta^p \pmod{p A}$ , e che  $\theta (h_i \zeta) \equiv (\theta h_i) (\zeta^p) \pmod{p A}$  per ogni  $i$ . Allora, per ogni  $\eta \in I[\dots, h_i \zeta, \dots]$ , si ha :

- 1)  $\theta \eta \equiv \eta^p \pmod{p A}$ ;
- 2)  $\theta (y \eta) \equiv (\theta y) \theta \eta \pmod{p A}$  per ogni  $y \in L$ ;
- 3)  $(\theta x_i) \theta \eta^{p^r} \equiv \theta (x_i (\eta^{p^r})) \pmod{p^{r+1} A}$ , se  $r \geq 0$ .

**DIM.** La 2) vale, per ipotesi, se  $\eta = \zeta$  e  $y = h_i$ , e quindi anche se  $\eta = \zeta$  e  $y \in L$ ; ma allora,  $\theta (y h_i \zeta) \equiv (\theta (y h_i)) \theta \zeta \equiv (\theta y) (\theta h_i) \theta \zeta \equiv (\theta y) \theta (h_i \zeta) \pmod{p A}$ , onde la 2) vale per  $\eta = h_i \zeta$ .

Dimostriamo ora che, per ogni  $\eta \in A$ , si ha

$$6.3 \quad x_{i+1} (\eta^p) \equiv (x_i \eta)^p \pmod{p A}.$$

Sia  $L'$  il prodotto tensoriale  $L \otimes \dots \otimes L$ ,  $p$  volte, e sia analogamente  $A' = A \otimes \dots \otimes A$ ; si indichi con  $x_{ij}$  l'elemento  $1 \otimes \dots \otimes 1 \otimes x_i \otimes 1 \otimes \dots \otimes 1$ , con  $x_i$  nell' $j$ -esimo fattore, e si ponga  $(z_0, z_1, \dots) = \sum_{j=1}^p (x_{0j}, x_{1j}, \dots)$ ; si faccia anche la convenzione  $x_{i1} = x_i$ . Se  $\mu$  indica l'applicazione multilineare  $v_1 \otimes \dots \otimes v_p \rightarrow v_1 v_2 \dots v_p$  di  $L'$  su  $L$ , od anche l'analogo di  $A'$  su  $A$ , si ha  $x_{i+1} (\eta^p) = \mu [z_{i+1} (\eta \otimes \dots \otimes \eta)]$ , dato che  $x^{(r)} (\eta^p) = \mu [(x^{(r)} \otimes 1 \otimes \dots \otimes 1 + \dots + 1 \otimes \dots \otimes 1 \otimes x^{(r)}) (\eta \otimes \dots \otimes \eta)]$ . Sia  $\lambda$  la permuta-

zione ciclica  $(1, \dots, p) \rightarrow (2, \dots, p, 1)$  dei secondi indici delle  $x_{ij}$ , od anche delle  $x_{ij}$  stesse.

Se  $g$  è un monomio nelle  $x_{nj}$ , che compare in  $z_{i+1}$ , e se  $\lambda g \neq g$ , il contributo dei  $\lambda^l g$  sia ad  $x_{i+1}(\eta^p)$ , che a  $(px)_{i+1} = \mu z_{i+1}$ , è  $\equiv 0 \pmod{pA}$ , o  $\pmod{pL}$  rispettivamente; se invece  $\lambda g = g$ , e se  $a \in I$  è il coefficiente con cui  $g$  compare in  $z_{i+1}$ , deve essere  $g = \prod_1^p x_{0j}^{n_0} \dots x_{ij}^{n_i}$ , con  $n_0 + pn_1 + \dots + p^i n_i = p^i$  (dovendo  $g$  avere peso  $p_{i+1}$  se si attribuisce il peso  $p^r$  ad  $x_r$ ); il contributo dei  $\lambda^l g$  a  $(px)_{i+1}$  è quindi  $\equiv ax_0^{pn_0} \dots x_i^{pn_i} \pmod{pL}$ . Poichè, per il teorema 2 di [10], si ha  $(px)_{i+1} \equiv x_i^p \pmod{pL}$ , è  $a \equiv 1 \pmod{pI}$  se  $n_0 = \dots = n_{i-1} = 0$  e  $n_i = 1$ , mentre  $a \equiv 0 \pmod{pI}$  negli altri casi. Pertanto  $x_{i+1}(\eta^p) = \mu [(x_i \otimes \dots \otimes x_i)(\eta \otimes \dots \otimes \eta)] = (x_i \eta)^p \pmod{pA}$ , che è appunto la 6.3.

Ciò premesso, e supposta la 1) valida per un dato  $\eta = h_j \zeta$ , si ha, tenendo presente che anche la 2) vale per tale  $\eta$ :

$\theta(x_i \eta) \equiv x_{i+1} \theta \eta \equiv x_{i+1}(\eta^p) \equiv (x_i \eta)^p \pmod{pA}$ , per 6.3; ciò dice che la 1) vale anche per  $x_i \eta$ ; quindi la 1), certo valida per  $\eta = \zeta$ , è valida per ogni  $\eta = h_i \zeta$ . Ma allora essa vale per ogni  $\eta \in I[\dots, h_i \zeta, \dots]$ , come richiesto.

Tornando alla 2), si osservi che la 6.3 si può ora scrivere:

$(\theta x_i) \theta \eta \equiv x_{i+1}(\eta^p) \equiv (x_i \eta)^p \equiv \theta(x_i \eta) \pmod{pA}$ , che è la 2) per ogni  $\eta$  e per  $y = x_i$ ; supposta allora la 2) valida per  $y = h_j$ , ne segue  $\theta(x_i h_j \eta) \equiv (\theta x_i) \theta(h_j \eta) \equiv (\theta x_i)(\theta h_j) \theta \eta = [\theta(x_i h_j)] \theta \eta \pmod{pA}$ , che è la 2) per  $y = x_i h_j$ ; quindi la 2) è valida per ogni  $y$  ed ogni  $\eta$ .

Resta da dimostrare la 3); si costruiscano allora le  $L', \Lambda', x_{rj}, z_j$  come prima, ma con  $p^r$  fattori anzichè  $p$ , e sia  $\lambda$  la permutazione  $(1, \dots, p^r) \rightarrow (2, \dots, p^r, 1)$ . Da 1) si ha  $\theta \eta \equiv \eta^p \pmod{pA}$ , onde  $\theta \eta^{p^r} \equiv \eta^{p^{r+1}} \pmod{p^{r+1}A}$ ; quindi  $(\theta x_i)(\theta \eta^{p^r}) \equiv x_{i+1}(\eta^{p^{r+1}}) = \mu [z_{i+1}(\eta^p \otimes \dots \otimes \eta^p)] \pmod{p^{r+1}A}$ . Ora,  $z_{i+1} = (\theta \otimes \dots \otimes \theta) z_i + q$ , ove  $q$  è somma di quelli, fra i termini che compaiono nel polinomio  $z_{i+1} \in I[\dots, x_{nj}, \dots]$ , che hanno grado positivo in qualche  $x_{0j}$ .

