ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

IACOPO BARSOTTI

Gli endomorfismi delle varietà abeliane su corpi di caratteristica positiva

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3^e série, tome 10, n^o 1-2 (1956), p. 1-24

<http://www.numdam.org/item?id=ASNSP_1956_3_10_1-2_1_0>

GLI ENDOMORFISMI DELLE VARIETÀ ABELIANE SU CORPI DI CARATTERISTICA POSITIVA

di IACOPO BARSOTTI (Los Angeles)

INTRODUZIONE

Presento qui alcuni risultati che discendono direttamente da quelli di [6] (v. bibliografia alla fine di questo lavoro), e dai metodi usati in [6].

L'idea centrale del presente lavoro è la seguente: se $\{x_1, \ldots, x_n\}$ è un insieme regolare di parametri dell'anello quoziente dell'identità di una varietà abeliana A di dimensione n sopra un corpo algebricamente chiuso k, la legge di composizione su A definisce, nell'anello $k\{x\}$ delle serie formali di potenze, una legge di gruppo, che a sua volta definisce un gruppo analitico G (gruppo formale di Lie); se k ha caratteristica $p \neq 0$, tali gruppi G sono stati studiati (indipendentemente dalle varietà abeliane) in [10], [11], [12], ed in altri lavori dello stesso autore. Se p^f è l'ordine del kernel di $p\,\delta_A$, G è prodotto diretto di due gruppi analitici G_l, G_r, ove G_l è prodotto diretto di f gruppi di dimensione 1 del tipo I_0 (o W^*) di [12], mentre G_r è un gruppo radicale, ossia tale che ogni sua iperderivazione invariante è pseudonulla. Un omomorfismo, ed in particolare un endomorfismo, di A si spezza in un omomorfismo di G_l ed uno di G_r; poichè tali omomorfismi possono venire studiati per mezzo di matrici ad elementi p-adici, si ottiene così la (fino ad ora mancante) rappresentazione p-adica dell'anello degli endomorfismi di A; è noto che le rappresentazioni q-adiche, per i primi $q \neq p$, sono state studiate in [14].

In questo lavoro presento soltanto quegli sviluppi che si riferiscono a G_l, dato che la parte riferentesi a G_r è complicata dal fatto che, a priori almeno, G_r può essere isogeno ad un gruppo analitico avente fattori diretti semplici di dimensione > 1, nel qual caso tale gruppo analitico ha probabilmente anche fattori diretti del tipo I_m di [12], con $m > 1$ (nel caso contrario, ha solo fattori diretti di tipo I_1); dato che lo studio di G_r è notevolmente semplificato quando fattori diretti di tale tipo sono assenti (in

tal caso gli omomorfismi di G_r sono completamente descritti da matrici ad elementi p-adici con $4(n-f)$ righe), vorrei, prima di considerarlo esaurito, o assicurarmi che tali fattori possono effettivamente comparire nei gruppi analitici che sorgono nello studio delle varietà abeliane, ovvero dimostrare che non vi compaiono mai; la seconda alternativa si avvera, ad esempio, quando $n-f \leq 2$.

La sezione 1 contiene una definizione dei gruppi analitici che considero più adatta ai nostri scopi di quella data in [10], in quanto esibisce specificamente tali gruppi come gruppi di punti di uno spazio affine; il resto della sezione 1 è dedicato a ridimostrare formule generali, e proprietà di G_l, già dimostrate in [10] e [12]; in tal modo questo articolo può essere letto indipendentemente dai [10], [11], e [12]; il lettore che già conosca tali lavori può limitarsi a leggere le definizioni.

La sezione 2 contiene il teorema sulla rappresentazione p-adica degli omomorfismi di A; la sezione 3 è dedicata ad una applicazione di quanto precede alla costruzione di una matrice p-adica emisimmetrica connessa ai cicli di A (cfr. § XI di [14]); tale matrice, che corrisponde, grosso modo, ai periodi secondari di funzioni intermediarie su A [8], è evidentemente collegata all'omomorfismo di A sulla propria varietà di Picard [4], ma non contiene ancora tutte le informazioni su tale omomorfismo che sarebbe desiderabile avere.

La sezione 4 contiene un risultato generale (4.2) sulla struttura dell'anello degli endomorfismi di A, valido per il caso in cui $n=f$ (ovvero in cui k abbia caratteristica zero); le A per cui ciò non accade sono quelle su cui si danno differenziali esatti non nulli di prima specie (cfr. 4.4 di [6]), e sono quindi di tipo molto speciale.

1. I gruppi analitici.

Sia k un corpo, e siano $x_1, x_2, \ldots$ indeterminate, in numero finito o no; indicheremo con $k\{x_1, x_2, \ldots\}$ l'anello delle serie formali di potenze nelle x_i, con esponenti interi non negativi e coefficienti in k, intendendosi che ogni serie contenga solo un numero finito di indeterminate; $k\{x_1, x_2, \ldots\}$ denoterà il corpo quoziente di $k\{x_1, x_2, \ldots\}$. È noto che $k\{x\}$ è dotato, in modo naturale, di una metrica. In generale, se $x_1, x_2, \ldots$ sono elementi di un campo d'integrità A contenente k e dotato di una metrica, e se ogni serie di potenze nelle x_i, a coefficienti in k, converge ad un elemento di A, indicheremo con $k\{x_1, x_2, \ldots\}$ l'anello dei limiti di tali serie, e con $k\{x_1, x_2, \ldots\}$ il corpo quoziente di $k\{x_1, x_2, \ldots\}$. In questa sezione fisseremo, una volta per tutte, k ed un insieme $v_1, v_2, \ldots$ numerabile di

indeterminate, e denoteremo con Ω l'insieme degli elementi di $k\{v\}$ privi di termine di grado 0 nelle v; l'anello Ω ha la proprietà che ogni serie di potenze di un numero finito di elementi di Ω, a coefficienti in k, priva di termine di grado 0, converge ad un elemento di Ω. Se $\xi_1, \ldots, \xi_n \in \Omega$, diremo che le ξ sono *analiticamente indipendenti* (*su k*) se non esiste nessuna serie di potenze nelle ξ, con coefficienti in k non tutti nulli, che converge a 0. Il corpo quoziente di Ω, che coincide con $k\{v\}$, sarà indicato con Ω^*.

Siano $x_1, \ldots, x_n$ indeterminate, e si consideri lo spazio proiettivo S su Ω^*, il cui punto generale non omogeneo è $\{x_1, \ldots, x_n\}$; sia G l'insieme dei punti di S, a distanza finita per le $\{x\}$, in cui le coordinate x_i hanno valori in Ω. Siano $y_1, \ldots, y_n$ e $z_1, \ldots, z_n$ altre indeterminate, e sia $\{g_1(x, y), \ldots, g_n(x, y)\}$ un insieme di serie di potenze nelle x ed y, a coefficienti in k, e tali che $g_i(x, 0) = x_i$, $g_i(0, y) = y_i$, $g_i(g(x, y), z) = g_i(x, g(y, z))$; allora, se P, Q sono elementi di G, di coordinate rispettivamente $\xi_1, \ldots, \xi_n$ ed $\eta_1, \ldots, \eta_n$, il punto R di coordinate $g_i(\xi, \eta)$ appartiene a G; se si pone $R = P\,Q$, si è definita una legge di composizione su G, ed è provato nella sezione 2 di [10] che in tal modo G diviene un gruppo, la cui identità E_G ha coordinate $0, \ldots, 0$. Ogni gruppo G così definito sarà da noi chiamato un *gruppo analitico di dimensione n su k* (*ed* Ω); l'insieme $\{x_1, \ldots, x_n\}$ dicesi il *punto generale di G* (1). Se G ha il significato precedente, e $P \in G$, e se y è elemento di $k\{x\}$, privo di termini di grado 0, la sostituzione di x_i col valore che x_i ha in P trasforma y in un elemento di Ω, che sarà indicato con $y(P)$. Si noti che un gruppo analitico è un gruppo topologico nel senso solito della parola.

Se G' è un altro gruppo analitico su k, con punto generale $\{y_1, \ldots, y_m\}$, un *omomorfismo di G su G'* è un'applicazione π di G su G', che è un omomorfismo nel senso della teoria dei gruppi, e tale inoltre che esistano m elementi $z_1, \ldots, z_m$ di $k\{x\}$, privi di termine di grado 0, ed aventi la proprietà espressa dalla relazione $z_i(P) = y_i(\pi P)$ per ogni $P \in G$. L'omomorfismo π è un *isomorfismo fra G e G'*, se esiste un omomorfismo π' di G' su G, tale che $\pi'\,\pi\,P = P$ per ogni $P \in G$. Se G' è immerso nello spazio proiettivo S', il *prodotto diretto* $G \times G'$ è l'insieme dei punti $P \times P'$ di $S \times S'$, quando P, P' variano in G, G' rispettivamente; e la legge di composizione in $G \times G'$ è ottenuta nel modo solitamente usato nella definizione dei prodotti diretti di gruppi.

---

(1) Per una teoria generale dei gruppi analitici, l'anello Ω dovrebbe essere più generale di quello scelto qui; ed inoltre, si dovrebbero ammettere come punti generali anche degli insiemi $\{x_1, \ldots, x_m\}$ ove le x_i non sono tutte analiticamente indipendenti. Per gli scopi del presente lavoro, le definizioni date sono però sufficienti.

Se π è un omomorfismo di G su tutto G', il gruppo analitico con punto generale $\{z\}$ è una copia di G', e sarà spesso indicato con lo stesso simbolo G'; pertanto, si può asserire che un omomorfismo π su tutto G' prescrive un'immersione di $k\{y\}$ in $k\{x\}$. Nel seguito, l'anello $k\{x\}$ sarà indicato con $k\{G\}$, ed il corpo $k(x)$ con $k(G)$. Si consideri ora un isomorfismo π fra G e G'; mediante l'identificazione precedente, si avrà in tal caso $k\{G\}=k\{G'\}$, e quindi il gruppo G può essere considerato come gruppo analitico in due modi distinti, che differiscono soltanto per il loro punto generale; la trasformazione dell'uno nell'altro modo di rappresentazione di G sarà considerata come un *cambiamento di coordinate*; è chiaro che ogni insieme di n elementi $t_1, \ldots, t_n$ di $k\{G\}$, privi di termini di grado 0, e tali che $k\{t\}=k\{G\}$, può essere scelto come punto generale di un gruppo analitico isomorfo a G. Il gruppo G è *commutativo* se $P'Q=QP$ per ogni coppia $\{P, Q\}$ di punti di G.

Un *gruppo logaritmico* di dimensione n è un gruppo analitico isomorfo al prodotto diretto di n gruppi analitici di dimensione 1, in ciascuno dei quali si abbia $g(x, y)=x+y+xy$, ovvero $1+g(x, y)=(1+x)(1+y)$; ciascuno di questi gruppi, che è perciò un gruppo logaritmico di dimensione 1, si dirà *gruppo logaritmico canonico*; e se G è un gruppo logaritmico, ogni elemento x di $k\{G\}$, tale che $x(PQ)=x(P)+x(Q)+x(P)x(Q)$ per $P, Q \in G$, si dirà un *elemento canonico di* G, ovvero *di* $k\{G\}$; un insieme di elementi canonici che sia anche un punto generale di (un gruppo isomorfo a) G dicesi un *insieme di coordinate canoniche*; il polinomio $g(X, Y)=X+Y+XY$, ove X, Y sono indeterminate, si dirà la *legge canonica logaritmica*.

D'ora in poi, ed in tutta questa sezione, si supporrà che k *sia algebricamente chiuso, ed abbia caratteristica* $p>0$.

Sia G un gruppo analitico di dimensione n su k, e sia $\{x_1, \ldots, x_n\}$ un punto generale di G (o di un gruppo analitico isomorfo a G); la definizione di *iperderivazione*, e di *iperderivazione invariante sinistra*, o *destra*, *su* G, o *in* $k\{G\}$, è identica a quella data nella sezione 1 di [6], od anche nelle sezioni 4, 5, 6 di [10]. In particolare, vi è un insieme $\{D_h\}$, con $h=\{h_1, \ldots, h_n\}$, h_i intero ≥ 0, $\Sigma_i h_i > 0$, di iperderivazioni invarianti sinistre su G, definite, per ogni $f \in k\{G\}$, dalle relazioni

$$f(PQ)=f(P)+\Sigma_h (D_h f)(P)\, x^h(Q) \tag{1.1}$$

per ogni $P, Q \in G$; qui, x^h sta per $x_1^{h_1} \ldots x_n^{h_n}$. Le D_h così definite si diranno *legate ad* $\{x\}$, e saranno talvolta indicate con $D_{x,h}$; indicheremo con ε_i l'insieme $\{h\}$ tale che $h_j=\delta_{ij}$ (simbolo di Kronecker). Se G è commutativo,

i simboli $\mathbf{D}(G)$, $\mathbf{D}_r(G)$, $\mathbf{S}_s(G)$ avranno lo stesso significato che hanno nel caso in cui G è una varietà gruppale commutativa (sezione 2 di [6]).

