Annali della
Scuola Normale Superiore di Pisa
Classe di Scienze

Carlo Traverso

Sulla classificazione dei gruppi analitici commutativi di caratteristica positiva

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3e série, tome 23, nº 3 (1969), p. 481-507

<http://www.numdam.org/item?id=ASNSP_1969_3_23_3_481_0>

SULLA CLASSIFICAZIONE DEI GRUPPI ANALITICI COMMUTATIVI DI CARATTERISTICA POSITIVA

CARLO TRAVERSO (*)

Di gruppi analitici si parla solo nel titolo; in nessun punto si parla di iperalgebre.

In questo lavoro viene data una classificazione dei K-moduli canonici; il titolo è giustificato dalla ben nota ([1], [2], [4]) equivalenza tra la categoria dei K-moduli canonici ed una categoria di gruppi analitici contenente i gruppi analitici equidimensionali.

Questa classificazione è diversa da quella data in [5], ma ad essa analoga. Il § 4 è sostanzialmente il confronto tra le due: si può vedere facilmente, ad esempio, che la topologia indotta sull'insieme delle classi di isomorfismo di K-moduli canonici dalla topologia di Zariski delle varietà parametrizzanti è la stessa nei due casi (con l'ovvia differenza che la classificazione di [5] spezza in più insiemi quello che qui è un solo insieme). La classificazione data qui permette di ottenere alcuni risultati non riconoscibili da [5], ad esempio la determinazione del numero di parametri di un gruppo analitico (teorema 4) e la specializzazione (§ 5). Quest'ultimo argomento si ricollega a [3], e ad un lavoro in preparazione di M. Poletti [6].

Nell'appendice viene trattato un problema di classificazione per una categoria più vasta di quella dei K-moduli canonici. Il presente lavoro ha origine dall'approfondimento di alcuni punti di una tesi di laurea sostenuta presso l'Università di Pisa nel Novembre 1967.

Pervenuto alla Redazione il 29 Marzo 1969.

(*) Lavoro eseguito nell'ambito del gruppo di ricerca per la Matematica N. 35 del C.N.R.

1. Preliminari e notazioni.

Sia k un corpo algebricamente chiuso di caratteristica $p > 0$, e K l'anello dei vettori di Witt su k; indichiamo con $\cdot^\pi$ l'automorfismo di Frobenius di K.

Se $\alpha \in k$, con $(\alpha)_n$ indichiamo la n-esima componente di α. Sia M un K modulo libero finito, dotato di un $\cdot^\pi$-semiendomorfismo π (ricordiamo che se λ è un omomorfismo gruppale tra due A moduli M, M', e σ un endomorfismo di A, λ si dice un σ-semiendomorfismo se per ogni $a \in A$, $m \in M$, abbiamo $\lambda(am) = \sigma(a)\lambda(m)$) e di un $\cdot^{\pi^{-1}}$ semiendomorfismo t; esso è detto un K-modulo canonico se, per ogni $m \in M$, $\pi t m = t \pi m = pm$.

Un omomorfismo tra k-moduli canonici è detto canonico se commuta con π e t.

Data una base (ossia un sistema libero di generatori) di M, $X = (x_1, \dots, x_n)^*$ di M, siano C_π, C_t le matrici ($n \times n$) a coefficienti in K tali che $C_\pi X = \pi X$, $C_t X = tX$. Tali matrici sono dette matrici caratteristiche di M rispetto alla base X. È immediato ([2], p. 281) che $C_\pi C_t^\pi = C_t C_\pi^{\pi^{-1}} = pI$ (e quindi $C_t^\pi C_\pi = pI$) e che, data una coppia di matrici quadrate A, B a coefficienti in K tali che $AB^\pi = pI$ esistono un K-modulo canonico ed una sua base tali che A, B ne siano le matrici caratteristiche. Due K-moduli canonici sono isomorfi (ovviamente come K-moduli con operatori, cioè deve esistere fra essi un isomorfismo canonico) se e solo se, fissata una base qualunque in entrambi, e indicando con (C_π, C_t), (C'_π, C'_t) le rispettive matrici caratteristiche, esiste una matrice invertibile A tale che

$$(1.1) \qquad A^\pi C_\pi = C'_\pi A \qquad\qquad C_t^\pi A^\pi = A C_t'^\pi .$$

Sono isomorfi modulo p^n se e solo se tali eguaglianze sono verificate modulo p^n.

Indichiamo con dimensione (risp. codimensione) di un K modulo canonico M, la k-dimensione di $M/\pi M$ (risp. M/tM); essa è uguale al valore p-adico del determinante di C_t (risp. C_π). Due K-moduli canonici si dicono isogeni se ciascuno è isomorfo a un sotto K modulo canonico dell'altro. Due K-moduli canonici isogeni hanno la stessa dimensione e codimensione.

Considereremo le varietà algebriche su k come insieme dei punti razionali su k. In tal modo i gruppi algebrici sono veri e propri gruppi. Un gruppo algebrico si dirà lineare se è sottogruppo di $GL(k^n)$. Per corrispondenza algebroide si intende un sottoinsieme localmente chiuso (nella topologia di Zariski) di una varietà prodotto di due varietà. Se tali due varietà sono entrambe uguali a V, si parlerà di una corrispondenza algebroide in V.

Indicheremo con $K_n = K/p^n K$ l'anello dei vettori di Witt di lunghezza n. È ben noto che K_n è un gruppo algebrico lineare di dimensione n, che come varietà è uno spazio affine di dimensione n.

2. Risolubilità di alcuni sistemi di equazioni.

TEOREMA 1. *Consideriamo il seguente sistema di equazioni a cofficienti in k, nelle incognite x_i:*

$$x_i^p = \sum_{1}^{m}{}_j\, a_{ij} x_j + c_i \qquad 1 \leq i \leq m. \tag{2.1}$$

Esso ha un numero finito di soluzioni in k.

DIM. Il sistema omogeneo associato

$$x_i^p = \sum_{1}^{m}{}_j\, a_{ij} x_j z^{p-1} + c_i z^p$$

ha una soluzione non identicamente nulla; ma se poniamo $z = 0$, otteniamo $x_i^p = 0$; perciò la varietà proiettiva associata non incontra l'iperpiano all'infinito, quindi ha dimensione 0, e il sistema non omogeneo ha un numero finito positivo di soluzioni. C.V.D.

TEOREMA 2. *Consideriamo il seguente sistema di equazioni a coefficienti in K, nelle incognite x_i, y_h:*

$$\text{(2.2)} \quad \alpha) \qquad x_i^{\pi} = \sum_{1}^{m}{}_j\, a_{ij} x_j + \sum_{1}^{n}{}_l\, b_{il} y_l \qquad 1 \leq i \leq m$$

$$\beta) \qquad p y_h^{\pi} = \sum_{1}^{m}{}_j\, c_{hj} x_j + \sum_{1}^{n}{}_l\, d_{hl} y_l \qquad 1 \leq h \leq n.$$

I. *Sia $(\bar{x}_i, \bar{y}_h)$ una soluzione del sistema in K_{n+u}; esiste allora una soluzione del sistema in K, $(\bar{x}'_i, \bar{y}'_h)$, tale che*

$$\bar{x}_i \equiv \bar{x}'_i \ (p^u); \qquad \bar{y}_h \equiv \bar{y}'_h \ (p^u).$$

II. *Considerando $(K_u)^{m+n}$ come gruppo algebrico su k, le soluzioni del sistema in K_u sono un sottogruppo algebrico di dimensione minore o uguale a n.*

Dim. Nel corso della dimostrazione useremo liberamente notazioni vettoriali e scalari, con ovvio uso dei simboli. Ogni volta che opereremo un cambiamento di coordinate, o trasformazioni analoghe, per non appesantire troppo la dimostrazione, non cambieremo il nome delle coordinate nè quello delle matrici che in conseguenza di questo debbano subire un cambiamento.

Applicare $\cdot^{\pi}$ o $\cdot^{\pi^{-1}}$ ad una matrice significa applicarlo ai singoli elementi. X, Y indicano i vettori incogniti.

Sarà spesso necessario «*spezzare*» i vettori incogniti, ossia considerare, ad esempio, invece del solo vettore $(x_1, \dots, x_s, x_{s+1}, \dots, x_m)^*$ i due vettori $(x_1, \dots, x_s)^*$ e $(x_{s+1}, \dots, x_m)^*$, e sarà necessario spezzare in corrispondenza le matrici dei coefficienti relative.

Nel corso della dimostrazione utilizzeremo la decomposizione di una matrice A a coefficienti in K nella forma $A = A'QA'' + pA'''$, con A', A'' quadrate invertibili, e Q a valori soltanto 0, 1, e con $(Q)_{ij} = 0$ se $i \neq j$. La possibilità di tale decomposizione è ovvia, considerando l'analoga decomposizione di ogni matrice a coefficienti in k. Ogni volta che decomporremo una matrice nel corso della dimostrazione, supporremo che si tratti di una decomposizione del genere.

Con Φ, Ψ, eventualmente indicizzati, indichiamo vettori di polinomi lineari omogenei generici in X, Y, a coefficienti in K; con φ, ψ indicheremo uno di tali polinomi.

2. Notiamo innanzitutto, per quel che riguarda II, che è ovvio che l'insieme delle soluzioni in K_w sia una varietà, ed è un sottogruppo essendo le equazioni Q-lineari. Per quanto riguarda II resta perciò da dimostrare solo l'asserzione riguardante la dimensione.

3. Dimostriamo il teorema per induzione su n.

Il caso $n = 0$ è contenuto nel punto 13 (perchè, con le notazioni che allora saranno in vigore, tutto il sistema si riduce ad $\alpha_{4\varrho})$).

