Annali della
Scuola Normale Superiore di Pisa
Classe di Scienze

Iacopo Barsotti

Metodi analitici per varietà abeliane in caratteristica positiva. Capitoli 1, 2

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3e série, tome 18, nº 1 (1964), p. 1-25
<http://www.numdam.org/item?id=ASNSP_1964_3_18_1_1_0>

METODI ANALITICI PER VARIETÀ ABELIANE IN CARATTERISTICA POSITIVA. CAPITOLI 1, 2.

IACOPO BARSOTTI [1]

Introduzione. Inizio qui la pubblicazione dei dettagli di certi risultati che fino ad ora sono stati esposti solo in seminari e conferenze (seminario alla Brown University nell'estate 1961; N. S. F. Report del luglio 1961; corso alla Scuola Normale Superiore di Pisa nell'anno 1961-62; conferenza al Colloque sur la théorie des groupes algébriques tenuta a Bruxelles nel giugno 1962, e pubblicata a p. 77 del volume omonimo). Questa prima parte, che consta di due capitoli, sviluppa la teoria dei bivettori e i metodi analitici veri e propri; nei capitoli successivi si fa largo uso dei risultati di MC (*Moduli canonici e gruppi analitici commutativi,* di I. Barsotti; Ann. Scuola Norm. Sup. Pisa, 13, 1959, p. 303). Ad evitare troppi richiami alle definizioni, una lista alfabetica di queste, e dei simboli più usati, compare alla fine del presente lavoro.

Desidero ringraziare H. Matsumura, le cui critiche precise e fondate hanno valso ad eliminare vari errori dalla prima stesura di questi, ed altri, capitoli.

CAPITOLO 1.

I covettori.

1. In questo capitolo indicheremo sempre con I l'anello degli interi, con Q il corpo razionale, con p un primo razionale fisso, con I_p l'anello

Pervenuto alla Redazione il 17 Luglio 1963 ed in forma definitiva il 28 Gennaio 1964.

(1) Questa ricerca è stata sostenuta finanziariamente dai seguenti enti: National Science Foundation, col grant G 15983 (Brown University, 1961); C. O. N. A. R. M. (1962); Institut des hautes études scientifiques (Aprile 1963); Office of Aerospace Research, col grant AFEOAR 6329 (dal Dicembre 1962).

degli interi p-adici razionali, con C_p il corpo fondamentale di caratteristica p. Gli anelli considerati saranno sempre commutativi con identità; i moduli saranno unitari sinistri; le algebre saranno (salvo avvertimento in contrario) commutative, con identità, e unitarie. Con *topologia gruppale non archimedea* (su un gruppo abeliano additivo) si intenderà una topologia definita da un insieme di intorni aperti dello zero che siano sottogruppi, e la cui intersezione sia ridotta all'elemento 0; si tratta quindi di topologie di Hausdorff. Se A è un anello ed M un A-modulo, una topologia *A-lineare* di M è una topologia gruppale non archimedea determinata da un insieme di intorni aperti dello zero che siano sotto-A-moduli; ciò si applica in particolare alle topologie A-lineari di A, per le quali gli intorni saranno quindi ideali.

Nel seguito, se si hanno elementi x_i di un sopraanello di un anello B, si parlerà di « monomi nelle x_i, a coefficienti in B, di peso h, e divisibili per una certa x_j (o di grado positivo in x_j), quando alle x_i si attribuiscano i pesi h_i »; con tale locuzione imprecisa si intenderà una espressione $f(\dots, x_i, \dots)$, quando $f(\dots, X_i, \dots)$ sia un monomio nelle indeterminate X_i su B, a coefficienti in B, di peso h quando alle X_i si attribuiscano i pesi h_i, e divisibile per la X_j. Premettiamo anche che chiamiamo *monomio ammesso* nelle x_i un monomio il cui coefficiente sia il prodotto di un elemento di I_p per i reciproci dei fattoriali degli esponenti: $q\,[(r_0\,!) \dots (r_s\,!)]^{-1}\, x_0^{r_0} \dots x_s^{r_s}$, con $q \in I_p$. Si noti che in questa definizione ogni fattoriale può essere sostituito con la potenza di p che lo divide esattamente; ed è utile osservare che l'esponente con cui p compare in $r\,!$ è $(p-1)^{-1}\,[r - S(r)]$, ove $S(r)$ indica, come sempre nel seguito, la somma delle cifre del numero r espresso nel sistema p-esimale.

Sia A un'algebra su Q (risp. su C_p), dotata di una topologia I_p-lineare (risp. C_p-lineare), e siano $i \rightarrow x_{ji}$ $(i = -1, -2, \dots)$ delle successioni di elementi di A; si attribuisca peso p^i alle x_{ji}. Diremo che tali successioni sono *simultaneamente ammesse* (se ve n'è una sola diremo che essa è *ammessa*) se: per ogni intorno U dello 0, e per ogni intero $m \geq 0$, esiste un intero positivo r tale che siano in U tutti i monomi ammessi (risp. monici) nelle x_{ji}, di peso p^{-m}, ciascuno dei quali abbia grado positivo in qualche x_{ji} con $i \leq -r$. Diremo poi che la topologia è *ammessa* se successioni ammesse qualsiansi, in numero finito, sono simultaneamente ammesse.

1.1 LEMMA. *Siano X_i delle indeterminate su Q, ed Y_j dei polinomi nelle X_i, che siano somme di monomi ammessi di gradi positivi; sia Z un monomio ammesso nelle Y_j; allora Z è somma di monomi ammessi nelle X_i.*

DIM. Si può supporre $Z = \prod_j (s_j\,!)^{-1}\, Y_j^{s_j}$; sia poi $Y_j = \Sigma_h\, V_{jh}$, ove i V_{jh} sono monomi ammessi di grado positivo nelle X_i. Quando si computa $Y_j^{s_j}$, ogni monomio nelle X_i che vi compare è del tipo

$$(s_j!)\,[\prod_h (r_{jh}!)^{-1}\, V_{jh}^{r_{jh}}], \quad \text{ove} \quad \Sigma_h\, r_{jh} = s_j\,;$$

poichè si può anche supporre $V_{jh} = \prod_l (n_{jhl}!)^{-1}\, X_l^{n_{jhl}}$, ogni monomio nelle X_i che compare in Z è del tipo

$$\prod_j \prod_h (r_{jh}!)^{-1} \prod_l (n_{jhl}!)^{-r_{jh}}\, X_l^{n_{jhl}\, r_{jh}},$$

ove per ogni j, h almeno un n_{jhl} è positivo.

Per dimostrare che questo è ammesso basta dimostrare che $(nr)!$ è divisibile per $(n!)^r$ quando n, r sono interi non negativi, ed anche per $(r!)\,(n!)^r$ se $n > 0$. Ora, se $n = 0$ o $r = 0$ ciò è ovvio; se n, r sono positivi, siano $x_1, \dots, x_r$ indeterminate, e si consideri lo sviluppo di $(x_1 + \dots + x_r)^{rn}$; esso contiene il termine $[(rn)!/(n!)^r]\,(x_1 \dots x_r)^n$, cosicchè $(rn)!$ è divisibile per $(n!)^r$. Poichè tale termine è invariante per tutte le permutazioni delle x_i, il suo coefficiente deve essere divisibile per $r!$, C. V. D..

2. È opportuno familiarizzarsi con le topologie di uso più frequente nel seguito. Chiameremo intanto *pseudovalutazione* di un anello R un'applicazione $x \longrightarrow w(x)$ di R su $\Gamma \cup \{\infty\}$ (Γ essendo l'insieme degli elementi non negativi di un gruppo ordinato addittivo) che soddisfi agli assiomi: $w(x+y) \geq \min(w(x), w(y))$, $w(xy) = w(x) + w(y)$, $w(1) = 0$, $w(0) = \infty$; ad una pseudovalutazione applicheremo la stessa nomenclatura che si applica ad una valutazione.

1.2 Lemma. *Sia R un anello di caratteristica p; siano w_r, $r \in \mathcal{I}$, sue pseudovalutazioni di rango ≤ 1, tali che $w_i(x) = \infty$ per ogni i solo se $x = 0$. Si munisca R della topologia R-lineare definita dal sistema di intorni dello* 0 *i cui elementi sono gli $U(r_1, \dots, r_h; s_1, \dots, s_h)$, con $r_1, \dots, r_h \in \mathcal{I}$, così definiti: $y \in U(r_1, \dots, r_h; s_1, \dots, s_h)$ se e solo se $w_{r_i}(y) \geq s_i$ (gli s_i sono reali non negativi). Siano $j \longrightarrow x_{ij}$ ($j = -1, -2, \dots$) successioni di elementi di R; sia $n \longrightarrow \alpha_r(n)$ la massima applicazione monotona non decrescente dell'insieme degli interi positivi sull'insieme dei reali non negativi, e dell'elemento ∞, che soddisfa la $\alpha_r(n) \leq p^n\, w_r(x_{i,-n})$ per ogni i; in altre parole, sia $\alpha_r(n) =$* estr inf *$p^j\, w_r(x_{i,-j})$, per i qualsiasi e $j \geq n$. Allora le $j \longrightarrow x_{ij}$ sono simultaneamente ammesse se e solo se tutte le serie $\sum_{1}^{\infty}{}_n\, p^{-n}\, \alpha_r(n)$ sono divergenti.*

Dim. Per semplificare le notazioni daremo la dimostrazione nel caso in cui vi sia una sola w_i, che chiameremo w, ed una sola successione, che chiameremo $j \longrightarrow x_j$; le modifiche da fare nel caso generale sono facili e non essenziali. Vi sarà anche una sola applicazione α_r, che chiameremo α. Anzitutto definiremo $\alpha(0) = 0$, e definiremo anche, per ogni $m > 0$, la applicazione β_m così: è la massima applicazione monotona non decrescente dell'insieme $\{0, \dots, m\}$ sui reali non negativi, e sull'elemento ∞, che soddisfa le $\beta_m(0) = 0$, $\beta_m(i) \leq p^i w(x_{-i})$ per $0 < i \leq m$. Si ha $\beta_m(i) \geq \alpha(i)$ per $0 < i \leq m$; inoltre, $\beta_m(i) = p^i w(x_{-i})$ per certi valori di i, che chiameremo $r_1 < r_2 < \dots < r_h$; è certamente $r_h = m$; definiremo anche $r_0 = 0$ per comodità.