Sia  $g$  un monomio che compare in  $z_{i+1}$  col coefficiente  $a \in I$ , e sia  $s$  il minimo intero  $\geq 0$ , e certo  $\leq r$ , tale che  $\lambda^{p^s} g = g$ ; allora  $z_{i+1}$  contiene  $p^s$  elementi distinti  $\lambda^l g$  tutti con lo stesso coefficiente  $a \in I$ , e il loro contributo a  $\mu [z_{i+1}(\eta^p \otimes \dots \otimes \eta^p)]$  è  $p^s a \mu [g(\eta^p \otimes \dots \otimes \eta^p)]$ ; d'altra parte, si può supporre  $g$  del tipo  $\prod_1^{p^r-s} \lambda^{m p^s} h_n$ ; qui distingueremo due casi: se  $g$  compare in  $q$ , ossia se  $h_n$  contiene il fattore  $x_0$ , da  $x_0(\eta^p) = p \eta^{p-1} x_0 \eta$  segue  $h_n(\eta^p) \equiv 0 \pmod{pA}$ , e perciò  $\mu [g(\eta^p \otimes \dots \otimes \eta^p)] = \eta^{p(p^r - p^{r-s})} [h_n(\eta^p)]^{p^r-s} \equiv 0 \pmod{p^{r-s+1}A}$ , onde infine il contributo dei  $\lambda^l g$  a  $\mu [z_{i+1}(\eta^p \otimes \dots \otimes \eta^p)]$  è  $\equiv 0 \pmod{p^{r+1}A}$ . Se invece  $g$  compare in  $(\theta \otimes \dots \otimes \theta) z_i$ , ossia se  $h_n$  non

contiene il fattore  $x_0$ , sarà  $h_n = \theta h_j$ ,  $g = (\theta \otimes \dots \otimes \theta) f$ , e, per 1) e 2),  $h_n(\eta^p) \equiv (\theta h_j) \theta \eta \equiv \theta(h_j \eta) \pmod{pA}$ , onde  $\mu[g(\eta^p \otimes \dots \otimes \eta^p)] \equiv \eta^{p(p^r - p^{r-s})} [h_n(\eta^p)]^{p^{r-s}} \equiv (\theta \eta)^{p^r - p^{r-s}} [\theta(h_j \eta)]^{p^{r-s}} \pmod{p^{r-s+1}A}$ ; in tal caso, il contributo dei  $\lambda^l g$  a  $(\theta x_i) \theta \eta^{p^r}$  è quindi  $\equiv p^s a (\theta \eta)^{p^r - p^{r-s}} [\theta(h_j \eta)]^{p^{r-s}} \pmod{p^{r+1}A}$ . D'altra parte, il contributo dei  $\lambda^l f$  a  $x_i(\eta^{p^r}) = \mu[z_i(\eta \otimes \dots \otimes \eta)]$  è  $p^s a \eta^{p^r - p^{r-s}} (h_j \eta)^{p^{r-s}}$ , donde la 3), C.V.D..

Se  $Q$  è il corpo razionale, l'estensione dell'algebra  $A$  su  $Q$  esiste; e sarà indicata con  $QA$ ; in  $QA$  introduciamo la metrica definita dalla successione  $\{M^n\}$  di ideali, ove  $M$  è generato dalle  $\xi_i$ , e indichiamo con  $A'$  il completamento di  $QA$  rispetto a tale metrica. Se  $\mathbf{1}$  è il vettore di Witt  $(1, 0, 0, \dots)$ , e  $\xi_{(i)}$  è il vettore di Witt  $t^i(\xi_i, 0, 0, \dots)$ , pongasi  $\zeta = \prod_{i=0}^{\infty} (\mathbf{1} - \xi_{(i)})$ ; la serie  $-\sum_{n=1}^{\infty} n^{-1} (\mathbf{1} - \zeta)^n$  ha per somma un vettore di Witt a componenti in  $A'$ , vettore che sarà indicato con  $\log \zeta$ , e che ha le componenti fantasma  $(\log \zeta)^{(i)} = \log \zeta^{(i)} = -\sum_{n=1}^{\infty} n^{-1} (1 - \zeta^{(i)})^n = \log [(1 - \xi_0^{p^i}) (1 - p \xi_1^{p^{i-1}}) \dots (1 - p^i \xi_i)]$ . Definiremo allora il vettore di Witt  $w = x \log \zeta$  mediante le  $w^{(i)} = x_i (\log \zeta)^{(i)}$ ; le componenti di  $w$  sono a priori in  $A'$ ; se però si tiene presente che  $x^{(r)} \log(1 - p^j \xi_j^{p^n}) = -p^j [x^{(r)} (\xi_j^{p^n})] (1 - p^j \xi_j^{p^n})^{-1}$ , si vede che in realtà  $w_i$  può scriversi come elemento dell'anello  $A_{(p)}$  definito nel modo seguente:  $A$  è l'anello delle frazioni con numeratore in  $A$  e denominatore nell'insieme moltiplicativamente chiuso generato da  $1$  e dagli  $1 - p^j \xi_j^{p^n}$ , ossia generato da elementi ciascuno dei quali è congruo, mod  $pA$ , ad una potenza di  $1 - \xi_0$  ad esponente intero  $\geq 0$ ;  $A_{(p)}$  è l'estensione di  $A$  sull'anello  $I_{(p)}$  dei numeri razionali del tipo  $m p^n$ , con  $m, n \in I$ . Dico che:

6.4 TEOREMA. Nelle notazioni precedenti,  $x \log \zeta$  ha tutte le componenti in  $A$ .

DIM. È ovviamente  $x \log \zeta = x \log(1 - \xi_{(0)}) + x \log(1 - \xi_{(1)}) + \dots$ , e quindi basta fare la dimostrazione per  $1 - \xi_{(l)}$ ; posto  $\xi_l = \eta$ , e  $w = x \log(1 - \xi_{(l)})$ , è  $w^{(n)} = 0$  se  $n < l$ , e  $w^{(n)} = x_n \log(1 - p^l \eta^{p^{n-l}}) = -x_n \sum_{i=1}^{\infty} i^{-1} p^{li} \eta^{ip^{n-l}}$  se  $n \geq l$ . Se il  $\theta$  del 6.2, operante ora su  $A'$ , è definito mediante le  $\theta(h_i \xi_j) = (\theta h_i) (\xi_j^p)$ , la 3) del 6.2 dà (non immediatamente, ma con calcolo facile):

$\theta w^{(n)} \equiv -x_{n+1} \sum_{i=1}^{\infty} i^{-1} p^{li} \eta^{ip^{n-l+1}} = w^{(n+1)} \pmod{p^{n+1}A'_p}$ , ove  $A'_p$  è il completamento dell'estensione  $A_p$  di  $A$  sull'anello dei razionali che sono interi