Sia dunque n qualunque, e supponiamo il teorema dimostrato per $n - 1$; esprimiamo la parte α) del sistema in forma vettoriale

$$\alpha) \qquad X^{\pi} = AX + BY.$$

Posto $B = B'QB'' + pB'''$, abbiamo

$$\alpha) \qquad ((B'^{\pi^{-1}})^{-1} X)^{\pi} = B'^{-1} AX + QB''Y + p\Phi$$

perciò, cambiando coordinate in X secondo $(B'^{\pi^{-1}})^{-1}$, e in Y secondo B'', il sottosistema α) si riduce alla forma

$$\alpha) \qquad X^\pi = QY + AX + p\Phi$$

(con A, Φ, eventualmente diversi da prima; ad esempio il nuovo A è uguale a $B'^{-1} AB'^{\pi^{-1}}$; inoltre anche i coefficienti della parte β) dovranno essere opportunamente modificati). Spezzando ora Y in Y_1 e Y_2 (con Y_2 base del nucleo di Q) e X in X_1 e X_2 come indicato sotto, α) si spezza in

$$\alpha_1) \qquad X_1^\pi = Y_1 + A_1 X + p\Phi_1$$

$$\alpha_2) \qquad X_2^\pi = A_2 X + p\Phi_2$$

e la α_1) sotto forma scalare è

$$(2.3) \quad \alpha_1) \qquad x_i^\pi = y_i + \sum_1^m{}_j a_{ij} x_j + p\varphi_i ; \qquad 1 \leq i \leq s$$

4 β), sotto forma vettoriale, è

$$\beta) \qquad pY^\pi = CX + DY$$

con $D = D' Q' D'' + pD'''$, cioè

$$\beta) \qquad pEY^\pi = Q' \widehat{Y} + CX + p\Psi$$

(con $Y = D'' Y$, $E = D'^{-1}$, C cambiato); ossia, sotto forma scalare,

$$(2.4) \quad \beta_1) \qquad \sum_1^n{}_h e_{ih}\, py_h = \widehat{y_i} + \sum_1^m{}_j c_{ij}\, x_j + p\psi_i \qquad 1 \leq i \leq s'$$

$$\beta_2) \qquad \sum_1^n{}_h e_{ih}\, py_h = \sum_1^m{}_j c_{ij}\, x_j + p\psi_i \qquad s' < i \leq n$$

5. Notiamo che le $(\widehat{y_i})_0$, $1 \leq i \leq s'$, sono linearmente indipendenti essendo componenti del prodotto di una matrice invertibile per il vettore di base Y. Possiamo inoltre supporre che le $(y_i)_0$, $1 \leq i \leq s$, siano linearmente indipendenti dalle $(\widehat{y_j})_0$, $1 \leq j \leq s'$; sia infatti, ad esempio, $y_s + \sum_1^{s-1}{}_j g_j y_j \equiv \equiv \sum_1^s{}_h f_h \widehat{y_h}\,(p)$. Eseguendo il cambiamento in Y_1 della coordinata y_s, definito da $y'_s = y_s + \sum_1^{s-1}{}_j g_j y_j$, e in X_1 il cambiamento della coordinata x_s, definito da $x'_s = x_s + \sum_1^{s-1}{}_j g_j^{\pi^{-1}} x_j$, per conservare ad α_1) la forma di 2.3, possiamo ri-

durci al caso in cui è

$$y_s \equiv \sum_{1}^{s'}{}_h f_h \widehat{y}_h \, (p) \tag{2.5}$$

Posto $x'_s = x_s - p \sum_{1}^{s'}{}_j f_j^{\pi-1} \sum_{1}^{n}{}_h e_{jh}^{\pi-1} y_h$ abbiamo

$$(x'_s)^\pi = x_s^\pi - \sum_{1}^{s'}{}_j f_j \, p \sum_{1}^{n}{}_h e_{jh} \, y_h^\pi$$

e, tenendo conto di 2.3, 2.4, 2.5, abbiamo

$$(x_s)^\pi = \sum_{1}^{m}{}_j a'_{sj} x_j + p\varphi_s$$

Inoltre $x_s \equiv x_s \, (p)$, perciò, sostituendo al secondo membro x'_s a x_s, si devono modificare solo le q e φ.

6. Siano allora le $(y_i)_0$, $1 \leq i \leq s$, e le $(\widehat{y}_j)_0$, $1 \leq j \leq s'$, linearmente indipendenti: possiamo perciò, cambiando coordinate in Y, fare sì che le y_i e le $\widehat{y}_j$ facciano parte di una base, cioè che le $\widehat{y}_j$ siano elementi di Y_2. Possiamo inoltre supporre che le $\widehat{y}_i$ costituiscano l'intero Y_2.

Supponiamo infatti, ad esempio, che y_n non sia una delle y_i nè una delle $\widehat{y}_j$. Poichè le y_i, $1 \leq i \leq s$, e le $\widehat{y}_i$, $1 \leq j \leq s'$, sono le uniche Y che compaiono al secondo membro con coefficiente non multiplo di p, y_n comparirebbe ovunque con coefficiente multiplo di p; moltiplicando allora β) a sinistra per E^{-1}, si ottiene un sistema del tipo definito in ipotesi in cui y_n compare ovunque con coefficiente divisibile per p; sostituendo allora $y'_n = py_n$, l'equazione n-esima di β) diventa un'equazione del tipo α), perciò il nuovo sistema ha n diminuito di 1 (e m aumentato di 1) perciò si può applicare l'ipotesi di induzione. Ovviamente ad ogni soluzione modulo p^w del vecchio sistema corrisponde una soluzione modulo p^w del nuovo, essendosi operate solo sostituzioni; inoltre se due soluzioni del nuovo sistema sono congrue modulo p^w, e ad esse corrispondono soluzioni del vecchio (ossia $(y'_n)_0 = 0$) le corrispondenti soluzioni del vecchio sono congrue modulo p^{w-1} (più precisamente, se $p\bar{y}_n = y'_n \equiv \tilde{y}'_n = p\tilde{y}_n \, (p^w)$, allora $\bar{y}_n \equiv \tilde{y}_n \, (p^{w-1})$; per le altre incognite invece la congruenza modulo p^w si conserva). Perciò I è dimostrato.

Per quanto riguarda II, notiamo che la varietà delle soluzioni del vecchio sistema in K_w è uguale alla varietà del nuovo, intersecata con l'iperpiano $(y'_n)_0 = 0$, e moltiplicata per lo spazio affine di dimensione 1 con punto generico $(y'_n)_w = (y_n)_{w-1}$; perciò la vecchia varietà ha dimensione maggiore al più di uno della dimensione della nuova, perciò, per induzione, pure II segue.

7. Possiamo allora supporre che le $\widehat{y}_j$, $1 \leq j \leq s'$, siano le Y_2. L'intero sistema è allora

$$(2.6)\quad \alpha_1)\qquad X_1^\pi = Y_1 + A_1 X + p\Phi_1$$

$$\alpha_2)\qquad X_2^\pi = A_2 X + p\Phi_2$$

$$\beta_1)\qquad pE_1 Y^\pi = Y_2 + C_1 X + p\Psi_1$$

$$\beta_2)\qquad pE_2 Y^\pi = C_2 X + p\Psi_2$$

Prendiamo ora in considerazione $\beta_2)$:

$$\beta_2)\qquad pE_2 Y^\pi = C_{21} X_1 + C_{22} X_2 + p\Psi_2$$

con $C_{21} = C'_{21} Q_{21} C''_{21} + pC'''_{21}$, perciò, cambiando coordinate in X_1 secondo C''_{21} (e in Y_1 secondo C''^π_{21} per conservare la forma delle α_1)) e modificando opportunamente le altre matrici, la $\beta_2)$ diventa

$$\beta_2)\qquad pE_2 Y^\pi = Q_{21} X_1 + C_{22} X_2 + p\Psi_2$$

e scindendo X_1 in X_{11} e X_{12}, $\beta_2)$ si scinde in

$$\beta_{21})\qquad pE_{21} Y^\pi = X_{11} + C_{212} X_2 + p\Psi_{21}$$

$$\beta_{22})\qquad pE_{22} Y^\pi = C_{222} X_2 + p\Psi_{22}\,.$$

Scindendo Y_1 in Y_{11} e Y_{12}, in corrispondenza della scissione operata in X_1, la $\alpha_1)$ si spezza quindi in

$$\alpha_{11})\qquad X_{11}^\pi = Y_{11} + A_{11} X + p\Phi_{11}$$

$$\alpha_{12})\qquad X_{12}^\pi = Y_{12} + A_{12} X + p\Phi_{12}\,.$$

Analogamente, cambiando quanto occorre, X_2 si scinde in X_{21} e X_{22}; β_{22} si scinde in

$$\beta_{221})\qquad pE_{221} Y^\pi = X_{21} + p\Psi_{221}$$

$$\beta_{222})\qquad pE_{222} Y^\pi = p\Psi_{222}\,.$$

Operiamo ora il cambiamento di coordinate $X'_{11} = X_{11} + C_{212} X_2$. Esso elimina il fattore con X_2 da β_{21}), e poichè X_{11} oltre che in β_{21}) compare solo nelle α_i) (e, al secondo membro, nella forma $A_i X$, con A_i matrice generica) e nelle Φ, Ψ, abbiamo

$$(X'_{11})^\pi = X_{11}^\pi + C_{212}^\pi X_2^\pi = Y_{11} + (A_1 + C_{212}^\pi A_2) X + p\Phi'_{11}$$

e la forma delle altre equazioni non viene modificata · β_{21}) è

$$\beta_{21}) \qquad pE_{21} Y^\pi = X_{11} + p\Psi_{21}.$$

Infine, operiamo il cambiamento di coordinate $Y'_{11} = Y_{11} + A_{11} X$, $Y'_{12} = Y_{12} + A_{12} X$, $Y'_2 = Y_2 + C_1 X$. Questo fa sì che A_{11}, A_{12} e C_1 diventino uguali a 0, e non influisce ulteriormente altro che sulle Φ e Ψ, perchè altrove le Y compaiono solo con coefficiente divisibile per p.

Il sistema in definitiva sarà dunque

$$
\begin{array}{lll}
(2\,7) & \alpha_{11}) & X_{11}^\pi = Y_{11} + p\Phi_{11} \\
 & \alpha_{12}) & X_{12}^\pi = Y_{12} + p\Phi_{12} \\
 & \alpha_{21} & X_{21}^\pi = A_{21} X + p\Phi_{21} \\
 & \alpha_{22}) & X_{22}^\pi = A_{22} X + p\Phi_{22} \\
 & \beta_1) & pE_1 Y^\pi = Y_2 + p\Psi_1 \\
 & \beta_{21}) & pE_{21} Y^\pi = X_{11} + p\Psi_{21} \\
 & \beta_{221}) & pE_{221} Y^\pi = X_{21} + p\Psi_{221} \\
 & \beta_{222}) & pE_{222} Y^\pi = \qquad p\Psi_{222}
\end{array}
$$

8. Possiamo supporre che β_{222}) sia privo di equazioni: infatti notiamo che $E = (E_1^*, E_{21}^*, E_{221}^*, E_{222}^*)^*$ è invertibile, essendo prodotto di matrici invertibili, come si vede dalla sua definizione. Pertanto, cambiando coordinate in Y secondo $E^{\pi^{-1}}$ le equazioni di β_{222}) diventano equazioni del tipo

$$\beta_{222}) \qquad py_j^\pi = p\,\psi_j, \quad s'' \leq j \leq n.$$

Consideriamo, ad esempio, l'ultima; dividendola per p, essa diventa un'equazione del tipo α), ed il nuovo sistema ha n diminuito di 1 (e m aumentato di 1), e per esso vale l'ipotesi di induzione.