I monomi monici nelle x_j, di peso 1, e divisibili per x_{-m}, sono gli $M_s = x_{-m}^{s_m} x_{-m+1}^{s_{m-1}} \dots x_{-1}^{s_1}$, ove (1) gli s_i sono interi non negativi, (2) $s_m > 0$, e (3) $\Sigma_i s_i p^{-i} = 1$. Si ha $w(M_s) = s_m w(x_{-m}) + \dots + s_1 w(x_{-1}) \geq s_m p^{-m} \beta_m(m) + \dots + s_1 p^{-1} \beta_m(1) = z_m(s)$. Vogliamo trovare il minimo di $z_m(s)$; a tal uopo, ordiniamo lessicograficamente l'insieme degli $s = (s_m, \dots, s_1)$, e osserviamo che il successore di un s (se esiste) si ottiene aumentando l'ultimo s_i (ossia quello col minimo i) passibile di essere aumentato senza toccare gli s_j che lo precedono, e diminuendo degli s_j con $j < i$ in maniera che la somma $\sum_{1}^{i}{}_r s_r p^{-r}$ rimanga invariata. Tale operazione aumenta però, o lascia invariata, la somma $\sum_{1}^{i}{}_r s_r p^{-r} \beta_m(r)$, cosicchè si può concludere che il minimo di $z_m(s)$ è raggiunto per il minimo s, che è $S_m = (p, p-1, p-1, \dots, p-1)$; tale valore di z_m è $z_m(S_m) = p^{-m} \beta_m(m) + (p-1) \sum_{1}^{m}{}_i p^{-i} \beta_m(i)$. Il minimo dei valori $w(M_s)$ sarà $\geq z_m(S_m)$, ed $= z_m(S_m)$ se questo è uno dei valori che $w(M_s)$ può assumere; dimostreremo che questo è proprio il caso. Se infatti si prendono tutti gli s_i eguali a 0, eccetto gli s_{r_j} $(j > 0)$, che vengono presi eguali a $p^{r_j - r_{j-1}} - 1$ se $j < h$, mentre $s_{r_h} = s_m = p^{m - r_{h-1}}$, si ha che $w(M_s) = w(x_{-m}) + \sum_{1}^{h}{}_i (p^{r_i - r_{i-1}} - 1) w(x_{-r_i}) = p^{-m} \beta_m(m) + \sum_{1}^{h}{}_i (p^{r_i - r_{i-1}} - 1) p^{-r_i} \beta_m(r_i)$. Osservando poi che $\beta_m(j) = \beta_m(r_i)$ se $r_{i-1} < j \leq r_i$ $(i = 1, \dots, h)$, si ha $(p^{r_i - r_{i-1}} - 1) p^{-r_i} \beta_m(r_i) = (p-1) \Sigma_j p^{-j} \beta_m(j)$, ove la sommatoria si estende da $r_{i-1} + 1$ ad r_i; pertanto $w(M_s) = z_m(S_m)$, come annunciato.

È ora chiaro che condizione necessaria e sufficiente acchè la $j \to x_j$ soddisfi, per i monomi di peso 1, la condizione per l'ammissibilità, è che $\lim_{m \to \infty} z_m(S_m) = \infty$; il termine $p^{-m} \beta_m(m)$ non ha evidentemente influenza sulla divergenza di $z_m(S_m)$, e quindi la condizione diviene

1.3 $$\lim_{m \to \infty} \sum_{1}^{m}{}_i p^{-i} \beta_m(i) = \infty;$$

ora, è certo $\sum_{1}^{m}{}_i p^{-i} \beta_m(i) \geq \sum_{1}^{m}{}_i p^{-i} \alpha(i)$, cosicchè la divergenza della serie

$\sum_1^m {}_i\, p^{-i} \alpha(i)$ è condizione sufficiente per l'ammissibilità, finchè si resta ai monomi di peso 1; d'altra parte, se la condizione per l'ammissibilità è soddisfatta, la $i \longrightarrow \alpha(i)$ non può intanto rimanere costante e finita per valori elevati di i, in quanto $\lim_{n \to \infty} p^n w(x_{-n}) = \infty$; quindi, se $\alpha(i)$ rimane finita, vi sono infiniti valori di m tali che $\alpha(m) < \alpha(m+1)$; e per ciascun tale valore di m si ha $\alpha(m) = p^m w(x_{-m})$, onde $\beta_m(i) = \alpha(i)$ per $0 < i \leq m$. Se perciò è verificata la 1.3, è anche verificata la $\sum_1^\infty {}_i\, p^{-i} \alpha(i) = \infty$, come detto nell'enunciato. Il risultato è così dimostrato per quanto riguarda i monomi di peso 1; si vede però subito che la considerazione dei monomi di peso p^{-r} dà luogo alla stessa condizione, C. V. D..

1.4 COROLLARIO. *Ipotesi come nell'*1.2*; suppongasi inoltre che le w_i siano tutte discrete. Allora la topologia è ammessa, e una successione $j \longrightarrow x_j$ è ammessa se e solo se per ogni i esiste un n tale che $w_i(x_{-j}) > 0$ per $j > n$.*

DIM. Per dimostrare l'ultima asserzione, si osservi che essendo la w_i discreta si ha, per un dato i, o $w_i(x_{-j}) = 0$ per infiniti valori di j, ovvero $w_i(x_{-j}) \geq 1$ per j elevato. Nel primo caso è $\alpha_i(n) = 0$ per ogni n, e quindi, per 1.2, la successione non è ammessa; nel secondo caso è $\alpha_i(n) \geq p^n$ per n elevato, e quindi la serie dell'1.2 diverge e la successione è ammessa. La prima asserzione discende ora subito da questo criterio, C. V. D..

1.5 COROLLARIO. *Ipotesi come nell'*1.2*; suppongasi che talune delle w_i non siano discrete. Allora la topologia di R può non essere ammessa, ed è certamente non ammessa se l'insieme delle pseudovalutazioni si riduce ad un solo elemento, ed R contiene elementi di valore p^{-i} per ogni intero non negativo i. In ogni caso è però simultaneamente ammesso un qualsiasi insieme finito di successioni ciascuna delle quali soddisfi la condizione seguente: se $j \longrightarrow x_j$ è la successione, per ogni i esiste un $\beta_i > 0$ tale che $w_i(x_{-j}) \geq \beta_i$ per j elevato; in altre parole, $\lim_{n \to \infty} \operatorname{estr\,inf}_{j \geq n} w_i(x_{-j}) > 0$.*

DIM. Dimostriamo la seconda asserzione: la condizione posta assicura che $\alpha_i(n) \geq p^n \beta_i$ per n elevato, onde la serie dell'1.2 diverge; se vi è più di una successione, basta usare, per ogni i, il minimo fra i β_i delle varie successioni.

Per dimostrare la prima asserzione supporremo che vi sia una sola pseudovalutazione w (che sarà quindi una valutazione), e che questa soddisfi alla condizione descritta. Daremo un esempio di due successioni ammesse ma non simultaneamente ammesse. La prima successione $j \longrightarrow x_j$ sia tale che per $2^{2n} \leq i < 2^{2n+2}$ $(n = 0, 1, 2, \ldots)$ si abbia $w(x_{-i}) = p^{2^{2n}-i}$; si ha allora, per gli stessi valori di i, $\alpha(i) = p^{2^{2n}}$. La seconda successione, $j \to y_j$, sia tale che per $2^{2n-1} \leq i < 2^{2n+1}$ $(n = 0, 1, 2, \ldots)$ si abbia $w(y_{-i}) = p^{2^{2n-1}-i}$, onde (scrivendo β in luogo di α) è $\beta(i) = p^{2^{2n-1}}$ per i detti valori di i. Le serie dell'1.2, per le due successioni, sono rispettivamente

$$\sum_1^\infty{}_i\, p^{-i}\alpha(i) = \sum_0^\infty{}_n\, p^{2^{2n}} \Sigma'_i\, p^{-i} = \sum_0^\infty{}_n (1 - p^{-1})^{-1}(1 - p^{-3\cdot 2^{2n}}),$$

e

$$\sum_1^\infty{}_i\, p^{-i}\beta(i) = p^{-1/2} + \sum_1^\infty{}_n\, p^{2^{2n-1}} \Sigma''_i\, p^{-i} =$$

$$= p^{-1/2} + \sum_1^\infty{}_n (1 - p^{-1})^{-1}(1 - p^{-3\cdot 2^{2n-1}});$$

qui, Σ' indica somma da 2^{2n} a $2^{2n+2} - 1$, mentre Σ'' indica somma da 2^{2n-1} a $2^{2n+1} - 1$. Queste serie sono ambedue divergenti, e le successioni sono ammesse.

L'α per la coppia di successioni, che sarà indicata con γ, è data da $\gamma(i) = p^{2^{n-1}}$ se $2^n \leq i < 2^{n+1}$; la relativa serie è

$$\sum_1^\infty{}_i\, p^{-i}\gamma(i) = \sum_0^\infty{}_n\, p^{2^{n-1}} \Sigma^*_i\, p^{-i} = (1 - p^{-1})^{-1} \sum_0^\infty{}_n (p^{-2^{n-1}} - p^{-3\cdot 2^{n-1}}),$$

ove Σ^* indica somma da 2^n a $2^{n+1} - 1$. Poichè questa è convergente, le due successioni non sono simultaneamente ammesse, C. V. D..

3. Si definiscano le funzioni razionali intere f_i $(i = 0, 1, \ldots)$ di $i + 1$ argomenti, a coefficienti in Q, per mezzo delle

1.6
$$\begin{aligned} Y_0 &= f_0(Y) \\ Y_1 &= f_1(Y_1, Y_0) + p^{-1}[f_0(Y_0)]^p \\ Y_2 &= f_2(Y_2, Y_1, Y_0) + p^{-1}[f_1(Y_1, Y_0)]^p + p^{-2}[f_0(Y_0)]^{p^2} \\ &\ldots\ldots\ldots\ldots, \end{aligned}$$

ove le Y_i formano un insieme di indeterminate su Q. Pongasi, per $i = 1, 2, \ldots$:

1.7
$$\psi_i(Y_{i-1}, \ldots, Y_0) = f_i(Y_i, \ldots, Y_0) - f_{i-1}(Y_i, \ldots, Y_1),$$

cosicchè

1.8
$$\psi_i(pY_{i-1}, \ldots, pY_0) \in pI[Y_{i-1}, \ldots, Y_0].$$

Si ha:

1.9 LEMMA. *$\psi_i(Y_{i-1}, \ldots, Y_0)$ è divisibile per Y_0, ed è isobarico di peso p^i quando ad Y_j si attribuisca il peso p^j; ogni monomio che compare in ψ_i ha grado maggiore di $(p-1)i$. Ed il monomio $Y_0^{r_0} \ldots Y_{i-1}^{r_{i-1}}$ compare in ψ_i con coefficiente del tipo $[(r_0!) \ldots (r_{i-1}!)]^{-1} m$, ove $m \in I$.*

DIM. L'asserzione della isobaricità è ovvia; inoltre, facendo $Y_0 = 0$ nelle 1.6 si ottiene che $f_i(Y_i, \ldots, Y_1, 0) = f_{i-1}(Y_i, \ldots, Y_1)$, il che prova la prima asserzione. L'asserzione sul grado discende dalle due precedenti, in quanto per ottenere un monomio di minimo grado, di peso p^i, e divisibile per Y_0, si deve dare esponente $p-1$ ad $Y_{i-1}, Y_{i-2}, \ldots, Y_1$, ed esponente p ad Y_0.