$p$ -adici; tale congruenza deve perciò essere valida anche modulo  $p^{n+1} A'_p \cap A_{(p)} = p^{n+1} A$ :

$$6.5 \quad \theta w^{(n)} \equiv w^{(n+1)} \pmod{p^{n+1} A}.$$

Suppongasi allora che sia vero che  $w^{(j)} \in A$  per  $j < n$ , dato che ciò è vero per  $j \leq l$ , e si scriva, per  $n > l$ ,

$$\begin{aligned} p^l w_l^{p^{n-l}} + p^{l+1} w_{l+1}^{p^{n-l-1}} + \dots + p^n w_n &= w^{(n)} \equiv \theta w^{(n-1)} = \\ &= p^l \theta w_l^{p^{n-l-1}} + p^{l+1} \theta w_{l+1}^{p^{n-l-2}} + \dots + p^{n-1} \theta w_{n-1} \pmod{p^n A}; \end{aligned} \text{dalla 1)}$$

di 6.2 si ricava  $p^{l+i} \theta w_{l+i}^{p^{n-l-i-1}} \equiv p^{l+i} w_{l+i}^{p^{n-l-i}} \pmod{p^n A}$  per  $i = 0, \dots, n-1-l$ , onde  $p^n w_n \equiv 0 \pmod{p^n A}$ , ossia  $w_n \in A$ , C.V.D. .

Il 6.4 mostra che  $x \log \zeta$  ha significato (riducendo mod  $p$  i coefficienti in  $Q$  che compaiono in esso) anche quando  $\zeta$  sia un vettore di Witt a componenti in un'algebra  $R$ , commutativa con identità, su un anello  $k$  di caratteristica  $p$ , purchè (per 6.1):

- 1)  $\zeta_0$  sia una unità di  $R$ ;
- 2)  $\zeta$  sia del tipo  $(\mathbf{1} - \xi_{(0)}) (\mathbf{1} - \xi_{(1)}) \dots$ , con  $\xi_{(i)} = t^i (\xi_i, 0, 0, \dots)$ ;
- 3)  $x$  sia un *vettore canonico di Witt di iperderivazioni di  $R$  su  $k$* , ossia:
  - a) gli  $x_i$  siano elementi, fra loro commutativi, dell'algebra  $A$  degli endomorfismi del  $k$ -modulo  $R$ ;
  - b) se  $P$  è l'applicazione di  $A$  su  $A \widehat{\otimes} A$  (prodotto tensoriale completo su  $k$ ) tale che, per  $\eta, \chi \in R$ , si abbia  $(P\eta) (\eta \widehat{\otimes} \chi) = \eta (\eta\chi)$ , allora

$$(Px_0, Px_1, \dots) = (x_0 \widehat{\otimes} 1, x_1 \widehat{\otimes} 1, \dots) + (1 \widehat{\otimes} x_0, 1 \widehat{\otimes} x_1, \dots).$$

D'altra parte, si vede subito che la condizione 2) è sempre verificata quando è verificata la 1), in quanto esistono i vettori di Witt, a componenti in  $R$ , dati da

$$\begin{aligned} \zeta' &= [\mathbf{1} - (1 - \zeta_0, 0, 0, \dots)]^{-1} \zeta = (1, \zeta'_1, \zeta'_2, \dots), \\ \zeta'' &= [\mathbf{1} - (0, -\zeta'_1, 0, 0, \dots)]^{-1} \zeta' = (1, 1, \zeta''_2, \zeta''_3, \dots), \text{ ecc.} \end{aligned}$$

In tali condizioni, il vettore  $\log \zeta$  naturalmente non ha significato, ma ha significato il vettore  $x \log \zeta$ ; esso ha componenti in  $R$ .

**6.6 TEOREMA.** *Sia  $R$  un'algebra commutativa con identità sull'anello  $k$  di caratteristica prima  $p > 0$ ; sia  $x$  un vettore canonico di Witt di iperderivazioni di  $R$  su  $k$ ; siano  $\zeta = (\zeta_0, \zeta_1, \dots)$ ,  $\eta = (\eta_0, \eta_1, \dots)$  vettori di Witt a*

componenti in  $R$ , con  $\zeta_0, \eta_0$  unità di  $R$  (ossia, siano  $\zeta, \eta$  elementi invertibili di  $\mathcal{W}(R)$ ); sia  $\alpha = (a, 0, 0, \dots)$ , con  $a \in k$ ; allora:

- 1)  $\zeta_0^{p^n} (x \log \zeta)_n \in R$ , e in particolare  $(x \log \zeta)_0 = \zeta_0^{-1} x_0 \zeta_0$ ;
- 2)  $x \log (\zeta \eta) = x \log \zeta + x \log \eta$ ;
- 3)  $(\alpha x) \log \zeta = \alpha (x \log \zeta)$ ;
- 4)  $x \log \pi \zeta = \pi [(tx) \log \zeta]$ ;
- 5)  $(tx) \log \zeta = t (x \log \zeta)$  se  $\zeta = (\zeta_0, 0, 0, \dots)$ .

DIM. Le 1) e 2) si dimostrano subito ricorrendo alle componenti fantasma; lo stesso dicasi per la 3), in quanto  $(\alpha x)_n = a^{p^n} x_n$ . Per la 4), usando le componenti fantasma, e nel caso particolare in cui  $\zeta = \mathbf{1} - \xi_{(l)}$ , con  $\xi_{(l)} = t^l (\chi, 0, 0, \dots)$ , dalla (c) di [10] si ricava  $[t(x \log \pi \zeta)]^{(n+1)} = p (x \log \pi \zeta)^{(n)} = p x_n \log (1 - p^l \chi^{p^{n-l+1}}) = p (tx)_{n+1} \log (1 - p^l \chi^{p^{n-l+1}}) = p [(tx) \log \zeta]^{(n+1)}$ , onde  $t(x \log \pi \zeta) = p [(tx) \log \zeta]$ , e quindi  $x \log \pi \zeta = \pi [(tx) \log \zeta]$ . Infine, la 5) deriva da 4) e 2) osservando che, in questo caso,  $\pi \zeta = \zeta^p$ , C.V.D..

Tornando ora ai significati primitivi di  $L$  e  $A$ , e ponendo  $\xi = (\xi_0, \xi_1, \dots)$ , definiremo il vettore di Witt  $x\xi$  mediante le  $(x\xi)^{(n)} = x_n \xi^{(n)}$ ; dico che  $x\xi$  ha le componenti in  $A$ . Basta evidentemente dimostrarlo quando  $\xi$  è sostituito da  $\xi_{(l)} = t^l (\xi_l, 0, 0, \dots)$ ; in tal caso, posto  $\xi_l = \eta$  e  $w = x\xi_{(l)}$ , è  $w^{(n)} = p^l x_n \eta^{p^{n-l}}$  se  $n \geq l$ , e  $w^{(n)} = 0$  se  $n < l$ ; per la 3) di 6.2 si ha allora  $\theta w^{(n)} \equiv w^{(n+1)} \pmod{p^{n+1} A}$ , che è la stessa della 6.5; come per la 6.5, se ne deduce appunto  $w_n \in A$ , come richiesto. Per tal motivo, l'espressione  $x\xi$  mantiene significato sotto le ipotesi del 6.6, ove ora però non vi è alcuna restrizione su  $\zeta_0$  ed  $\eta_0$ . Si vede anzi che, formalmente,  $x \log \zeta$  è ottenuto come  $x\xi$ , quando  $\xi = \log \zeta$ . Si osservi che non c'è pericolo di confondere  $x\xi$  con un normale prodotto di vettori di Witt, quest'ultimo potendo essere definito solo se il prodotto fra componenti è commutativo.