Ad ogni soluzione modulo p^w del vecchio sistema corrisponde una soluzione modulo p^{w-1} del nuovo, inoltre ogni soluzione modulo p^w del nuovo sistema è una soluzione modulo p^w del vecchio; perciò I è dimostrato per induzione. Per quanto riguarda II, notiamo che la varietà delle soluzioni del nuovo sistema, V', è uguale a $V \cap V''$, con V varietà delle soluzioni del vecchio sistema, (che è pura essendo un gruppo algebrico) e V'' determinata dall'equazione $(y_n^\pi - \psi_n)_{w-1} = 0$, e siccome $V \cap V'' \neq \emptyset$, abbiamo $\dim V' \geq \dim V - 1$, perciò per induzione segue II.

Colle semplificazioni fatte, la dimostrazione del teorema riposa ora sul lemma seguente (la cui numerazione interna prosegue quella del Teorema 2):

9. Lemma. *Se il teorema 2 vale per $n-1$, esso vale anche per il sistema seguente (scritto in forma vettoriale)*

$$
\begin{array}{lllr}
(2.8) & \alpha_1) & & X_1^\pi = Y_1 + p\,\Phi_1 \\
& \alpha_2) & & X_2^\pi = Y_2 + p\,\Phi_2 \\
& \alpha_3) & & X_3^\pi = A_3 X + p\,\Phi_3 \\
& \alpha_4) & & X_4^\pi = A_4 X + p\,\Phi_4 \\
& \beta_1) & & pE_1 Y^\pi = Y_3 + p\,\Psi_1 \\
& \beta_2) & & pE_2 Y^\pi = X_1 + p\,\Psi_2 \\
& \beta_3) & & pE_3 Y^\pi = X_3 + p\Psi_3
\end{array}
$$

in cui le equazioni di β_1), β_2), β_3) sono in totale n.

Dim. Nel corso della dimostrazione, nella notazione degli indici, si evita l'uso delle virgole; è da intendere che ogni simbolo costituisce un indice staccato, a meno che due non siano uniti da un $+$ o un $-$; ad esempio, $4r+12$ è da intendere $4, r+1, 2$.

10. Suddividiamo X_2 e X_4 (salvi opportuni cambiamenti di coordinate) in due sottoinsiemi ciascuno, $X_{2\varrho}$ e $X_{2\sigma}$, $X_{4\varrho}$ e $X_{4\sigma}$ nel modo sotto descritto in A e B:

A Se $X_3 = \emptyset$, poniamo $X_{2\varrho} = X_2$, $X_{4\varrho} = X_4$, $X_{2\sigma} = X_{4\sigma} = \emptyset$.

B Se $X_3 \neq \emptyset$, poniamo innanzitutto:

$$(2.9) \qquad X_{20} = X_2 \quad X_{40} = X_3 \quad X_{50} = X_4 \quad X_{60} = X_1 \cup X_3$$

e definiamo poi per induzione su r, e nel modo che andremo a descrivere, delle X_{2r}, X_{4r}, X_{5r}, X_{6r}, in modo che soddisfino le seguenti proprietà:

$$\begin{array}{lll}
(2.10) & a) & X_{2r} \cup X_{5r} \cup X_{6r} = X \\
 & b) & X_{2r} \cap X_{5r} = X_{5r} \cap X_{6r} = X_{6r} \cap X_{2r} = \emptyset \\
 & c) & X_{2r+1} \subseteq X_{2r} \subseteq X_2 \\
 & d) & X_{5r+1} \subseteq X_{5r} \subseteq X_4 \\
 & e) & X_{4r+1} \cup X_{5r+1} = X_{5r} \\
 & f) & X_{6r+1} = X_{6r} \cup X_{4r+1} \cup (X_{2r} - X_{2r+1}) \supseteq X_{60} \\
 & g) & X_{5r} \cup \bigcup_{s=1}^{r} X_{4s} = X_4
\end{array}$$

Si noti che X_{6r} è l'unione dei seguenti sottoinsiemi disgiunti: $X_{6r} \cap X_2$ X_1 (per f) e 2.9); X_3; X_{4s}, $1 < s \leq r$ (per f). La parte α) del sistema, scritta nelle variabili X_r sarà la seguente (interpretando $X_{2\cap 6r}$ come $X_2 \cap X_{6r}$ e analogamente $Y_{2\cap 6r}$) ricordando che $X_{40} = X_3$:

$$\begin{array}{llll}
(2.11) \quad \alpha_{2r}) & X_{2r}^{\pi} = Y_{2r} + p\,\Phi_{2r} & & \\
\alpha_{2\cap 6r}) & X_{2\cap 6r}^{\pi} = Y_{2\cap 6r} + p\,\Phi_{2\cap 6r} & & \\
\alpha_{1}) & X_{1}^{\pi} = Y_{1} + p\,\Phi_{1} & & \\
\alpha_{3}) & X_{3}^{\pi} = A_{3}X + p\,\Phi_{3} & & \\
\alpha_{4s}) & X_{4s}^{\pi} = A_{4s}X + p\,\Phi_{4s} & & 1 \leq s < r \\
\alpha_{4r}) & X_{4r}^{\pi} = A_{4r}X + p\,\Phi_{4r} & & \\
\alpha_{5r}) & X_{5r}^{\pi} = A_{5r}X + p\,\Phi_{5r}. & &
\end{array}$$

Provvediamo ora a ridurre opportunamente la forma di α_{4r}); supporremo che A_{4s} sia già ridotto alla forma in cui ridurremo A_{4r}. Abbiamo:

$$\alpha_{4r}) \qquad X_{4r}^{\pi} = A_{4r2}X_{2r} + A_{4r5}X_{5r} + A_{4r6}X_{6r} + p\,\Phi_{4r}$$

con $A_{4r2} = A'_{4r2}\, Q_{4r2}\, A''_{4r2} + p\, A'''_{4r2}$; perciò cambiando coordinate in X_{2r} secondo A''_{4r2}, (e in Y_{2r} secondo $(A''_{4r2})^{\pi}$ in modo di non cambiare la forma di α_{2r})) otteniamo, facendo i soliti cambiamenti e spezzando X_{2r} in X_{2r1} e X_{2r2}:

$$\alpha_{4r1}) \qquad C_{4r1}\, X_{4r}^{\pi} = X_{2r1} + A_{4r15}\, X_{5r} + A_{4r16}\, X_{6r} + p\, \Phi_{4r1}$$

$$\alpha_{4r2}) \qquad C_{4r2}\, X_{4r}^{\pi} = \qquad A_{4r25}\, X_{5r} + A_{4r26}\, X_{6r} + p\, \Phi_{4r2}\,.$$

Eseguendo il cambiamento di coordinate $X'_{2r1} = X_{2r1} + A_{2r15}\, X_{5r}$ si elimina il termine con X_{5r} da α_{4r1}):

$$(2.12) \quad \alpha_{4r1}) \qquad C_{4r1}\, X_{4r}^{\pi} = X_{2r1} + A_{4r16}\, X_{6r} + p\, \Phi_{4r1}$$

ma α_{2r1}) diventa:

$$\alpha_{2r1}) \qquad X_{2r1}^{\pi} = Y_{2r1} + A_{2r1}\, X + p\, \Phi_{2r1}$$

con $A_{2r1}\, X = A_{4r15}^{\pi}\, X_{5r}^{\pi}$ ricavato da α_{5r}).

Eseguendo poi il cambiamento di coordinate $Y'_{2r1} = Y_{2r1} + A_{2r1}\, X$ si elimina A_{2r1} da α_{2r1}); inoltre, come abbiamo già visto in 7 in una occasione simile, tale cambiamento non modifica ulteriormente la forma del sistema. Così α_{2r1}) è tornato alla forma

$$\alpha_{2r1}) \qquad X_{2r1}^{\pi} = Y_{2r1} + p\, \Phi_{2r1}\,.$$

Consideriamo ora α_{4r2}); operando come al solito, lo spezziamo in

$$(2.13) \quad \alpha_{4r21}) \qquad C_{4r21}\, X_{4r}^{\pi} = X_{5r1} + A_{4r216}\, X_{6r} + p\, \Phi_{4r21}$$

$$\alpha_{4r22}) \qquad C_{4r22}\, X_{4r}^{\pi} = \qquad A_{4r226}\, X_{6r} + p\, \Phi_{4r22}\,.$$

Notiamo infine che $C_{4r} = (C_{4r1}^{*}, C_{4r21}^{*}, C_{4r22}^{*})^{*}$ è invertibile; pertanto, moltiplicando α_{4r}), nella forma finale, a sinistra per C_{4r}^{-1}, si ottiene un sistema di forma analoga a quello di partenza, ma con in più A_{4r} nella forma opportuna che si era annunciata; inoltre, se gli α_{4s}), $s < r$, erano già nella forma a cui si è ridotto α_{4r}), coi cambiamenti di coordinate che si sono operati in α_{4r}) la loro forma non viene modificata. Procediamo quindi coll'induzione, e poniamo:

$$(2.14) \qquad \begin{aligned} X_{4r+1} &= X_{5r1} \\ X_{5r+1} &= X_{5r2} = X_{5r} - X_{5r1} \\ X_{2r+1} &= X_{2r2} = X_{2r} - X_{2r1} \\ X_{6r+1} &= X_{6r} \cup X_{5r1} \cup X_{2r1}\,. \end{aligned}$$

Le 2.10 sono ovviamente verificate.