Resta da dimostrare l'ultima asserzione, e questa basta provarla per $f_i(Y_i, \ldots, Y_0)$. Ciò sarà fatto per induzione su i, dato che essa è vera per $i = 0$. Sia D_i la derivazione $\partial/\partial Y_i$, e sia σ l'omomorfismo di $Q[Y]$ che applica ogni Y_j sullo 0; sia $bY_0^{r_0} \ldots Y_{i-1}^{r_{i-1}}$ il monomio considerato; se esso si riduce a bY_i, la i-esima fra le 1.6 dice subito che $b = 1$; altrimenti, l'applicazione di $\sigma D_0^{r_0} \ldots D_{i-1}^{r_{i-1}}$ alla i-esima fra le 1.6 dà che $b(r_0!) \ldots (r_{i-1}!)$ è una somma di termini del tipo

$$(p^j - 1)!\,[\sigma\Delta_1 f_{i-j}(Y_{i-j}, \ldots, Y_0)] \ldots [\sigma\Delta_{p^j} f_{i-j}(Y_{i-j}, \ldots, Y_0)],$$

con $j = 1, \ldots, i$, e ove i Δ_h sono monomi monici nelle $D_1, D_2, \ldots$, il cui prodotto è $D_0^{r_0} \ldots D_{i-1}^{r_{i-1}}$. Ora, per l'ipotesi di ricorrenza, ciascuna delle espressioni in parentesi quadra è un intero, C. V. D..

Un gruppo addittivo topologico G sarà detto *quasi completo* se ogni successione di Cauchy $i \longrightarrow g_i$ $(i = 1, 2, \ldots)$ di elementi di G converge ad un elemento di G. Se la topologia è numerabile, ossia determinata da un insieme numerabile di intorni dello 0, o equivalentemente se essa è determinata da una metrica, G è quasi completo se e solo se è completo. In generale, il *quasi completamento* di G è l'insieme G' dei limiti, nel completamento di G, delle successioni di Cauchy di elementi di G; G' è quasi completo.

1.10 TEOREMA. *Sia A un'algebra su Q, quasi completa rispetto ad una topologia I_p-lineare; sia $i \longrightarrow x_i$ $(i = -1, -2, \ldots)$ una successione ammessa di elementi di A, e pongasi, per $i = -1, -2, \ldots$:*

(a) $$y_i = x_i + p^{-1} x_{i-1}^p + p^{-2} x_{i-2}^{p^2} + \ldots$$

Allora la $i \longrightarrow y_i$ è ammessa, e si ha:

(b) $$x_i = y_i + \psi_1(y_{i-1}) + \psi_2(y_{i-1}, y_{i-2}) + \ldots$$

Reciprocamente, se $i \longrightarrow y_i$ è una qualsiasi successione ammessa di elementi di A, e se le x_i sono date da (b), *la $i \longrightarrow x_i$ è ammessa e la* (a) *è valida.*

DIM. La convergenza delle (a) è ovvia, essendo la $i \longrightarrow x_i$ ammessa; quella delle (b) è conseguenza di 1.9.

Suppongasi ora che la $i \longrightarrow x_i$ sia ammessa; un monomio ammesso di peso p^{-h} nelle y_i è, per la (a) e l'1.1, limite di somme di monomi ammessi dello stesso peso nelle x_j; e se esso contiene (con esponente positivo) delle y_i con i elevato, ogni termine di tali somme contiene, per la (a), delle x_j con j elevato; quindi la $j \longrightarrow y_j$ è ammessa.

Il reciproco, ossia l'essere la $i \longrightarrow x_i$ ammessa quando lo è la $j \longrightarrow y_j$, si dimostra nello stesso modo, usando le (b), 1.1 e 1.9.

Si considerino ora le indeterminate $Y_{-1}, Y_{-2}, \ldots$ su Q e si scriva, in analogia alle 1.6:

$$Y_{-i} = f_0(Y_{-i})$$

$$Y_{-i+1} = f_1(Y_{-i+1}, Y_{-i}) + p^{-1}[f_0(Y_{-i})]^p$$

$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$

$$Y_{-1} = f_{i-1}(Y_{-1}, \ldots, Y_{-i}) + p^{-1}[f_{i-2}(Y_{-2}, \ldots, Y_{-i})]^p + \ldots$$
$$+ p^{-i+1}[f_0(Y_{-i})]^{p^{i-1}}.$$

Supposta la $i \longrightarrow y_i$ ammessa, si fissi un intorno U dello 0, e si scelga i in modo che siano in U i monomi ammessi di peso p^{-1} nelle y_j, di grado positivo in qualche y_{-s} con $s > i$. Si ha, dalle relazioni precedenti:

$$y_{-1} = f_{i-1}(y_{-1}, \ldots, y_{-i}) + p^{-1}[f_{i-2}(y_{-2}, \ldots, y_{-i})]^p + \ldots$$
$$+ p^{-i+1}[f_0(y_{-i})]^{p^{i-1}}.$$

Per l'ipotesi su i, e per 1.7, 1.9, 1.1, si constata che

$$p^{1-r}[f_{i-r}(y_{-r}, \ldots, y_{-i})]^{p^{r-1}} =$$

$$p^{1-r}[y_{-r} + \psi_1(y_{-r-1}) + \psi_2(y_{-r-1}, y_{-r-2}) + \ldots + \psi_{i-r}(y_{-r-1}, \ldots, y_{-i})]^{p^{r-1}}$$

differisce dalla $p^{1-r} x_{-r}^{p^{r-1}}$ di (b) per un elemento di U; pertanto vale la (a).

Sia invece data la $i \longrightarrow x_i$, ammessa, e si definiscano le funzioni razionali intere g_i $(i = 0, 1, \ldots)$ di $i+1$ argomenti, a coefficienti in Q, per mezzo delle:

$$X_0 = g_0(X_0)$$
$$X_1 = g_1(X_1, X_0) + \psi_1(g_0(X_0))$$
$$X_2 = g_2(X_2, X_1, X_0) + \psi_1(g_1(X_1, X_0)) + \psi_2(g_1(X_1, X_0), g_0(X_0))$$
$$\dots\dots\dots\dots\dots ,$$

ove le X_j formano un insieme di indeterminate su Q. Queste si scrivono anche, per la 1.7:

$$X_0 = f_0(g_0(X_0))$$
$$X_1 = f_1(g_1(X_1, X_0), g_0(X_0))$$
$$X_2 = f_2(g_2(X_2, X_1, X_0), g_1(X_1, X_0), g_0(X_0))$$
$$\dots\dots\dots\dots\dots ,$$

e dimostrano che le applicazioni

$$\{X_0, \dots, X_i\} \to \{g_0(X_0), \dots, g_i(X_i, \dots, X_0)\}$$

e

$$\{Y_0, \dots, Y_i\} \to \{f_0(Y_0), \dots, f_i(Y_i, \dots, Y_0)\}$$

sono reciproche l'una dell'altra. Ma la reciproca della seconda applicazione è anche fornita dalla 1.6, il che dimostra che

$$g_i(X_i, \dots, X_0) = X_i + p^{-1} X_{i-1}^p + \dots + p^{-i} X_0^{p^i}.$$

Si può quindi ripetere il ragionamento precedente, dopo aver scambiato le y_j con le x_j, le f_j con le g_j, e, come si è visto, le $\psi_i(y_{-r}, y_{-r-1}, \dots, y_{-r-i+1})$ con le $p^{-i} x_{-r-i+1}^{p^i}$. Il risultato è che se le y_j sono date da (a), esse soddisfano la (b), C. V. D..

4. Sia $\{X_0, X_1, \dots; Y_0, Y_1, \dots\}$ un insieme di indeterminate su Q; dalla teoria dei vettori di Witt è nota l'esistenza di funzioni razionali intere φ_i' $(i = 0, 1, \dots)$ di $2i + 2$ argomenti, a coefficienti interi, tali che, in notazioni di vettori di Witt, si abbia $(X_0, X_1, \dots) + (Y_0, Y_1, \dots) = (\varphi_0'(X_0; Y_0), \varphi_1'(X_1, X_0; Y_1, Y_0), \dots)$; ciò equivale a dire che per $n = 0, 1, \dots$ si ha:

$$\sum_0^n{}_i\, p^{-i} X_{n-i}^{p^i} + \sum_0^n{}_i\, p^{-i} Y_{n-i}^{p^i} = \sum_0^n{}_i\, p^{-i} [\varphi_{n-i}'(X_{n-i}, \dots, X_0; Y_{n-i}, \dots, Y_0)]^{p^i}.$$

Pongasi, per $i = 1, 2, \ldots$,

$$\varphi_i(X_{i-1}, \ldots, X_0 ; \; Y_{i-1}, \ldots, Y_0) = \varphi'_i(X_i, \ldots, X_0 ; \; Y_i, \ldots, Y_0) -$$

$$- \varphi'_{i-1}(X_i, \ldots, X_1 ; \; Y_i, \ldots, Y_1) ;$$

è ben noto che se ad X_j ed Y_j si attribuisce il peso p^j, la $\varphi_i(X_{i-1}, \ldots, X_0 ; Y_{i-1}, \ldots, Y_0)$ è isobara di peso p^i; inoltre essa è divisibile per $X_0 Y_0$. Porremo poi $\varphi_0(X_0 ; Y_0) = \varphi'_0(X_0 ; Y_0) = X_0 + Y_0$, ed useremo gli stessi simboli per indicare le funzioni razionali intere ottenute riducendo i coefficienti di queste modulo p.

Per il seguito faremo la seguente convenzione: se $i \longrightarrow x_i$ è ammessa, l'elemento y_i dato dalla (a) di 1.10 sarà indicato con $x^{(i)}$; se poi è data una $i \longrightarrow x^{(i)}$ ammessa, le x_i saranno ottenute dalle $x^{(j)}$ come nella (b) di 1.10, quando in essa si legga $x^{(j)}$ in luogo di y_j.