Per ogni $P \in G$, esiste un autoisomorfismo σ_P di $k\{G\}$ su k tale che per ogni $f \in k\{G\}$, e per ogni $Q \in G$, si abbia $(\sigma_P f)(P\,Q) = f(Q)$; la formula (1.1) mostra allora che si può scrivere, simbolicamente,

$$\sigma_P^{-1} = \pi_P + \Sigma_h\, x^h\, \pi_P\, D_h\,, \tag{1.2}$$

ove $\pi_P f = f(P)$ per ogni $f \in k\{G\}$. Se G è commutativo, si può anche scrivere:

$$\sigma_P^{-1} = 1 + \Sigma_h\, x^h\, (P)\, D_h\,. \tag{1.3}$$

Da (1.1) si deduce facilmente la

(1.4) *Formula di Leibnitz*: $D_h(x\,y) = x\,D_h\,y + y\,D_h\,x + \underset{r+s=h}{\Sigma}(D_r\,x)\,(D_s\,y)$, per $x, y \in k\{G\}$.

Da (1.3) segue anche, se G è commutativo, $\sigma_P^{-p} = 1 + \Sigma_h\, x^{ph}\,(P)\, D_h^p$, da cui il 2.5 di [6] discenderebbe agevolmente; comunque, da $\sigma_P^{-p}(x\,y) = (\sigma_P^{-p}\,x)\,\sigma_P^{-p}\,y$ e dalla formula precedente si deduce che, se G è commutativo,

$$D_h^p(x\,y) = x\,D_h^p\,y + y\,D_h^p\,x + \underset{r+s=h}{\Sigma}(D_r^p\,x)\,(D_s^p\,y). \tag{1.5}$$

Sia A una varietà gruppale nonsingolare (ossia senza singolarità fuori del suo luogo di degenerazione) di dimensione n su k (e qui k potrebbe anche avere caratteristica 0), e sia $\{x_1, \ldots, x_n\}$ un insieme regolare di parametri di $Q(E_A/A)$; siano A_1, A_2, A_3 delle copie di A, e siano $\{y\}$, $\{z\}$, $\{t\}$ le copie di $\{x\}$ in $k(A_1)$, $k(A_2)$, $k(A_3)$ rispettivamente; si supponga $k(A_2) \subseteq k(A \times A_1)$ come prescritto dalla legge di composizione su A; poichè il completamento (topologico) di $Q(E_{A_2}/A_2)$ è contenuto nel completamento di $Q(E_A \times E_{A_1}/A \times A_1)$, esistono delle serie di potenze $g_1, \ldots, g_n$ nelle x, y, con coefficienti in k, tali che $z_i = g_i(x, y)$; e le g_i necessariamente soddisfano le $g_i(x, 0) = x_i$, $g_i(0, y) = y_i$, $g_i(g(x, y), t) = g_i(x, g(y, t))$. Pertanto A definisce un gruppo analitico G di dimensione n su k, con punto generale $\{x\}$, ed è chiaro che G è unico, e non dipende dalla scelta delle x_i, a meno di isomorfismi. Il gruppo analitico G si dirà il *completamento di* A. È ora facile vedere che G può essere definito anche scegliendo le x_i nel completamento di $Q(E_A/A)$; G è commutativo se, e solo se tale è A; ogni omomorfismo di A può essere esteso ad un omomorfismo di G in

modo unico, ed ogni iperderivazione invariante sinistra su A ad una, unicamente determinata, su G. Ma si ha di più: scelte le x_i in $Q(E_A/A)$, ogni iperderivazione invariante sinistra su G è combinazione lineare, a coefficienti in k, di un numero finito di $D_{x,h}$, e pertanto induce una iperderivazione invariante sinistra su A; si può così concludere che *gli anelli delle iperderivazioni invarianti sinistre su A e G sono isomorfi, e possono quindi essere identificati.* Si noti che G è un sottogruppo della estensione di A su Ω^*. Cogliamo quest'occasione per dimostrare esplicitamente un facile risultato, di cui si è fatto uso nella dimostrazione del 4.3 di [6]:

(1.6) LEMMA. *Sia G un gruppo analitico commutativo di dimensione n su k, e, per $j=0,1,\dots,s$, sia $\{D_{1j},\dots,D_{nj}\}$ un insieme di iperderivazioni invarianti su G, che inducono in $k\{G^{p^j}]$ una k-base di $\mathbf{D}_0(G^{p^j})$. Allora l'insieme dei monomi di grado positivo nelle D_{ij} $(i=1,\dots,n;\ j=0,\dots,s)$, con coefficiente 1, e grado $<p$ in ogni D_{ij}, è una k-base indipendente di $\mathbf{S}_{s+1}(G)$.*

DIM. Per $j=0,\dots,s$, siano $x_{1j},\dots,x_{nj}$ elementi di $k\{G^{p^j}]$, senza termine di grado 0, tali che $(D_{ij}\,x_{hj})(E_G)=\delta_{ih}$, cosicchè le x_{ij}^r, per j fisso, $i=1,\dots,n$, ed $r=0,\dots,p-1$, formano una $k\{G^{p^{j+1}}]$-base indipendente di $k\{G^{p^j}]$. Si esprima ogni intero positivo a nella rappresentazione p-adica, vale a dire $a=a_0+a_1p+a_2p^2+\dots+a_rp^r$, ove $0\leq a_i<p$, e pongasi $x_i^a=x_{i0}^{a_0}x_{i1}^{a_1}\dots x_{ir}^{a_r}$; se $b=\{b_1,\dots,b_n\}$, pongasi anche $x^b=x_1^{b_1}\dots x_n^{b_n}$. Infine, si scriva $\Delta_{i,a}=D_{i0}^{a_0}D_{i1}^{a_1}\dots D_{ir}^{a_r}$, $\Delta_b=\Delta_{1,b_1}\dots\Delta_{n,b_n}$. Si vuole dimostrare che l'insieme delle Δ_b, quando $b=\{b_1,\dots,b_n\}$ è tale che $0\leq b_i<p^{s+1}$, $\Sigma_i b_i>0$, è una k-base indipendente di $\mathbf{S}_{s+1}(G)$. L'asserzione è vera per $s=0$; supposta la vera per $s<m>0$, la dimostrerò vera per $s=m$. A tale scopo, è necessario, e sufficiente, dimostrare che non si annulla il determinante H_{m+1} delle $(\Delta_b\,x^h)(E_G)$, ove $b=\{b_1,\dots,b_n\}$ e $h=\{h_1,\dots,h_n\}$ sono tali che $0\leq b_i<p^{m+1}$, $0\leq h_i<p^{m+1}$, $\Sigma_i b_i>0$, $\Sigma_i h_i>0$. Ora, ogni b si può scrivere nella forma $b=b_0+p^m b_1$, ove $b_0=\{b_{01},\dots,b_{0n}\}$ con $b_{0i}<p^m$, e $b_1=\{b_{11},\dots,b_{1n}\}$ con $0\leq b_{1i}<p$; ed analogamente, si può scrivere $h=h_0+p^m h_1$. Ciò posto, si ha

$$(\Delta_b\,x^h)(E_G)=(\Delta_{b_0}\Delta_{p^m b_1}(x^{h_0}x^{p^m h_1}))(E_G)=[\Delta_{p^m b_1}(x^{p^m h_1}\Delta_{b_0}x^{h_0})](E_G)=$$

$$=[(\Delta_{p^m b_1}x^{p^m h_1})(E_G)]\,[(\Delta_{b_0}x^{h_0})(E_G)]+[x^{p^m h_1}(E_G)]\,[(\Delta_b\,x^{h_0})(E_G)].$$

Ora,

$$(\Delta_{p^m b_1}x^{p^m h_1})(E_G)=(h_1!)\,\delta_{b_1 h_1},\ \text{ove } h_1!=(h_{11}!)\dots(h_{1n}!)$$

se $h_1 = \{h_{11}, \ldots, h_{1n}\}$; se $K \neq 0$ è il determinante di questi elementi, e se $K \times H_m$ indica «prodotto diretto» di determinanti, si può pertanto scrivere H_{m+1} nella forma $\left|\begin{array}{c|c} K \times H_m & S \\ \hline 0 & H_m \end{array}\right|$, ove S è la matrice delle $(\Delta_b\, x^{h_0})\,(E_G)$ quando b è tale che $b_1 \neq 0$; e questo determinante è certo non nullo, perchè $K \times H_m \neq 0 \neq H_m$, c. v. d.

Il (1.6) permette di fissare una base di $\mathbf{D}\,(G)$, distinta dalla $\{D_{x,h}\}$, non appena il punto generale $\{x\}$ di G sia dato; tale base è l'insieme delle $D^*_{x,h}$, ove $D^*_{x,h}$ è definito a partire dalle $D_{x,p^i\varepsilon_j} = D^*_{x,p^i\varepsilon_j}$ nello stesso modo in cui il Δ_h della dimostrazione precedente è definito a partire dalle D_{ij} di (1.6).

Siano x, y elementi canonici di un gruppo logaritmico G, e sia g la legge canonica; si definisca $x.y = y.x = g\,(x, y)$; allora $z = x.y$ è elemento canonico di G, poichè si ha, per $P, Q \in G$: $z\,(P\,Q) = (g\,(x, y))\,(P\,Q) = g\,(x(P\,Q), y\,(P\,Q)) = g\,(g\,(x\,(P), \; x\,(Q)), \; g\,(y\,(P), \; y\,(Q))) = g\,(g\,(x\,(P), \; y\,(P)), \; g\,(x\,(Q), \; y\,(Q))) = g\,(z(P), z\,(Q))$, per l'associatività e la commutatività. In particolare, si porrà $x^{(r)} = x.x \ldots x$ (r volte), se r è intero positivo, e $x^{(0)} = 0$. È allora facile vedere che $(x.y).z = x.(y.z)$ se z è un altro elemento canonico di G. Sia $r = r_0 + r_1\,p + r_2\,p^2 + \ldots$ un intero p-adico, con $0 \leq r_i < p$, e pongasi $s_i = \sum_0^i r_j\,p^j$, cosicchè $r = \lim_{i \to \infty} s_i$; si consideri la successione $x_0, x_1, x_2, \ldots$, ove $x_i = x^{(s_i)}$, x essendo un elemento canonico di G. Poichè $x^{(p)} = x^p$, il $\lim_{i \to \infty} x_i$ esiste, e sarà indicato con $x^{(r)}$. Si ha facilmente, per $P, Q \in G$: $x^{(r)}\,(P\,Q) = \lim_{i \to \infty} x_i\,(P\,Q) = \lim_{i \to \infty} g\,(x_i(P), x_i(Q)) = g\,(x^{(r)}\,(P), x^{(r)}(Q))$, onde $x^{(r)}$ è elemento canonico di G; inoltre $x^{(r)}.\,x^{(s)} = x^{(r+s)}$, $(x^{(r)})^{(s)} = x^{(rs)}$, $x^{(0)} = 0$, $x^{(1)} = x$, $(x\,.\,y)^{(r)} = x^{(r)}\,.\,y^{(r)}$, e ciò prova che l'insieme V degli elementi canonici di G è un I_p-modulo, se I_p è l'anello degli interi p-adici. Dico che V è un I_p-modulo libero, di ordine eguale alla dimensione n di G, avente per I_p-base indipendente un insieme $\{x_1, \ldots, x_n\}$ di coordinate canoniche su G.

Si indichi infatti con G_i il gruppo logaritmico di dimensione 1 il cui punto generale è x_i, cosicchè $G = G_1 \times \ldots \times G_n$, e sia V_i l'I_p-modulo degli elementi canonici di G_i. Se $z \in V$, per $i = 1, \ldots, n$ esiste un elemento $z_i \in k\,\{G_i\}$ tale che per ogni $P_i \in G_i$ si abbia $z_i\,(P_i) = z\,(E_{G_1} \times \ldots \times E_{G_{i-1}} \times P_i \times E_{G_{i+1}} \times \ldots \times E_{G_n})$; evidentemente $z_i\,(P_i\;Q_i) = g\,(z_i\,(P_i), \; z_i\,(Q_i))$, onde $z_i \in V_i$. Poichè $z \in V$, si ha $z\,(P_1 \times \ldots \times P_n) = g\,(z_1\,(P_1), \; z\,(E_{G_1} \times P_2 \times \ldots \times P_n)) = \ldots = g\,(z_1\,(P_1), \quad g\,(z_2\,(P_2), \ldots, g\,(z_{n-1}\,(P_{n-1}), \; z_n\,(P_n)) \ldots)) = (z_1 \cdot z_2 \ldots z_n)\,(P_1 \times \ldots \times P_n)$, onde $z = z_1 \cdot z_2 \ldots z_n$. D'altra parte, se gli $z_i \in V_i$ sono assegnati arbitrariamente, è certo $z = z_1 \cdot z_2 \ldots z_n \in V$, e $z \neq 0$ se non tutti gli z_i sono nulli. Pertanto, V è la somma complementare dei V_i. Se allora si indica con V uno qual-

siasi dei V_i, e con x il corrispondente x_i, resta da dimostrare che V è un I_p-modulo libero di base x.