Dalle prime due delle 2.14 si vede che o $X_{4r+1} = \emptyset$, ovvero $X_{5r+1} \subset X_{5r}$; se per ogni r fosse $X_{4r} \neq \emptyset$, si avrebbe $X_{5r} = \emptyset$ per r elevato, quindi $X_{4r+1} = \emptyset$; pertanto $X_{4r} = \emptyset$ per r elevato. Sia l il minimo numero tale che $X_{4l+1} = \emptyset$; poniamo allora

$$(2.15) \qquad X_{2\varrho} = X_{2l+1} = \bigcap_{0}^{l+1}{}_r\, X_{2r}$$

$$X_{2\sigma} = X_2 - X_{2\varrho} = \bigcup_{0}^{l}{}_r\, X_{2r1} = X_2 \cap X_{6l+1}$$

$$X_{4\varrho} = X_{5l+1} = \bigcap_{0}^{l+1}{}_r\, X_{\,r}$$

$$X_{4\sigma} = X_4 + X_{4\varrho} = \bigcup_{0}^{l}{}_r\, X_{5r1} = \bigcup_{1}^{l+1}{}_r\, X_{4r} = X_4 \cap X_{6l+1}$$

$\left(\text{si nota infatti per induzione che } X_2 - X_{2r} = \bigcup_{0}^{r-1}{}_s\, X_{2s1}\,,\ X_4 - X_{4r} = \bigcup_{0}^{r-1}{}_s\, X_{5s1}\right)$.

Con ciò gli $X_{\cdot\varrho}$, $X_{\cdot\sigma}$ sono definiti in tutti i casi.

Il sistema 2.11, al passo $l + 1$, tenendo conto di 2.10, 2.14, 2.15 risulta:

$$\alpha_1) \qquad X_1^\pi = Y_1 + p\,\Phi_1$$

$$\alpha_{2\sigma}) \qquad X_{2\sigma}^\pi = Y_{2\sigma} + p\,\Phi_{2\sigma}$$

$$\alpha_{2\varrho}) \qquad X_{2\varrho}^\pi = Y_{2\varrho} + p\,\Phi_{2\varrho}$$

$$\alpha_3) \qquad X_3^\pi = A_{31}\,X_1 + A_{33}\,X_3 + A_{32\sigma}\,X_{2\sigma} + A_{34\sigma}\,X_{4\sigma} + p\,\Phi_3$$

$$\alpha_{4\sigma}) \qquad X_{4\sigma}^\pi = A_{4\sigma 1}\,X_1 + A_{4\sigma 3}\,X_3 + A_{4\sigma 2\sigma}\,X_{2\sigma} + A_{4\sigma 4\sigma}\,X_{4\sigma} + p\,\Phi_{4\sigma}$$

$$\alpha_{4\varrho}) \qquad X_{4\varrho}^\pi = A_{4\varrho}\,X + p\,\Phi_{4\varrho}$$

$$\beta_1) \qquad pE_1 Y^\pi = Y_3 + p\,\Psi_1$$

$$\beta_2) \qquad pE_2 Y^\pi = X_1 + p\,\Psi_2$$

$$\beta_3) \qquad pE_3 Y^\pi = X_3 + p\,\Psi_3$$

Infatti

$$X_{2\sigma} = X_2 \cap X_{6l+1}\,;\ \alpha_3) = \alpha_{401}) \cup \alpha_{4021}) \cup \alpha_{4022})\,;\ \alpha_{4\sigma}) = \bigcup_{1}^{l+1}{}_r\,(\alpha_{4r1}) \cup \alpha_{4r21}) \cup \alpha_{4r22}))\,;$$

$$X_{6r} \subseteq X_1 \cup X_3 \cup \bigcup_{1}^{l}{}_r\, X_{2r} \cup \bigcup_{1}^{l+1}{}_r\, X_{4r} = X_1 \cup X_3 \cup X_{2\sigma} \cup X_{4\sigma}\,.$$

11. Supponiamo dapprima $X_{2\varrho} \neq \emptyset$. Moltiplichiamo allora $\alpha_{2\varrho})$, $\alpha_{4\varrho})$ per p. Abbiamo allora che $X_{2\varrho}$, $X_{4\varrho}$, $Y_{2\varrho}$ compaiono ovunque con coefficiente divisibile per p; possiamo allora operare le sostituzioni $X'_{2\varrho} = pX_{2\varrho}$; $X'_{4\varrho} = pX_{4\varrho}$; $Y'_{2\varrho} = pY_{2\varrho}$.

Otteniamo così un nuovo sistema, per cui il teorema vale per ipotesi, perchè abbiamo ridotto n di un numero pari alla cardinalità di $Y_{2\varrho}$; inoltre ogni soluzione modulo p^w del primo sistema è soluzione modulo p^w del secondo, e se due soluzioni del secondo sono congrue modulo p^{w+1} e ad esse corrispondono soluzioni del primo sono congrue moduli p^w; quindi vale I.

Sia ora V la varietà delle soluzioni in K_w del vecchio sistema, e V' la analoga varietà del nuovo. Indichiamo con g la cardinalità di $X_{2\varrho}$ (e di $Y_{2\varrho}$) e con g' la cardinalità di $X_{4\varrho}$; Sia V'' la varietà lineare determinata da $(X'_{2\varrho})_0 = 0$, $(Y'_{2\varrho})_0 = 0$ e $(X'_{4\varrho})_0 = 0$; sia V''' lo spazio affine di dimensione g con punto generico $(Y'_{2\varrho})_w = (Y_{2\varrho})_{w-1}$; sia $W = (V' \cap V'') \times V''')$, V^{IV} lo spazio affine con punto generico $(X_{2\varrho}, X'_{4\varrho})_w = (X_{2\varrho}, X_{4\varrho})_{w-1}$ (di dimensione $g + g'$) e V^{V} la varietà determinata dalle equazioni $(\alpha_{2\varrho})_{w-1}$ e $(\alpha_{4\varrho})_{w-1}$. Abbiamo $V = (W \times V^{\mathrm{IV}}) \cap V^{\mathrm{V}}$. Ma per ogni punto $P \in W$, abbiamo che $(P \times W^{\mathrm{IV}}) \cap V^{\mathrm{V}}$ ha dimensione 0 (per il Teorema 1), perciò $\dim V = \dim W \leq \leq \dim V + g$, cioè vale II.

12. Supponiamo allora $X_{2\varrho} = \emptyset$; notiamo che, in tal caso, per ogni r, $\alpha_{4r22})$ deve essere privo di equazioni. Indichiamo infatti con $g_\cdot$ il numero di equazioni di $\alpha_\cdot)$, e con $g'_\cdot$ il numero di equazioni di $\beta_\cdot)$. Ovviamente $g_1 = g_2$ e $g_2 = g'_3$. Inoltre, poichè ogni Y compare una ed una sola volta al secondo membro al di fuori delle Φ, Ψ, abbiamo $n = g'_1 + g'_2 + g'_3 = g_1 + g_2 + g'_1$ quindi $g_2 = g'_3 = g_3$.

Notiamo che $g_{4r} = g_{4r1} + g_{4r21} + g_{4r22} = g_{2r1} + g_{4r+1} + g_{4r22}$; perciò sommando rispetto a tutti gli r, e ricordando che $g_3 = g_{40}$, abbiamo

$$g_3 = \sum_{0}^{l}{}_r\, g_{2r1} + \sum_{0}^{l}{}_r\, g_{4r2} = g_{2\sigma} + \sum_{0}^{l}{}_r\, g_{2r22}\,;$$

ma $g_{2\sigma} = g_2 - g_{2\varrho} = g_2 = g_3$, perciò $\sum_{0}^{l}{}_r\, g_{4r22} = 0$.

13. Riscriviamo l'intero sistema nella forma definitiva:

$$
(2.17)\quad
\begin{array}{lllllll}
\alpha_1) & & X_1^\pi & -(Y_1 & + & & p\,\Phi_1\ \ )=0 \\
\alpha_{201} & & X_{201}^\pi & -(Y_{201} & + & & p\,\Phi_{201}\ \ )=0 \\
\alpha_{211}) & & X_{211}^\pi & -(Y_{211} & + & & p\,\Phi_{211}\ \ )=0 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\alpha_{2l1}) & & X_{2l1}^\pi & -(Y_{2l1} & + & & p\,\Phi_{2l1}\ \ )=0 \\
\alpha_{401}) & C_{401} & X_3^\pi & -(X_{201} & +A_{4016} & X_{60} & +p\,\Phi_{401}\ \ )=0 \\
\alpha_{402}) & C_{402} & X_3^\pi & -(X_{41} & +A_{4026} & X_{60} & +p\,\Phi_{402}\ \ )=0 \\
\alpha_{411}) & C_{411} & X_{41}^\pi & -(X_{211} & +A_{4116} & X_{61} & +p\,\Phi_{411}\ \ )=0 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\alpha_{4l-11}) & C_{4l-11} & X_{4l-1}^\pi & -(X_{2l-11} & +A_{4l-116} & X_{6l-1} & +p\,\Phi_{4l-11})=0 \\
\alpha_{4l-12}) & C_{4l-12} & X_{4l-1}^\pi & -(X_{4l} & +A_{4l-126} & X_{6l-1} & +p\,\Phi_{4l-12})=0 \\
\alpha_{4l1}) & C_{4l1} & X_{4l}^\pi & +(X_{2l1} & +A_{4l16} & X_{6l} & +p\,\Phi_{4l1}\ \ )=0 \\
\alpha_{4l2}) & & & \emptyset & & & \\
\alpha_{4\varrho}) & & X_{4\varrho}^\pi & -(A_{4\varrho}X & & & +p\,\Phi_{4\varrho}\ \ )=0 \\
\beta_1) & p\,E_1\,Y^\pi & & -(Y_3 & & & +p\,\Psi_1\ \ )=0 \\
\beta_2) & p\,E_2\,Y^\pi & & -(X_1 & & & +p\,\Psi_2\ \ )=0 \\
\beta_3) & p\,E_3\,Y^\pi & & -(X_3 & & & +p\,\Psi_3\ \ )=0
\end{array}
$$

Esso è ora tale che, datane una soluzione in K_w, ne esiste una in K_{w+1} congrua ad essa modulo p^w. Il problema si riduce a risolvere una congruenza modulo p.