1.11 TEOREMA. *Le φ_i sono le uniche funzioni razionali intere che soddisfano alle condizioni seguenti:*

1. $\varphi_i(X_{i-1}, \ldots, X_0 ; \; Y_{i-1}, \ldots, Y_0)$ *è divisibile per $X_0 Y_0$ quando $i > 0$ (qui, le X_j, Y_j sono indeterminate);*

2. *Per ogni algebra A su Q, o risp. su C_p, che sia quasi completa rispetto ad una topologia I_p-lineare, o risp. C_p-lineare, e per ogni coppia $i \longrightarrow x_i$, $i \longrightarrow y_i$ di successioni simultaneamente ammesse di elementi di A (ove $i = -1, -2, \ldots$), la*

$$\varphi_0(x_{-1} ; \; y_{-1}) + \sum_1^{\infty} {}_i\, \varphi_i(x_{-2}, \ldots, x_{-i-1} ; \; y_{-2}, \ldots, y_{-i-1})$$

converge ad un elemento $\Phi(x_{-1}, x_{-2}, \ldots ; \; y_{-1}, y_{-2}, \ldots)$ di A (e questa è la definizione di Φ);

3. *Nelle ipotesi di 2, e quando A è un'algebra su Q, posto $z_{-i} = \Phi(x_{-i}, x_{-i-1}, \ldots ; y_{-i}, y_{-i-1}, \ldots)$, la $i \longrightarrow z_i$ è ammessa e si ha $z^{(i)} = x^{(i)} + y^{(i)}$.*

Se poi si ha un insieme S di successioni simultaneamente ammesse, e se S contiene le $i \longrightarrow x_i$ ed $i \longrightarrow y_i$, anche l'insieme ottenuto aggiungendo ad S la $i \longrightarrow z_i$ consta di successioni simultaneamente ammesse.

DIM. Dimostriamo dapprima l'unicità, ammessa l'esistenza di funzioni φ_i (non necessariamente quelle definite più sopra) che soddisfino le 1, 2, 3. Sia A un prolungamento di trascendenza infinita di Q, con la topologia discreta. Se x_{-1}, y_{-1} sono elementi di A, algebricamente indipendenti su Q, le successioni $\{x_{-1}, 0, 0, \ldots\}$, $\{y_{-1}, 0, 0, \ldots\}$ sono simultaneamente ammesse, e le 1, 2, 3 dicono subito che $\varphi_0(x_{-1} ; \; y_{-1}) = x_{-1} + y_{-1}$, come voluto.

Suppongasi poi che la unicità delle $\varphi_0, \dots, \varphi_{n-1}$ sia stata dimostrata, e si considerino le successioni simultaneamente ammesse $\{x_{-1}, \dots, x_{-n-1}, 0, 0, \dots\}$, $\{y_{-1}, \dots, y_{-n-1}, 0, 0, \dots\}$, con le x_i, y_j algebricamente indipendenti su Q. Le 1, 2, 3 comportano allora che, in notazioni di vettori di Witt, $(x_{-n-1}, \dots, x_{-1}) + (y_{-n-1}, \dots, y_{-1}) = (z_{-n-1}, \dots, z_{-1})$; ciò dimostra che anche φ_n deve essere quella sopra definita.

Resta da dimostrare che le φ_i introdotte soddisfano le 1, 2, 3; ora, la 1 si è visto essere vera, e la 2 discende dall'essere le $i \to x_i$, $i \to y_i$ simultaneamente ammesse. Quanto alla 3, si ha intanto che, nelle notazioni della dimostrazione dell'1.10, è

$$g_n(x_{-1}, \dots, x_{-n-1}) + g_n(y_{-1}, \dots, y_{-n-1}) = g_n(\varphi'_n, \dots, \varphi'_0),$$

ove φ'_{n-i} sta per $\varphi'_{n-i}(x_{-i-i}, \dots, x_{-n-1}; y_{-i-1}, \dots, y_{-n-1})$.

Si consideri la differenza $g_n(\varphi'_n, \dots, \varphi'_0) - g_m(\varphi'_n, \dots, \varphi'_{n-m})$, ove $n > m$; essa è data da $p^{-m-1}\varphi'^{p^{m+1}}_{n-m-1} + \dots + p^{-n}\varphi'^{p^n}_0$; ora, per la 1 dell'1.11, già dimostrata, φ'_{n-i} è somma di x_{-i-1}, y_{-i-1}, e di termini ciascuno dei quali è divisibile per $x_{-j}y_{-j}$, ove j varia fra $-i-2$ e $-n-1$. Pertanto, dato un intorno U dello 0, esiste un m tale che per $n > m$ l'elemento $g_n(\varphi'_n, \dots, \varphi'_0)$ differisce per un elemento di U da $g_m(\varphi'_n, \dots, \varphi'_{n-m})$; quindi, facendo $n \to \infty$, la relazione precedente mostra che $x^{(-1)} + y^{(-1)}$ differisce per un elemento di U da $g_m(z_{-1}, \dots, z_{-m-1})$. Se ora si fa $m \to \infty$ ne segue $x^{(-1)} + y^{(-1)} = z^{(-1)}$, come voluto. L'ultima asserzione è ora evidente, C. V. D..

5. Sia A un'algebra su Q, ovvero su C_p, quasi completa rispetto ad una topologia I_p-lineare, o rispettivamente C_p-lineare. Una successione ammessa $i \to x_i$ $(i = -1, -2, \dots)$ sarà anche chiamata un *covettore* (di Witt), e indicata con $x = (\dots, x_{-2}, x_{-1})$; le x_i ne sono le *componenti*, e nel caso delle algebre su Q le $x^{(i)}$ ne sono le *componenti fantasma*; la stessa nomenclatura si usa per una qualsiasi I-algebra A che sia sottoalgebra di una Q-algebra.

Se due covettori x, y sono simultaneamente ammessi, si può definire il covettore z dato da: $z_{-i} = \Phi(x_{-i}, x_{-i-1}, \dots; y_{-i}, y_{-i-1}, \dots)$; tale z sarà indicato con $x + y$. Vogliamo dimostrare che l'operazione $+$ gode, quando è definita, delle proprietà dell'operazione di composizione in un gruppo abeliano (additivo), lo 0 essendo $(\dots, 0, 0)$; e in particolare che $-x$ esiste per ogni covettore x. Queste asserzioni sono ovvie, per 1.11, quando A sia un'algebra su Q, o una sotto-I-algebra di una tale algebra; nel caso di un'algebra su C_p, esse possono essere dimostrate col metodo di riduzione mod p, di cui daremo un esempio nel dimostrare l'associatività.

Siano x, y, z covettori simultaneamente ammessi a componenti nell'algebra A su C_p; si considerino indeterminate X_{-i}, Y_{-i}, Z_{-i} ($i = 1, 2, ...$) su Q, e si dia peso p^{-i} ad $x_{-i}, y_{-i}, z_{-i}, X_{-i}, Y_{-i}, Z_{-i}$. Si doti $Q[X, Y, Z]$ della topologia così definita : se la topologia di A è discreta, anche $Q[X, Y, Z]$ viene dotato della topologia discreta; se la topologia di A non è discreta, per ogni intorno U dello 0 in A, e per ogni intero non negativo n si scelga un intero positivo $m = m(U, n)$ tale che siano in U tutti i monomi monici di peso p^{-n} nelle x_i, y_i, z_i, ciascuno dei quali abbia grado positivo in almeno una x_i, o y_i, o z_i con $i \leq -m$; e si scelga questo $m(U, n)$ in modo che non esista nessuna coppia $\{n, N\}$ di interi tale che $m(U, n) < N$ per ogni U (ciò è possibile non appena l'insieme degli U è infinito). Si indichi con U' il sotto-I_p-modulo di $Q[X, Y, Z]$ generato da tutti i monomi ammessi nelle X_i, Y_i, Z_i ciascuno dei quali (1) ha peso p^{-n} per qualche n, e (2) è divisibile per qualche X_i, o Y_i, o Z_i con $i \leq -m(U, n)$. Gli U', presi come intorni dello 0, determinano in $Q[X, Y, Z]$ una topologia che rende continuo l'omomorfismo σ di $I_p[X, Y, Z]$ su $F' = C_p[x, y, z]$ che applica X_i, Y_i, Z_i rispettivamente su x_i, y_i, z_i, e che applica I_p su tutto C_p secondo l'omomorfismo naturale. Quindi σ può essere esteso ad un omomorfismo continuo, ancora indicato con σ, del quasi completamento B di $I_p[X, Y, Z]$ sulla chiusura F di F' in A; inoltre B è sottoanello del quasi completamento B' di $Q[X, Y, Z]$, e quest'ultimo è un'algebra su Q. Le successioni $i \longrightarrow X_i$, $i \longrightarrow Y_i$, $i \longrightarrow Z_i$ sono simultaneamente ammesse, e si possono considerare i covettori $X = (..., X_{-2}, X_{-1})$, Y, Z, per i quali si ha $(X + Y) + Z = X + (Y + Z)$. Applicando σ si ottiene $(x + y) + z = x + (y + z)$, come richiesto. Si noti che qualunque sia il covettore x, l'elemento $-x$ esiste sempre, e gli elementi x, $-x$ sono simultaneamente ammessi.

Nel seguito supporremo d'aver scelto un insieme di covettori a componenti in A, tali che (1) un numero finito di essi siano sempre simultaneate ammessi, (2) essi formino un gruppo additivo, e (3) tale insieme contenga tutti i covettori aventi una sola componente non nulla; una ulteriore condizione sarà imposta al n⁰ 6. Tale insieme sarà indicato con $\operatorname{cov} A$. Per quanto precede, se la topologia di A è ammessa si può prendere per $\operatorname{cov} A$ l'insieme di tutti i covettori a componenti in A; e per l'1.5, se la topologia è quella descritta nell'1.2, si può scegliere per $\operatorname{cov} A$ l'insieme degli x tali che: per ogni i, i w_i-valori degli x_{-j} con j elevato sono inferiormente limitati da un $\beta_i > 0$.

