ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

FRANCESCO BALDASSARRI

Una funzione intera p-adica a valori interi

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4e série, tome 2, nº 2 (1975), p. 321-331

<http://www.numdam.org/item?id=ASNSP_1975_4_2_2_321_0>

Una funzione intera p-adica a valori interi.

FRANCESCO BALDASSARRI (*)

La funzione descritta nel titolo è una serie di potenze $\Psi(x)$ in una indeterminata, a coefficienti interi razionali (ed esponenti ovviamente interi non negativi) che converge per ogni elemento del corpo p-adico Q_p ad un intero p-adico (teorema 12); ed anzi, se Ω è una estensione di Q_p completa rispetto ad una valutazione v, di rango 1, che induce la valutazione p-adica su Q_p e $\xi \in \Omega$, la condizione che $v(\Psi(p^n \xi))$ resti non negativo è necessaria e sufficiente a che ξ, a priori elemento di Ω, sia in realtà in Q_p (corollario 15).

Queste proprietà abbastanza strane, e di natura aritmetica, consigliano l'esposizione autonoma qui presentata. In realtà la $\Psi(x)$ è sorta nel corso della mia tesi di laurea, il cui oggetto era l'interpretazione di certe iperalgebre e dei loro anelli di bivettori di Witt alla luce delle considerazioni svolte da I. Barsotti in una conferenza all'Istituto Nazionale di Alta Matematica (1973). Una applicazione della Ψ alla costruzione di un omomorfismo continuo che estende la funzione esponenziale, nonchè, eventualmente, le considerazioni di « analisi funzionale p-adica » dalle quali Ψ è scaturita saranno forse esposte separatamente.

Quantunque se ne usino solo i primissimi risultati, i riferimenti all'[MA] della bibliografia sono continui: l'1 è il lemma 1.2 di [MA] tradotto in caratteristica 0, ed è con esso sinottico come buona parte di ciò che precede il teorema principale 12 (escluso). Vanno notate delle differenze: l'1 dà solo una condizione sufficiente mentre l'1.2 di [MA] dava anche la condizione necessaria; però le pseudovalutazioni qui usate sono più generali; le algebre del tipo descritto all'1 sono analoghe alle algebre topologiche localmente convesse dell'analisi classica.

(*) Università di Padova.
Pervenuto alla Redazione il 4 giugno 1974.

Desidero ringraziare I. Barsotti che mi ha guidato nello svolgimento di questo lavoro.

1. – La lettera Q indicherà sempre il corpo razionale, Z l'anello degli interi e p un primo razionale fissato; Q_p e Z_p saranno i completamenti di Q e Z nella uniformità indotta dalla valutazione p-adica v, normalizzata con $v(p)=1$. Z'_p invece indicherà gli interi p-adici razionali, cioè $Z_p \cap Q$ (intersezione fatta in Q_p); gli anelli saranno sempre commutativi con identità. Ω indicherà un corpo di caratteristica 0, completo rispetto ad una valutazione v, di rango 1, che induce in $Q_p \subseteq \Omega$ la v precedentemente descritta; invece Ω_p indicherà il completamento della chiusura algebrica di Q_p, sicchè Ω_p è un particolare Ω.

Ripeto ora alcune definizioni che si trovano al principio di [MA]. Se $x_0, x_1, \ldots, x_i, \ldots$ sono elementi di una Q-algebra di caratteristica 0, un *monomio ammesso* nelle x_i è un monomio del tipo $q[(r_0!) \ldots (r_s!)]^{-1}x_0^{r} \ldots x_s^{r_s}$ ove $q \in Z'_p$. Sia A una Q-algebra, dotata di una topologia Z'_p-lineare (cioè tale che una base di intorni dello 0 sia formata da Z'_p-moduli, con intersezione ridotta all'elemento 0), e siano $i \to x_{ji}$ $(i=-1,-2,\ldots)$ delle successioni di elementi di A; si attribuisca peso p^i a x_{ji}. Tali successioni sono *simultaneamente ammesse* (se ve n'è una sola, la si dirà *ammessa*) se: per ogni intorno U dello 0, e per ogni intero $m \geqslant 0$, esiste un intero positivo r tale che siano in U tutti i monomi ammessi nelle x_{ji}, di peso p^{-m}, ciascuno dei quali abbia grado positivo in qualche x_{ji} con $i \leqslant -r$.

2. – Una *pseudovalutazione* di un anello R è una applicazione $x \to w(x)$ di R su $\Gamma \cup \{+\infty\}$ (Γ essendo un gruppo ordinato additivo) che soddisfi gli assiomi seguenti: $w(x+y) \geqslant \min\big(w(x), w(y)\big)$, $w(xy) \geqslant w(x)+w(y)$, $w(1)=0$, $w(0)=+\infty$. Alle pseudovalutazioni si applica la stessa nomenclatura che si applica alle valutazioni.