Ora, se $0 \neq z \in V$, sia s il minimo intero tale che $D_{x,s} z \neq 0$; se $p^r < s < p^{r+1}$, si ha che $D^*_{x,m}$ induce 0 in $k\{z\}$ per $m \leq p^r$, onde $D_{x,s} z = 0$, assurdo. Pertanto deve essere $s = p^r$ per qualche $r \geq 0$. La formula di Leibnitz (1.4) mostra allora che D_{x,p^r} induce una derivazione invariante non nulla in $k\{z\}$, che sarà pertanto del tipo $a D_{z,1}$, con $0 \neq a \in k$; poichè $D^p_{x,p^r} = D_{x,p^r}$ e $D^p_{z,1} = D_{z,1}$, si ha $a^p = a$, $a \in C_p$ (= sottocorpo fondamentale di k); si indichi con a anche l'intero razionale > 0 e $< p$, la cui classe residua *mod* p è a, e pongasi $x_1 = x^{(ap^r)}$, e quindi $1 + x_1 = (1 + x)^{ap^r}$; pongasi anche $z_1 = x_1^{(-1)} \cdot z$. Poichè $x_1 \in k\{x^{p^r}]$, si ha $D_{x,s} x_1 = 0$ per $s < p^r$, ed evidentemente $D_{x,p^r} x_1 = a(1 + x_1)$, onde la relazione $x_1 \cdot z_1 = z$, ovvero la $(1 + x_1)(1 + z_1) = 1 + z$, dà $(1 + z_1) D_{x,p^r} x_1 + (1 + x_1) D_{x,p^r} z_1 = a(1 + z)$, ed anche $a(1 + z_1)(1 + x_1) + (1 + x_1) D_{x,p^r} z_1 = a(1 + z)$, o infine $D_{x,p^r} z_1 = 0$. Ora lo stesso ragionamento si può applicare a z_1 anzichè z, ottenendo un x_2, ed uno $z_2 = x_2^{(-1)} \cdot z_1$, tali che $D_{x,p^s} z_2 = 0$, con $s > r$. Così proseguendo si ottiene una successione $x_1, x_2, \ldots$, generalmente infinita, tale che $(x_1 . x_2 \ldots x_n)^{(-1)} . z \in k\{x^{p^m}]$, ove $m \to \infty$ quando $n \to \infty$. Ma allora, $t = \lim_{n \to \infty} x_1 \cdot x_2 \ldots x_n$ esiste, ed è tale che $t^{(-1)} \cdot z \in k\{x^{p^m}]$ per ogni m, ossia $t^{(-1)} \cdot z \in k$. Poichè $t^{(-1)} \cdot z \in V$, esso deve essere $= 0$, ossia $t = z$; siccome $t = x^{(h)}$ per un opportuno $h \in I_p$, l'asserto è dimostrato.

Si considerino ora due gruppi logaritmici G, G', di dimensioni n ed m rispettivamente; sia $\{x_1, \ldots, x_n\}$ un punto generale di G, e sia $\{y_1, \ldots, y_m\}$ uno di G'; suppongasi che ciascun x_i e ciascun y_i sia elemento canonico; sia π' un omomorfismo di G su G'. Allora esistono degli elementi $z_1, \ldots, z_m \in k\{G]$, tali che per ogni $P \in G$ si abbia $z_i(P) = y_i(\pi' P)$; pertanto, $z_i(P\,Q) = y_i((\pi' P)(\pi' Q)) = g(y_i(\pi' P), y_i(\pi' Q)) = g(z_i(P), z_i(Q))$, se g è la legge canonica logaritmica. Ciò mostra che ogni z_i che non è nullo può essere considerato come punto generale di un gruppo logaritmico A_i di dimensione 1, e che inoltre z_i è coordinata canonica di A_i.

Detti V, V' gli I_p-moduli degli elementi canonici di G, G' rispettivamente, è chiaro che per ogni $y \in V'$ esiste uno $z \in V$ tale che $y(\pi' P) = z(P)$ per ogni $P \in G$, e che, in particolare, $z = z_i$ se $y = y_i$; l'applicazione $y \to z$ è evidentemente un omomorfismo π dell'I_p-modulo V' sull'I_p-modulo V, ed è determinata non appena le z_i siano state assegnate. Ora, V e V' hanno ordini rispettivamente n ed m; pertanto, π è completamente determinato da una matrice, con elementi in I_p, ad m righe ed n colonne; un cambiamento di base per V o V' sostituisce tale matrice con una equivalente. La matrice in questione, quando una scelta di base sia stata effettuata,

si indicherà con $M_{pl}(\pi')$. È altresì chiaro che se G'' è un terzo gruppo logaritmico, dopo una scelta di base si ha $M_{pl}(\varrho'\,\pi') = M_{pl}(\varrho')\,M_{pl}(\pi')$, se ϱ' è un omomorfismo di G' su G''; ed è pure palese che $M_{pl}(\pi') = 0$ se e solo se $\pi' = 0$. Dico che è anche vero che, se π' e ϱ' sono omomorfismi di G su G', si ha $M_{pl}(\pi' + \varrho') = M_{pl}(\pi') + M_{pl}(\varrho')$; si intende che $\pi' + \varrho'$ è definito da $(\pi' + \varrho')\,(P) = (\pi'\,P)\,(\varrho'\,P)$ per ogni $P \in G$. Ed infatti, si indichino con π, ϱ, λ gli omomorfismi di V' su V legati a π', ϱ' e $\pi' + \varrho'$ rispettivamente, o se si vuole, alle rispettive matrici. L'omomorfismo π è definito, nella notazione esponenziale, dalla relazione $y^{(\pi)}\,(P) = y\,(\pi'\,P)$ per ogni $P \in G$; ora, si ha: $y^{(\lambda)}(P) = y\,((\pi' + \varrho')\,P) = y\,((\pi'\,P)\,(\varrho'\,P)) = g\,(y\,(\pi'\,P),\ y\,(\varrho'\,P)) = g\,(y^{(\pi)}\,(P),\ y^{(\varrho)}\,(P)) = [y^{(\pi)}\,.\,y^{(\varrho)}]\,(P)$, onde $y^{(\lambda)} = y^{(\pi)}.y^{(\varrho)}$, e pertanto $\lambda = \pi + \varrho$, come richiesto. Resta così provato che, se $G' = G$, le corrispondenze $\pi' \to M_{pl}(\pi')$ e $\pi' \to \pi$ sono isomorfismi di anelli; questo fatto ci permette di affermare (come è già stato dimostrato in [12]) che l'anello degli *endomorfismi* (= omomorfismi su se stesso) *di* G è isomorfo all'anello di tutte le matrici di ordine n ad elementi in I_p; si noti che tale anello è una schiera massima, su I_p, nell'algebra regolare (ossia di tutte le matrici) di grado n sul corpo R_p dei numeri p-adici (cfr. [1] o [9]).

Se π' è un omomorfismo di G su G', diremo che π' ha *grado* 0 se $\pi'\,G$ ha dimensione $< n = dim\ G$, ossia se $k\,\{\pi'\,G\}$ è un anello locale completo di dimensione $< n$. Se π' non ha grado 0, ciò significa che $k\,\{\pi'\,G\}$ ha dimensione n; ed allora, se $\{x_1, \ldots, x_n\}$, $\{y_1, \ldots y_m\}$ sono i punti generali di G, G' rispettivamente, $k\,\{x\}$ e $k\,\{y^{(\pi)}\}$ sono anelli locali della stessa dimensione; in tal caso, le $y_i^{(\pi)}$ formano la base di un ideale di $k\,\{x\}$ che è un primario appartenente al primo massimo $\mathfrak{p}$ di $k\,\{x\}$; la lunghezza di tale primario, che coincide col grado $[k\,\{x\} : k\,\{y^{(\pi)}\}]$ (cfr. Teoremi 8 e 23 di [7]), è un intero positivo, che dicesi il *grado di* π'.

(1.7) Teorema. *Siano G, G' gruppi logaritmici, di dimensioni n, m rispettivamente, su k, e sia π' un omomorfismo di G su G'; allora la caratteristica di $M_{pl}(\pi')$ eguaglia la dimensione di $\pi'\,G$. Se tale dimensione è n, sia ν la valutazione p-adica di R_p; allora il grado di π' è p^v, ove v è il minimo fra i $\nu(\Delta)$ quando Δ varia fra i minori di ordine n di $M_{pl}(\pi')$.*

Dim. Nelle notazioni precedenti, la caratteristica di $M_{pl}(\pi')$ eguaglia il numero di elementi $y_i^{(\pi)}$ che sono indipendenti su I_p; e poichè $k\,\{y^{(\pi)}\}$ è analiticamente isomorfo a $k\,\{\pi'\,G\}$, la caratteristica di $M_{pl}(\pi')$ è anche la dimensione di $\pi'\,G$.

Se $\pi'\,G$ ha dimensione n, il precedente risultato mostra che qualche Δ è non nullo, onde il minimo v dei $\nu(\Delta)$ è un intero non negativo. Poichè in I_p ogni ideale è principale, mediante una trasformazione delle basi $\{x_i\}$, $\{y_i\}$ è possibile fare in modo che $M_{pl}(\pi')$ divenga una matrice (a_{ij})

tale che $a_{ij} = 0$ se $i \neq j$, e certo $a_{ii} \neq 0$ per ogni i, dato che $M_{pl}(\pi')$ ha caratteristica n (e quindi $m \geq n$). Per tale scelta di base, si ha $v = \nu(a_{11}) + \nu(a_{22}) + \ldots + \nu(a_{nn})$, ed inoltre si sa che v è indipendente dalla scelta della base. Basta quindi provare il risultato nel caso in cui $M_{pl}(\pi')$ ha la forma accennata. Ma in tal caso si ha $y_i^{(\pi)} = 0$ se $i > n$, e $y_i^{(\pi)} = x_i^{(a_{ii})}$ se $i \leq n$; ora, l'ultima relazione definisce un omomorfismo π_i' del gruppo G_i di dimensione 1 e punto generale x_i sul gruppo G_i' di dimensione 1 e punto generale y_i, ed è chiaro che il grado di π_i', ossia $[k\{x_i\} : k\{x_i^{(a_{ii})}\}]$, è precisamente $p^{\nu(a_{ii})}$; pertanto il grado di π' è p^v, c. v. d..