Siano infatti X', Y' tali che (indicando il sistema in forma sintetica):

$$(X')^\pi - AX' - BY' \equiv 0\ (p^w)$$

$$(p\,Y')^\pi - CX' - DY' \equiv 0\ (p^w)$$

e sia

$$(X')^{\pi} - AX' - BY' \equiv p^{w} F(p^{w+1})$$

$$(pY')^{\pi} - CX' - DY' \equiv p^{w} G(p^{w+1})$$

e supponiamo di riuscire a trovare X'', Y'' tali che

$$(X'')^{\pi} - AX'' - BY'' \equiv F(p)$$

$$- CX'' - DY'' \equiv G(p)$$

Allora $X' - p^{w} X''$, $Y' - p^{w} Y''$ è soluzione del sistema modulo p^{w+1}.

Il problema è allora ricondotto a trovare una soluzione del sistema 2.17 modulo p, con al secondo membro costanti arbitrarie; cioè alla soluzione di

$$(2.18)\quad \begin{array}{llllllll}
\alpha_1) & & X_1^{\pi} & + & & & F_1 & \equiv Y_1 \\
\alpha_{201}) & & X_{201}^{\pi} & + & & & F_{201} & \equiv Y_{201} \\
\alpha_{211}) & & X_{211}^{\pi} & + & & & F_{211} & \equiv Y_{211} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\alpha_{2l1}) & & X_{2l1}^{\pi} & + & & & F_{2l1} & \equiv Y_{2l1} \\
\alpha_{401}) & C_{401} & X_3^{\pi} & - & A_{4016} & X_{60} & + F_{401} & \equiv X_{201} \\
\alpha_{402}) & C_{402} & X_3^{\pi} & - & A_{4026} & X_{60} & + F_{402} & \equiv X_{41} \\
\alpha_{411}) & C_{411} & X_{41}^{\pi} & - & A_{4116} & X_{60} & + F_{411} & \equiv X_{211} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\alpha_{4l-11}) & C_{4l-11} & X_{4l-1}^{\pi} & - & A_{4l-116} & X_{6l-1} & + F_{4l-11} & \equiv X_{2l-11} \\
\alpha_{4l-12}) & C_{4l-12} & X_{4l-1}^{\pi} & - & A_{4l-126} & X_{6l-1} & + F_{4l-12} & \equiv X_{4l} \\
\alpha_{4l1}) & C_{411} & X_{4l}^{\pi} & - & A_{4l16} & X_{6l} & + F_{4l1} & \equiv X_{2l1} \\
\alpha_{4\varrho}) & & X_{4\varrho}^{\pi} & - & A_{4\varrho 6} & X_{6l+1} & + F_{4\varrho} & \equiv A_{4\varrho\varrho} X_{4\varrho} \\
\beta_1) & & & & & & G_1 & \equiv Y_3 \\
\beta_2) & & & & & & G_2 & \equiv X_1 \\
\beta_3) & & & & & & G_3 & \equiv X_3
\end{array}$$

Con tutte le congruenze modulo p, F_i e G_i costanti.

Tali congruenze sono in effetti equazioni in k sulla componente 0 di X, Y. Tale sistema ha soluzione qualunque siano F, G, e ne ha un numero finito: da β_1), β_2), β_3) ricaviamo infatti il valore della componente 0 di Y_3, X_1, X_3; sostituendo i valori trovati ovunque possibile, si determina la componente 0 di Y_1 da α_1), di X_{201} da α_{401}), di X_{41} da α_{402}), e sostituendo X_{201} in α_{201}), si ricava Y_{201}.

Per induzione determiniamo perciò la componente 0 di X_{4r+1} e di X_{2r1} e da questa la componente 0 di Y_{2r1}, notando che quando si viene a considerare α_{4r1}) e α_{4r2}), $X_{6r} = X_1 \cup X_3 \cup \bigcup_1^r {}_s X_{4s} \cup \bigcup_0^{r-1} {}_s X_{2s1}$ (da (2.14)) è già stato determinato.

Determiniamo così la componente 0 di X_1, X_2, X_3, $X_{4\sigma}$, Y_1, Y_2, Y_3, e resta da determinare $X_{4\varrho}$; ma operando tutte le sostituzioni possibili in $\alpha_{4\varrho}$) questo si riduce ad un sistema del tipo studiato nel teorema 1, ed ha perciò un numero finito positivo di soluzioni.

È così dimostrata l'esistenza di una soluzione modulo p^{w+1} congrua a quella data modulo p^w, e passando al limite si ottiene I; per induzione su W si dimostra inoltre che le soluzioni modulo p^w sono in numero finito, e il lemma (e con esso il Teorema 2) è completamente dimostrato. C. V. D.

3. Classificazione.

Teorema 3. *Siano M, M' K-moduli canonici di dimensione d e codimensione c, isomorfi modulo p^n, con $n = cd + 1$.*
Allora $M \cong M'$.

Dim. Notiamo che, dato un K-modulo canonico M di codimensione c, ne esiste una base tale che, rispetto ad essa, $C_\pi = QA$, con A invertibile, e $(Q)_{ij} = \delta_{ij}$ se $i \leq c$, $(Q)_{ij} = p\,\delta_{ij}$ se $i > c$; sia infatti $x'_{c+1}, \dots, x'_{c+d}$ una k-base di tM/pM; estendiamola ad una base $x'_1, \dots, x'_{c+d}$ di M/pM; siano $x_1, \dots, x_{c+d}$ rappresentanti in M di $x'_1, \dots, x'_{c+d}$; essi costituiscono una base di M che soddisfa alle condizioni richieste, perchè $\pi x_{c+i} \in \pi\, tM = pM$. Sia Q' tale che $QQ' = p$; rispetto alla base trovata sarà $C_t^\pi = A^{-1} Q'$.

Siano ora (C_π, C_t) e (C'_π, C'_t) matrici caratteristiche rispettivamente di M ed M' rispetto a basi scelte come sopra, e sia $C_\pi = QA$, $C'_\pi = QA'$.

Il teorema sarà dimostrato se troveremo una soluzione del sistema, scritto in forma matriciale con incognita la matrice quadrata X di ordine $c + d$:

$$\lambda) \qquad X^\pi Q = QA' XA^{-1}$$

$$\mu) \qquad Q' X^\pi = A' XA^{-1} Q'$$

tale che, inoltre, X sia invertibile, ossia $(\det X)_0 \neq 0$.

L'isomorfismo modulo p^n di M e M' assicura l'esistenza di una matrice invertibile X' che sia soluzione modulo p^n del sistema. Indichiamo con λ_{ij} (risp. μ_{ij}) l'equazione nelle X_{ij} che si ottiene eguagliando le componenti (i,j) delle matrici della prima (risp. seconda) equazione. Abbiamo che

$p\,\lambda_{ij}$ coincide con μ_{ij} se $i \leq c,\ j \leq c$

λ_{ij} » » μ_{ij} se $i > c,\ j \leq c$ opp. $i \leq c,\ j > c$

λ_{ij} » » $p\mu_{ij}$ se $i > c,\ j > c$

perciò possiamo limitarci a considerare λ_{ij} per $j \leq c$, e μ_{ij} per $j > c$, e le altre equazioni sono conseguenza di queste. λ_{ij}, per $j \leq c$, è del tipo

$$X_{ij}^{\pi} = \sum_{h,l} a_{ijhl} X_{hl}$$

e così pure μ_{ij} per $i > c,\ j > c$; se invece $i \leq c,\ j > c$, μ_{ij} è del tipo

$$p\,X_{ij}^{\pi} = \sum_{h,l} a_{ijhl} X_{hl}$$

In complesso perciò abbiamo un sistema del tipo considerato nel Teorema 2, con cd equazioni del tipo β); esiste perciò una soluzione in K, X'', tale che $X' \equiv X''\,(p)$; perciò $\det X' \equiv \det X''\,(p)$, quindi X'' è invertibile c.v.d.

Cor. *Siano M, M' K-moduli canonici di dimensione d e codimensione c ed esista un isomorfismo φ di K-moduli tra di essi tali che* $\varphi\pi \equiv \pi\varphi$ (p^{n+1}), *con* $n = cd + 1$ *: allora* $M \cong M'$.

Dim. Le ipotesi implicano che esistono basi di M e M' tali che, rispetto ad esse, $C_\pi \equiv C'_\pi\,(p^{n+1})$; allora $pC_t^{\pi} = C_t'^{\pi}\,C'_\pi\,C_t^{\pi} \equiv C_t'^{\pi}\,C_\pi\,C_t^{\pi} \equiv pC_t'^{\pi}\,(p^{n+1})$, quindi $C_t \equiv C'_t\,(p^n)$, $M \cong M'$ mod p^n.

Teorema 4. *Fissati c e d, esistono un gruppo algebrico lineare irriducibile G ed una varietà affine irriducibile V, sulla quale G opera razionalmente, tali che le classi di K-moduli canonici di dimensione d e codimensione c rispetto all'isomorfismo siano in corrispondenza biunivoca colle orbite di G in V; ogni orbita ha codimensione in V minore o uguale a cd.*

Dim. Sia M un K-modulo canonico; per il cor. del teorema 3 esso è determinato a meno di isomorfismo assegnando le prime $n + 1$ componenti della matrice C_π rispetto ad una base qualunque, con $n = cd + 1$. In particolare possiamo scegliere tale base come nella dimostrazione del teorema 3. L'insieme di tali matrici è l'insieme delle matrici A, quadrate di ordine $m = c + d$, a elementi in K_{n+1}, tali che $A_{ij} \in pK_{n+1}$ se $i > c$, e che la matrice B a elementi in k, definita da $B_{ij} = (A_{ij})_0^p$ se $i < c$; $B_{ij} = (A_{ij})_1$ se $i > c$; abbia determinante non nullo.

Tale insieme è una varietà affine irriducibile di dimensione $m^2(n+1) - md$.

Due matrici A, A' provengono da moduli isomorfi se e solo se esiste una matrice invertibile X, a elementi in K_{n+1}, tali che $X^\pi AX^{-1} = A'$. Una matrice X invertibile trasforma in tal modo un punto di V in un altro punto di V se e solo se $(X_{ij})_0 = 0$, quando $j > c$, $j \leq c$ (cioè se trasforma in sè tM/pM).

Tali matrici formano un gruppo algebrico lineare irriducibile G di dimensione $m^2(n+1) - cd$.

Sia $A \in V$; l'applicazione $\varphi_A : G \times A \to V$ è razionale, e gli elementi X di G tali che $\varphi_A X = A$ sono un sottogruppo algebrico G' di g. Sia $A = QA'$, con A' invertibile.