1) Lemma. *Sia R' una Q-algebra di caratteristica* 0; *siano w_r*, con r *percorrente un insieme $\mathfrak{J}$, sue pseudovalutazioni di rango $\leqslant 1$, tali che $w_r(x)=+\infty$ per ogni $r \in \mathfrak{J}$ solo se $x=0$, e che ogni w_r induca su Q la valutazione p-adica v, con $w_r(p)=1$. Sia R il sottoanello di R' formato dagli elementi x di R' tali che $w_r(x) \geqslant 0$ per ogni r di $\mathfrak{J}$; si munisca R' della topologia R-lineare definita dal sistema di intorni dello* 0 *i cui elementi sono gli R-moduli $U(r_1, \ldots, r_h; s_1, \ldots, s_h)$, con $r_1, \ldots, r_h \in \mathfrak{J}$ e $s_1, \ldots, s_h$ reali, così definiti: $y \in U(r_1, \ldots, r_h; s_1, \ldots, s_h)$ se e solo se $w_{r_i}(y) \geqslant s_i$ per $i=1, \ldots, h$. Siano $j \to x_{ij}$ $(j=-1,-2,\ldots)$ successioni di elementi di R'; sia $n \to \alpha_r(n)$ la massima applicazione monotona non decrescente dell'insieme degli interi positivi sull'insieme dei reali e degli elementi $-\infty$, $+\infty$, che soddisfa la $\alpha_r(n) \leqslant p^n\big(w_r(x_{i,-n})-1/(p-1)\big)$ per ogni i e n; in altre parole, sia $\alpha_r(n)=\inf p^j\big(w_r(x_{i,-j})-1/(p-1)\big)$, per i qualsiasi e $j \geqslant n$. Si*

supponga che le α_r non assumano mai il valore $-\infty$ e che per n grande ($> N_r$) sia $\alpha_r(n) \geqslant 0$.

Allora se tutte le serie $\sum_n^{\infty}{}_1\, p^{-n}\alpha_r(n)$ sono divergenti, le $j \to x_{ij}$ sono simultaneamente ammesse.

DIM. (Svolta nel caso di una sola w_r, che chiameremo w, e di una sola successione $j \to x_j$; vi è una sola α_r, che chiameremo α. Inoltre la condizione di ammissibilità sarà verificata solo per i monomi di peso 1, la dimostrazione essendo la stessa per i monomi di peso p^{-m}).

Un monomio ammesso nelle x_j, di peso 1, e divisibile per x_{-m}, può per semplicità essere supposto del tipo: $M_s = [(s_r!) \dots (s_1!)]^{-1} x_{-r}^{s_r} \dots x_{-1}^{s_1}$, ove (1) gli s_i sono interi non negativi, (2) $s_m > 0$, (3) $\sum_i s_i p^{-i} = 1$. Si ha:

$$w(M_s) \geqslant s_r w(x_{-r}) + \dots + s_1 w(x_{-1}) - v\big((s_r!) \dots (s_1!)\big) \geqslant s_r w(x_{-r}) + \\ + \dots + s_1 w(x_{-1}) - \frac{\sum_i s_i}{p-1} = \sum_1^r{}_i\, s_i \left(w(x_{-i}) - \frac{1}{p-1}\right) \geqslant \sum_1^r{}_i\, s_i p^{-i} \alpha(i) = z(s)\,.$$

Cerchiamo il minimo valore, sia esso z_m, assunto da $z(s)$ tra gli s come sopra, assumendo inoltre, senza restrittività, che $m = r$. Prima però mostriamo che se $t_1, \dots, t_r$ sono interi non negativi e $\sum_1^r{}_i\, t_i p^{-i} = kp^{-r}$ con k intero non negativo, il minimo di $z(t) = \sum_1^r{}_i\, t_i p^{-i}\alpha(i)$ è assunto dal $t = (t_1, \dots, t_r)$, caratterizzato univocamente dalla proprietà che $t_2, \dots, t_r$ sono $\leqslant p-1$. Se quanto asserito è vero per $r = n-1$ (banalmente vero per $r = 1$) e per ogni k, sia $t' = (t_1', \dots, t_n')$ punto di minimo per $z(t)$ nell'insieme dei t con $t_n = t_n'$ (fissato tra i possibili valori); allora $t_2', \dots, t_{n-1}'$ sono $\leqslant p-1$. Inoltre il passaggio da t_n' a $t_n' + p$ (successivo possibile t_n) dà come punto di minimo relativo a $t_n' + p$: $t'' = (t_1', \dots, t_{d-1}', t_d' - 1, p-1, \dots, p-1, t_n' + p)$ se $t_{n-1}' = t_{n-2}' = \dots = t_{d+1}' = 0$ e $t_d' \neq 0$, dato che t_i'' è in tal caso $\leqslant p-1$, per $i = 2, \dots, n-1$. Ma $z(t'') \geqslant z(t')$, e dunque il minimo possibile $t_n (\leqslant p-1)$ fornisce, come minimo relativo, il minimo assoluto di $z(t)$. [1]