6.7 TEOREMA. Siano  $R, k, x, \alpha, \zeta, \eta$  come al 6.6, ma senza le restrizioni su  $\zeta_0$  ed  $\eta_0$ ; sia  $b$  un elemento di  $\mathcal{W}(k)$ ; allora:

- 1)  $x(\zeta + \eta) = x\zeta + x\eta$ ;
- 2)  $x(b\zeta) = b(x\zeta)$ ;
- 3)  $x\pi\zeta = \pi[(tx)\zeta]$ ;
- 4)  $(tx)(t\zeta) = t(x\zeta)$ ;
- 5)  $(\alpha x)\zeta = \alpha(x\zeta)$ .

DIM. Le 1), 2), 5) sono evidenti; la 3) si dimostra come la 4) del 6.6; per la 4), si ha, da 1) e 3):  $p(x\zeta) = xp\zeta = x\pi t\zeta = \pi[(tx)(t\zeta)]$ , donde  $t(x\zeta) = (tx)(t\zeta)$ , C.V.D..

Nel seguito, la componente di indice  $n$  del vettore di Witt  $x\zeta$  (in caratteristica  $p$ ) verrà indicata con  $w_n(x_0, \dots, x_n; \zeta_0, \dots, \zeta_n)$ .

Le operazioni  $x\zeta$  e  $x \log \zeta$  godono di altre proprietà, che però riescono più espressive nell'ambiente delle « iperclassi » (per uno schizzo delle applicazioni dell'operazione «  $x \log$  » ora introdotta, vedasi il § 7 di [14]). Passeremo invece ad altro argomento, che ha attinenza diretta con la presente investigazione.

Sia nuovamente  $Q$  il corpo razionale,  $I$  l'anello degli interi, e  $p$  un numero primo positivo; siano  $\xi_0, \xi_1, \dots, \eta_0, \eta_1, \dots$  indeterminate su  $Q$ , ed in  $Q[\dots, \xi_i, \dots; \dots, \eta_j, \dots]$  si consideri la metrica determinata dalla successione  $\{M^n\}$  di ideali, ove  $M$  ha la base  $\{\xi_0, \eta_0, \xi_1, \eta_1, \dots\}$ ; sia  $A'$  il completamento di  $Q[\xi; \eta]$  rispetto a tale metrica. Pongasi

$$\xi^{(i)} = \xi_i + p^{-1} \xi_{i+1}^p + p^{-2} \xi_{i+2}^{p^2} + \dots \in A',$$

ed analogamente per  $\eta^{(i)}$ ; posto  $\zeta^{(i)} = \xi^{(i)} + \eta^{(i)}$ , le relazioni  $\zeta^{(i)} = \zeta_i + p^{-1} \zeta_{i+1}^p + \dots$  definiscono le  $\zeta_i$  come elementi della chiusura  $A$  di  $I[\xi; \eta]$  in  $A'$ : infatti, in notazioni di vettori di Witt, la componente  $n$ -esima ( $n$  fisso e  $< i$ ) del vettore  $(\zeta_i, \zeta_{i-1}, \dots, \zeta_0)$  differisce dalla componente  $n$ -esima del vettore  $(\xi_i, \xi_{i-1}, \dots, \xi_0) + (\eta_i, \eta_{i-1}, \dots, \eta_0)$  per elementi di  $M^j$ , ove  $j \rightarrow \infty$  quando  $i \rightarrow \infty$ . Scriveremo allora, simbolicamente,  $(\dots, \xi_2, \xi_1, \xi_0) + (\dots, \eta_2, \eta_1, \eta_0) = (\dots, \zeta_2, \zeta_1, \zeta_0)$ ; è chiaro che esiste una  $\Phi'(\xi_0, \xi_1, \dots; \eta_0, \eta_1, \dots) \in A$  tale che  $\zeta_i = \Phi'(\xi_i, \xi_{i+1}, \dots; \eta_i, \eta_{i+1}, \dots)$ ; gli enti  $(\dots, \xi_2, \xi_1, \xi_0)$  saranno chiamati *covettori di Witt, di componenti  $\xi_i$  e componenti fantasma  $\xi^{(i)}$* ; indicheremo con  $\Phi$  ciò che si ottiene riducendo i coefficienti che compaiono in  $\Phi'$  modulo  $p$ .

L'insieme  $\mathcal{W}'(R^+)$  dei covettori di Witt a componenti in un anello  $R^+$  di caratteristica  $p$ , formano un gruppo abeliano additivo non appena in  $R^+$  sia data una metrica rispetto alla quale  $\Phi$  abbia significato (ossia converga); in particolare, ciò è verificato quando  $R^+$  sia il primo massimo di un anello locale completo  $R$  di caratteristica  $p$ ; in tal caso, se  $k$  è un sottocorpo algebricamente chiuso di  $R$ , e  $K$  ha lo stesso significato che ha nel § 5,  $\mathcal{W}'(R^+)$  forma anche un  $K$ -modulo (sinistro o destro) qualora si definisca l'operazione di prodotto nel modo seguente: per  $a = (a_0, a_1, \dots) \in K$ , e  $\zeta = (\dots, \zeta_1, \zeta_0) \in \mathcal{W}'(R^+)$ , il covettore  $\zeta a = a\zeta = (\dots, \eta_1, \eta_0) \in \mathcal{W}'(R^+)$  è definito col porre anzitutto, per ogni  $i$ ,  $(\xi_{i+1}, \dots, \xi_{i_0}) = [\pi^{-i}(a_0, \dots, a_i)](\zeta_i, \dots, \zeta_0)$  (vettori di Witt), e poi  $\eta_n = \lim_{i \rightarrow \infty} \xi_{in}$ ; che il limite esista si vede osservando che, a norma del (14) di [10], nel caso particolare in cui  $a = (0, \dots, 0, a_r, 0, \dots) = t^r(a_r, 0, 0, \dots)$ , si ha  $\xi_{in} = a_r^{p^{-n+r}} \zeta_{n+r}^{p^r}$  per  $i$  elevato.