2. I completamenti delle varietà abeliane.

In questa sezione, k è un corpo algebricamente chiuso di caratteristica $p > 0$. È dimostrato in [12] che ogni gruppo analitico commutativo è prodotto diretto di un gruppo logaritmico, e di un gruppo analitico *radicale*, tale cioè che ogni sua iperderivazione invariante è pseudonulla, necessariamente di ordine potenza di p; la dimensione del fattore diretto logaritmico eguaglia il massimo numero di derivazioni invarianti D, linearmente indipendenti, che soddisfano la relazione $D^p = D$. Se pertanto A è varietà abeliana non singolare di dimensione n su k, e se p^f è l'ordine del kernel di $p\,\delta_A$, il 4.3 di [6] mostra che il completamento di A è prodotto diretto di un gruppo logaritmico di dimensione f, e di un gruppo radicale. In questo articolo ci limitiamo alla considerazione della parte logaritmica, ed allora ne possiamo stabilire l'esistenza (se non come fattore diretto, almeno come immagine omomorfa massima) in modo diretto:

(2.1) LEMMA. *Sia A una varietà abeliana non singolare su k; posto $\mathfrak{o} = Q(E_A/A)$, e $\mathfrak{p} = \mathbf{P}(E_A/A)$, sia y un elemento di $\mathfrak{o}$, tale che $y \equiv 1$ (mod $\mathfrak{p}$), e che $y^{-1}\,dy$ sia un differenziale invariante non nullo su A. Sia $\bar{\mathfrak{o}}$ il completamento di $\mathfrak{o}$, e pongasi $\bar{\mathfrak{p}} = \mathfrak{p}\bar{\mathfrak{o}}$; siano A_1, A_2 copie di A, e supponga si $k(A_2) \subseteq k(A \times A_1)$ come prescritto dalla legge di composizione su A. Allora esiste un $x \in \bar{\mathfrak{o}}$ tale che:* 1) $x \equiv 1$ (*mod* $\bar{\mathfrak{p}}$); 2) $y^{-1}x \in \bar{\mathfrak{o}}^p$ (= *anello delle potenze p-esime degli elementi di* $\bar{\mathfrak{o}}$); 3) $x_2 = xx_1$, *se x_i è la copia di x legata ad A_i.*

DIM. Voglio dimostrare che esiste una successione $y_1 = y$, y_2, $y_3, \ldots$ di elementi di $\mathfrak{o}$ tali che: a) $y_i \in Y(A, \delta_{i,A})$ (v. sezioni 1 e 3 di [6] per le definizioni di $\delta_{i,A}$ e di $Y(A, \alpha)$ rispettivamente); b) $y_i \equiv 1$ (*mod* $\mathfrak{p}$); c) $y_i^{-1}\,y_{i-1} \in \mathfrak{o}^{p^{i-1}}$ se $i > 1$. Per $i = 1$, queste tre condizioni sono soddisfatte, la condizione a) essendo equivalente al fatto che $y^{-1}\,dy$ è un differenziale invariante su A. Supposto dunque che le $y_1, \ldots, y_{r-1}$, soddisfa

centi alle condizioni a), b), c), siano state trovate, procederemo a dimostrare la possibilità di trovare y_r. Sia p^f l'ordine del kernel di $p\,\delta_A$; l'esistenza del differenziale invariante non nullo $y^{-1}\,dy$ mostra, per il 4.3 di [6], che $f > 0$; lo stesso ragionamento usato nella dimostrazione di 4.1 di [6] prova anche che $Y(A\,,\ \delta_{r,A})/k\,(A^{p^r})_0$ (ove $k\,(A^{p^r})_0$ è il gruppo degli elementi non nulli di $k\,(A^{p^r})$) è un gruppo di ordine p^{rf}. Sia Z l'insieme dei prodotti di un elemento di $Y(A\,,\ \delta_{r,A})$ per un elemento di $k\,(A^{p^{r-1}})_0$; allora $Z \subseteq Y(A\,,\ \delta_{r-1,A})$, e $Z/k\,(A^{p^{r-1}})_0 \cong Y(A\,,\ \delta_{r,A})/Y(B\,,\ \delta_{1,B})$, ove $B = A^{p^{r-1}}$, per il secondo teorema di omomorfismo sui gruppi; l'ultimo gruppo, a sua volta, è isomorfo a $[Y(A\,,\ \delta_{r,A})/k\,(A^{p^r})_0]/[Y(B\,,\delta_{1,B})/k(B^p)_0]$, che è un gruppo di ordine $p^{rf}/p^f = p^{(r-1)f}$. Quindi $Z/k\,(A^{p^{r-1}})_0$ ha lo stesso ordine di $Y(A\,,\ \delta_{r-1,A})/k\,(A^{p^{r-1}})_0$, e pertanto $Z = Y(A\,,\ \delta_{r-1,A})$; ciò dimostra che esistono una $z \in Y\ (A\,,\ \delta_{r,A})$, ed un $t \in k\,(A^{p^{r-1}})_0$, tali che $y_{r-1} = z\,t$. Per ogni $P \in A$, si ha $\sigma_P z = z\,t_P$, ove $t_P \in k\,(A^{p^r})_0$, ed è possibile scegliere P in modo che $\sigma_P z \in \mathfrak{o} - \mathfrak{p}$, nel qual caso $y_{r-1} = (\sigma_P z)\,t_P^{-1}\,t$, ove $t_P^{-1}t \in k(A^{p^{r-1}})$. Si può quindi supporre che la z originale soddisfacesse già la condizione $z \in \mathfrak{o} - \mathfrak{p}$. Ora, se $z \equiv a\ (mod\ \mathfrak{p})$, con $0 \neq a \in k$, pongasi $y_r = a^{-1}\,z$; si ha così $y_r \in Y\,(A\,,\ \delta_{r,A})$, $y_{r-1} = y_r\,t'$, con $t' \in k\ (A^{p^{r-1}})$, e infine $y_r \equiv 1\ (mod\ \mathfrak{p})$. Ne segue $y_r - y_{r-1} = y_r(1 - t')$, e perciò $t' \equiv 1\ (mod\ \mathfrak{p})$; ma allora, $1 - t' \in \mathfrak{p} \cap k\,(A^{p^{r-1}}) \subseteq \mathfrak{p}^{p^{r-1}}$, e pertanto $y_r - y_{r-1} \in \mathfrak{p}^{p^{r-1}}$, ed $y_r^{-1}\,y_{r-1} = t' \in \mathfrak{o}^{p^{r-1}}$. L'esistenza della successione $\{y_i\}$ è pertanto dimostrata. Si noti che $\mathfrak{p}^{p^{r-1}}$ indica, come di solito, la p^{r-1}-esima potenza di $\mathfrak{p}$.

Pongasi ora $x = \lim_{i\to\infty} y_i$, che, come si è visto, esiste, ed è elemento di $\bar{\mathfrak{o}}$; allora $x \equiv 1\ (mod\ \mathfrak{p})$, per la condizione b), e questa è la condizione 1) dell'enunciato; inoltre, per ricorrenza sulla condizione c), $y_r\,y^{-1} \in \mathfrak{o}^p$ per ogni r, e quindi $x\,y^{-1} \in \bar{\mathfrak{o}}^p$, che è la condizione 2) dell'enunciato. Infine, pongasi $\mathbf{O} = Q\,(E_A \times E_{A_1}/A \times A_1)$, $\mathbf{P} = \mathbf{P}\,(E_A \times E_{A_1}/A \times A_1)$; si ha $y_r^{-1}\,y_{r+1} = 1 + m_r$, con $m_r \in \mathfrak{p} \cap \mathfrak{o}^{p^r}$, e quindi $y_r^{-1}\,y_{r+i} = 1 + m_{r,i}$, con $m_{r,i} \in \mathfrak{p} \cap \mathfrak{o}^{p^r}$, e pertanto $y_r^{-1}\,x = 1 + q_r$, ove $q_r \in \bar{\mathfrak{p}} \cap \bar{\mathfrak{o}}^{p^r}$. Ora, $(xx_1)^{-1}x_2 = (y_r\,(y_r)_1)^{-1}\,(y_r)_2\,[(1 + q_r)\,(1 + q_r)_1]^{-1}\,(1 + q_r)_2$; ma per il 3.1 di [6], la condizione $y_r \in Y\,(A\,,\ \delta_{r,A})$ comporta che $(y_r\,(y_r)_1)^{-1}\,(y_r)_2 \in k\,(A^{p^r} \times A_1^{p^r})$, e che pertanto $(xx_1)^{-1}\,x_2$ appartiene al corpo quoziente di $\bar{\mathbf{O}}^{p^r}$; essendo ciò valido per ogni r, si conclude che $x_2 = a\,xx_1$, con $a \in k$; e poichè $x \equiv 1$, $x_1 \equiv 1$, $x_2 \equiv 1\ (mod\ \bar{\mathbf{P}})$, ove $\bar{\mathbf{P}} = \mathbf{P}\bar{\mathbf{O}}$, è certo $a = 1$. Questa è la condizione 3) dell'enunciato, c. v. d..

Sia ora A una varietà abeliana non singolare di dimensione n su k, e sia p^f l'ordine del kernel di $p\,\delta_A$; a norma del 4.3 di [6], sia $\{y_1^{-1}\,dy_1\,,\ \ldots\,,\ y_f^{-1}\,dy_f\}$ una k-base indipendente del k-modulo Ω definito in quel teorema, e si scelgano le y_i in modo che $y_i \in \mathfrak{o}$, $y_i \equiv 1\ (mod\ \mathfrak{p})$; qui, $\mathfrak{p}$ ed $\mathfrak{o}$ hanno lo stesso significato che hanno in (2.1); ciò è sempre

possibile, eventualmente mediante una sostituzione del tipo $y_i \to a_i \sigma_{P_i} y_i$, con $P_i \in A$ e $0 \neq a_i \in k$. Per ogni $i \leq f$, sia $1 + x_i \in \bar{0}$ legata ad y_i come x è legata ad y in (2.1). Se G è il completamento di A, il (2.1) mostra che $\{x_1, \ldots, x_f\}$ è un insieme di coordinate canoniche di un gruppo logaritmico G_l, di dimensione f, che è immagine omomorfa di G in un omomorfismo γ; inoltre, ogni omomorfismo α di G su un gruppo logaritmico è del tipo $\alpha = \beta\gamma$, ove β è un omomorfismo di G_l. Gli elementi canonici di G_l si diranno gli *elementi canonici logaritmici di* A:

(2.2) TEOREMA. *Sia A una varietà abeliana di dimensione n su k, e sia p^f l'ordine del kernel di $p\,\delta_A$; allora l'insieme degli elementi canonici logaritmici di A è un I_p-modulo libero di ordine f.*

L'I_p-modulo degli elementi canonici logaritmici di A sarà indicato con $V_l(A)$; e per ogni primo q, $\mathfrak{g}_q(A)$ indicherà il gruppo dei $P \in A$ tali che $P^{q^i} = E_A$ per qualche intero non negativo i; se $f = 0$, $\mathfrak{g}_p(A)$ si riduce ad E_A, mentre se $f > 0$, la teoria svolta ai nn. 28, 29, 30, 31 di [14] è applicabile a $\mathfrak{g}_p(A)$. Nel seguito, avremo occasione di parlare di matrici ad m righe ed n colonne, senza esserci assicurati preventivamente che $m > 0$ ed $n > 0$; una volta per tutte, faremo la convenzione che in ogni formula in cui una tale matrice, od un ente legato ad essa, appare, la matrice stessa, o quell'ente, debba considerarsi non scritta se $m = 0$ o $n = 0$; e che parimenti, ogni asserzione concernente una tale matrice, od un tale ente, con $m = 0$ o $n = 0$, debba considerarsi non fatta.

(2.3) TEOREMA. *Siano A, B varietà abeliane non singolari su k, di dimensioni n ed m rispettivamente; siano p^f, p^h gli ordini dei kernels di $p\,\delta_A$, $p\,\delta_B$ rispettivamente; dopo aver scelto delle basi in $\mathfrak{g}_p(A)$, $V_l(A)$, $\mathfrak{g}_p(B)$, $V_l(B)$ (supposte coincidenti se $A = B$), per ogni omomorfismo π di A su B esistono due matrici $M_p(\pi)$, $M_{pl}(\pi)$, unicamente determinate, ad elementi in I_p; ed aventi h righe ed f colonne, e tali che:*

1) $M_p(\pi + \varrho) = M_p(\pi) + M_p(\varrho)$, $M_{pl}(\pi + \varrho) = M_{pl}(\pi) + M_{pl}(\varrho)$, *se ϱ è un omomorfismo di A su B;*

2) *se C è una terza varietà abeliana non singolare su k, e ϱ è un omomorfismo di B su C, si ha $M_p(\varrho\,\pi) = M_p(\varrho)\,M_p(\pi)$, ed $M_{pl}(\varrho\,\pi) = M_{pl}(\varrho)\,M_{pl}(\pi)$;*

3) *$M_p(\pi)$ ed $M_{pl}(\pi)$ hanno la stessa caratteristica; se $f = n$, tale caratteristica è la dimensione di πA;*

4) *se dim $\pi G = n$, ossia se π ha grado positivo, siano p^a, p^b le massime potenze di p che dividono, rispettivamente, tutti i minori di ordine f estratti da $M_p(\pi)$, e tutti i minori di ordine f estratti da $M_{pl}(\pi)$; allora p^a è anche la massima potenza di p che divide l'ordine del kernel di π, ossia il*

grado di una componente separabile di π, *e* p^b *divide l'inseparabilità di* π, *ed uguaglia tale inseparabilità se* $f = n$;

5) *se in particolare* $B = A$ *ed* $f = n$, *e se* $\varphi_p(\pi, X)$, $\varphi_{pl}(\pi, X)$ *sono i polinomi caratteristici di* $M_p(\pi)$, $M_{pl}(\pi)$ *rispettivamente, il prodotto* $\varphi_p(\pi, X)\ \varphi_{pl}(\pi, X)$ *è il polinomio caratteristico di* π, *ed ha perciò coefficienti interi razionali.*

DIM. L'omomorfismo π può essere esteso ad un omomorfismo π del completamento G di A sul completamento G' di B; l'esistenza ed unicità di $M_p(\pi)$ ed $M_{pl}(\pi)$ sono allora conseguenza del Teorema 14 di [14], e delle considerazioni che precedono il (1.7); l'asserzione 2) è conseguenza di (1.7), e delle considerazioni che seguono il Teorema 14 di [14]; l'asserzione 1) è conseguenza di (1.7) e del Teorema 14 di [14]. Occorre ora provare che $M_p(\pi)$ ed $M_{pl}(\pi)$ hanno la stessa caratteristica. Sia c la caratteristica di $M_p(\pi)$, e si consideri il gruppo $\mathbf{g}$ dei $P \in \mathbf{g}_p(A)$ il cui corrispondente vettore p-adico v_P soddisfa la condizione $M_p(\pi)\, v_P \equiv 0 \pmod 1$; allora $\mathbf{g}$ ha la proprietà che il sottogruppo di $\mathbf{g}$ i cui elementi hanno per periodo un divisore di p^r, con r intero positivo, è prodotto diretto di $f - c$ gruppi ciclici di ordine p^r; inoltre, $\mathbf{g}_p(\pi A) \cong \mathbf{g}_p(A)/\mathbf{g}$, e pertanto l'ordine del kernel di $p\ \delta_{\pi A}$ è p^c; quindi, per (2.2), c è l'ordine di $V_l(\pi A)$, onde p^c è la caratteristica di $M_{pl}(\pi)$, per (1.7). Questo dimostra l'asserzione 3).