6. Per ogni covettore x, esiste il covettore tx definito da : $(tx)_i = x_{i-1}$; se poi l'applicazione $\pi : a \longrightarrow a^p$ di A su se stesso è continua, per ogni covettore x esiste anche il covettore πx definito da: $(\pi x)_i = \pi(x_i) = x_i^p$. Si

scriverà talvolta x^t, x^π in luogo di tx, πx; t è un endomorfismo rispetto all'operazione $+$, e π è tale quando A è algebra su C_p; è poi $t\pi = \pi t$. Quando A è un'algebra su Q, si ha anche $(tx)^{(i)} = x^{(i-1)}$, $(\pi x)^{(i)} = p\,(x^{(i+1)} - x_{i+1})$, ove si dia valore arbitrario ad x_0. Quindi è anche

$$(t\pi x)^{(i)} = px^{(i)} - px_i = (px)^{(i)} - px_i\,;$$

a questa si può applicare il metodo del n^0 5 per ottenere un risultato valido quando A abbia caratteristica p; tenendo conto della 1.8, il risultato è:

1.12 Teorema. *Se A è un'algebra su C_p, quasi completa rispetto ad una topologia C_p-lineare, e se π è un'applicazione continua di A, per ogni covettore x a componenti in A si ha $t\pi x = px$.*

Nel seguito, supporremo anche che $\operatorname{cov} A$ sia tale che $t \operatorname{cov} A \subseteq \operatorname{cov} A$, e che $\pi \operatorname{cov} A \subseteq \operatorname{cov} A$ se π è applicazione continua di A; questo è automaticamente il caso quando $\operatorname{cov} A$ è scelto come alla fine del n^0 5.

7. Sia A un anello di caratteristica p, quasi completo rispetto ad una topologia A-lineare; se U è un intorno dello 0 in A, indicheremo con U' l'insime degli $x \in \operatorname{cov} A$ tali che $x_i \in U$ per ogni valore di i; gli U' sono sottogruppi di $\operatorname{cov} A$, e se vengono presi come intorni dello 0 determinano in $\operatorname{cov} A$ una topologia gruppale non archimedea.

1.13 Teorema. *Sotto le ipotesi descritte,* $\operatorname{cov} A$ *può essere esteso in modo da risultare quasi completo rispetto alla topologia descritta; in particolare, se la topologia di A è quella descritta all'*1.2*, e se* $\operatorname{cov} A$ *è stato scelto come alla fine del* n^0 5, $\operatorname{cov} A$ *è quasi completo.*

Dim. Sia $j \longrightarrow y_j$ una successione di Cauchy di elementi di $\operatorname{cov} A$; la successione $i \longrightarrow x_i = y_{i+1} - y_i$ è una zero-successione; ed allora, per ogni h le $i \longrightarrow x_{ih}$ sono zero-successioni, uniformemente rispetto ad h. Da ciò segue subito che le $j \longrightarrow y_{jh}$ sono di Cauchy, uniformemente rispetto ad h; esse hanno quindi in A dei limiti z_h.

Fissato l'intorno U dello 0 in A, si trovi un j tale che $z_h - y_{jh} \in U$ per ogni h; dato poi un intero $n \geq 0$, ed attribuito peso p^h alle y_{jh} e z_h, si trovi il minimo h_0 tale che siano in U i monomi monici di peso p^{-n} nelle y_{jh} di grado positivo in qualche y_{jh} con $h < -h_0$ (j fissato come descritto); si vede allora che lo stesso vale per gli analoghi monomi delle z_h; quindi $z = (\dots, z_{-2}, z_{-1})$ è un covettore.

Aggiungeremo allora al dato insieme $\operatorname{cov} A$ tutti gli z ottenuti in questo modo, e chiameremo Z l'insieme così ottenuto. Si vede subito, con lo stesso metodo ora usato, che elementi di Z, in numero finito, sono simultaneamente ammessi, e che Z è un gruppo additivo; inoltre $tZ \subseteq Z$, e $\pi Z \subseteq Z$. Una topologia può essere introdotta in Z nello stesso modo in cui è stata introdotta in $\operatorname{cov} A$, e tale topologia induce in $\operatorname{cov} A$ quella data. Si prenderà quindi Z come l'estensione di $\operatorname{cov} A$ di cui si vuol dimostrare l'esistenza, e resta solo da provare che $\operatorname{cov} A$ è denso in Z, o meglio che, nelle notazioni precedenti, $z = \lim_{j \to \infty} y_j$. Ed infatti, le $j \longrightarrow (y_j - z)_h$ sono di Cauchy, uniformemente rispetto ad h, e tendono uniformemente a $(z - z)_h$; il che è quanto dire che z è il limite della $j \longrightarrow y_j$.

Per dimostrare che il $\operatorname{cov} A$ descritto alla fine del n⁰ 5 è già quasi completo basta osservare che se, per un dato w_i, si ha $w_i(y_{j+1,h} - y_{j,h}) > \alpha_i > 0$ per ogni h e per $j \geq j_0$, mentre $w_i(y_{j_0,h}) > \beta_i > 0$ per $h < h_0$, allora $w_i(z_h) \geq$ $\geq \min(\alpha_i, \beta_i) > 0$ per $h < h_0$, C. V. D..

Ferme restando le ipotesi dell'ultima parte dell'1.13, suppongasi che A sia un'algebra su un anello k perfetto, di caratteristica p, e privo di elementi pseudonulli: ciò è equivalente al dire che ogni elemento di k ha in k una unica radice p-esima. Si indichi con $\operatorname{vect} k$ l'anello dei vettori (infiniti) di Witt ad elementi in k: gli elementi $a \in \operatorname{vect} k$ saranno indicati al solito con $(a_0, a_1, \ldots)$. Si consideri dapprima un $a_{(r)} \in \operatorname{vect} k$ del tipo $a_{(r)} = (0, 0, \ldots, 0, a_r, 0, 0, \ldots)$, ove r zeri precedono a_r. Se $x \in \operatorname{cov} A$, definiremo $a_{(r)} x$ come il covettore $y_{(r)}$ tale che $(y_{(r)})_{-i} = a_r^{p^{-r-i}} x_{-r-i}^{p^r}$; questo appartiene certamente a $\operatorname{cov} A$. È chiaro che la successione $r \longrightarrow y_{(r)}$ è una zero-successione, onde esiste in $\operatorname{cov} A$ l'elemento $y = \sum_0^\infty{}_r\, y_{(r)}$. Porremo per definizione $y = ax$ se $a = \sum_0^\infty{}_r\, a_{(r)} = (a_0, a_1, \ldots)$.

1.14 TEOREMA. *Nelle ipotesi dette (ossia se A ha caratteristica p ed è quasi completa rispetto alla topologia descritta all'* 1.2, *se k è perfetto e privo di elementi pseudonulli, e se* $\operatorname{cov} A$ *è scelto come alla fine del* n⁰ 5), $\operatorname{cov} A$ *diviene un* $(\operatorname{vect} k)$*-modulo; la topologia di* $\operatorname{cov} A$ *è* $(\operatorname{vect} k)$*-lineare, e l'applicazione* $\{a, x\} \longrightarrow ax$ *è un'applicazione continua di* $(\operatorname{vect} k) \times (\operatorname{cov} A)$ *su* $\operatorname{cov} A$, *qualora in* $\operatorname{vect} k$ *si ponga la topologia in cui gli intorni dello* 0 *che la definiscono sono i* $p^n \operatorname{vect} k$, *per* $n = 0, 1, \ldots$.

DIM. Dati a ed x come nella definizione, si noti anzitutto che, come già visto nella dimostrazione dell'1.13, si ha $(ax)_{-i} = \lim_{r \to \infty} (a_{(0)} x + a_{(1)} x +$ $+ \ldots + a_{(r)} x)_{-i}$; ora per un vettore (finito o infinito) a, e rispettivamente per un covettore x, si indichi con $\varrho_r a$, e rispettivamente con $\varrho_r x$, il vettore finito di Witt $(a_0, \ldots, a_{r-1})$, e rispettivamente $(x_{-r}, \ldots, x_{-1})$, ad r componenti. Allora, dalle definizioni, è

$$t^r \varrho_{i-r}(a_{(r)} x) = (\pi^{-i} \varrho_i a_{(r)})(\varrho_i x) \qquad \text{per } i > r,$$

il che significa che per $i > r$ le ultime $i - r$ componenti di $a_{(r)}\, x$ coincidono con le ultime $i - r$ componenti di $(\pi^{-i}\, \varrho_i\, a_{(r)})\, (\varrho_i\, x)$.

Scelti allora un $s > 0$ ed un intorno U dello 0 in A, per $i - r$ abbastanza elevato le ultime s componenti di

$$(\pi^{-i}\, \varrho_i\, (a_{(0)} + a_{(1)} + \dots + a_{(r)}))\, (\varrho_i\, x)$$

differiscono dalle corrispondenti ultime s componenti di $a_{(0)}\, x + \dots + a_{(r)}\, x$ per elementi di U; e prendendo anche r abbastanza elevato si vede che sono in U le differenze fra le ultime s componenti di $(\pi^{-i}\, \varrho_i\, a)\, (\varrho_i\, x)$ e le corrispondenti ultime s componenti di ax. Poichè

$$(\pi^{-i}\, \varrho_i\, (a + b))\, (\varrho_i\, x) = (\pi^{-i}\, \varrho_i\, a)\, (\varrho_i\, x) + (\pi^{-i}\, \varrho_i\, b)\, (\varrho_i\, x),$$

si conclude che $(a + b)\, x = ax + bx$. La relazione $a\,(x + y) = ax + by$ si ottiene poi nello stesso modo, osservando che per i elevato le ultime s componenti di $\varrho_i\,(x + y)$ differiscono per elementi di U dalle corrispondenti componenti di $\varrho_i\, x + \varrho_i\, y$. Infine la $a\,(bx) = (ab)\, x$ discende dalla definizione di prodotto.

È così provato che cov A è un (vect k)-modulo. Le rimanenti asserzioni dell'enunciato sono ora ovvie, C. V. D..

Si noti che la dimostrazione precedente mostra anche che la definizione di prodotto ax ora data è collegata a quella data a p. 366 di MC nel modo seguente:

$$(ax \text{ nel senso di MC}) = (\pi^{-1}\, a)\, x.$$

(Si noti anche che l'esponente nell'ultima riga di p. 366 di MC deve essere p^{-n-r} anzichè p^{-n+r}).

Il risultato seguente è immediato:

1.15 Teorema. *Nelle ipotesi di* 1.14, *è* $\pi\,(ax) = (\pi a)\, (\pi x)$, $t\,(ax) = (\pi^{-1} a)\, (tx)$, $t\,(a \pi x) = (ta)\, x$.

Capitolo 2.

I bivettori.