Nelle notazioni precedenti (in caratteristica 0), ma partendo da  $Q[\dots, \xi_i, \dots]$  in luogo di  $Q[\dots, \xi_i, \dots; \dots, \eta_j, \dots]$ , siano  $x_0, x_1, \dots$  altre indeterminate su  $Q$ , e si ponga  $L = Q[\dots, x_i, \dots]$ ; come al principio di questo paragrafo, si introducano le nuove indeterminate  $h_i \xi_j$ , si costruiscano  $\Delta = Q[\dots, \xi_i, \dots]$  e  $\Delta = Q[\dots, h_i \xi_j, \dots]$ , e siano  $\Delta', \Delta'$  i completamenti di  $\Delta, \Delta$  rispettivamente nella metrica  $\{M^n\}$  di  $\Delta, M$  avendo la base  $\{\xi_0, \xi_1, \dots\}$ ; il prodotto  $y \zeta$  ( $y \in L, \zeta \in \Delta'$ ) è unicamente determinato dalle 6.1, e dalla condizione di bilinearità e continuità. Si considerino  $x = (x_0, x_1, \dots)$ , e  $\xi = (\dots, \xi_1, \xi_0)$  come un vettore e un covettore di Witt rispettivamente, e sia  $P$  l'isomorfismo (di algebre su  $Q$ ) di  $L$  su  $L \otimes L$  definito da  $Px^{(i)} = x^{(i)} \otimes 1 + 1 \otimes x^{(i)}$ ; allora, per  $y \in L$  ed  $\eta, \zeta \in \Delta'$ , è  $y(\zeta \eta) = (Py)(\zeta \overline{\eta})$ , purchè si faccia la convenzione che  $\sum_{ij} (y_i \otimes z_j)(\zeta_j \overline{\eta}_i) = \sum_{ij} (y_i \zeta_j)(z_j \eta_i)$ . Si indichi con  $P$  anche l'isomorfismo continuo di  $\Delta'$  su  $\Delta' \overline{\Delta'}$  definito da  $P\xi^{(i)} = \xi^{(i)} \overline{1} + 1 \overline{\xi^{(i)}}$ , e sia  $N$  la chiusura dell'ideale di  $\Delta'$  generato da tutte le espressioni  $(yz)\eta - (y \otimes z)(P\eta)$ , con  $y, z \in L$  ed  $\eta \in \Delta'$ ; si ha  $M \subseteq N$ , poichè  $-\xi^{(i)} = (11)\xi^{(i)} - (1 \otimes 1)P\xi^{(i)}$ , e pertanto  $\sigma \xi_i = 0$  se  $\sigma$  è l'omomorfismo di  $\Delta'$  di nucleo  $N$ . Scriveremo  $y \circ \eta$  in luogo di  $\sigma(y\eta)$ , se  $y \in L$  ed  $\eta \in \Delta'$ ; poichè  $1 \circ \eta = 0$  per  $\eta \in M \cap \Delta'$ , per ogni  $y \in L$  esiste un  $n$  tale che  $y \circ \eta = 0$  se  $\eta \in M^n \cap \Delta'$ ; quindi la topologia di  $\sigma\Delta'$  indotta da quella di  $\Delta'$  è la topologia discreta, e si ha  $\sigma\Delta' = Q[\dots, h_i \circ \xi_j, \dots]$ . Riepilogando, valgono le relazioni:

$$6.8 \quad \left\{ \begin{array}{l} (Px_0, Px_1, \dots) = x \otimes 1 + 1 \otimes x \\ (\dots, P\xi_1, P\xi_0) = \xi \overline{1} + 1 \overline{\xi} \\ 1 \circ 1 = 1, 1 \circ \xi_i = x_i \circ 1 = 0 \\ y \circ \zeta \eta = Py \circ (\zeta \overline{\eta}) \\ yz \circ \eta = (y \otimes z) \circ P\eta. \end{array} \right.$$

Ciò premesso, si fissi un intero  $m \geq 0$ , e si consideri il vettore di Witt  $v$ , ad  $m + 1$  componenti in  $\sigma\Delta'$ , tale che

$$v^{(i)} = x^{(i)} \circ \xi^{(m-i)} = p^i x_i \circ \xi^{(m-i)} = x^{(i)} \circ \xi_{m-i};$$

poichè, come si deduce dalle 6.8, è  $x_i \circ \zeta^{p^l} = 0$  se  $l > i$ , si può anche scrivere  $v^{(i)} = x_i \circ (\xi_m^{p^i} + p^{p^i-1} + \dots + p^i \xi_{m-i})$ , e queste, confrontate con la definizione di  $x\zeta$  nel senso del 6.7, ci informano che  $v_i$  è esprimibile come polinomio nelle  $h_j \circ \xi_i$  a coefficienti interi, e che anzi

$$v_i = \sigma[w_i(x_0, \dots, x_i; \xi_m, \dots, \xi_{m-i})].$$

Ciò resta vero quando le  $x_i, \xi_j$  siano elementi di anelli di caratteristica  $p$ , purchè valgano le 6.8.

### 7. Rappresentazione dei $\Pi$ -moduli canonici e della trasposizione.

In questo paragrafo,  $k$  e  $K$  ritorneranno ad avere i significati che avevano nei §§ 1, ..., 5 (con  $\omega = p$ ); ricordiamo che se  $R$  è un anello locale completo contenente  $k$  come sottoanello, i covettori di Witt  $\zeta = (\dots, \zeta_1, \zeta_0)$  ( $\zeta_i \in R^+$ ) sono definiti, e che il loro insieme  $\mathcal{W}(R^+)$  forma un  $K$ -modulo. Se si definisce, al solito,  $\pi(\dots, \zeta_1, \zeta_0) = (\dots, \zeta_1^p, \zeta_0^p)$ ,  $t(\dots, \zeta_2, \zeta_1, \zeta_0) = (\dots, \zeta_2, \zeta_1)$ , si vede che è ancora  $\pi t = t\pi = p = \text{moltiplicazione per } p$ ; inoltre, per  $a \in K$  sono valide le  $\pi(a\zeta) = a^p\pi\zeta$ ,  $at\zeta = t(a\zeta)$ ; pertanto  $\mathcal{W}(R^+)$  diviene, in maniera evidente, un  $\Pi$ -modulo (sinistro), qualora si faccia l'identificazione  $\pi\zeta = \pi\zeta$ . L'analoga di 2.2 essendo verificata per ogni sotto- $\Pi$ -modulo di  $\mathcal{W}(R^+)$ , si conclude che ogni tale sotto- $\Pi$ -modulo finito  $N$  è canonico se e solo se  $pN \subseteq \pi N$ , ossia se e solo se  $tN \subseteq N$ ; se  $N$  è ancora un sotto- $\Pi$ -modulo di  $\mathcal{W}(R^+)$ , e se  $S^+$  è il minimo sottoanello di  $R$  che contiene tutte le componenti di tutti gli elementi di  $N$ , diremo che  $k \oplus S^+ = S$  è il *campo involupante di  $N$* ; esso è certamente un anello locale; diremo poi che  $S$  *involuppa  $N$  liberamente*, o che è un suo *campo involupante libero*, se esiste un insieme minimo di generatori  $\{\zeta_1, \dots, \zeta_n\}$  di  $N$ , con  $\zeta_i = (\dots, \zeta_{i1}, \zeta_{i0})$ , tale che gli  $\zeta_{i0}$  formino un insieme regolare di parametri di  $S$ .