L'asserzione di 4) che si riferisce ad $M_p(\pi)$ è conseguenza immediata della Proposizione 13 di [14]; la parte rimanente è conseguenza di (1.7), e del fatto che il grado di π, come omomorfismo di G, eguaglia l'inseparabilità di π, come omomorfismo di A; quest'ultima asserzione si dimostra nel modo seguente: se $\{y\}$ è un insieme regolare di parametri di $Q(E_{\pi A}/\pi A)$, per definizione il grado di π nel primo senso è la molteplicità $e\,(Q(E_A/A); y)$; invece il grado di π nel secondo senso è $[k(A): k(\pi A)]$; ora, per il Lemma 2.2 di [2], se r è l'ordine del kernel di π si ha $re\,(Q(E_A/A); y) = [k(A): k(\pi A)]$, come richiesto.

L'asserzione 5) si dimostra nello stesso modo usato per il Teorema 36 di [14]: si indichi con ν la valutazione p-adica di R_p (normalizzata in modo che $\nu(p) = 1$), che si intenderà estesa ad ogni prolungamento finito di R_p; per ogni endomorfismo λ di A, l'asserzione 4) dell'enunciato implica che $\nu(\textit{grado di } \lambda) = \nu(\textit{det } M_p(\lambda)) + \nu(\textit{det } M_{pl}(\lambda))$. Ma se $\omega_1, \ldots, \omega_{2n}$ sono le radici caratteristiche di λ, in un conveniente prolungamento finito di R_p, si ha $\nu(\textit{grado di } \lambda) = \nu(\omega_1 \omega_2 \ldots \omega_{2n})$. D'altra parte, se $\{\eta_1, \ldots, \eta_n\}$, $\{\eta_{n+1}, \ldots, \eta_{2n}\}$ sono gli zeri di $\varphi_p(\lambda, X)$, $\varphi_{pl}(\lambda, X)$ rispettivamente, si ha anche $\nu(\textit{det } M_p(\lambda)) = \nu(\eta_1 \ldots \eta_n)$, e $\nu(\textit{det } M_{pl}(\lambda)) = \nu(\eta_{n+1} \ldots \eta_{2n})$, cosicchè $\nu(\omega_1 \ldots \omega_{2n}) = \nu(\eta_1 \ldots \eta_{2n})$. Sia $F(Y)$ un polinomio a coefficienti interi razionali, e pongasi $\lambda = F(\pi)$; per il Teorema 35 di [14], le radici caratteristiche di λ sono le $F(\omega_i)$, se le ω_i, η_j sono ora legate a π

anzichè a λ; inoltre, $M_p(\lambda) = F(M_p(\pi))$, e $M_{pl}(\lambda) = F(M_{pl}(\pi))$, cosicchè, per il teorema di Sylvester sulle matrici, gli zeri di $\varphi_p(\lambda, X)$, $\varphi_{pl}(\lambda, X)$ sono rispettivamente gli $F(\eta_i)$ $(i = 1, \ldots, n)$ e gli $F(\eta_i)$ $(i = n+1, \ldots, 2n)$. Pertanto, $\nu(\prod_1^{2n} F(\omega_i)) = \nu(\prod_1^{2n} F(\eta_i))$; ed allora, a norma del Lemma 12 di [14], il polinomio caratteristico di π è proprio $\varphi_p(\pi, X)\,\varphi_{pl}(\pi, X)$; esso ha coefficienti razionali per il Corollario 2 del Teorema 37 di [14], c. v. d.

3. La matrice p-adica legata ad un ciclo.

In questa sezione, *fermo restando il significato di k come nella sezione precedente,* daremo una applicazione dei risultati precedenti alla generalizzazione del contenuto del § XI di [14]. Prima di tutto, una definizione: siano A, B varietà abeliane non singolari di dimensioni n, m rispettivamente sopra un corpo algebricamente chiuso, e sia π un omomorfismo di B su A; supponga si dapprima che π operi su tutta A, e sia X un ciclo irriducibile di dimensione $n-1$ su A; allora $\pi\{X\}^* = \Sigma_i a_i z_i$, ove gli a_i sono interi positivi, e gli z_i sono sottovarietà irriducibili distinte di $B_{k(X)}$; ogni z_i opera su una sottovarietà irriducibile Z_i di dimensione $m-1$ di B, e si porrà $N_\pi^{-1} X = \Sigma_i a_i Z_i$. Se X non è irriducibile, $N_\pi^{-1} X$ verrà definita per linearità; si noti che se π ha grado positivo, questa definizione coincide con quella data nella dimostrazione del (12) di [4], come si vede dai risultati di [2]. Se ora π non opera su tutta A, si porrà $N_\pi^{-1} X = N_\pi^{-1}(X \cap \pi B, A)$ se $(X \cap \pi B, A)$ è definita; negli altri casi, $N_\pi^{-1} X$ non è definita. Si noti che se $X = div_A \vartheta$, per uno $\vartheta \in k(A)$, e se ϱ denota riduzione di $Q(\pi B/A)$ $(mod\ \mathbf{P}(\pi B/A))$, è $N_\pi^{-1} X = div_B \varrho\, \vartheta$.

(3.1) THEOREMA. *Sia A varietà abeliana non singolare di dimensione n su k, e sia p^f l'ordine del kernel di $p\,\delta_A$; fissate delle basi di $\mathfrak{g}_p(A)$ e $V_l(A)$, ad ogni ciclo X (virtuale intero) di dimensione $n-1$ su A si può far corrispondere una matrice quadrata $E_p(X)$, ad elementi in I_p, di ordine f, in modo che:*

1) $E_p(X) = 0$ *se* $X \equiv 0$ *(o, il che è lo stesso, per il* 4.3 *di* [6], *se* $X \approx 0$);

2) $E_p(X + Y) = E_p(X) + E_p(Y)$;

3) *se* $P \in \mathfrak{g}_p(A)$, *e* $v(P)$ *è il corrispondente vettore p-adico, mod 1, si ha* $E_p(X)\,v(P) \equiv 0$ *(mod 1) se e solo se* $\sigma_p X \sim X$;

4) *se π è un omomorfismo su A di un'altra varietà abeliana non singolare B su k, e se $N_\pi^{-1} X$ è definito, si ha* $E_p(N_\pi^{-1} X) = [M_{pl}(\pi)]_{-1}\, E_p(X)\, M_p(\pi)$.

DIM. Posto $q = p^r$, con r intero non negativo, e $C = \alpha A$, ove $\alpha = q\,\delta_A$, sia Z un ciclo di dimensione $n-1$ su A, tale che $qZ \sim 0$, e siano ϑ_{Zq}, y_{Zq} elementi di $k(A)$ tali che si abbia $div_A\,\vartheta_{Zq} = qZ$, e $\vartheta'_{Zq} = y^q_{Zq}$, se ϑ'_{Zq} è la copia di ϑ_{Zq} in $k(C)$; tali ϑ_{Zq} ed y_{Zq} esistono per la Proposizione 32 di [14], e sono determinati a meno di costanti moltiplicative in k. Si noti subito che se Z' è la copia di Z su C, è $div_C\,\vartheta'_{Zq} = q\,Z'$; pertanto, $q\,N_\alpha^{-1}\,Z' = div_A\,\vartheta'_{Zq}$, onde $N_\alpha^{-1}\,Z' = div_A\,y_{Zq}$; si osservi che se P appartiene al kernel di α, si ha $\sigma_P\,N_\alpha^{-1}\,Z' = N_\alpha^{-1}\,Z'$, onde $\sigma_P\,y_{Zq} = h_P\,y_{Zq}$; ma la relazione $P^q = E_A$ dà immediatamente $h_P^q = 1$, onde $h_P = 1$, e perciò $y_{Zq} \in k(\beta A)$, se β è una componente separabile di α (v. sezione 1 di [6] per la definizione). Se invece P è un punto qualsiasi di A, il divisore, su A, di $y_{Zq}^{-1}\,\sigma_P\,y_{Zq}$ è $N_\alpha^{-1}(\sigma_{\alpha P}\,Z' - Z')$; ora, $Z' \equiv 0$ poichè $qZ' \sim 0$, e pertanto $Z' \sim \sigma_{\alpha P}\,Z'$, onde $y_{Zq}^{-1}\,\sigma_P\,y_{Zq} \in k(C)$, o in altre parole, $y_{Zq} \in Y(A,\alpha)$. Come nella dimostrazione di (2.1), esistono un $h \in k$, ed un $P \in A$, tali che $1 + z_{Zq} = h\,\sigma_P\,y_{Zq}$ appartenga a $Q(E_A/A)$, e sia $\equiv 1 \pmod{\mathbf{P}(E_A/A)}$. Si consideri z_{Zq} come un elemento di $k\{G\}$, ove G è il completamento di A, e sia $\{\xi_1, \ldots, \xi_n\}$ un insieme regolare di parametri di $Q(E_A/A)$; allora, per P, $Q \in G$, e come conseguenza del 3.1 di [6], si ha che $z_{Zq}(P\,Q) = z_{Zq}(P) + z_{Zq}(Q) + z_{Zq}(P)\,z_{Zq}(Q) + (1 + z_{Zq}(P))(1 + z_{Zq}(Q))\,w$, ove w è una serie di potenze, senza termini di grado 0, nelle $\xi_i^q(P)$ e $\xi_i^q(Q)$. Ed allora, con ragionamento analogo a quello usato nella dimostrazione di (2.1), si può dimostrare che esiste un elemento canonico logaritmico x_{Zq} di A tale che $z_{Zq} - x_{Zq} \in \mathbf{p}^q$, $\mathbf{p}$ essendo il primo massimo di $k\{G\}$. Evidentemente, $1 + x_{Zq}$ è determinato, a meno di un fattore moltiplicativo in $k\{G^q\}$, unicamente da Z e q. Se m è un'altra potenza di p, si ha naturalmente $mq\,Z \sim 0$, cosicchè ϑ_{Zmq} esiste, e può essere scelto $= \vartheta_{Zq}^m$; in tal caso, pongasi $\gamma = mq\,\delta_A$, $Z'' = $ *copia di* Z *su* γA, $\eta = m\,\delta_C$, cosicchè $\gamma = \eta\,\alpha$. Allora $div_A(y_{Zmq}\,y_{Zq}^{-m}) = N_\gamma^{-1}\,Z'' - m\,N_\alpha^{-1}\,Z' = N_\alpha^{-1}(N_\eta^{-1}\,Z'' - m\,Z')$; ma per la Proposizione 31 di [14], è $N_\eta^{-1}\,Z'' \sim m\,Z'$, e pertanto $y_{Zmq}\,y_{Zq}^{-m} \in k(C)$; ciò comporta che $x_{Zmq} \cdot x_{Zq}^{(-m)} \in k\{G^q\}$; se $v_q(Z)$ è il vettore a coordinate in I_p, determinato *mod* q, che corrisponde ad x_{Zq}, è così provato che $v_{mq}(Z) \equiv m\,v_q(Z) \pmod q$. Si noti inoltre che se T è un altro ciclo di dimensione $n-1$ su A, tale che $q\,T \sim 0$, è certo $v_q(Z+T) \equiv v_q(Z) + v_q(T) \pmod q$; inoltre, è $Z \sim 0$ se, e solo se $y_{Zq} \in k(C)$, ossia se e solo se $v_q(Z) \equiv 0 \pmod q$.