Il calcolo di z_m ora è semplice: $z_m = z(s) = z\big((s_1, \dots, s_m)\big)$ con $s_2, \dots, s_{m+1} \leqslant p-1$; s_m certo deve essere multiplo di p e la precedente scrittura di t'' mostra che il minimo si ha per $s_m = p$. Ma allora $s_2 = s_3 = \dots = s_{m-1} = p-1$. Infine $s_1 = p-1$. Dunque

$$z_m = z\big((p-1, p-1, \dots, p)\big) = \sum_1^m{}_i\, (p-1)p^{-i}\alpha(i) + p^{-m}\alpha(m)\,.$$

[1] Questo ragionamento chiarisce anche la dimostrazione del lemma 1.2 di [MA].

Chiaramente, perchè $j \to x_j$ sia ammessa basta che $\lim_{m\to+\infty} z_m = +\infty$, e questo succede certamente se $\sum_1^\infty {}_i\, p^{-i}\alpha(i)$ è divergente. C.V.D.

2) Corollario. *Ipotesi come all'1; suppongasi inoltre che le w_i siano tutte discrete. Allora una successione $j \to x_j$ è ammessa se per ogni i esiste un n tale che $w_i(x_{-j}) > 1/(p-1)$ per $j > n$; successioni verificanti questa condizione con un n indipendente dalla particolare successione, dipendente cioè solo da i, sono simultaneamente ammesse.*

Dim. Se $p = 2$ la condizione significa $w_i(x_{-j}) \geqslant 2$ per $j > n$; se $p > 2$ significa $w_i(x_{-j}) \geqslant 1$ per $j > n$. Nel primo caso $\alpha_i(n) \geqslant p^n$ e nel secondo $\alpha_i(n) \geqslant \big((p-2)/(p-1)\big)\ p^n$, per n grande. Allora la serie dell'1 diverge e la successione è ammessa. La seconda asserzione è ovvia, da 1. C.V.D.

3. – Sia x una indeterminata su Q_p di pendenza 0 (vedasi [VP], sez. 2). La topologia canonica di $Q_p[x]$ ha allora come sistema fondamentale di intorni di 0 i V_h $(h = 0, 1, 2, \ldots)$ così definiti: V_h è il sotto-Z_p-modulo di $Q_p[x]$ generato dai monomi ax^m tali che $v(a) \geqslant h(1+m)$. È chiaro da [1], lemma 1.2, che V_h è lo Z_p-modulo dei polinomi a coefficienti in Q_p che assumono v-valore $\geqslant h$ sul disco chiuso $C_{-h} = \{x \in \Omega_p | v(x) \geqslant -h\}$. Dunque la topologia canonica di $Q_p[x]$ è indotta dalle seguenti pseudovalutazioni discrete w_h $(h = 0, 1, 2, \ldots)$: $w_h(f(x)) = \min_{\xi \in C_{-h}} v(f(\xi))$, per $f(x) \in Q_p[x]$. Il completamento di $Q_p[x]$ nella topologia canonica si indica con $Q_p[\![x]\!]$ ed è l'anello delle serie di potenze della x, a coefficienti in Q_p, convergenti su tutto Ω_p; si ha cioè $Q_p[\![x]\!] = \left\{\sum_0^\infty {}_m\, a_m x^m \middle| \lim_{m\to+\infty} v(a_m)/m = +\infty\right\}$.

3) Lemma. *La successione $x, px, p^2x, \ldots$ è ammessa nella topologia canonica di $Q_p[\![x]\!]$.*

Dim. $\operatorname{Lim}_{i\to+\infty} w_h(p^i x) = +\infty$ per $h = 0, 1, 2, \ldots$, e l'asserzione segue allora da 2. C.V.D.