7.1 LEMMA. *Sia  $N$  un  $\Pi$ -modulo canonico di covettori di Witt a componenti nell'anello locale  $R$  su  $k$ , e sia  $R$  il campo involupante libero di  $N$ ; allora, per un insieme minimo  $\{\eta_1, \dots, \eta_n\}$  di generatori di  $N$ , con  $\eta_i = (\dots, \eta_{i1}, \eta_{i0})$ , le  $\eta_{i0}$  formano un insieme regolare di parametri di  $R$ .*

DIM. Se le  $\zeta_1, \dots, \zeta_n$  sono tali che le  $\zeta_{i0}$  formino un insieme regolare di parametri di  $R$ , dalla legge di composizione dei covettori di Witt si vede subito che l'ideale  $R^+$ , generato dalle  $\zeta_{i0}$ , è contenuto nell'ideale  $(\eta_{10}, \dots, \eta_{n0}) + (R^+)^p$ ; ciò comporta appunto che le  $\eta_{j0}$  generano  $R^+$ , C.V.D..

Come nel caso analogo dei vettori di Witt (§ 5), se  $\zeta = (\dots, \zeta_1, \zeta_0)$  è un covettore di Witt a componenti nell'anello locale  $R$  contenente  $k$ , e se  $\sigma$  è un semiomorfismo di  $R$  (come algebra su  $k$ ), indicheremo con  $\sigma\zeta$  il covettore  $(\dots, \sigma\zeta_1, \sigma\zeta_0)$ ; indicheremo poi con  $\zeta \overline{\times} 1$  il covettore  $(\dots, \zeta_1 \overline{\times} 1, \zeta_0 \overline{\times} 1)$ , a componenti in  $R \overline{\times} R$ . Se  $R$  è un ipercampo con la legge  $P$ ,  $\mathcal{C}(R)$  denoterà il  $\Pi$ -modulo degli  $\zeta \in \mathcal{W}(R^+)$  tali che  $P\zeta = \zeta \overline{\times} 1 + 1 \overline{\times} \zeta$ ; esso soddisfa evidentemente la  $t\mathcal{C}(R) \subseteq \mathcal{C}(R)$ ; gli elementi di  $\mathcal{C}(R)$  saranno chiamati i *covettori canonici di Witt a componenti in  $R$* , od anche gli *elementi canonici di  $\mathcal{W}(R^+)$* .

Avendo identificato  $K$  con l'anello dei vettori (infiniti) di Witt a componenti in  $k$ , l'algebra  $k_n$  su  $K$  (cfr. § 3) sarà identificata con l'algebra dei

vettori di Witt ad  $n + 1$  componenti in  $k$ ; ed un elemento  $u = [u_0, u_1, \dots] \in \mathcal{K}$  sarà una successione di tali vettori di Witt.

**7.2 TEOREMA.** *Siano  $A, R$  rispettivamente un'iper algebra e un ipercampo duali l'uno dell'altro, e sia  $O$  il punto  $O$  di  $G(R, \Omega)$ ; allora  $N = \mathcal{C}(R)$  è un  $\Pi$ -modulo canonico, trasposto di  $M = \mathcal{C}(A)$ , l'operazione di trasposizione essendo data da  $x \circ \zeta = [(x \circ \zeta)_0, (x \circ \zeta)_1, \dots]$ , con  $(x \circ \zeta)_m = (w_{m0}, \dots, w_{mm})$ , ove  $w_{mi} = [w_i(x_0, \dots, x_i; \zeta_m, \dots, \zeta_{m-i})](O)$ .*

*Inoltre  $R$  è il campo invilupante libero di  $N$ .*

**DIM.**  $N$  è un  $\Pi$ -modulo canonico se è un  $\Pi$ -modulo finito. È  $y \circ \zeta \eta = \mathbf{P}y \circ (\zeta \overline{\times} \eta)$ , e  $yz \circ \eta = (y \overline{\otimes} z) \circ \mathbf{P}\eta$  per  $y, z \in A$  e  $\zeta, \eta \in R$ ; quindi le considerazioni che chiudono il § 6 sono applicabili previa riduzione mod  $p$  (cfr. 6.8). Pertanto, come si vede passando alle componenti fantasma, è certo  $(x \circ (\zeta + \eta))_m = (x \circ \zeta)_m + (x \circ \eta)_m$ , e  $((x + y) \circ \zeta)_m = (x \circ \zeta)_m + (y \circ \zeta)_m$ . Poi, essendo  $x_i \circ \eta^p = (x_{i-1} \circ \eta)^p$  ( $o = 0$  se  $i = 0$ ) (o anche per la 3) di 6.7), la componente di indice  $i$  di  $(x \circ \pi \zeta)_m$  è 0 se  $i = 0$ , e  $[w_i(0, x_0, \dots, x_{i-1}; \zeta_m, \dots, \zeta_{m-i})]^p(O)$  se  $i > 0$ ; passando alle componenti fantasma, si vede che questa uguaglia la  $w_{m-1, i-1}^p$ ; quindi  $(x \circ \pi \zeta)_m = (x \circ \zeta)_{m-1}^{\pi}$ , ossia  $x \circ \zeta t = x \circ \pi \zeta = (x \circ \zeta) t$ , come desiderato (cfr. § 3). Nello stesso modo si vede che  $tx \circ \zeta = t(x \circ \zeta)$ . Le  $\pi x \circ \zeta = \pi(x \circ \zeta)$ ,  $x \circ \zeta \pi = x \circ t \zeta = (x \circ \zeta) \pi$  si dimostrano in modo analogo se si stabilisce prima che  $y^p \circ \zeta_i = (y \circ \zeta_{i+1})^p$  per ogni  $y \in A$ . Ora, per  $\eta \in R$  si sa che  $\pi y \circ \eta = (y \circ t \eta)^p$  (questa essendo la definizione del  $t$  di  $R$  data nel § 5); basta quindi dimostrare che  $t \zeta_i = \zeta_{i+1}$ , ossia che è proprio  $t \zeta = (\dots, t \zeta_1, t \zeta_0)$  come vuole la nostra convenzione. Se allora  $Q \in G(R, \Omega)$ , si sa essere  $(\dots, \pi t \zeta_1(Q), \pi t \zeta_0(Q)) = (\dots, \zeta_1(pQ), \zeta_0(pQ)) = p(\dots, \zeta_1(Q), \zeta_0(Q))$ , onde  $\pi(\dots, t \zeta_1, t \zeta_0) = \pi t(\dots, \zeta_1, \zeta_0)$ , e quindi  $(\dots, t \zeta_1, t \zeta_0) = t(\dots, \zeta_1, \zeta_0)$ , come richiesto.

Sia  $a \in K$ , e per esempio  $a = \sum_0^\infty a_i p^i$ , con  $a_i = (a_i, 0, 0, \dots)$ ,  $a_i \in K$ ;

poichè, come si vede con verifica diretta sulle componenti fantasma, è  $a_i x \circ \zeta = a_i(x \circ \zeta)$ , e  $x \circ a_i \zeta = (x \circ \zeta) a_i$ , per quanto precede anche le  $ax \circ \zeta = a(x \circ \zeta)$ ,  $x \circ a \zeta = (x \circ \zeta) a$  sono verificate.