8. Le convenzioni rimanendo le stesse del n⁰ 1, sia R un anello di caratteristica p, quasi completo rispetto ad una topologia C_p-lineare. Un *bivettore* (di Witt) *a componenti in* R è un'applicazione $x : i \to x_i$ di I su R tale che, per ogni $n \in I$, il $y_n = (\dots, x_{n-1}, x_n)$ sia un covettore. Il bivettore x sarà usualmente indicato con $(\dots, x_{-1}\,; x_0, x_1, \dots)$; gli elementi di un in-

sieme di bivettori diconsi *simultaneamente ammessi* se tali sono, per ogni n, i corrispondenti covettori y_n. Se x, y sono bivettori simultaneamente ammessi, si definirà $x+y$ mediante la

$$(x+y)_i = \Phi(x_i, x_{i-1}, \dots ; y_i, y_{i-1}, \dots);$$

per il n⁰ 5, questa operazione di somma gode, quando hanno senso, delle proprietà commutativa e associativa; il bivettore $-x$ tale che $-x+x = = 0 = (\dots, 0; 0, 0, \dots)$ esiste sempre. Fra i bivettori vi sono quelli *speciali*, per i quali $x_{-i}=0$ per i elevato; e fra questi vi sono quelli tali che $x_i = 0$ per $i<0$; questi ultimi formano un gruppo additivo isomorfo a vect R (gruppo additivo dei vettori infiniti di Witt a componenti in R), e saranno senz'altro identificati coi vettori. Le definizioni di t e π, operanti sui bivettori, sono analoghe a quelle del n⁰ 6; e l'analogo dell'1.12 resta valido.

9. Nel resto di questo capitolo si supporrà che l'R introdotto al n⁰ 8 sia perfetto e privo di elementi pseudonulli; si supporrà poi che la sua topologia sia del tipo descritto all'1.2, e che R sia quasi completo rispetto ad essa. Indicheremo con biv R l'insieme dei bivettori x, a componenti in R, tali che: per ogni intero positivo i, esiste un $\beta_i > 0$ tale che $w_i(x_{-j}) \geq \beta_i$ per j elevato. Nelle notazioni del n⁰ 8, ed avendo scelto per cov R quello descritto alla fine del n⁰ 5, è quanto dire che $x \in \operatorname{biv} R$ se e solo se $y_n \in \operatorname{cov} R$ per qualche n, e quindi per tutti gli n. Si vede allora che biv R è un gruppo rispetto all'operazione $+$, e che il gruppo dei bivettori speciali è divisorio, e coincide quindi con $Q \operatorname{vect} R$, mentre $\operatorname{cov} R \cong \operatorname{biv} R/\operatorname{vect} R$.

Sia Q' l'insieme dei razionali non negativi del tipo mp^n, con n, m interi; chiameremo *Q'-polinomio* un polinomio in cui gli esponenti degli argomenti possano prendere valori in Q'. Ciò premesso, la topologia di R soddisfa evidentemente alle condizioni seguenti:

(A) l'applicazione π è un omeomorfismo di R;

(B) esiste un sistema di intorni dello 0 (*che sarà quello costantemente usato nel resto di questo capitolo*), tale che per ogni suo intorno U sia in U ogni Q'-monomio monico di grado 1 i cui argomenti siano in U.

Se U è un intorno dello 0, indicheremo con U_n (per $n \in I$) l'insieme degli $x \in \operatorname{biv} R$ tali che siano in U tutti gli $x_i^{p^{-i}}$ con $i \leq n$. Per quanto precede, gli U_n sono sottogruppi di biv R, ed al variare di U e di n formano un insieme di intorni dello 0 per una topologia gruppale non archimedea di biv R. Il gruppo vect R è anche un anello; pertanto è un anello, in modo naturale, l'insieme Q vect R dei bivettori speciali; vogliamo dimostrare che la topologia indotta in questo anello dalla topologia di biv R sopra introdotta rende Q vect R anello topologico, ossia rende continua l'applicazione prodotto.

Si indichi allora (*notazione sempre mantenuta nel seguito*) con $\{a\}$ il bivettore $(\ldots, 0, 0; a, 0, 0, \ldots) \in \operatorname{biv} R$; un elemento $x \in Q \operatorname{vect} R$ può mettersi sotto la forma $x = \sum_r^\infty{}_i p^i (x_i')$, ove $x_i' = \pi^{-i} x_i$; se y viene espresso analogamente (con s in luogo di r), dalla teoria dei vettori di Witt segue subito che

$$xy = \sum_{s+r}^{\infty}{}_i\, p^i \sum_{a+b=i} \{x_a' y_b'\}.$$

Se quindi $x \in U_m$ ed $y \in V_n$, si ha che $xy \in (U + V)_{n+m+1}$; da questa si vede appunto che l'applicazione prodotto è continua.

10. Vogliamo ora dimostrare che:

2.1 Teorema. *Sia R come descritto al* n^0 9*; allora* Q vect R *è denso in* biv R*; se R' è un sottoanello di R, denso in R, anche* Q vect R' *è denso in* biv R. *Se infine $i \longrightarrow y_i$ è una successione di Cauchy di elementi di* biv R, *e se gli y_i soddisfano uniformemente alla condizione dell'* 1.5 (nel senso che preciseremo subito), *allora la successione converge ad un elemento di* biv R.

Il dire che gli y_i soddisfano uniformemente alla condizione dell'1.5 significa questo: per ogni r, è $\lim_{n \to \infty}$ estr inf $w_r(y_{i,-j}) > 0$, ove l'estremo inferiore è preso su tutti gli i e sugli $j \geq n$. Per 1.2 questa condizione implica che gli y_i sono simultaneamente ammessi.

Dim. Q vect R è denso in biv R perchè se $x \in \operatorname{biv} R$ si ha $x = \lim_{n \to \infty} (\ldots, 0, 0, x_{-n}, x_{-n+1}, \ldots, x_{-1}; x_0, x_1, \ldots)$. Ora occorre dimostrare che Q vect R' è denso in Q vect R. Se $x = (\ldots, 0, x_{-n}, \ldots, x_{-1}; x_0, x_1, \ldots) \in Q \operatorname{vect} R$, si scelgano un intorno U dello 0 in R, ed un intero $m > 0$; si scelgano poi gli elementi $y_{-n}, y_{-n+1}, \ldots, y_m \in R'$ per ricorrenza nel modo seguente: $x_{-n} + y_{-n} \in \pi^{-n} U$; poi, supposti trovati gli $y_{-n}, \ldots, y_r\ (-n \leq r < m)$, e chiamato Y_i l'elemento di Q vect R' la cui unica componente non nulla è quella di indice i, tale componente essendo y_i, si supponga dimostrato che $Z_r = x + Y_{-n} + Y_{-n+1} + \ldots + Y_r \in U_r$ (ciò è vero per $r = -n$); si scelga $y_{r+1} \in R'$ in modo che $(Z_r)_{r+1} + y_{r+1} \in \pi^{r+1} U$. Allora $Z_{r+1} = x + Y_{-n} + \ldots + Y_{r+1} \in U_{r+1}$. Si giunge così a $Z_m \in U_m$, ossia $x + (Y_{-n} + \ldots + Y_m) \in U_m$, con $Y_{-n} + \ldots + Y_m \in Q \operatorname{vect} R'$, come richiesto.

Sia infine $i \longrightarrow y_i$ una successione come descritta nell'enunciato; pongasi $x_1 = y_1$, e $x_i = y_i - y_{i-1}$ per $i > 1$; la $i \longrightarrow x_i$ è una zero-successione, e gli x_i sono simultaneamente ammessi. Dato un intero positivo r, si ha $y_{i+1,j} = y_{i,j} + P_{ijr} + Q_{ijr}$, ove P_{ijr} è un polinomio nelle $y_{i,j-1}, \ldots, y_{i,j-r}$, $x_{i,j}, \ldots, x_{i,j-r}$, mentre Q_{ijr} è una serie nelle $y_{i,s}, x_{i,s}\ (s < j)$, ogni cui monomio ha peso p^j (attribuendo i soliti pesi alle $x_{i,j}, y_{i,j}$) ed è divisibile per un $y_{i,s}$ od un $x_{i,s}$ con $s < r$. Scelto un intorno U dello 0 in R, e fissato j, essendo gli x_i, y_i simultaneamente ammessi è possibile trovare r in modo che, per ogni i, $Q_{ijr} \in U$; dato che inoltre la $i \longrightarrow x_i$ è una zero-successione, è possibile trovare i_0 in modo che per $i > i_0$ siano in U le P_{ijr}. Pertanto la $i \longrightarrow y_{i,j}$ è di Cauchy, ed ha in R un limite z_j; per la condizione posta, per ogni r si ha $\lim_{n\to\infty} \operatorname{estr\,inf}_{j \geq n} w_r(z_{-j}) > 0$, e quindi $z = (\ldots, z_{-1}; z_0, \ldots) \in \operatorname{biv} R$. Infine, se $x_i \in U_n$ per $i > s$, anche $z - y_s \in U_n$, C. V. D..

Nelle notazioni e ipotesi di 2.1, i completamenti di biv R, Q vect R, Q vect R' coincidono; essi saranno indicati con Biv R; se H è un intorno aperto dello 0 in biv R, si indicherà ancora con H l'interno della chiusura di H in Biv R. L'operazione di prodotto, definita in Q vect R, è bilineare e continua; quindi può essere estesa in modo unico, bilinearmente e continuamente, a Biv R per il 2.1.

2.2 COROLLARIO. *Nelle ipotesi di* 2.1, Biv R *è un anello topologico completo, ed è un'algebra su* Q; *più precisamente, se* U, V *sono intorni dello* 0 *in* R, *si ha* $U_n V_m \subseteq (U + V)_{n+m+1}$. *La topologia di* Biv R *è* (vect R)-*lineare, e* biv R *è un* (Q vect R)-*modulo.*

DIM. Le prime due asserzioni sono ottenute, per continuità, da fatti già noti; la topologia di Biv R è (vect R)-lineare perchè ogni elemento y di vect R appartiene ad ogni V_{-1}, cosicchè $y V_n \subseteq (V + V)_n = V_n$. Resta da dimostrare che biv R è un (Q vect R)-modulo, e per qnesto basta dimostrare che se $y \in \operatorname{biv} R$ ed $x \in \operatorname{vect} R$, si ha $xy \in \operatorname{biv} R$. Ora, per definizione xy è la somma degli z_i dati da $z_{i,j} = x_i^{p^{-i+j}} y_{j-i}^{p^i}$, per $i = 0, 1, \ldots$. Si constata subito che gli z_i, e quindi le somme di essi in numero (finito) qualsiasi, soddisfano uniformemente alla condizione dell'1.5; ed allora per 2.1 la $\Sigma_i z_i$ è un elemento di biv R, C. V. D..