4) Corollario. *Le successioni $\xi, p\xi, p^2\xi, \ldots$, al variare di ξ fra gli elementi di Ω di v-valore maggiore di un reale preassegnato sono simultaneamente ammesse nella v-topologia di Ω.*

Dim. Infatti il Q_p-algebra omomorfismo di $Q_p[x]$ su Ω che applica x su ξ è continuo, ed è perciò unicamente estensibile, per continuità, ad un Q_p-algebra omomorfismo di $Q_p[\![x]\!]$ su Ω. C.V.D.

Sia A una Q-algebra *quasi completa* (cioè tale che le successioni di Cauchy di elementi di A convergano in A) in una topologia Z_p'-lineare. Una successione ammessa $i \to x_i$ $(i = n, n-1, \ldots)$, ove n è un intero fissato, di elementi di A, è chiamata in [MA] un *covettore* di *componenti* x_i e di *componenti fantasma* $x^{(i)}$, date da:

5) $$x^{(i)} = x_i + p^{-1}x_{i-1}^p + p^{-2}x_{i-2}^{p^2} + \ldots \quad (i = n, n-1, \ldots).$$

In tal caso anche $i \to x^{(i)}$ $(i = n, n-1, \ldots)$ risulta, per 1.10 di [MA], un covettore a componenti in A; esistono inoltre funzioni razionali intere $\psi_i(Y_{i-1}, \ldots, Y_0)$ (le Y_j qui sono indeterminate) di i argomenti, a coefficienti in Q, tali che:

6) $$x_i = x^{(i)} + \psi_1(x^{(i-1)}) + \psi_2(x^{(i-1)}, x^{(i-2)}) + \ldots \ (i = n, n-1, \ldots).$$

E anzi, dato un qualunque covettore $i \to x^{(i)}$ $(i = n, n-1, \ldots)$, le 6 convergono e la successione $i \to x_i$ ottenuta è un covettore a componenti in A le cui componenti fantasma date da 5 sono proprio le $x^{(i)}$ da cui si era partiti. Vale inoltre, per 1.9 di [MA], il seguente:

7) LEMMA. *$\psi_i(Y_{i-1}, \ldots, Y_0)$ è divisibile per Y_0, ed è isobarico di peso p^i quando a Y_j si attribuisca peso p^j; ogni monomio che compare in ψ_i ha grado maggiore di $(p-1)i$, ed è ammesso. Inoltre*

$$h_i(Y_{i-1}, \ldots, Y_0) = \frac{\psi_i(pY_{i-1}, \ldots, pY_0)}{pY_0} \in Z[Y_0, \ldots, Y_{i-1}];$$

questa è la definizione di $h_i(Y_{i-1}, \ldots, Y_0)$.

La somma di covettori (simultaneamente ammessi) è definita all'1.11 di [MA]: se $x: i \to x_i$ e $y: i \to y_i$ $(i = n, n-1, \ldots)$ sono siffatti covettori, $z = x + y$ è il covettore definito da:

8) $$z_i = \Phi(x_i, x_{i-1}, \ldots; y_i, y_{i-1}, \ldots) =$$
$$= x_i + y_i + \sum_1^\infty {}_j\, \varphi_j(x_{i-1}, \ldots, x_{i-j}; y_{i-1}, \ldots, y_{i-j}) \qquad (i = n, n-1, \ldots),$$

ove le φ_j sono funzioni razionali intere a coefficienti interi. Si ha:

$$z^{(i)} = x^{(i)} + y^{(i)} \qquad (i = n, n-1, \ldots).$$

I *bivettori* a componenti in A sono successioni infinite nei due sensi $x: i \to x_i$ $(i \in Z)$ tali che, per ogni $n \in Z$, $i \to x_i$ $(i = n, n-1, \ldots)$ sia un covettore: per i bivettori valgono le formule 5, 6 e 8; quando un bivettore x è indicato esplicitamente come $(\ldots, x_{-1}; x_0, x_1, \ldots)$, è importante il punto e virgola prima della componente di posto 0, che serve appunto ad identificarla.

Applichiamo tutto ciò al caso $A = Q_p[\![x]\!]$, $x^{(i)} = p^{-i}x$, $(i \in Z)$, il che è possibile per 3; si ottiene che

$$i \to x_i = p^{-i}x + \psi_1(p^{-i+1}x) + \psi_2(p^{-i+1}x, p^{-i+2}x) + \dots \qquad (i \in Z)$$

è un bivettore a componenti in $Q_p[\![x]\!]$. Definiamo allora:

$$9) \quad \Psi(x) = x_0 = x + \sum_1^{\infty}{}_i\, \psi_i(px, \dots, p^i x) \in Q_p[\![x]\!] ;$$

si noti che $Q_p[\![x]\!]$ è sottoanello di $Q_p\{x\}$ (anello delle serie di potenze formali a coefficienti in Q_p), per [VP], lemma 1.1 e sez. 2. Si ha dunque, da 1.10 di [MA]:

$$10) \qquad x = \sum_0^{\infty}{}_j\, p^{-j}\Psi(p^j x)^{p^j},$$

ove la serie a secondo membro converge sia nella topologia canonica di $Q_p[\![x]\!]$, sia nella topologia di serie formali (discreta su Q_p) di $Q_p\{x\}$ (ovviamente). Ed anzi, la 10 definisce univocamente la serie formale $\Psi(x)$.