Se  $\zeta$  è tale che  $x \circ \zeta = 0$  per ogni  $x$ , è anche  $x \circ t^i \zeta = (x \circ \zeta) \pi^i = 0$  per ogni  $x$ , onde  $x_0 \circ \zeta_i = 0$ ; se  $J$  è l'ideale di  $R$  generato dalle  $\zeta_i$ , si ha  $\mathbf{P}J \subseteq J \overline{\times} R + R \overline{\times} J$ , e quindi, per il 4 di 5.8,  $J$  è il nocciolo di un omomorfismo  $\sigma_{-1}$  di immersione di un ipercampo  $S$  in  $R$ ; poichè  $x_0 \circ J = 0$  per ogni  $x_0 \in A^*$ , per la 8 di 5.7 il nocciolo di  $\sigma$  contiene  $A^*$ , e quindi contiene  $A_1$ ; pertanto, per la 12 di 5.7,  $S \subseteq R^p$ , e  $\zeta_i \in R^p$  perchè  $\zeta_i \in S$  per la 15 di 5.7. Si è così visto che se  $x \circ \zeta = 0$  per ogni  $x$ , allora  $\zeta = \pi \zeta'$  per uno  $\zeta' \in N$ ; ma allora  $(x \circ \zeta') t = x \circ \pi \zeta' = 0$ , onde  $x \circ \zeta' = 0$ , il che

dà  $\zeta' = \pi \zeta''$ , ecc.; in conclusione,  $\zeta = 0$ , e ciò prova che  $\zeta$  può essere considerato come un omomorfismo del  $T$ -modulo  $M$  sul  $T$ -modulo sinistro  $\mathcal{K}$ , ossia come un elemento del trasposto  $M_{-1}$  di  $M$ ; quindi  $N$  può essere considerato come un sotto- $\Pi$ -modulo, certo canonico, di  $M_{-1}$ . Per dimostrare che  $N = M_{-1}$ , basta dimostrare che  $\dim N = \dim M$ : in tal caso, infatti, sia  $\{\xi_1, \dots, \xi_n\}$  un insieme minimo di generatori di  $N$ , tali che esistano interi  $s_1, \dots, s_n$  per i quali i  $\pi^{-s_i} \xi_i$  formino un insieme minimo di generatori di  $M_{-1}$  (cfr. 2.6); se allora  $\{x_1, \dots, x_n\}$  è un insieme minimo di generatori di  $A$ , e se, per esempio,  $s_1 > 0$ , è anche  $x_i \circ \xi_1 = (x_i \circ \pi^{-s_1} \xi_1) t^{s_1}$ , onde  $x_{i0} \circ \xi_{1m} = 0$  per ogni  $i$  ed ogni  $m$ , dal che segue, come si è visto prima,  $\xi_1 \in \pi N$ , assurdo. Resta quindi da dimostrare che  $\dim N = \dim M$ .

Suppongasì che ciò sia vero quando  $R$  è isomorfo ad  $R_{r,s}$ ; allora resterà vero quando  $R$  è il completamento di un prodotto tensoriale di vari  $R_{r,s}$ , e quindi anche quando  $R$  è isogeno ad un tale completamento, ossia in ogni caso. Dimosteremo perciò che  $\dim N = \dim M = \dim R$  nell'ipotesi che  $R \cong R_{r,s}$ .

Sia  $R = k\{\eta_1, \dots, \eta_r\}$ , con le  $\eta_i$  indeterminate (analiticamente indipendenti) su  $k$ ; sia  $s$  un intero positivo primo con  $r$ , ovvero sia  $s = \infty$ , od anche  $s = 0$  se  $r = 1$ , e pongasi

$$\zeta_1 = (\dots, \eta_r^{p^{2s}}, \dots, \eta_1^{p^{2s}}, \eta_r^{p^s}, \dots, \eta_1^{p^s}, \eta_r, \dots, \eta_1),$$

con  $\eta_i^{p^{js}} = 0$  se  $s = \infty$  e  $j > 0$ ; sia poi  $\zeta_i = t^{i-1} \zeta_1$  ( $i = 1, \dots, r$ ). Se  $\zeta_1 \overline{\times} 1 + 1 \overline{\times} \zeta_1 = (\dots, \xi_r, \dots, \xi_1)$ , sia  $P$  l'omomorfismo (di algebre su  $k$ ) di  $R$  su  $R \overline{\times} R$  tale che  $P\eta_i = \xi_i$ ; si constata subito che, con la legge  $P$ ,  $R$  diviene un ipercampo, certo di dimensione  $r$ ; se poi  $N'$  è il  $\Pi$ -modulo generato dalle  $\zeta_i$ ,  $N'$  è canonico ed isomorfo ad  $N_{r,s}$ ; poichè  $\dim N' = r$ , ed anche (come si è visto prima)  $\dim \mathcal{C}(R) \leq r$ ,  $N'$  è isogeno a  $\mathcal{C}(R)$ , e  $\mathcal{C}(R)$  ha dimensione  $r$ . Ma allora  $\mathcal{C}(A)$  è isogeno ad  $M_{s,r}$ ,  $A$  è isogeno ad  $A_{r,s}$ , ed  $R$  è isogeno ad  $R_{r,s}$ ; resta così dimostrato che  $\dim \mathcal{C}(R) = \dim R$  quando  $R$  è un particolare ipercampo isogeno ad  $R_{r,s}$ , e quindi anche quando  $R \cong R_{r,s}$ .

Infine,  $R$  inviluppa  $N$  liberamente (nel caso generale) perchè  $N = M_{-1}$ , e per il 3.5, C.V.D..

Nelle notazioni dell'ultima parte della precedente dimostrazione, sia  $\{z_h\}$  ( $h \in I^r$ ) la base strutturale di  $A$  (iperalgebra duale di  $R$ ) legata a  $\{\eta_1, \dots, \eta_r\}$ ; dall'essere  $z_{s(i)} \circ \eta_j = \delta_{ij}$  segue, per il 3.5, che le  $\zeta_i$  generano  $\mathcal{C}(R)$ , ossia che  $N' = \mathcal{C}(R)$ ; quindi  $M \cong M_{r,s}$ ,  $A \cong A_{r,s}$ , ed  $R \cong R_{r,s}$ ; pertanto le considerazioni sulla struttura di vari ipercampi, date alla fine del § 5, sono tutte incluse nell'enunciato seguente:

7.3 TEOREMA. Sia  $R = k\{\eta_1, \dots, \eta_r\}$ ; sia poi

$$\zeta_i = t^{i-1}(\dots, \eta_r^{p^{2s}}, \dots, \eta_1^{p^{2s}}, \eta_r^{p^s}, \dots, \eta_1^{p^s}, \eta_r, \dots, \eta_1)$$

( $i = 1, \dots, r$ ), con la convenzione  $\eta_i^{p^{js}} = 0$  se  $j > 0$  ed  $s = \infty$ ; sia  $P$  l'omomorfismo (di algebre su  $k$ ) di  $R$  su  $R \overline{\times} R$  tale che  $P\zeta_i = \zeta_i \overline{\times} 1 + 1 \overline{\times} \zeta_i$  (esso esiste ed è unico); allora  $R \cong R_{r,s}$ , e  $\mathcal{C}(R)$  è isomorfo ad  $N_{r,s}$  ed ha  $\{\zeta_1, \dots, \zeta_r\}$  come insieme minimo di generatori.