G' è la sottovarietà di G intersezione di G colla varietà U delle soluzioni di $X^\pi Q = QA'XA'^{-1}$. Tale sistema è del tipo studiato nel Teorema 2, ed in esso compaiono dm equazioni del tipo β); perciò G' ha dimensione minore o uguale a dm; quindi l'orbita che contiene A è di dimensione almeno $m^2(n+1) - cd - dm$; quindi ha codimensione in V al più cd C.V.D.

Notiamo che la codimensione cd è effettivamente raggiunta; basta infatti considerare il K-modulo canonico $N_{c,d}$ ([2], P. 303) con semplici calcoli, seguendo la traccia del Teorema 2, si vede che la sua orbita ha codimensione cd.

La scelta di V e G, nel corso della dimostrazione del teorema 4, è in buona parte arbitraria, sia perchè si sono considerate matrici C_π modulo p^n con $n = cd + 1$, anzicchè modulo p^r, con $r > n$; inoltre si è richiesto che le matrici C_π siano considerate rispetto ad una base opportuna, invece che rispetto ad una base qualunque. Infine potrebbe essere scelta la matrice C_t invece della C_π. Si può vedere però che questa arbitrarietà non è essenziale, essendovi relazioni precise tra le varietà che si ottengono nei varii casi; in particolare, la struttura topologica dello spazio quoziente di V per G è la stessa in ogni caso.

Se nella dimostrazione del teorema si prende, invece della V descritta, la varietà V' delle prime $n + i + 1$ componenti della matrice C_π (sempre scelta rispetto ad una base del tipo considerato nella dimostrazione) e il corrispondente G' che opera su V', indicando con A^r lo spazio affine su k di dimensione r, abbiamo $V' \cong V \times A^{im^2}$, $G' \cong G \times A^{im^2}$ (quest'ultimo isomorfismo inteso come varietà e non come gruppo), ad ogni orbita di G', in V' è uguale, per il teorema 3, alla corrispondente orbita di G in V moltiplicata per A^{1m^2}. Consideriamo invece, al posto della V descritta, la varietà V' delle prime $n+1$ componenti delle matrici C_π rispetto ad una base qualunque, ed il corrispondente gruppo $G' = GL((K_{n+1})^m)$. V è sotto-varietà di V', e G di G': l'applicazione razionale $V' \times G' \to V'$ induce una applicazione razionale $V \times G' \to V'$, che è surgettiva, e tale che il prodotto di un'orbita di G in V per G' vada in un'orbita di G' in V'. Lo spazio topologico quoziente di V' per G' è omeomorfo allo spazio quoziente di $V \times G'$ per $G \times G'$ (V' è infatti omeomorfo al quoziente di $V \times G'$ determinato dall'applicazione razionale $V \times G' \to V'$), e il quoziente di $V \times G'$ per $G \times G'$ è omeomorfo al quoziente di V per G.

Infine consideriamo la matrice C_t invece della C_π, sempre rispetto ad una base come nel teorema 4. Per quanto abbiamo visto nel primo caso, tenendo presente che tutte le varietà che consideriamo sono definite su un corpo primo e sono pertanto isomorfe al $\cdot^p$ di loro stesse, è sufficiente dimostrare che esiste un isomorfismo che porta orbite in orbite tra la varietà V delle prime $n+1$ componenti delle $Q^{-1} C_\pi$ e la varietà delle prime $n+1$ componenti delle $C_t^\pi (Q')^{-1}$ (Q, Q' come nel teorema 3). Tali varietà sono isomorfe a $GL((K_{n+1})^m)$, e l'isomorfismo cercato è la φ definita da $\varphi(X) = X^{-1}$.

4. Corrispondenze algebroidi in V.

Dal Teorema 4 si vede che la corrispondenza che ad ogni $A \in V$ associa l'insieme dei punti che corrispondono a K-moduli canonici isomorfi è una corrispondenza algebroide di V (tale corrispondenza è l'immagine dell'applicazione $G \times V \to V \times V$ che porta (X, A) in $(X(A), A)$.)

Qui esaminiamo altre corrispondenze.

Sia $L = (l_1, \dots, l_s)$, $l_i \in N$, $0 \leq l_1 \leq \dots \leq l_s$. Sia M un K-modulo libero finito di ordine s, M' un suo sotto K-modulo; diciamo che M' ha livello L su M se esiste una base $x = (x_1, \dots, x_s)$ di M tale che $p^L X = (p^{l_1} x_1, \dots, p^{l_s} x_s)$ sia una base di M'.

TEOREMA 5. *Sia V come del teorema 4. La corrispondenza che ad ogni K-modulo canonico M di dimensione d e codimensione c associa l'insieme dei suoi sotto K-moduli canonici aventi un determinato livello L su M, induce su V una corrispondenza algebroide.*

DIM. Sia M' un sotto K-modulo canonico di M di livello L su M, siano X, X' basi qualunque di M, M', e C_π, C'_π le relative matrici caratteristiche per π. Per ipotesi esiste $\overline{X}$ base di M tale che $p^L \overline{X}$ sia base di M'; esistono cioè matrici invertibili E, F, tali che, indicando con $\overline{C}_\pi$, $\overline{C}'_\pi$ le matrici caratteristiche per π rispetto a $\overline{X}, p^L \overline{X}$, si abbia $E^\pi C_\pi E^{-1} = \overline{C}_\pi$, $\overline{C}'_\pi = (F^{-})^\pi C'_\pi F$. Deve essere $\overline{C}'_\pi p^L = p^L \overline{C}_\pi$, perciò abbiamo

$$F^\pi p^L E^\pi C_\pi = C'_\pi F p^L E \,. \tag{4.1}$$

Inoltre, dati C_π e C'_π, se esistono F, G invertibili tali che valga 4.1, esse sono matrici caratteristiche per π di un K-modulo canonico e di un suo sotto K-modulo canonico di livello L. Sia $l = l_{c+d}$; consideriamo come V, anzicchè quella del teorema 4, la varietà delle matrici C_π modulo p^{n+l+1} rispetto ad una base qualunque.

La 4.1 definisce una corrispondenza algebroide in V, composta dalle coppie (A, B) con $BFp^L E = F^\pi p^L E^\pi A$, con $A, B \in V$, $E, F \in G$. Tale corrispondenza, per il teorema 3, tenendo presente che si è moltiplicato al più per p^i con $i \leq l$, è la corrispondenza definita in ipotesi.

Le osservazioni finali del § 3 assicurano che tale corrispondenza, costante sulle orbite di G in V, è algebroide anche per le altre possibili scelte di V esaminate.

COR. *La relazione di isogenia induce una corrispondenza algebroide in V.*

DIM. Da [5] si sa che, dati c, d, esiste un livello L tale che se M, M' sono isogeni di dimensione d e codimensione c, esiste un sotto K-modulo canonico di M, avente su di M livello minore di L, isomorfo a M'; pertanto la corrispondenza definita in ipotesi è unione di un numero finito di corrispondenze algebroidi, quindi è algebroide.

5. Cambiamento di corpo base. Specializzazione.

Sia $\mathbf{k}$ un corpo algebricamente chiuso contenente k; possiamo considerare $\mathbf{K} = \mathit{vect}\,\mathbf{k}$, i $\mathbf{K}$-moduli canonici e le varietà $\mathbf{V}$, $\mathbf{G}$ corrispondenti come dal teorema 4.

$\mathbf{V}$, $\mathbf{G}$ sono estensione di V, G a $\mathbf{k}$, e i $\mathbf{K}$-moduli canonici che sono estensione a $\mathbf{K}$ di K-moduli canonici corrispondono alle orbite di $\mathbf{G}$ in $\mathbf{V}$ che hanno punti razionali su k (equivalentemente, che sono definite su k, poichè $\mathbf{G}$ è definito sul corpo primo).

Siano $\mathbf{M}, M$ rispettivamente un $\mathbf{K}$-modulo canonico e un K-modulo canonico; diciamo che M è specializzazione di $\mathbf{M}$ se esiste una schiera valutante $\mathfrak{k}$ di $\mathbf{k}$ con corpo residuo k e, posto $\mathfrak{K} = \mathit{vect}\,\mathfrak{k}$, se esiste un $\mathfrak{K}$-modulo libero finito $\mathfrak{M}$ con operatori t, π, tale che $\mathbf{M} \simeq \mathfrak{M} \otimes_{\mathfrak{K}} \mathbf{K}$, $M \simeq \mathfrak{M} \otimes_{\mathfrak{K}} K$. L'insieme di $\mathfrak{k}$, $\mathfrak{M}$, e degli isomorfismi di definizione è detta una specializzazione di $\mathbf{M}$ in M.

Notiamo che, dato un $\mathfrak{K}$-modulo libero finito $\mathfrak{M}$ con t e π tali che $t\pi = p$, $M = \mathfrak{M} \otimes_{\mathfrak{K}} K$ è un K-modulo canonico, che ha come base l'immagine di una base di $\mathfrak{M}$.

TEOREMA 6. *Siano M, M' K-moduli canonici di dimensione d e codimensione c; siano V, G come nel teorema 4. Sono equivalenti:*

a) *L'orbita di G in V corrispondente a M è contenuta nella chiusura dell'orbita di G in V corrispondente ed N.*

b) *Esiste* $\mathbf{k}$ *algebricamente chiuso contenente k, tale che M sia specializzazione di $N \otimes_K \mathbf{K}$.*

La schiera $\mathfrak{k}$ di $\mathbf{k}$ *può essere presa archimedea.*

DIM. ($a \Longrightarrow b$) Sia Y un punto generale di G, e sia $\mathbf{k}$ un corpo algebricamente chiuso su cui Y sia razionale; Y corrisponde ad un cambiamento di coordinate di $\mathbf{K}$-moduli.

Sia data una base di M ed una di N, ed i relativi punti $A \in V$, $B \in V$.

Il punto X di $\mathbf{V}$ ottenuto da B operandovi tramite Y, è un punto generale su k dell'orbita di G in V contenente B, quindi A è specializzazione su k di X. Sia $\mathfrak{k}$ una schiera valutante archimedea di $\mathbf{k}$ con corpo residuo k, che induca una specializzazione di X in A.