È opportuno notare che la identificazione di cov R con biv R/vect R dà una topologia in cov R, che non è in generale la stessa definita al n⁰ 7; se k è un sottoanello perfetto di R, il 2.2 dà un modo di definire una struttura di (vect k)-modulo su cov R; un confronto con la definizione di prodotto data al n⁰ 7 mostra che questa struttura è, algebricamente ma non sempre topologicamente, la stessa di cui l'1.14 asserisce l'esistenza.

2.3 COROLLARIO. *Siano* $x, y \in \operatorname{biv} R$, *e suppongasi che per ogni* w_r *esista un reale* $\beta_r > 0$ *tale che* $p^{i-j} w_r(x_{-i}) + p^{-i} w_r(y_{i-j}) \geq \beta_r$ *per* i, j *elevati. Allora* $xy \in \operatorname{biv} R$.

DIM. Nelle notazioni della dimostrazione del 2.2, basta dimostrare che anche gli z_{-i}, con i intero elevato, soddisfano uniformemente alla condizione dell' 1.5. Ora, $w_r(z_{-i,-j}) = p^{i-j} w_r(x_{-i}) + p^{-i} w_r(y_{i-j}) \geq \beta_r$, C. V. D..

11. È opportuno notare esplicitamente che vi sono degli R per i quali $\operatorname{biv} R$ non è completo; ed anzi, tali che qualsiasi scelta di $\operatorname{biv} R$, come gruppo addittivo di bivettori contenente quelli del tipo $\{x\}$, produce un gruppo non completo. Ecco un esempio: preso un corpo perfetto k di caratteristica $p > 2$, e presa un'indeterminata ξ, sia R l'anello delle serie di potenze nella ξ, per le quali gli esponenti possano prendere i valori razionali non negativi della forma mn^{-1}, ove n ha al più i fattori primi 2 e p. L'anello R è perfetto, ed è una schiera valutante completa per una valutazione w di rango 1 e non discreta, che supporremo normalizzata in modo da rendere $w(\xi) = 1$. Si indichi con U^α l'intorno dello 0 formato dagli elementi di w-valore $\geq \alpha$; la serie $\sum_{-\infty}^{\infty}{}_i\, p^i \{\xi^{(2/p)^i}\}$ converge ad un elemento $x \in \operatorname{Biv} R$, in quanto $p^i \{\xi^{(2/p)^i}\} \in U_m^\alpha$ non appena $i > m$, ovvero $i \leq m$ ma $(2/p)^i > \alpha$. Supposto che x sia un bivettore, si chiami τ l'automorfismo continuo di R che induce l'identità in k, e che applica ξ su $\xi^{1/2}$; si può far operare τ anche sui bivettori mediante le componenti. Si ha $px = \sum_{-\infty}^{\infty}{}_i\, p^i \{\xi^{(2/p)^{i-1}}\} = \pi\tau x$, onde $tx = \tau x$, ossia $x_i = \tau^{-i} x_0$, e quindi $w(x_i) = 2^i w(x_0)$; poichè $\lim_{i\to\infty} p^i w(x_{-i}) = \infty$, è $w(x_0) = c > 0$. La $i \longrightarrow x_i$ deve essere ammessa $(i = -1, -2, \ldots)$, e perciò si deve avere $\lim_{i\to\infty} (x_{-i}^p\, x_{-i+1}^{p-1}\, x_{-i+2}^{p-1} \ldots x_{-1}^{p-1}) = 0$, ossia $\lim_{i\to\infty} [p2^{-i} + (p-1)(2^{-i+1} + 2^{-i+2} + \ldots + 2^{-1})] = \infty$. Ma ciò è falso perchè il limite ora scritto è in realtà $p - 1$; questo conclude il controesempio.

12. Supporremo ora che R contenga un sottocorpo perfetto k, necessariamente di caratteristica p, e porremo $K = \operatorname{vect} k$; è noto che K è una schiera valutante completa rispetto ad una valutazione p-adica non ramificata v, che supporremo normalizzata mediante la $v(p) = 1$; poichè la topologia di R induce in k quella discreta, la topologia di $\operatorname{biv} R$ induce in K quella p-adica. Indicheremo con $K' = QK \subseteq Q \operatorname{vect} R$ il corpo quoziente di K; si noti che $Q \operatorname{vect} R = K' \operatorname{vect} R$.

2.4 Lemma. *Nelle ipotesi precedenti, sia* $x = \sum_{-\infty}^{\infty}{}_i\, p^i \{x'_i\}$ *un elemento di* $\operatorname{biv} R$*; sia* U *un intorno dello* 0 *in* R*, e siano* $m \geq 0$, $n > 0$ *interi; sia* $a \in K'$, *e si considerino gli elementi* $y_h = \prod_1^n{}_s\, x'_{h_s}$ *tali che* $\sum_1^n{}_s\, h_s \leq m - v(a)$. *Condizione sufficiente a che* $ax^n \in U_m$ *è che siano in* U *tutti gli* y_h.

Dim. Per 2.1, basta dimostrarlo sotto l'ipotesi che $x \in Q \operatorname{vect} R$; in tal caso, ax^n differisce per elementi di $p^{m+1} \operatorname{vect} R \subseteq U_m$ da una combinazione lineare, a coefficienti interi razionali, degli $ap^{r_h}\{y_h\}$, ove $r_h = \sum_1^n{}_s h_s$. La condizione posta assicura appunto che tale combinazione è essa stessa in U_m, C. V. D..

13. Il 2.4 dà un criterio di convergenza, in Biv R, della serie $\sum_0^\infty{}_n a_n x^n$, ove $a_n \in K'$ ed $x \in \operatorname{biv} R$; in particolare, per le serie *logaritmica* ed *esponenziale*, in cui è rispettivamente $a_n = - n^{-1}$ (per $n = 1, 2, \dots$) ed $a_n = (n!)^{-1}$ (per $n = 0, 1, \dots$), si ha $v(a_n) \geq - \log_p n$, e rispettivamente $v(a_n) \geq -(n-1)(p-1)^{-1}$ (più precisamente, come si è già visto, nel secondo caso è $v(a_n) = -(p-1)^{-1}(n - S(n)))$; in 2.4 basta quindi considerare le y_h per le quali $\sum_1^n{}_s h_s \leq q$, ove $q = m + \log_p n$ nel primo caso, e $q = m + (n-1)(p-1)^{-1}$ nel secondo. Occorre trovare gli insiemi h che soddisfano a queste relazioni: ora, fissato un intero positivo N, si vede che per n elevato o gli $h_s \leq 0$ sono in numero maggiore di N, ovvero, se sono in numero $\leq N$, la loro somma è, in valore assoluto, $\geq n - N - q$, cosicchè in questo caso almeno un h_s negativo ha valore assoluto $\geq (n-q)N^{-1} - 1$.

Ciò mostra che nel caso della serie logaritmica, od anche in quello della serie esponenziale quando $p \neq 2$, dato un intero positivo N, per n elevato ogni y_h o contiene più di N fattori x_i' con $i \leq 0$, ovvero ne contiene almeno uno con $i < -N$. Se allora x è tale che, fissato un intorno U dello 0, per N elevato tanto i monomi monici di grado $\geq N$ nelle x_0', x_{-1}', ..., quanto gli x_i' con $i < -N$, siano in U, si conclude che la serie logaritmica, e quella esponenziale se $p \neq 2$, convergono. Si noti però che la seconda condizione è sempre soddisfatta per la definizione stessa di bivettore.

Quanto alla serie esponenziale per $p = 2$, si ha analogamente che o il numero degli $h_s \leq 1$ è $> N$, ovvero, se esso è $\leq N$, la somma dei valori assoluti di quelli ≤ 0 è $\geq n - 2N - m + 1$, e quindi almeno uno di questi è, in valore assoluto, $\geq (n - m + 1)N^{-1} - 2$; questo è di nuovo crescente al crescere di n, e si può fare un ragionamento analogo al precedente. In conclusione, per la convergenza delle serie esponenziale e logaritmica basta che per ogni intorno U dello 0 in R esista un $N > 0$ tale che siano in U tutti i monomi monici di grado $\geq N$ nelle x_0, x_{-1}^p, $x_{-2}^{p^2}$, ...; nel caso della caratteristica 2 e della serie esponenziale, a questi occorre aggiungere $x_1^{p^{-1}}$. Ciò significa che per ogni r deve esistere un $\beta_r > 0$ tale che $p^i w_r(x_{-i}) \geq \beta_r$ per $i \geq 0$ (o $i \geq -1$ nel caso esponenziale se $p = 2$). Ora, essendo x elemento di biv R, questa è automaticamente soddisfatta per i abbastanza elevato; basta quindi assicurarsi che $w_r(x_{-i}) > 0$ per i rimanenti valori di i:

2.5 TEOREMA. *Se R soddisfa alla condizione posta all'inizio del* n^0 12, *e se $x \in \operatorname{biv} R$, la serie logaritmica* $-\sum_{1}^{\infty}{}_n\, n^{-1} x^n$ *converge in* $\operatorname{Biv} R$ *se per ogni r ed ogni $i \leq 0$ si ha $w_r(x_i) > 0$. La serie esponenziale* $\sum_{0}^{\infty}{}_n (n!)^{-1} x^n$ *converge sotto le stesse condizioni se $p \neq 2$; se $p = 2$, la condizione diviene: $w_r(x_i) > 0$ per ogni r e per $i \leq 1$.*

I limiti di queste serie saranno indicati con $\log(1 - x)$ ed $\exp x$ rispettivamente.

14. Occorre ora togliere la condizione $x \in \operatorname{biv} R$ da quanto precede.

2.6 LEMMA. *Sia $x \in \operatorname{Biv} R$, e sia U un intorno dello 0 in R; allora esiste un intero n tale che $x \in U_n$.*

DIM. Sia $y \in \operatorname{biv} R$ tale che $x - y \in U_0$; sia poi r tale che $y \in U_r$; allora $x \in U_n$, ove $n = \min(0, r)$, C. V. D..

2.7 TEOREMA. *Se R soddisfa alla condizione posta all'inizio del* n^0 12, *per ogni intorno U dello 0 in R pongasi $U_i' = \bigcup_{0}^{\infty}{}_N\, \pi^{-N} U_i$. Se allora $x \in \operatorname{Biv} R$, e se $x \in U_0'$ per ogni U, la serie logaritmica per* $\log(1 - x)$ *converge. Lo stesso vale per la serie esponenziale per* $\exp x$ *quando $p \neq 2$; quando invece $p = 2$, U_0' va sostituito con U_1'.*

DIM. Ragioniamo, per esempio, sul caso esponenziale, e per $p \neq 2$. Suppongasi dapprima $x \in \operatorname{biv} R$; allora la condizione espressa nel 2.5 è equivalente alla condizione dell'enunciato.