Si considerino ora due indeterminate x, y su Q_p, di pendenza nulla, e sia $Q_p[\![x, y]\!]$ il completamento di $Q_p[x, y]$ nella topologia canonica (VP] sez. 2). Si tratta di nuovo dell'anello delle serie di potenze a coefficienti in Q_p, convergenti su tutto $\Omega_p \times \Omega_p$, munito della topologia indotta dalle pseudovalutazioni w_h $(h = 0, 1, 2, \dots)$, ove:

$$w_h(f(x, y)) = \min_{(\xi,\eta) \in C_{-h} \times C_{-h}} v(f(\xi, \eta))$$

per ogni $f(x, y) \in Q_p[\![x, y]\!]$. Infatti un sistema fondamentale di intorni di 0 nella topologia canonica è formato dai V_h $(h = 0, 1, \dots)$, ove V_h è il sotto–Z_p-modulo di $Q_p[x, y]$ generato dai monomi $ax^r y^s$, con (r, s) tali che: $v(a) \geqslant h(1 + r + s)$, e coincide con lo Z_p-modulo dei polinomi $f(x, y)$ di $Q_p[x, y]$ tali che $w_h(f(x, y)) \geqslant h$, per [1], lemma 1.2. In $Q_p[\![x, y]\!]$ le successioni $x, px, p^2x, \dots$ e $y, py, p^2y, \dots$ sono simultaneamente ammesse, e l'1.11 di [MA] assicura che:

$$11) \quad \Psi(x + y) = \Phi(\Psi(x), \Psi(px), \dots; \Psi(y), \Psi(py), \dots) ,$$

ove Φ è appunto la funzione definita nell'1.11 di [MA], e la serie che la definisce converge sia nella topologia canonica di $Q_p[\![x, y]\!]$, sia nella topologia di serie formali di $Q_p\{x, y]$, dato che il grado di ogni monomio che compare in $\varphi_i(x_{i-1}, \dots, x_0; y_{i-1}, \dots, y_0)$ (qui x_j, y_j sono indeterminate) è almeno $(p-1)i$ (vedi pag. 10 di [MA]). L'uguaglianza 11 vale in $Q_p[\![x, y]\!]$ e dunque in $Q_p\{x, y]$ ([VP], lemma 1.1 e pag. 114); anzi, dato che

$$\Psi(x) = x + \sum_1^\infty {}_i\, \psi_i(px, \dots, p^i x) = x + \sum_1^\infty {}_i\, p^i x h_i(x, \dots, p^{i-1}) \in Z\{x]$$

(cfr. 7), e che le φ_i sono a coefficienti interi, la 11 vale in $Z\{x, y]$.

Si noti infine che anche la 10 vale in $Z\{x]$.

4. – Si osservi ora che per $\xi, \eta \in \Omega$, l'omomorfismo di Q_p-algebre:

$$\varphi: Q_p[x, y] \to \Omega$$
$$x, y \to \xi, \eta$$

è continuo se su $Q_p[x, y]$ si pone la topologia canonica, e si può dunque unicamente estendere per continuità a $Q_p[\![x, y]\!]$. Le formule 10 e 11 restano pertanto valide sostituendovi x e y con ξ ed η e danno delle uguaglianze in Ω.

Il seguente è il teorema fondamentale:

12) TEOREMA. *$\Psi(x)$ è serie di potenze a coefficienti interi tale che $\Psi(\xi)$ esiste (converge) per ogni $\xi \in \Omega$. Inoltre per ogni $\xi \in Q_p$ si ha $\Psi(\xi) \in Z_p$.*

DIM. Resta da dimostrare l'ultimo asserto. In base all'1.10 di [MA] si tratta di provare che se $\xi \in Q_p$ e si pone, per $i = 0, -1, -2, \dots, x^{(i)} = p^{-i}\xi$, allora $x_i \in Z_p$ per ogni $i = 0, -1, -2, \dots$.

a) Sia $\xi = p^{-n}\eta$ con $\eta^p = \eta$ ed $n > 0$, e poniamo, per $m \leqslant n$, e in accordo con 6, $x_m = \Psi(p^{-m}\eta)$; si ha (9, 7):

$$x_{-j} = p^j\eta + \sum_1^\infty {}_i\, \psi_i(p^{j+1}\eta, \dots, p^{j+i}\eta) = p^j\eta + \sum_1^\infty {}_i\, p^{j+i}\eta h_i(p^j\eta, \dots, p^{j+i-1}\eta)\,,$$

onde $x_{-j} \equiv p^j\eta \bmod p^{j+1}Z_p$, se $j \geqslant 0$.