X è il punto di $\mathbf{V}$ individuato dalle prime $n+1$ componenti della matrice $\mathbf{C}_\pi$ di un $\mathbf{K}$ modulo canonico isomorfo ad $N \otimes_K \mathbf{K}$ rispetto ad una base opportuna. Per il teorema 3, salvo operare un cambiamento di base, possiamo supporre che le componenti di posto maggiore di n dei vettori (di Witt) che sono elementi di tale matrice $\mathbf{C}_\pi$ siano uguali a 0.

Tale matrice $\mathbf{C}_\pi$ è della forma $Q\mathbf{A}$, con $\mathbf{A}$ invertibile in $\mathbf{K}$, $\mathbf{A}$ a elementi in $\mathfrak{K}$, e $\mathbf{A} \otimes_{\mathfrak{K}} K$ invertibile; perciò $\mathbf{A}$ è invertibile in $\mathfrak{K}$. Ne segue che esiste una matrice $\mathbf{C}_t$ a elementi in $\mathfrak{K}$ tale che $\mathbf{C}_\pi \mathbf{C}_t^\pi = p$; queste due matrici individuano un t ed un π di un $\mathfrak{K}$-modulo $\mathfrak{N}$ tale che

$$\mathfrak{N} \otimes_{\mathfrak{K}} \mathbf{K} \simeq N \otimes_K \mathbf{K}, \quad \mathfrak{N} \otimes_{\mathfrak{K}} K \simeq M.$$

(Questo secondo isomorfismo è ovvio come isomorfismo di K moduli; l'immagine del π di $\mathfrak{N}$ è congrua al π di M modulo p^{n+1}, quindi si ha l'isomorfismo di $\mathfrak{N} \otimes_{\mathfrak{K}} K$ con M).

($b \Longrightarrow a$) Consideriamo invece della V descritta nel teorema 4, la varietà corrispondente alle matrici C_π modulo p^{n+1} rispetto ad una base qualunque; per l'osservazione finale del § 3 questo non ha influenza sul risultato del teorema, che riguarda soltanto la struttura topologica del quoziente di V per G.

Consideriamo una base dell'$\mathfrak{M}$ definito dall'ipotesi; il π di $\mathfrak{M}$ definisce una matrice $\mathbf{C}_\pi$ a elementi in $\mathfrak{K}$, che individua un punto $\mathbf{A}$ di $\mathbf{V}$. Tale punto $\mathbf{A}$ di $\mathbf{V}$ è il trasformato di un punto A di $\mathbf{V}$ razionale su k (ottenuto prendendo come base di $N \otimes_K \mathbf{K}$ una base di N) secondo un punto di $\mathbf{G}$; è pertanto specializzazione di un punto $\mathbf{X}$ generale su $\mathbf{K}$ dell'orbita di $\mathbf{G}$ in $\mathbf{V}$ contenente $\mathbf{A}$. $\mathbf{X}$ è a maggior ragione punto generale dell'orbita di G in V contenente A. Ma l'omomorfismo di $\mathfrak{M}$ in M e la base di $\mathfrak{M}$ che definisce $\mathbf{C}_\pi$ individuano una base di M tale che il corrispondente punto $B \in V$ sia specializzazione di $\mathbf{A}$. Ne segue che B è specializzazione di $\mathbf{X}$, è cioè aderente all'orbita di G in V contenente A. C.V.D.

APPENDICE

Può avere interesse studiare K-moduli canonici « *non necessariamente liberi* », (ossia K-moduli finiti dotati di π e t con $t\pi = \pi t = p$) sopratutto perchè tale categoria (ovviamente abeliana) è equivalente ad una categoria di gruppi analitici facilmente identificabile.

Nel corso di questa sezione, parlando di K-moduli canonici, si intende sempre « *non necessariamente liberi* ».

Se M è un K-modulo X, con M_τ indicheremo il sotto K-modulo degli elementi a torsione. Se M è canonico, M_τ è canonico.

Notiamo che ogni K-modulo finito M ha una topologia naturale in cui $p^n M$ sono un sistema fondamentale di intorni di 0.

È l'unica topologia separata che rende M un K-modulo topologico con topologia K-lineare, dato che K è linearmente compatto; con questa topologia M è completo; pertanto qualunque considerazione topologica è naturale e priva di difficoltà.

OSSERVAZIONE. *Sia M un K-modulo canonico tale che $\pi M = M$; per ogni $x \in M$, abbiamo $\pi x = 0 \Longrightarrow x = 0$.*

DIM. Sia, per ogni i, $M_i = \{x \in M \mid \pi^i x = 0\}$. Per noetherianità, esiste n tale che $M_n = M_{n+1}$.

Sia x tale che $\pi x = 0$. Poichè $\pi^n M = M$, esiste x' tale che $\pi^n x' = x$; ma allora $x' \in M_{n+1} = M_n$, quindi $x = \pi^n x' = 0$.

COR. *Sia M un K-modulo canonico tale che $\pi M = M$, M' un sotto K-modulo canonico; allora $\pi M' = M'$.*

DIM. Si applica l'osservazione a M/M'.

COR. *Sia M un K-modulo canonico tale che $\pi M = M$; se $x \in M$ e $\pi x \in tM$, allora $x \in tM$.*

DIM. $tM = pM$; *sia* $py = \pi x$; *allora* $ty = x$.

TEOREMA A1. *Sia M un K-modulo canonico tale che $\pi M = M$; esiste un sistema minimale di generatori di M, $(x_1, \dots, x_n)$ tale che $\pi x_i = x_i$.*

DIM. Sia $X = (x_1, \dots, x_n)$ un sistema minimale di generatori di M (equivalentemente, un insieme tale che, ridotto modulo p, dia una k-base). Sia C_π una matrice tale che $C_\pi X = \pi X$. C_π è invertibile, e l'esistenza di un sistema di generatori come richiesto discende dall'esistenza di una matrice invertibile A tale che $C_\pi A = A^\pi$. Tale equazione è del tipo studiato nel Teorema 2 con incognita A e $n = 0$. Pertanto basta dimostrare l'esistenza di A tale che $C_\pi A \equiv A^\pi (p)$, ossia dimostrare il teorema quando $pM = 0$. In tal caso M è uno spazio vettoriale su k.

Sia $x_1 \in M$, $x_1 \neq 0$, e sia $x_{i+1} = \pi x_i$; sia $\pi x_n = \sum_1^n {}_i\, a_i x_i$; non tutti gli a_i sono nulli, per l'osservazione precedente.

Consideriamo il sistema di equazioni

$$a_1 X_n^p = X_1$$

$$X_{i-1}^p + a_i X_n^p = X_i \qquad 1 < i \leq n.$$

Con sostituzioni successive, si riduce ogni soluzione del sistema ad una soluzione della

$$\Phi = a_1^{p^{n-1}} X_n^{p^n} + a_2^{p^{n-2}} X_n^{p^{n-1}} + \dots + a_n X_n^p - X_n = 0.$$

Poichè $\dfrac{d\Phi}{dX_n} = -1$, la soluzione $X_n = 0$ è soluzione semplice, e siccome non tutti gli a_i sono nulli, esiste una soluzione non nulla; partendo da questa ricaviamo una soluzione del sistema non identicamente nulla; sia essa $(b_1, \dots, b_n)$.

Posto $y = \sum_1^n {}_i\, b_i x_i$, abbiamo $\pi y = \sum_1^n {}_i\, b_i^p \pi x_i = \sum_1^{n-1} {}_i\, b_i^p x_{i+1} + b_n^p \sum_1^n {}_i\, a_i x_i = \sum_1^n {}_i\, b_i x_i = y$.

Consideriamo ora $M' = M/Ky$; M' è un K-modulo canonico tale che $\pi M' = M'$, $pM' = 0$, ed ha ordine minore di quello di M; per induzione, ha una base $(z_1, \ldots, z_{n-1})$ tale che $\pi z_i = z_i$. Sia y_i un rappresentante di z_i in M; sia $\pi y_i = y_i + d_i y$; sia c_i soluzione dell'equazione

$$d_i + X^p = X$$

allora $\pi(y_i + c_i y) = y_i + d_i y + c_i^p y_i + c_i y$; allora $(y, y_1 + c_1 y, \ldots, y_n + c_n y)$ è una base di M che soddisfa alle condizioni richieste. C.V.D.

Cor. *Sia M un K-modulo canonico tale che $\pi M = M$; esiste un K-modulo canonico libero di cui M è quoziente.*

Notiamo infine che tutto quanto precede resta valido sostituendo ovunque t con π e viceversa.

Teorema A2. *Sia M un K-modulo canonico; e si definisca*

$$M_t = \bigcap_1^\infty{}_n \pi^n M \quad M_\pi = \bigcap_1^\infty{}_n t^n M \quad M_r = \{x \in M \mid \lim t^n x = \lim \pi^n x = 0\}$$

M_t, M_π, M_r sono sotto K-moduli canonici di M, e inoltre $\pi M_t = M_t$, $tM_\pi = M_\pi$, $M = M_t \oplus M_\pi \oplus M_r$.

Dim. L'unica asserzione non ovvia è $M = M_t \oplus M_\pi \oplus M_r$. Sia $x \in M_t \cap M_\pi$; se $x \neq 0$, esiste n tale che $x \notin p^n M_t = t^n M_t$; abbiamo perciò $\pi^i x \notin t^n M_t$ qualunque sia $i \geq 0$; d'altra parte, se $x \in M_\pi$, $\lim \pi^i x = 0$, perchè $\pi M_t = pM_t$; perciò deve essere $M_t \cap M_\pi = 0$.

Supponiamo ora $x \in M_t$, $y \in M_\pi$, $x + y \in M_r$; allora $\lim t^n(x+y) = 0$; ma abbiamo pure $\lim t^n x = 0$, perciò $\lim t^n y = 0$, $y = 0$.

Analogamente $x = 0$, e la somma $M_t + M_\pi + M_r$ è diretta.

Resta da verificare che essa coincide con M, e questo sarà fatto per induzione (transfinita) sul rango di M e sulla lunghezza di M_r ordinati lessicograficamente.

Se $M_t = M_\pi = 0$, abbiamo $\pi^n M \subseteq p^m M$, $t^n M \subseteq p^m M$, se n è maggiore di un opportuno n_m; perciò $M = M_r$. Sia invece, ad esempio, $M_t \neq 0$, e poniamo $N = M/M_t$; N precede M: infatti se $M_t \subseteq M_\tau$, il rango di N è uguale a quello di M, ma la lunghezza di N_τ è minore di quella di M_τ; altrimenti il rango di N è minore di quello di M.