Dato X, applichiamo quanto precede a $Z = \sigma_P\,X - X$, ove $P \in \mathbf{g}_p(A)$; tale applicazione è certo possibile, perchè $q\,Z \sim 0$ per ogni q tale che $P^q = E_A$. Dato un vettore t, con componenti (in numero di f) in I_p, per ogni intero non negativo i sia P_i un punto di $\mathbf{g}_p(A)$ il cui corrispondente vettore p-adico è $\equiv p^{-i}\,t \pmod 1$, e pongasi $Z_i = \sigma_{P_i}\,X - X$; poichè

$P_i^{p^i} = E_A$, lo $z_i = v_{p^i}(Z_i)$ esiste, ed è determinato *mod* p^i. Si ha $P_{i+1}^{p} = P_i$, onde $p\, Z_{i+1} \sim Z_i$, per il Corollario 2 al Teorema 30 di [14], e perciò $v_{p^i}(Z_i) \equiv p\, z_{i+1}\ (mod\ p^{i+1})$; ma $v_{p^{i+1}}(Z_i) \equiv p z_i\ (mod\ p^i)$, onde $z_{i+1} \equiv z_i\ (mod\ p^{i-1})$, e pertanto lo $z = \lim_{i\to\infty} z_i$ esiste, dipende solo da X e t, ed ha componenti in I_p. Se t' è un altro vettore a componenti in I_p, pongasi $t'' = t + t'$, e siano z_i', z' e z_i'', z'' legati ad X e, rispettivamente, t' e t'' come z_i, z lo sono ad X e t; si vede allora che $z_i'' \equiv z_i + z_i'\ (mod\ p^i)$, onde $z'' = z + z'$. Quindi l'applicazione $t \to z = F(t)$ soddisfa la $F(t + t') = F(t) + F(t')$, ed in particolare $F(p^j t) = p^j F(t)$, onde $F(t) \equiv 0\ (mod\ p^j)$ se $t \equiv 0\ (mod\ p^j)$; questa significa che la $F(t)$ è funzione continua, secondo la topologia indotta da quella di R_p; ma allora, $F(a\, t) = a\, F(t)$ per $a \in I_p$; questa relazione, fra l'altro, permette di definire $F(t)$ quando t ha componenti in R_p, e mostra, insieme alla $F(t + t') = F(t) + F(t')$, che F è lineare, ossia che esiste una matrice $E_p(X)$, ad elementi in I_p, tale che $F(t) = E_p(X)\, t$, se t viene interpretato come matrice ad f righe ed una colonna. La relazione $v_q(Z+T) \equiv v_q(Z) + v_q(T)\ (mod\ q)$ dà subito $E_p(X + Y) = E_p(X) + E_p(Y)$.

Nelle notazioni precedenti, sia $P \in \mathfrak{g}_p(A)$, e suppongasi $P^{p^j} = E_A$; posto $p^{-j} t \equiv v(P)\ (mod\ 1)$, t è vettore ad elementi in I_p, e si ha $\sigma_P X \sim X$ se e solo se, per $i \geq j$, $v_{p^i}(Z_i) \equiv 0\ (mod\ p^j)$, ossia $z_i \equiv 0\ (mod\ p^j)$; questa, a sua volta, è equivalente a $z \equiv 0\ (mod\ p^j)$, od anche $F(v(P)) \equiv 0\ (mod\ 1)$. Le asserzioni 2) e 3) dell'enunciato sono pertanto dimostrate. L'asserzione 1) segue dal fatto che se $X \equiv 0$, è $\sigma_P X \sim X$ per ogni $P \in \mathfrak{g}_p(A)$, onde $E_p(X)\, t \equiv 0\ (mod\ 1)$ per ogni vettore p-adico t; l'ultima relazione implica appunto $E_p(X) = 0$.

Sia ora B una varietà abeliana non singolare su k, e sia π un omomorfismo di B su A; sia X ciclo di dimensione $n-1$ su A tale che $X' = N_\pi^{-1} X$ sia definito; sia ϱ l'omomorfismo di $Q(\pi\, B/A)$ su $k(\pi\, B)$ il cui kernel è $\mathbf{P}(\pi\, B/A)$. Sia t' un vettore ad elementi in I_p, e pongasi $t = M_p(\pi) t'$; a partire da t', e da t, si costruiscano i punti P_i', P_i come nella costruzione precedente; essi sono punti di $\mathfrak{g}_p(B)$, $\mathfrak{g}_p(A)$ rispettivamente, e si ha $P_i = \pi\, P_i' \in \pi\, B$. Posto $Z_i = \sigma_{P_i} X - X$, $Z_i' = \sigma_{P_i'} X' - X'$, si vede facilmente che $Z_i' = N_\pi^{-1} Z_i$; se allora si ripete la costruzione precedente, cominciando da $\vartheta_{Z_i q}$ e $\vartheta_{Z_i' q}$, su Z_i e Z_i', si vede che, per $q = p^i$, si può scegliere $\vartheta_{Z_i' q} = \varrho\, \vartheta_{Z_q}$, dato che $\vartheta_{Z_q} \in Q(\pi\, B/A)$; quindi si può anche scegliere $x_{Z_i' q} = \varrho\, x_{Z_i q}$, e pertanto $z_i' = [M_{pl}(\pi)]_{-1}\, z_i$. Ne segue che $z' = [M_{pl}(\pi)]_{-1}\, z$; ma $z' = E_p(X')\, t'$, $z = E_p(X)\, t$, onde $E_p(X')\, t' = [M_{pl}(\pi)]_{-1}\, E_p(X)\, M_p(\pi)\, t'$, c. v. d.

Ci si può chiedere se l'asserzione 1) di (3.1) sia invertibile, e cioè se sia vero che la relazione $E_p(X) = 0$ implica $X \equiv 0$; che così non sia si

vede subito nel caso in cui A sia prodotto diretto di varietà abeliane, una delle quali (ma non tutte), sia essa B, ha la proprietà che il kernel di $p\,\delta_B$ è E_B. La questione però rimane significativa nel caso in cui A sia semplice, e tale che il kernel di $p\,\delta_A$ abbia ordine > 1; in tal caso, la risposta è affermativa, ossia la $E_p(X) = 0$ implica $X \equiv 0$, come si vede subito osservando che, per l'asserzione 3) di (3.1), la $E_p(X) = 0$ implica $\sigma_P X \sim X$ per ogni $P \in \mathfrak{g}_p(A)$, e questo, a sua volta, mostra che $\mathfrak{g}_p(A)$ è contenuto nel kernel dell'omomorfismo λ_X introdotto alla sezione 2 di [4]; pertanto, essendo A semplice, tale kernel coincide con A, e quindi $\lambda_X = 0$, onde, per (9) di [4], $X \equiv 0$.

Nelle notazioni dell'asserzione 4) di (3.1), si scelga $B = J =$ *jacobiana di una curva* C; allora, se $N_\pi^{-1} X$ è definita, e se π'_X ha il significato stabilito al n^0 45 di [14], pongasi, per $P \in A$, $N_\pi^{-1}\,\sigma_P X - N_\pi^{-1} X = Z_P$; per il Corollario 1 al Teorema 32 di [14], ed in quelle notazioni, si può scegliere $x_{Z_P q} = x_{\theta_P q}$, ove $\theta_P = \sigma_{\pi'_X P}\,\theta - \theta$; quindi, come nell'ultima parte della dimostrazione di (3.1), si ottiene

$$[M_{pl}(\pi)]_{-1}\, E_p(X) = E_p(\theta)\, M_p(\pi'_X). \tag{3.2}$$

Questa resta valida anche se $N_\pi^{-1} X$ non è definita, dato che $N_\pi^{-1} Y$ è certo definita per qualche $Y \equiv X$.

Ora, per il Corollario 3 al Teorema 30 di [14], è $\sigma_P\,\theta \sim \theta$ se e solo se $P = E_J$, cosicchè, per (3.1), $E_p(\theta)$ è modulare (ossia il suo determinante è una unità di I_p), ed in particolare $[E_p(\theta)]^{-1}$ esiste; pertanto,

$$M_p(\pi'_X) = [E_p(\theta)]^{-1}\,[M_{pl}(\pi)]_{-1}\, E_p(X). \tag{3.3}$$

Posto qui $A = J$, $X = \theta$, e ricordando che, per il Teorema 25 di [14], è $\pi'_\theta = \pi' =$ *corrispondente di* π *nell'involuzione di Rosati su* J, si ottiene:

(3.4) TEOREMA. *Sia J la jacobiana, supposta non singolare, di una curva su k; sia π un endomorfismo di J, e sia π' il corrispondente di π nell'involuzione di Rosati; allora*

$$M_p(\pi') = [E_p(\theta)]^{-1}\,[M_{pl}(\pi)]_{-1}\, E_p(\theta),$$

ove θ è il ciclo su J definito al n^0 41 di [14].

Se ora A è varietà abeliana non singolare semplice su k, e se per ogni endomorfismo α di A, α' denota l'endomorfismo reciproco definito al n^0 71 di [14], si ha da (3.3) (scrivendo π invece di λ):

$$M_p(\alpha') = H\,[M_{pl}(\alpha)]_{-1}\, H^{-1}, \tag{3.5}$$

ove

$$H = M_p(\pi)\,[E_p(\theta)]^{-1}\,[M_{pl}(\pi)]_{-1};$$

se invece si considera la α^* ottenuta mediante la reciprocità definita al n. 72 di [14], si ha:

$$M_p(\alpha^*) = [E_p(X)]^{-1}\,[M_{pl}(\alpha)]_{-1}\,E_p(X). \tag{3.6}$$

Sia $E_p^*(X)$ la matrice emisimmetrica $\begin{pmatrix} & -[E_p(X)]_{-1} \\ E_p(X) & \end{pmatrix}$, e pongasi $M_p^*(\pi) = \begin{pmatrix} M_p(\pi) & \\ & M_{pl}(\pi) \end{pmatrix}$; allora la 4) di (3.1), e le (3.4), (3.5), (3.6) possono essere espresse per mezzo di queste matrici; in particolare, la (3.4) diviene

$$M_p^*(\pi') = [E_p^*(\theta)]^{-1}\,[M_p^*(\pi)]_{-1}\,E_p^*(\theta). \tag{3.7}$$

Un esame della dimostrazione del teorema di dualità ((14) di [4]) pel caso di caratteristica zero mostra che tale dimostrazione è basata sul fatto che $M_q(\lambda_X) = U\,E_q(X)$, per un primo q, ove U è matrice modulare ad elementi in I_q; ora che siamo in possesso della matrice $E_p(X)$, è facile convincersi che $M_p(\lambda_X) = U\,E_p(X)$; questo però non dà nessuna informazione su $M_{pl}(\lambda_X)$, e pertanto, anche nel caso più favorevole in cui $f = n$, non permette di migliorare in alcun modo quanto è noto sul teorema di dualità per il caso di varietà abeliane su corpi di caratteristica positiva; ed a tal proposito, voglio cogliere l'occasione per sottolineare che l'osservazione che conchiude la sezione 3 di [4] resta, al momento in cui scrivo, l'approssimazione migliore ad un teorema di dualità, inquantochè ogni maggiore precisazione che è dato di trovare qua e là nella letteratura è o illusoria, o non dimostrata. Ad esempio, un'analisi della dimostrazione del Teorema 3 di [13] mostra che tale teorema (a prescindere dal suo enunciato) non dice nulla di più, per quanto riguarda *la* varietà di Picard di A, di quanto espresso in [4]; inoltre, il risultato generosamente attribuitomi dal recensore del mio lavoro [4] (cfr. Math. Rev., 16, 1955, p. 616), secondo cui la varietà di Picard della varietà di Picard di A è legata ad A da un «isomorfismo puramente inseparabile», non è stato da me dimostrato, od enunciato, nè allora, nè ora; e l'ulteriore informazione, meno generosamente fornita dal recensore, secondo cui il teorema di dualità è ormai parte del teorema generale sulla dualità fra la varietà di Picard e la varietà di Albanese di una qualsiasi varietà normale, sembra peccare di eccessivo ottimismo, in quanto sfortunatamente nessuna dimostrazione di tale teorema generale è reperibile, fino al momento in cui scrivo, nella letteratura.

4. L'anello degli endomorfismi.

In questa sezione, k denota un corpo algebricamente chiuso di caratteristica $p \geq 0$. Il corpo razionale sarà indicato con R, e l'anello degli interi razionali con I; R_q ed I_q denoteranno, al solito, il corpo q-adico, e l'anello degli interi q-adici, q essendo un primo razionale.