Poi, per 5, $x_1 + p^{-1}x_0^p + p^{-2}x_{-1}^{p^2} + \dots = p^{-1}\eta$; ma, per quanto si è visto, $x_0^p \equiv \eta^p = \eta \bmod p^2 Z_p$, e $p^{-j-1}x_{-j}^{p^{j+1}} \equiv 0 \bmod p^{j+1}Z_p$ se $j > 0$, e dunque: $x_1 \equiv 0 \bmod pZ_p$.

Ipotesi induttiva: $x_m \equiv 0 \bmod pZ_p$ per tutti gli $m > 0$ e $\leqslant N$, con $N < n$; si ha: $x_{N+1} + p^{-1}x_N^p + p^{-2}x_{N-1}^{p^2} + \dots + p^{-N-1}x_0^{p^{N+1}} + p^{-N-2}x_{-1}^{p^{N+2}} + \dots = p^{-N-1}\eta$. Tutti i termini scritti, esclusi (per ora) x_{N+1}, $p^{-N-1}x_0^{p^{N+1}}$, $p^{-N-1}\eta$, sono $\equiv 0 \bmod pZ_p$, sicchè $x_{N+1} \equiv p^{-N-1}(\eta - x_0^{p^{N+1}}) \equiv 0 \bmod pZ_p$:

L'induzione è così dimostrata. Notiamo per uso futuro che resta in particolare dimostrato che $\Psi(p^{-m}) \equiv 0 \bmod pZ_p$ per $m \neq 0$.

b) Caso generale. Se $v(\xi) > 0$, con $\xi \in Q_p$, è $\Psi(\xi) \in pZ_p$. Supposto $\Psi(\xi) \in Z_p$ per ogni ξ di Q_p tale che $v(\xi) > -n$, sia $\eta \in Q_p$ tale che $v(\eta) = -n$; chiamiamo $\{\eta_{-n}\}$ il rappresentante moltiplicativo, in Z_p, della immagine di $p^n\eta$ modulo p: sia cioè

$$\{\eta_{-n}\} = \lim_{r \to +\infty} (p^n\eta)^{p^r}, \qquad (r = 1, 2, 3, \dots).$$

Allora $\{\eta_{-n}\}^p = \{\eta_{-n}\}$ e $v(\eta - \{\eta_{-n}\}p^{-n}) > -n$; si ponga $\xi = \eta - \{\eta_{-n}\}p^{-n}$. Si ha (11):

$$\Psi(\eta) = \Phi\big(\Psi(\xi), \Psi(p\xi), \dots; \Psi(\{\eta_{-n}\}p^{-n}), \Psi(\eta_{-n}\}p^{-n+1}), \dots\big) \in Z_p. \qquad \text{C.V.D.}$$

Nel seguito si utilizzeranno ([MA], capitolo 2) bivettori a componenti in anelli di caratteristica p; nel nostro caso tali anelli saranno dei corpi perfetti dotati della topologia discreta: il corpo di p elementi F_p, oppure il corpo residuo F di Ω, che dovrà quindi essere supposto perfetto; in questa sezione è anzi opportuno supporre non solo che F sia perfetto, ma anche che Ω contenga l'estensione massima non ramificata di Q_p (il cui corpo residuo è la chiusura algebrica $\overline{F}_p$ di F_p). Se l'Ω inizialmente scelto non soddisfacesse a queste condizioni, lo estenderemo opportunamente (per esempio prendendo il completamento della sua chiusura algebrica); tuttavia gli enunciati che seguono non contengono questa condizione su Ω, in quanto è immediatamente verificabile che se essi valgono per l'Ω esteso debbono valere anche per l'Ω dato.

Gli anelli di bivettori $\operatorname{biv} F_p$, $\operatorname{biv} \overline{F}_p$, $\operatorname{biv} F$ coincidono, come è noto, con le estensioni su Q dei corrispondenti anelli di vettori infiniti di Witt; è noto che $\operatorname{biv} F_p = Q_p$ e che $\operatorname{biv} F \subseteq \Omega$. Per la definizione degli endomorfismi π e t di $\operatorname{biv} F$ si veda al capitolo 1 di [MA], e in particolare all'1.12 per la proprietà $\pi t = t\pi = p\iota$ (moltiplicazione per p).