Per il caso generale occorre rifarsi alla dimostrazione del 2.5; in essa si è visto (sostituendo N con p^N) che: esiste una funzione $n = n(m, N, r)$ $(m, N, r = 0, 1, \ldots)$, a valori interi positivi, tale che $(i!)^{-1} x^i \in U_m$ per ogni $i \geq n$ e per ogni $x \in \operatorname{biv} R$ che appartenga a $U_{-r} \cap \pi^{-N} U_0$ (risp. $U_{-r} \cap \pi^{-N} U_1$ se $p = 2$); ed anzi il valore di n fornito dalla dimostrazione del 2.5 è

$$n(m, N, r) = \textit{minimo intero} \geq (p-2)^{-1}\,[(p-1)(m + p^N(r+1)) - 1] \text{ se } p \neq 2,$$

ovvero $n(m, N, r) = 2^N(r + 2) + m - 1$ se $p = 2$.

Sia ora $x \in U_0'$ (in $\operatorname{Biv} R$) per ogni U; allora, e per 2.6, ad ogni U corrispondono un N ed un r tali che $x \in U_{-r} \cap \pi^{-N} U_0$. Per ogni tale U, e per ogni intero $h > 0$, si scelga in $\operatorname{biv} R$ un $x_{U_h} \in U_{-r} \cap \pi^{-N} U_0 \cap (x + U_h)$; allora $(j!)^{-1} x_{U_h}^j \in U_m$ quando $j \geq n(m, N, r)$. La successione generalizzata $U_h \to x_{U_h}$ tende ad x, onde la $U_h \to (j!)^{-1} x_{U_h}^j$ (j fisso e $\geq n$) tende a

$(j!)^{-1} x^j$; questo pertanto appartiene ad U_m, e ciò prova che la serie per $\exp x$ converge, C. V. D..

D'ora in poi, la locuzione « $\exp x$ esiste », e analogamente per $\log(1-x)$, significherà che x soddisfa la condizione espressa al 2.7.

2.8 TEOREMA. *Sia* $x \in \mathrm{Biv}\, R$ *tale che* $\exp x$ (*e quindi* $\log(1-x)$) *esista; pongasi* $z = 1 - \exp x$ (*risp.* $z = \log(1-x)$); *allora* $x = \log(1-z)$ (*risp.* $x = 1 - \exp z$). *Si ha poi*

$$(\exp x)(\exp y) = \exp(x+y),$$

$$\log(1-x) + \log(1-y) = \log[(1-x)(1-y)],$$

nel senso che l'esistenza dei primi membri comporta anche quella dei secondi. Infine, le applicazioni $x \longrightarrow \exp x$ *e* $x \longrightarrow \log(1-x)$ *sono continue.*

DIM. Sia $\pi^N x \in U_0$ (risp. $\in U_1$ se $p = 2$) per N elevato; basta dimostrare che $\pi^N \log(1-x) \in U_0$ e $\pi^N(1 - \exp x) \in U_0$ (risp. $\in U_1$). Essendo π un endomorfismo di anelli, basta verificare che $\log(1 - \pi^N x) \in U_0$ e che $1 - \exp \pi^N x \in U_0$ (risp. $\in U_1$). Scrivendo x in luogo di $\pi^N x$, e supponendo quindi $x \in U_0$ (risp. $\in U_1$), le relazioni volute saranno conseguenza della $(i!)^{-1} \in U_0$ (risp. $\in U_1$) per $i \geq 1$; ma questa è conseguenza immediata del 2.2, ovvero anche del fatto che, nelle notazioni della dimostrazione del 2.7, si ha $n(0,0,0) = 1$.

Stabilita così l'esistenza di $\log(1-z)$ e rispettivamente di $1 - \exp z$, occorrerebbe far vedere che questi coincidono con x; ma ciò è verificabile in maniera puramente formale, e sarà omesso. Puramente formale è anche la verifica delle altre formule. Resta da provare la continuità.

Sia dunque U_m $(m \geq 0)$ un intorno dello 0 in $\mathrm{Biv}\, R$; se $x \in U_m$, a maggior ragione anche $(i!)^{-1} x^i \in U_m$ per ogni i (cfr. 2.2), onde $\exp x \in U_m$; ciò prova la continuità di $\exp x$ nel punto $x = 0$. Se $x \neq 0$, si ha che $\exp(x+z) = (\exp x)(\exp z)$; se perciò $z \in U_m$, $\exp(x+z)$ appartiene ad $(\exp x)\, U_m$; se $\exp x \in U_r$ per qualche r (come certo accade per 2.6), si ha $\exp(x+z) \in U_{m+r+1}$, il che mostra appunto la continuità nel punto x.

Per il logaritmo, la continuità nel punto 0 si dimostra nello stesso modo; poi, $\log[1-(x+z)] = \log[(1-x)(1-z(1-x)^{-1})]$. Ora, $(1-x)^{-1} = 1 + y$ se $y = x + x^2 + x^3 + \ldots$, onde $\log[1-(x+z)] = \log(1-x) + \log[1 - z(1+y)]$; se $z \in U_m$ ed $y \in U_r$ $(r < 0)$, sarà $z(1+y) \in U_{m+r+1}$, e di qui segue la continuità di log nel punto x, C. V. D..

15. Definiamo la *funzione di Artin-Hasse* nel solito modo:

2.9 $$F(z) = \exp(z + p^{-1} z^p + p^{-2} z^{p^2} + \ldots) = \prod (1 - z^n)^{-\mu(n)/n},$$

ove il $\prod$ è esteso a tutti gli n interi positivi primi con p, e ove $\mu(\ )$ indica la funzione di Möbius, ossia

$$\mu(n)=\begin{cases} 0 \text{ se } n \text{ è divisibile per il quadrato di un primo} \\ 1 \text{ se } n=1 \\ (-1)^{\alpha} \text{ se } n \text{ è il prodotto di } \alpha \text{ primi distinti.}\end{cases}$$

Se l'anello in cui si sta operando è un'algebra su Q, la 2.9 è valida non appena la topologia sia I_p-lineare, l'anello sia quasi completo, e la successione $\{z, z, z, \ldots\}$ sia ammessa; condizione sufficiente per questo è di avere $\lim_{n\to\infty} z^n/n! = 0$; si intende che $(1-z^n)^{-\mu(n)/n}$ va interpretato mediante la corrispondente serie binomiale. Se l'anello è un'algebra su C_p, la prima definizione di 2.9 perde significato e solo la seconda resta valida (con la detta interpretazione delle potenze ad esponente razionale), sempreché la topologia sia C_p-lineare, l'anello sia quasi completo, e si abbia $\lim_{n\to\infty} z^n = 0$.

2.10 Teorema. *Sia* $y \in \operatorname{Biv} R$*; allora* $y \in \operatorname{biv} R$ *e* $ty = y$ *se e solo se esiste un* $x \in R$ *tale che* $y = \log\{x\}$*, o equivalentemente* $\{x\} = \exp y$*. Se la condizione è verificata si ha anche* $\lim_{i\to\infty}(1-x)^i = 0$*,* $\lim_{i\to\infty}\pi^i y = 0$*,* $\lim_{i\to\infty} y_0^i = 0$*, e* $x = F(y_0)$.

Dim. Dimostriamo le varie asserzioni separatamente.

1. $ty = y$ comporta $\lim_{i\to\infty}\pi^i y = 0$, ed anche $\lim_{i\to\infty} y_0^i = 0$ se $y \in \operatorname{biv} R$. Sia infatti U_n un intorno dello 0 in $\operatorname{Biv} R$; per un $m < n$ opportuno si ha $y \in U_m$; se $ty = y$ si avrà $y = t^{n-m} y \in t^{n-m} U_m = \pi^{m-n} U_n$, e $\pi^i y \in U_n$ per $i \geq n-m$.

2. $y = \log\{x\}$ comporta $\lim_{i\to\infty}(1-x)^i = 0$. Ciò è vero per la nostra convenzione sulla esistenza del logaritmo.

3. $y = \log\{x\}$ comporta $ty = y$ ed $y \in \operatorname{biv} R$. Infatti, da $\{x\}^p = \pi\{x\}$ e da 2.8 segue $py = \pi y$, onde $ty = y$. Pongasi poi $z = -\Sigma_i' \, i^{-1}(1-\{x\})^i \in \operatorname{vect} R$, ove Σ_i' è estesa a tutti gli interi positivi i non divisibili per p; allora $y = \log\{x\} = \sum_{j=0}^{\infty} p^{-j}\pi^j z = \sum_{j=0}^{\infty} t^{-j} z$. Ogni componente di $1-\{x\}$ è divisibile per $1-x$, onde ogni componente di z ha la stessa proprietà; pertanto, e dato che $\lim_{i\to\infty}(1-x)^i = 0$, i bivettori $t^{-j} z$ soddisfano uniformemente alla condizione dell'1.5, e ciò prova, per 2.1, che $y \in \operatorname{biv} R$.

4. $ty = y$ ed $y \in \operatorname{biv} R$ comporta $\exp y = \{x\}$, con $x = F(y_0)$. Si noti intanto che $\exp y$ esiste per 1. Pongasi poi $z = (\ldots, y_0, y_0; y_0, 0, 0, \ldots)$, co-

sicchè $y = \lim_{i \to \infty} t^i z$. Si ha $\exp t^i z = \pi^{-i} \exp p^i z = \pi^{-i} [\exp z]^{p^i}$. È però $z = \{y_0\} + p^{-1}\{y_0\}^p + p^{-2}\{y_0\}^{p^2} + \ldots$, onde $\exp t^i z = \pi^{-i} [F(\{y_0\})]^{p^i}$; per 2.9 questo è elemento di vect R, e quindi la sua componente di posto 0 è $\pi^{-i} [F(y_0)]^{p^i} = F(y_0)$. Passando al limite per $i \to \infty$ si deduce, per 2.8, che $\exp y \in$ vect R e che $(\exp y)_0 = F(y_0)$. D'altra parte, la $ty = y$ dà $py = \pi y$, $(\exp y)^p = \pi \exp y$; questa, combinata con l'essere $\exp y \in$ vect R, implica che $\exp y = \{x\}$ per qualche x, e quindi per $x = F(y_0)$, C. V. D..

INDICE ALFABETICO DELLE DEFINIZIONI E DEI SIMBOLI