Dimostriamo che non esiste nessun $y \in N$, $y \neq 0$ tale che $\pi y = y$; supponiamo che esista, esso sarà immagine di un $x \in M$ tale che $\pi x - x \in M_t$, e cioè $x = \pi x + z_1$, $z_1 \in M_t = \pi M_t$; sia $z_1 = \pi z_2$, avremo $x = \pi(x + z_2) = \pi x_2$, $\pi x_2 - x_2 = -z_2 \in M_t$; così procedendo per induzione determiniamo $x_i \in M$ tali che $\pi^i x_i = x$; ciò vuol dire però $x \in M_t$, ovvero $y = 0$.

Per il teor. A1 abbiamo perciò $N_t = 0$, e per ipotesi di induzione $N = N_\pi + N_r$. Ciò vuol dire, considerando che $y \in N_\pi + N_r \Longrightarrow \lim \pi^n y = 0$, che per ogni m esiste i_m tale che se $i > i_m$, $\pi^i x \in p^m M + M_t$, ossia che esiste $z'_m \in M_t$ tale che $\pi^{i_m} x - \pi^{i_m} z'_m \in p^m M$, ossia $\pi^i (z'_{m+1} - z'_m) \in p^m M$; sia $z' = \lim z'_m$; $z' \in M_t$. Avremo $\pi^i (x - z') \in p^m M$ per $i \geq i_m$, quindi $\lim \pi^i (x - z') = 0$.

Consideriamo ora $M' = \{y \in M \mid \lim \pi^n y = 0\}$. M' è un sotto K-modulo canonico di M, e contiene $M_\pi + M_r$; ha intersezione 0 con M_t, perciò precede M: infatti, se $M_t \subseteq M_\tau$, la lunghezza di M'_τ è minore di quella di M_τ ed il rango non maggiore, altrimenti il rango di M' è minore di quello di M.

Per induzione avremo perciò $M' = M'_\pi + M'_r = M_\pi + M_r$; ma abbiamo dimostrato che ogni elemento di M è somma di un elemento di M_t e di uno di M', perciò $M = M_t + M' = M_t \oplus M_\pi \oplus M_r$. C.V.D.

TEOREMA A3. *Sia M un K-modulo canonico a torsione; esiste un K-modulo canonico libero di cui M è quoziente.*

DIM. Abbiamo $M = M_t \oplus M_\pi \oplus M_r$; perciò possiamo considerare i tre fattori separatamente.

Se $M = M_t$ (oppure $M = M_\pi$) il teorema è già stato dimostrato; sia allora $M = M_r$. Poichè $M = M_r$, esiste l tale che $p^l M = 0$, perciò esiste h tale che $t^h M = \pi^h M = 0$.

Consideriamo il K-modulo canonico a torsione L così definito: un suo sistema di generatori è dato da x_i, x'_i $0 \leq i \leq h$ con $x_0 = x'_0$, $p^{h-i} x'_i = = p^{h-i} x'_i = 0$ e nessun'altra relazione;

$$\pi x_i = x_{i+1}, \quad t x_i = p x_{i-1}, \quad \pi x'_i = p x'_{i-1}, \quad t x'_i = x'_{i+1}.$$

Si nota immediatamente che L è quoziente del K-modulo canonico libero che ha un sistema di generatori omologo a quello di L, con le relazioni $x_0 = x'_0$, $x_h = x'_h$, e su cui t e π sono definiti come su L.

Sia ora $z \in M$; esiste un omomorfismo canonico φ_z di L in M che porta x in z, così definito: $\varphi_z x_i = \pi^i z$; $\varphi_z x'_i = t^i z$ ed esteso per linearità. Esso è ben definito: se $\sum_{0}^{h}{}_i\, a_i x_i + \sum_{1}^{h-1}{}_i\, a'_i x'_i = 0$, abbiamo che a_i, a'_i è multiplo di p^{h-i}, e allora $a_i \pi^i z = \bar{a}_i p^{h-1} \pi^i z = \bar{a}_i t^{h-i} \pi^h z = 0$; analogamente $a'_i t^i z = 0$. Poichè M è somma di un numero finito di immagini di omomorfismi φ_z, è quoziente di un K-modulo canonico libero. C. V. D.

TEOREMA A.4. *Sia M un K-modulo canonico; esiste un K-modulo canonico libero di cui M è quoziente.*

DIM. Sia $x \in M$, e sia M_x il minimo sotto K-modulo canonico di M che contenga x (ossia il sotto K-modulo di M generato da $\{t^i x, \pi^i x\}_{0 \leq i}$). E' sufficiente dimostrare il teorema per M_x, perciò supponiamo $M = M_x$.

Sia $(\tau_1, \ldots, \tau_r)$ un sistema minimale di generatori di M_τ.

Dimostriamo che esiste un sistema minimale di generatori di M del tipo $\{\tau_l, x, t^i x, \pi^j x \mid 1 \leq l \leq r, 1 \leq i \leq m, 1 \leq j \leq n\}$. È sufficiente dimostrarlo quando $M_\tau = 0$, perchè altrimenti si può passare a M/M_τ.
M, che è generato da $\{x, t^i x, \pi^j x \mid 1 \leq i, 1 \leq j\}$ essendo noetheriano è generato da un suo sottoinsieme finito, ossia da $\{x, t^i x, \pi^j x \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ e bisogna dimostrare che m, n possono essere scelti in modo che esso sia un sistema minimale di generatori, ossia, passando a M/pM, indicando con y l'immagine di x, in modo che $\{y, t^i y, \pi^j y \mid 1 \leq i \leq m, 1 \leq j \leq n\} = Y_{m,n}$ sia una base del k modulo M/pM.

Sia (m, n) minimali tra le coppie tali che $Y_{m,n}$ generi M/pM; $Y_{m,n}$ è allora una base. Supponiamo che sia invece, ad esempio, $t^h y = \sum_{i \neq h} a_i t^i y + \sum b_j \pi^j y + a_0 y$: se abbiamo qualche $a_l \neq 0$ con $l > h$, abbiamo $t^l y = -a_l^{-1}(\sum_{i \neq h\, l} a_i t^i y + \sum b_j \pi^j y + a_0 y - t^h y)$; altrimenti abbiamo, per ogni $s > 0$, $t^{h+s} y = \sum_{1}^{h-1}{}_i\, a_i^{\pi^{-s}} t^{i+s} y + a_0 t^s y$ (ricordando che $t\pi = p = 0$), e (m, n) non sarebbe minimale

Sia allora $x_i = t^i x$, $x_{m+j} = \pi^{n-j+1} x$, $0 \leq i \leq m$, $1 \leq j \leq n$. Abbiamo

$$
\begin{array}{llll}
\pi x_i = x_{i+1} & 0 \leq i < m & t x_0 = x_{n+m} & \\
\pi x_m = \sum a_i x_i + \sigma & & t x_i = p x_{i-1} & 1 \leq i \leq m \\
\pi x_i = p x_{i+1} & m < i < m + n & t x_{m+1} = \sum b_i x_i + \sigma' & \\
\pi x_{m+n} = p x_1 & & t x_i = x_{i-1} & m + 1 < i
\end{array}
$$

con $\sigma, \sigma' \in M_\tau$, $a_i, b_i \in K$.

Poichè deve essere $\pi t x_{m+1} = p x_{m+1}$, $t \pi x_m = x_m$, si deve avere

$$\pi \sigma' = b_m^\pi \sigma; \; t\sigma = a_{m+1}^{\pi^{-1}} \sigma'; \; b_m^\pi = \frac{p}{a_{m+1}};$$

$$b_i^\pi = - b_i^\pi = - b_m^\pi a_{i+1} = \frac{-p a_{i+1}}{a_{m+1}} \; 0 \leq i < m;$$

$$b_{n+m}^\pi = \frac{-a_0}{a_{m+1}}; \; b_i^\pi = -\frac{a_{i+1}}{a_{m+1}} \; m < i < m + n.$$

Sia ora M_τ quoziente del K-modulo canonico libero N secondo l'omomorfismo λ; consideriamo il K-modulo libero L con base $\{y_i \mid 0 \leq i \leq m+n\}$. Notiamo ora che o a_{m+1} o b_m sono unità; supponiamo ad esempio che a_{m+1} sia unità, e sia $s \in N$ tale che $\lambda(s) = \sigma$; posto $s' = (a_{m+1}^{\pi-1})^{-1} ts$, abbiamo $\lambda(s') = \sigma'$. Consideriamo $M' = N \oplus L$; esso diventa canonico, definendo t e π su L come segue:

$$
\begin{array}{llll}
\pi y_i = y_{i+1} & 0 \leq i < m & t y_1 = y_{n+m} & \\
\pi y_m = \Sigma\, a_i\, y_i + s & & t y_i = p y_{i-1} & 1 \leq i \leq m \\
\pi y_i = p y_{i+1} & m < i < m+n & t y_{m+1} = \Sigma\, b_i\, y_i + s' & \\
\pi y_{m+n} = p y_1 & & t y_i = y_{i-1} & m+1 < i.
\end{array}
$$

Date le relazioni tra a_i, b_i, s, s', si verifica immediatamente che $t\pi = \pi t = p$; è anche immediato che M è quoziente del K-modulo canonico libero M'. C. V. D.

Pisa, Università

BIBLIOGRAFIA

[1] I. BARSOTTI: *Moduli canonici e gruppi analitici commutativi* - Ann. Sc. Norm. Sup. 13, (1959) p. 302-327.

[2] I. BARSOTTI: *Metodi analitici per varietà abeliane in caratteristica positiva*, cap. 3-4 - Ann. Sc. Norm. Sup. 19, (1965) p. 277-330.

[3] I. BARSOTTI: *Varietà abeliane su corpi p-adici* - Symposia Mathematica 1, (1968) p. 109-173.

[4] J. DIEUDONNÈ: *Lie groups and lie hyperalgebras over a field of characteristic $p > 0$* (IV) - Amer. J. Math. 77, (1955) p. 429-452.

[5] YU. MANIN: *Teoria dei gruppi formali commutativi su corpi di caratteristica finita.* (russo) Uspeki Mat. Nauk 18, (1963) 6, p. 3-90 (tradotto in « Russian Math. Surveys »).

[6] M. POLETTI: *Iperalgebre su schiere valutanti* (in corso di stampa su questi Annali).