Ora se $\xi \in \Omega$ ha la proprietà che $v\big(\Psi(p^n\xi)\big) \geqslant 0$ per ogni $n \in Z$, si consideri il bivettore a componenti in F: $b = (\dots, \sigma\Psi(p\xi); \sigma\Psi(\xi), \sigma\Psi(p^{-1}\xi), \dots) \in \Omega$ ove σ indica la riduzione modulo il primo massimo $\mathfrak{M}$ della schiera valutante $\mathfrak{V}$ di Ω. La moltiplicazione per p di ξ produce la moltiplicazione per p delle componenti fantasma $p^{-n}\xi$, $p^{-n+1}\xi$, ... del covettore di componenti $\Psi(p^{-n}\xi)$, $\Psi(p^{-n+1}\xi)$, ..., per ogni n; è dunque

$$pb = (\dots, \sigma\Psi(p^2\xi); \sigma\Psi(p\xi), \dots) = tb,$$

onde $\pi b = b$. Pertanto $\sigma\Psi(p^n\xi) \in F_p$ per ogni $n \in Z$ e $b \in Q_p$. Ciò premesso, vale il:

13) LEMMA. *L'applicazione* $\gamma\colon \xi \to (\ldots, \sigma(\Psi(p\xi));\ \sigma(\Psi(\xi)), \sigma(\Psi(p^{-1}\xi)), \ldots)$ *di* Q_p *in* $\operatorname{biv} F_p = Q_p$ *è l'isomorfismo identico.*

DIM. $\gamma(\xi + \eta) = \gamma(\xi) + \gamma(\eta)$ per $\xi, \eta \in Q_p$; inoltre γ è applicazione continua, ed è quindi omomorfismo di Q_p-moduli; ma applica 1 su 1, in quanto, come si è osservato alla fine del caso 1 nella dimostrazione del 12, si ha $\sigma\Psi(p^m) = 0$ per $m \neq 0$. C.V.D.

14) TEOREMA. *Sia* $\zeta \in \Omega$ *tale che* $v(\Psi(p^n\zeta)) > 0$ *per ogni* $n \in Z$; *allora* $\zeta = 0$.

DIM. Se fosse $\zeta \neq 0$ esisterebbe un $m \in Z$ tale che $-1 < v(p^m\zeta) \leqslant 0$, e in tal caso, anticipando il teorema 17 del numero successivo (la cui dimostrazione è indipendente dai 14, 15), si avrebbe $\beta(\Psi(p^m\zeta)) = p^m\zeta$.

Ma questo è assurdo perchè $\beta(x)$ converge per $x = \Psi(p^m\zeta) \in \mathfrak{M}$ ad un elemento di $\mathfrak{M}$, mentre $p^m\zeta \notin \mathfrak{M}$. C.V.D.

15) COROLLARIO. *Sia* $\xi \in \Omega$ *tale che* $v(\Psi(p^n\xi)) \geqslant 0$ *per ogni* $n \in Z$; *allora* $\xi \in Q_p$.

DIM. Si chiami ancora γ l'applicazione $\xi \to b$, ove b è l'elemento di $\operatorname{biv} F_p = Q_p$ definito prima di 13; γ è ora applicazione di un sottoinsieme di Ω su Q_p, tale che $\gamma(\xi + \eta) = \gamma(\xi) + \gamma(\eta)$, questa essendo valida non appena due fra i tre termini esistono. Si ponga in questa formula $\eta = -b$ e si osservi che $\gamma(\xi - b)$ esiste ed è $= 0$, in quanto $\gamma(\xi - b) = \gamma(\xi) - \gamma(b)$, e $\gamma(b) = b = \gamma(\xi)$ per 13. Ciò è quanto dire che $\Psi(p^n(\xi - b)) \in \mathfrak{M}$ per ogni $n \in Z$. Il 14 comporta allora che $\xi = b$. C.V.D.

5. – Nel lemma che segue, C_h indicherà l'insieme degli $\xi \in \Omega$ tali che $v(\xi) \geqslant h$; in particolare $C_{-\infty} = \Omega$ e $C_{+\infty} = (0)$.