Se A, B sono varietà abeliane su k, $\mathfrak{o}(A, B)$ denoterà l'I-modulo degli omomorfismi di A su B; esso è un I-modulo finito, certo libero, per il Teorema 37 di [14]; in particolare, porremo $\mathcal{A}(A) = \mathfrak{o}(A, A)$; come è indicato nel n^0 54 di [14], $\mathfrak{o}(A, B)$ è immerso in un R-modulo, che indicherò con $\mathbf{H}(A, B)$; porrò analogamente $\mathbf{A}(A) = \mathbf{H}(A, A)$, cosicchè $\mathbf{A}(A)$ è un'algebra su R, ed $\mathcal{A}(A)$ è una schiera di $\mathbf{A}(A)$ su I, ossia formata da elementi interi rispetto ad I. È facile vedere che $\mathfrak{o}(A, B)$ è anche un $\mathcal{A}(A)$-modulo destro ed un $\mathcal{A}(B)$-modulo sinistro, e che $\mathbf{H}(A, B)$ è un $\mathbf{A}(A)$-modulo destro ed un $\mathbf{A}(B)$-modulo sinistro. L'elemento δ_A è l'unità di $\mathcal{A}(A)$, e verrà talvolta indicato con 1; $\mathbf{A}(A)$ è sempre un'algebra semisemplice, che è semplice se, e soltanto se, A è isogena al prodotto diretto di varietà abeliane semplici isogene l'una all'altra, ed è divisoria se, e soltanto se, A è varietà abeliana semplice (cfr. Teorema 29 di [14]); se A e B sono isogene, $\mathbf{H}(A, B)$ è un $\mathbf{A}(A)$-modulo destro di ordine 1, ossia del tipo $\lambda\,\mathbf{A}(A)$, con $\lambda \in \mathbf{H}(A, B)$; ed analogamente, esso è un $\mathbf{A}(B)$-modulo sinistro di ordine 1: infatti, se A e B sono isogene, è mostrato al n^0 54 di [14] che esistono un $\lambda \in \mathbf{H}(A, B)$ ed un $\lambda^{-1} \in \mathbf{H}(B, A)$, tali che $\lambda\lambda^{-1} = \delta_B$; se quindi $\varrho \in \mathbf{H}(A, B)$, è certo $\lambda^{-1}\varrho \in \mathbf{A}(A)$, e $\varrho = \lambda(\lambda^{-1}\varrho) \in \lambda\,\mathbf{A}(A)$.

Sia A una varietà abeliana su k; al n^0 53 di [14], la categoria di A è definita come l'insieme di tutte le varietà abeliane isogene ad A; in quanto segue, daremo alla parola «categoria» un significato meno esteso, vale a dire: la *categoria di* A è un insieme S di varietà abeliane su k, tale che 1) $A \in S$, 2) se B è isogena ad A, B è isomorfa ad un elemento di S, 3) se $B \in S$, B è isogena ad A, e 4) elementi distinti di S non sono isomorfi. Si vede facilmente che tale definizione evita difficoltà di ordine logico; la categoria di A non è unicamente determinata, ma fra due di esse esiste una corrispondenza biunivoca in cui elementi corrispondenti sono isomorfi. Gli elementi della categoria di A saranno indicati in generale con A_i, ove i percorre un certo insieme, per esempio di numeri ordinali; in particolare, $A_0 = A$; si porrà anche $\mathbf{H}_{ij} = \mathbf{H}(A_j, A_i)$, $\mathfrak{o}_{ij} = \mathfrak{o}(A_j, A_i)$, $\mathbf{A}_i = \mathbf{H}_{ii}$, $\mathcal{A}_i = \mathfrak{o}_{ii}$. Le $\mathbf{A}_i$ sono tutte isomorfe fra loro, cosicchè si può considerare un'algebra $\mathbf{A}$ su R, certo semisemplice, isomorfa ad ogni $\mathbf{A}_i$.

L'insieme degli elementi delle $\mathbf{H}_{ij}$, che verrà indicato con $\mathbf{H}(cat\ A)$, ha una struttura algebrica, che porta ad un anello una simiglianza del tipo di quella che un gruppoide di Brandt porta ad un gruppo; perciò chiamerò tale insieme, con tale struttura algebrica, un *anelloide*; un altro esempio di anelloide è dato dall'unione $\mathfrak{H}(cat\ A)$ delle $\mathfrak{H}_{ij}$. I concetti di isomorfismo e omomorfismo fra anelloidi si definiscono nel solito modo; fra gli omomorfismi di un anelloide $\mathbf{B}$ su un anelloide $\mathbf{B}'$ vi sono certi omomorfismi η, che non sono necessariamente isomorfismi, e che hanno la proprietà seguente: se $b, c \in \mathbf{B}$, $\eta b = \eta c$, e $b - c$ esiste, allora $b = c$; tali omomorfismi si diranno *quasi-isomorfismi.*

(4.1) LEMMA. *Sia A una varietà abeliana su k, e sia $\mathbf{B} = \mathbf{H}(cat\ A)$; nelle notazioni precedenti, sia $\mathbf{A}$ un'algebra isomorfa, su R, ad ogni $\mathbf{A}_i$, e sia ζ un quasi-isomorfismo su R di $\mathbf{B}$ su tutta $\mathbf{A}$; allora, per ogni i, j, ζ induce un isomorfismo di R-moduli fra $\mathbf{H}_{ij}$ e $\zeta\,\mathbf{H}_{ij} = \mathbf{A}$, che è anche un isomorfismo di algebre su R se $i = j$. Viceversa, dato un isomorfismo ζ_0 su R di $\mathbf{A}_0$ su $\mathbf{A}$, ed assegnato, in ogni $\mathbf{H}_{i0}$ con $i \neq 0$, un λ_{i0} tale che λ_{i0}^{-1} esista, vi è un solo omomorfismo ζ su R di $\mathbf{B}$ su $\mathbf{A}$ che induce ζ_0 fra $\mathbf{A}_0$ ed $\mathbf{A}$, e tale che $\zeta\,\lambda_{i0} = 1$ per ogni i; tale ζ è un quasi-isomorfismo su R di $\mathbf{B}$ su tutta $\mathbf{A}$.*

DIM. La prima parte è palese. Per dimostrare la seconda, per ogni $\alpha \in \mathbf{B}$ pongasi $\zeta\,\alpha = \zeta_0(\lambda_{i0}^{-1}\,\alpha\,\lambda_{j0})$ se $\alpha \in \mathbf{H}_{ij}$, avendo supposto, per uniformità, $\lambda_{00} = 1 = \delta_{A_0}$; se $\beta \in \mathbf{H}_{ij}$, si ha $\zeta(\alpha + \beta) = \zeta_0(\lambda_{i0}^{-1}(\alpha + \beta)\,\lambda_{j0}) = \zeta\,\alpha + \zeta\,\beta$; se invece $\beta \in \mathbf{H}_{jr}$, si ha $\zeta(\alpha\,\beta) = \zeta_0(\lambda_{i0}^{-1}(\alpha\,\beta)\,\lambda_{r0}) = \zeta_0[(\lambda_{i0}^{-1}\,\alpha\,\lambda_{j0})(\lambda_{j0}^{-1}\,\beta\,\lambda_{r0})] = (\zeta\,\alpha)(\zeta\,\beta)$; pertanto ζ è un omomorfismo di $\mathbf{B}$ su tutta $\mathbf{A}$; inoltre, $\zeta\,\lambda_{i0} = \zeta_0(\lambda_{i0}^{-1}\,\lambda_{i0}\,\lambda_{00}) = \zeta_0\,\delta_{A_0} = 1$; ed anche, se $\alpha, \beta \in \mathbf{H}_{ij}$, e $\zeta\,\alpha = \zeta\,\beta$, è necessariamente $\lambda_{i0}^{-1}(\alpha - \beta)\,\lambda_{j0} = 0\,\delta_{A_0}$, onde $\alpha = \beta$, il che prova che ζ è un quasi-isomorfismo. Finalmente, se ζ' è un omomorfismo su R di $\mathbf{B}$ su $\mathbf{A}$ che induce ζ_0 fra $\mathbf{A}_0$ ed $\mathbf{A}$, e tale che $\zeta'\,\lambda_{i0} = 1$, per $\alpha \in \mathbf{H}_{ij}$ si ha: $\zeta'\,\alpha = (\zeta'\,\lambda_{i0}^{-1})(\zeta'\,\alpha)(\zeta'\,\lambda_{j0}) = \zeta'(\lambda_{i0}^{-1}\,\alpha\,\lambda_{j0}) = \zeta_0(\lambda_{i0}^{-1}\,\alpha\,\lambda_{j0}) = \zeta\,\alpha$, onde $\zeta' = \zeta$, c. v. d.

Nel seguito, una varietà abeliana su k sarà detta *speciale* se possiede differenziali esatti non nulli di prima specie.

(4.2) TEOREMA. *Notazioni come in* (4.1), *e suppongasi che A sia non speciale; sia ζ un dato quasi-isomorfismo (su R) di $\mathbf{B}$ su tutta $\mathbf{A}$; se $\mathfrak{o}$ è schiera massima di $\mathbf{A}$ su I, esistono un $A_i \in cat\ A$, ed un $b \in \mathbf{A}$, tali che $\mathfrak{o} = b^{-1}(\zeta\,\mathfrak{A}_i)\,b$; in particolare, $\mathfrak{A}_i$ è schiera massima di $\mathbf{A}_i$ su I.*

DIM. Daremo la dimostrazione per il caso $p > 0$; le semplificazioni da apportare alla dimostrazione nel caso $p = 0$ sono ovvie. Sia A_0 fissato, e sia ζ_0 l'isomorfismo di $\mathbf{A}_0$ su tutta $\mathbf{A}$ indotto da ζ; si scelga in ogni A_j una

base di $\mathbf{g}_q(A_j)$, per ogni primo razionale q, ed anche una base di $V_l(A_j)$. Per ogni $\alpha \in \mathfrak{H}_{ij}$ si indichi con $M(\alpha)$ la matrice $\begin{pmatrix} M_p(\alpha) & \\ & M_{pl}(\alpha) \end{pmatrix}$; allora le matrici $M(\alpha)$ ed $M_q(\alpha)$, per $q \neq p$, sono definite, per linearità, per ogni $\alpha \in \mathbf{B}$, e le applicazioni $\alpha \to M_q(\alpha)$, $\alpha \to M(\alpha)$ sono quasi-isomorfismi, su R, di $\mathbf{B}$ su algebre $\mathbf{M}_q$, $\mathbf{M}_p$ rispettivamente, ove $\mathbf{M}_q$ è regolare su I_q, ed $\mathbf{M}_p$ è somma diretta di al massimo due algebre regolari su I_p; se $\mathbf{O}_q$, $\mathbf{O}_p$ sono le schiere massime (Teorema 11, § 1, Cap. VI di [9]) formate dalle matrici di $\mathbf{M}_q$, $\mathbf{M}_p$ con elementi in I_q, I_p rispettivamente, si ha $M_q(\mathfrak{H}_{ij}) \subseteq \mathbf{O}_q$, $M(\mathfrak{H}_{ij}) \subseteq \mathbf{O}_p$. Sia $\mathfrak{H}'$ l'insieme degli $\alpha \in \mathbf{H}_{ij}$ tali che $M(\alpha) \in \mathbf{O}_p$ e $M_q(\alpha) \in \mathbf{O}_q$ per ogni $q \neq p$; è certo $\mathfrak{H}_{ij} \subseteq \mathfrak{H}'$; dico che $\mathfrak{H}_{ij} = \mathfrak{H}'$. Se così non fosse, si potrebbe trovare un $\alpha \in \mathfrak{H}'$ che non apparterrebbe ad $\mathfrak{H}_{ij}$; sia r il minimo intero positivo tale che $r\alpha \in \mathfrak{H}_{ij}$; allora $r > 1$, ed r è divisibile per un primo q. Se $q \neq p$, si ha che $M_q(r\alpha)$ è divisibile per q in $\mathbf{O}_q$, e quindi il kernel di $q\,\delta_{A_j}$ è contenuto nel kernel di $r\alpha$; ma allora $r\alpha$ è divisibile, nel senso indicato nella sezione 1 di [6], per $q\,\delta_{A_j}$, ossia $r\alpha = q\beta$, ove $\beta \in \mathfrak{H}_{ij}$, e quindi $r q^{-1}\alpha \in \mathfrak{H}_{ij}$, il che contraddice la scelta di r. Se invece $q = p$, si ha che $M(r\alpha)$ è divisibile per p in $\mathbf{O}_p$, e questo implica, nello stesso modo, che anzitutto $r\alpha$ è divisibile per una componente separabile di $p\,\delta_{A_j}$, ed in secondo luogo anche che $r\alpha$ è divisibile per una componente inseparabile di $p\,\delta_{A_j}$; ma allora, per l'1.2 di [6], $r\alpha$ è divisibile per $p\,\delta_{A_j}$, ed il resto della dimostrazione procede nello stesso modo.