Da 7.2, 5.2, e 5.3 segue:

7.4 TEOREMA. Ogni  $II$ -modulo canonico è isomorfo a  $\mathcal{C}(R)$  per un opportuno ipercampo  $R$ .

Il 7.3 dice, in particolare, che se  $\Phi$  ha il significato introdotto alla fine del § 6, è  $R_{1,s} = k\{\eta\}$ , con la legge

$$P\eta = \Phi(\eta \overline{\times} 1, \eta^{p^s} \overline{\times} 1, \eta^{p^{2s}} \overline{\times} 1, \dots; 1 \overline{\times} \eta, 1 \overline{\times} \eta^{p^s}, \dots).$$

Si noti che, per un qualsiasi ipercampo  $R$ , uno  $(\dots, \zeta_1, \zeta_0) \in \mathcal{C}(R)$  è univocamente determinato da  $\zeta_0$ , dato che  $\zeta_i = t^i \zeta_0$ ; un elemento  $\zeta_0 \in R$  tale che  $(\dots, t^2 \zeta_0, t \zeta_0, \zeta_0)$  sia un covettore canonico si dirà un *elemento canonico di Witt di  $R$* ; la trasposizione «  $\circ$  » introdotta al 7.2 può quindi pensarsi come un'operazione fra vettori canonici di Witt a componenti in  $A$ , e gli elementi canonici di Witt di  $R$ . Questi ultimi formano un  $II$ -modulo canonico, isomorfo a  $\mathcal{C}(R)$ , rispetto alle operazioni  $\dot{+}$  e  $\cdot$  (prodotto scalare) così definite:

$$7.5 \quad \begin{cases} \zeta \dot{+} \eta = \Phi(\zeta, t\zeta, t^2\zeta, \dots; \eta, t\eta, t^2\eta, \dots), \\ (a, 0, 0, \dots) \cdot \zeta = a\zeta \quad (a \in k). \end{cases}$$

La legge su  $\mathcal{G}(R, \Omega)$  si scrive ora semplicemente:

$$7.6 \quad \zeta(P + Q) = \zeta(P) \dot{+} \zeta(Q), \text{ per un qualsiasi elemento canonico di Witt } \zeta \text{ di } R.$$

La discussione sui semiomomorfismi canonici che segue la dimostrazione del 5.8 può ora essere completata coll'introdurre il semiomomorfismo  $\sigma_{-1}^*$  di  $\mathcal{C}(R')$  su  $\mathcal{C}(R)$  che coincide con  $\sigma_{-1}$  quando gli elementi di  $\mathcal{C}(R')$  (e di  $\mathcal{C}(R)$ ) vengono sostituiti coi corrispondenti elementi canonici di  $R'$  (e di  $R$ ); tale  $\sigma_{-1}^*$  è anche il trasposto di  $\sigma^*$ . È  $\dim \sigma_{-1} = \dim \sigma_{-1}^*$ ,  $\text{codim } \sigma_{-1} = \text{codim } \sigma_{-1}^*$ ,  $\text{ins } \sigma_{-1} = \text{ins } \sigma_{-1}^*$ ; se  $H$  è il nucleo di  $\sigma_{-1}$ ,  $H$  è il nocciolo di un  $\sigma'_{-1}$ , la cui immagine  $S$  ha la proprietà che  $\mathcal{C}(S)$  è il nucleo di  $\sigma_{-1}^*$ . Varie altre relazioni fra  $\sigma_{-1}$  e  $\sigma_{-1}^*$  son evidenti.

## BIBLIOGRAFIA

1. DIEUDONNÉ J., *Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique  $p > 0$  (VII)*; Math. Ann., 134, 1957, p. 114.
2. ORE O., *Theory of non-commutative polynomials*; Ann. of Math., 34, 1933, p. 480.
3. JACOBSON N., *The theory of rings*; New York, 1943.
4. ALBERT A. A., *Structure of algebras*; Amer. Math. Soc. Coll. Publ., 1939.
5. DEURING M., *Algebren*; Erg. der Math., 4, 1935.
6. DIEUDONNÉ J., *Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique  $p > 0$* ; Comm. Math. Helv., 28, 1954, p. 87.
7. BARSOTTI I., *Gli endomorfismi delle varietà abeliane su corpi di caratteristica positiva*; Ann. Scuola Norm. Sup., 10, 1956, p. 1.
8. BARSOTTI I., *Abelian varieties over fields of positive characteristic*; Rend. Circ. Mat. Palermo, 5, 1956, p. 145.
9. DIEUDONNÉ J., *Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique  $p > 0$  (V)*; Bull. Soc. Math. de France, 84, 1956, p. 207.
10. WITT E., *Zyklische Körper und Algebren der Charakteristik  $p$  vom Grad  $p^m$ . Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik  $p$* ; Journ. Reine Angew. Math., 176, 1937, p. 126.
11. BARSOTTI I., *On Witt vectors and periodic group-varieties*; Illinois Journ. of Math., 2, 1958, p. 99; *Corrections to the paper « ... »*; ibid., p. 608.
12. DIEUDONNÉ J., *Sur les groupes de Lie algébriques sur un corps de caractéristique  $p > 0$* ; Rend. Circ. Mat. Palermo, 1, 1952, p. 380.
13. DIEUDONNÉ J., *Witt groups and hyperexponential groups*; Mathematika, 2, 1955, p. 21.
14. BARSOTTI I., *Risultati e problemi nella teoria delle varietà grupali*; Atti Convegno Internaz. Geom. Algebrica, Taormina, Nov. 1958, in corso di stampa, Univ. Messina.
15. DIEUDONNÉ J., *Lie groups and Lie hyperalgebras over a field of characteristic  $p > 0$  (IV)*; Amer. Journ. of Math., 77, 1955, p. 429.
16. CARTIER P., *Théorie différentielle des groupes algébriques*; Comptes Rend. Acad. Sciences Paris, 244, 1957, p. 540.
17. MORITA K., *Duality for modules and its applications to the theory of rings with minimum condition*; Science Rep. Tokyo Kyoiku Daigaku, 6, 1958, p. 83.
18. BARSOTTI I., *Repartitions on abelian varieties*; Illinois Journ. of Math., 2, 1958, p. 43.
19. CARTIER P., *Dualité des variétés abéliennes*; note ciclostilate Sem. Bourbaki, Paris, Mai 1958.
20. SERRE J.-P., *Quelques propriétés des variétés abéliennes en caractéristique  $p$* ; Amer. Journ. of Math., 80, 1958, p. 715.
21. ROSENBLICHT M., *Extensions of vector groups by abelian varieties*; Amer. Journ. of Math., 80, 1958, p. 685.
22. DIEUDONNÉ J., *On the Artin-Hasse exponential series*; Proc. Amer. Math. Soc., 8, 1957, p. 210.