Ciò premesso, sia $\mathbf{o}$ una schiera massima di $\mathbf{A}$ su I, e sia $r \in I$ tale che $r\mathbf{o} \subseteq \zeta\mathfrak{A}_0 = \xi_0\mathfrak{A}_0$; se $\{\alpha_1, \ldots, \alpha_n\}$ è una I-base di $\zeta_0^{-1}\mathbf{o}$, sia β un massimo comun divisore, nel senso dell'1.1 di [6], delle $r\alpha_i \in \mathfrak{A}_0$. Allora $M_q(\beta)$ (o $M(\beta)$) è un comun divisore destro, in $\mathbf{O}_q$ (o in $\mathbf{O}_p$) delle $M_q(r\alpha_i)$ (o delle $M(r\alpha_i)$); nel modo seguito in precedenza è facile dimostrare che se M è elemento di $\mathbf{O}_q$ che divide a destra le $M_q(r\alpha_i)$, esso necessariamente divide a destra $M_q(\beta)$: ed infatti, se M ha tale proprietà, sia $P \in \mathbf{g}_q(A)$, e sia x il corrispondente vettore q-adico; se $Mx \equiv 0 \pmod 1$, P appartiene al kernel di ogni α_i, e quindi al kernel di β, e pertanto $M_q(\beta)x \equiv 0 \pmod 1$; ciò prova che $M_q(\beta)M^{-1}y \equiv 0 \pmod 1$ se $y \equiv 0 \pmod 1$, onde M è divisore destro di $M_q(\beta)$. Nel caso di $M(\beta)$, si scriva $M = \begin{pmatrix} M_1 & \\ & M_2 \end{pmatrix}$; allora lo stesso ragionamento prova che M_1 divide a destra $M_p(\beta)$; è poi palese che M_2 divide a destra $M_{pl}(\beta)$, come richiesto. Si consideri ora l'$\mathbf{O}_q$-ideale sinistro $\mathbf{O}_q M_q(\zeta_0^{-1}\mathbf{o}) = r^{-1}\mathbf{O}_q M_q(r\zeta_0^{-1}\mathbf{o})$; per il Teorema 13, § 11, Cap. VI di [9], esso è principale, e per quanto precede esso coincide con $r^{-1}\mathbf{O}_q M_q(\beta)$; analogamente, $\mathbf{O}_p M(\zeta_0^{-1}\mathbf{o}) = r^{-1}\mathbf{O}_p M(\beta)$. La schiera (massima) destra di questo ideale è quindi $[M_q(\beta)]^{-1}\mathbf{O}_q M_q(\beta)$, o rispettivamente $[M(\beta)]^{-1}\mathbf{O}_p M(\beta)$, ed essa contiene evidentemente $M_q(\zeta_0^{-1}\mathbf{o})$, o rispettivamente $M(\zeta_0^{-1}\mathbf{o})$. Pertanto,

$M_q(\zeta_0^{-1}\mathfrak{o}) \subseteq [M_q(\beta)]^{-1}\mathfrak{O}_q M_q(\beta)$; pongasi ora $A_1 = \beta A_0$, cosicchè $\mathfrak{A}_0 = \beta^{-1}\mathfrak{A}_1\beta$; allora la relazione precedente, e l'analoga $M(\zeta_0^{-1}\mathfrak{o}) \subseteq [M(\beta)]^{-1}\mathfrak{O}_p M(\beta)$, dice che se $\alpha \in \zeta_0^{-1}\mathfrak{o}$, è $M_q(\beta\alpha\beta^{-1}) \in \mathfrak{O}_q$, ed $M(\beta\alpha\beta^{-1}) \in \mathfrak{O}_p$; ciò mostra, per il risultato trovato più sopra, che $\beta\alpha\beta^{-1} \in \mathcal{A}_1$, onde $\beta(\zeta_0^{-1}\mathfrak{o})\beta^{-1} \subseteq \mathcal{A}_1$, od anche $\zeta_0^{-1}\mathfrak{o} \subseteq \beta^{-1}\mathcal{A}_1\beta$, $\mathfrak{o} \subseteq b^{-1}(\zeta\mathcal{A}_1)b$, se $b = \zeta\beta$; di qui segue subito che $\mathcal{A}_1$ è schiera massima, c. v. d.

Ci si può chiedere se non sia vero che ogni $\mathcal{A}_i$ è schiera massima di $\mathfrak{A}_i$; che così in generale non sia si vede dal seguente

(4.3) TEOREMA. *Notazioni come in* (4.1); *se* $\mathfrak{A}$ *non è normale su* R, *esiste qualche* $\mathcal{A}_i$ *che non è schiera massima di* $\mathfrak{A}_i$ *su* I.

DIM. Suppongasi che si possa scegliere A_0 in modo tale che $\mathcal{A}_0$ sia schiera massima di $\mathfrak{A}_0$; detti $\mathcal{C}_i$, $\mathfrak{C}_i$ i centri di $\mathcal{A}_i$ ed $\mathfrak{A}_i$ rispettivamente, per ipotesi è $R \subset \mathfrak{C}_i$, e quindi $I \subset \mathcal{C}_i$; in particolare, $\mathcal{C}_0$ è la chiusura aritmetica (integral closure) di I in $\mathfrak{C}_0$. Sia α_0 un elemento di $\mathcal{C}_0$, ma non di I; allora, esistono un intero positivo r ed un $P \in A_0$ tali che $P^r = E_{A_0}$, e che $\alpha_0 P$ non sia una potenza di P. Supporremo che r sia precisamente il periodo di P, cosicchè il gruppo K delle potenze di P ha ordine r. Sia β un omomorfismo separabile di A_0 il cui kernel è K; posto $A_1 = \beta A_0$, è $\beta \in \mathfrak{H}_{10}$, e per il Teorema 27 di [14] esiste un $\gamma \in \mathfrak{H}_{01}$ tale che $\beta\gamma = r\delta_{A_1}$, cosicchè $\beta^{-1} = r^{-1}\gamma$. Si consideri l'elemento $\alpha_1 = \beta\alpha_0\beta^{-1}$ di $\mathfrak{A}_1$; esso appartiene a $\mathfrak{C}_1$; se dimostro che $\alpha_1 \notin \mathcal{A}_1$, ciò proverà che $\alpha_1 \notin \mathcal{C}_1$, e che quindi $\mathcal{C}_1$ non è aritmeticamente chiuso in $\mathfrak{C}_1$, onde $\mathcal{A}_1$ non è schiera massima di $\mathfrak{A}_1$ su I. Se fosse $\alpha_1 \in \mathcal{A}_1$, l'elemento $\beta\alpha_0\gamma = r\beta\alpha_0\beta^{-1} = r\alpha_1$ sarebbe divisibile per $r\delta_{A_1}$, nel senso della sezione 1 di [6], e quindi il suo kernel conterrebbe il kernel di $r\delta_{A_1}$; in particolare, esso conterrebbe un punto $Q \in A_1$ tale che $\gamma Q = P$; infatti, per ogni tale Q si ha $r\delta_{A_1}Q = \beta\gamma Q = \beta P = E_{A_1}$. Si deve perciò avere $\beta\alpha_0\gamma Q = E_{A_1}$; d'altra parte, $\beta\alpha_0\gamma Q = \beta\alpha_0 P \neq E_{A_1}$, poichè $\alpha_0 P \notin K$, c. v. d.

In conclusione, si può affermare che se A è non speciale, *cat* A è l'unione di due insiemi disgiunti M, N, tali che $\mathcal{A}_i$ è schiera massima di $\mathfrak{A}_i$ se e solo se $A_i \in M$; N è, in generale, non vuoto; infine, se due elementi A_i, A_j di M si dicono dello stesso *tipo* quando $\mathcal{A}_i \simeq \mathcal{A}_j$ su I, il contenuto del § 8, Cap. VI di [9] ci permette di affermare che *il numero dei tipi distinti in cui* M *è suddiviso è finito, ed eguale al numero dei tipi delle schiere massime di* $\mathfrak{A}$.

(4.4) TEOREMA. *Sia* A *varietà abeliana non speciale su* k, *e sia* $p > 0$; *suppongasi che* A *sia estensione su* k *di una varietà abeliana sopra un corpo assolutamente algebrico. Allora* $\mathfrak{A}(A)$ *ha ordine* > 1 *su* R, *e se* $\mathfrak{o}$ *è una sua schiera massima su* I, $p\mathfrak{o}$ *non è ideale primo.*

DIM. Se A è estensione su k di una varietà abeliana su un corpo assolutamente algebrico, essa è anche estensione su k di una varietà abeliana su un corpo finito C, contenente p^q elementi. È noto che l'essere o no p o ideale primo è indipendente dalla scelta di $\mathfrak{o}$; si può quindi supporre, per (4.2), che $\mathcal{A}(A)$ sia schiera massima, e che $\mathfrak{o} = \mathcal{A}(A)$. Il fatto che $A = B_k$, per una varietà abeliana B su C, mostra che $A^{p^q} \cong A$, ossia che $\delta_{q,A} \in \mathcal{A}(A)$; poichè il kernel $p\,\delta_A$ ha ordine > 1, ogni elemento $r\,\delta_A$ di $\mathcal{A}(A)$ (per r intero > 1) ha un kernel di ordine > 1, e quindi $\delta_{q,A}$ non è uno di essi. Ciò prova che $\mathbf{A}(A)$ ha ordine > 1 su R, come richiesto. Inoltre, se r è una potenza conveniente di p, $\delta_{q,A}$ divide $r\,\delta_A$, per esempio $r\,\delta_A = \delta_{q,\alpha A}\,\alpha$; suppongasi che r sia il minimo per cui ciò è vero; è certo $r > 1$. Allora, per ogni $\beta \in \mathcal{A}(A)$, $p\,\delta_A$ divide $\delta_{q,\beta\alpha A}\,\beta\,\alpha = \delta_{q,A}\,\beta\alpha$, il che prova che l'ideale bilatero intero $p\,\mathcal{A}(A)$ di $\mathcal{A}(A)$ divide il prodotto degli ideali bilateri interi $\mathcal{A}(A)\,\delta_{q,A}\,\mathcal{A}(A)$, $\mathcal{A}(A)\,\alpha\,\mathcal{A}(A)$; però, $p\,\mathcal{A}(A)$ non divide nessuno dei fattori, poichè nè $\delta_{q,A}$, nè α sono contenuti in $p\,\mathcal{A}(A)$; pertanto $p\,\mathcal{A}(A)$ non è un ideale primo di $\mathcal{A}(A)$, c. v. d.

Il risultato (4.2), qui provato per varietà abeliane non speciali, resta valido per varietà abeliane speciali; la sua dimostrazione, però, richiede allora l'uso di matrici p-adiche connesse agli omomorfismi del gruppo radicale G_r. Osserverò in ultimo che il (4.2), e varie sue conseguenze, fu dimostrato, per il caso delle curve ellittiche speciali o no, da M. Deuring nel 1941; per una esposizione elementare dei risultati di questo autore, vedasi ad esempio il suo articolo *La teoria aritmetica delle funzioni algebriche di una variabile* (Rend. di Mat. e Appl., 2, 1941, p. 361).

BIBLIOGRAFIA

[1] A. A. ALBERT, *Structure of algebras*, New York, 1939.

[2] I. BARSOTTI, *Local properties of algebraic correspondences*, Trans. Amer. Math. Soc., 71, 1951, p. 349.

[3] I. BARSOTTI, *A note on abelian varieties*, Rend. Circ. Mat. Palermo, 2, 1953, p. 236.

[4] I. BARSOTTI, *Il teorema di dualità per le varietà abeliane ed altri risultati*, Rend. di Mat. e Appl., 13, 1954, p. 98.

[5] I. BARSOTTI, *Factor sets and differentials on abelian varieties*, presentato all'Amer. Journ. of Math. nel luglio 1955; da pubblicarsi altrove.

[6] I. BARSOTTI, *Abelian varieties over fields of positive characteristic*, in corso di pubblicazione nei Rend. Circ. Mat. Palermo.

[7] I. S. COHEN, *On the structure and ideal theory of complete local rings*, Trans. Amer. Math. Soc., 59, 1946, p. 54.

[8] F. CONFORTO, *Funzioni abeliane e matrici di Riemann*, Roma, 1942.

[9] M. DEURING, *Algebren*, Erg. der Mat., 4, 1935.

[10] J. DIEUDONNÉ, *Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique* $p > 0$, Comm. Mat. Helv., 28, 1954, p. 87.

[11] J. DIEUDONNÉ, *Sur la notion de variables canoniques*, Anais Acad. Bras. Ciencias, 1955, p. 251.

[12] J. DIEUDONNÉ, *Lie groups and Lie hyperalgebras over a field of characteristic* $p > 0$ (II), Amer. Journ. of Math., 77, 1955, p. 218.

[13] H. MORIKAWA, *On abelian varieties*, Nagoya Math. Journ., 6, 1953, p. 151.

[14] A. WEIL, *Variétés abéliennes et courbes algébriques*, Paris, 1948.