16) LEMMA. *Siano* $A(x) = \sum_{0}^{\infty}{}_i\, a_i x^i$ *e* $B(x) = \sum_{1}^{\infty}{}_j\, b_j x^j$ *serie di potenze a coefficienti in* Ω *nella indeterminata* x; *sia* $D(x) = A(B(x))$ *e si supponga che* $B(\zeta)$ *e* $D(\zeta)$ *convergano per* $\zeta \in C_h$, *per un certo* h. *Sia* $k = \inf\limits_{\zeta \in C_h} v(B(\zeta))$ *e si supponga che* $A(\eta)$ *converga per* $\eta \in C_k$; *allora per ogni* $\zeta \in C_h$, *si ha*: $D(\zeta) = A(B(\zeta))$.

DIM. Si può supporre $h \neq -\infty$. Indichiamo con $A_m(x)$, $B_m(x)$, $D_m(x)$ le somme parziali m-esime delle serie di potenze che rappresentano rispettivamente $A(x)$, $B(x)$, $D(x)$. Dato n, esiste un $M(n) \geqslant n$ tale che per $m > M(n)$ ogni monomio che compare in $A_m(B_m(x)) - D_m(x)$ ha grado $> n^2$ (questo è conseguenza immediata dell'ipotesi $A(B(x)) = D(x)$). Ogni tale monomio o compare in $D_m(x)$, o in $A_m(B_m(x))$; si osservi che i monomi di grado $> n^2$ che compaiono in $A_m(B_m(x))$ sono tutti e soli i monomi di grado $> n^2$ che compaiono in $A_m(B_m(x)) - A_n(B_n(x))$, dato che $A_n(B_n(x))$ ha grado n^2.

Dato un reale H, esiste un reale I tale che per $i > I$ sia $v(A(B_i(\zeta)) - A(B(\zeta))) > H$ per ogni $\zeta \in C_h$, perchè $\eta \to A(\eta)$ è funzione uniformemente continua in C_k; poi esiste un reale J tale che per $j > J$ sia $v(A_j(B_i(\zeta)) - A(B_i(\zeta))) > H$ per ogni i e per ogni $\zeta \in C_h$. Quindi per $i > I$ e $j > J$, e per ogni $\zeta \in C_h$, è $v(A_j(B_i(\zeta)) - A(B(\zeta))) > H$; in particolare, dato H esiste un n tale che per $m > M(n)$ sia

$$v(A_m(B_m(\zeta)) - A(B(\zeta))) > H \quad \text{e} \quad v(A_m(B_m(\zeta)) - A_n(B_n(\zeta))) > H$$

per ogni $\zeta \in C_h$. Questo comporta che se $P(x)$ è un monomio di grado $> n^2$ che compare in $A_m(B_m(x))$, e quindi, come si è visto sopra, in $A_m(B_m(x)) - A_n(B_n(x))$, deve essere $v(P(\zeta)) > H$ per ogni $\zeta \in C_h$. Se n viene scelto anche in modo che ogni monomio $Q(x)$ di grado maggiore di n^2 comparente in $D(x)$ sia tale che $v(Q(\zeta)) > H$ per ogni $\zeta \in C_h$, abbiamo così dimostrato che $v(A_m(B_m(\zeta)) - D_m(\zeta))) > H$ per ogni $\zeta \in C_h$ e per $m > M(n)$. Da ciò, e da quanto precede consegue che $v(A(B(\zeta)) - D(\zeta)) > H$. C.V.D.

Sia ora $\beta(x) = \sum_{1}^{\infty}{}_i\, b_i x^i \in Z\{x\}$, la serie reciproca di $\Psi(x)$; si abbia cioè, formalmente: $\Psi(\beta(x)) = \beta(\Psi(x)) = x$. Si ponga $\Psi(x) = \sum_{1}^{\infty}{}_i\, a_i x^i$; la formula ricorrente, ricavata da 10, che dà gli a_r, è:

$$a_1 = 1\,,$$

$$a_r = -\sum_{1}^{[\log_p r]}{}_h \sum_{(e_1,\dots,e_{r-1})} \frac{p^h!}{(e_1!)\,\dots\,(e_{r-1}!)}\, p^{h(r-1)} a_1^{e_1} \dots a_{r-1}^{e_{r-1}},$$

se $r > 1$, ove la $\sum\limits_{(e_1,\dots,e_{r-1})}$ è estesa ai vettori di numeri interi non negativi tali che $\sum e_i = p^h$ e $\sum i e_i = r$; pertanto $v(a_r) \geqslant r-1$ per ogni r. I coefficienti di $\beta(x)$ sono dati invece dalle:

$$b_1 = 1\,,$$

$$b_h = -\sum_{1}^{h-1}{}_j\, b_j \sum_{(e_1,\dots,e_h)} \frac{j!}{(e_1!)\dots(e_h!)}\, a_1^{e_1} \dots a_h^{e_h}\,,$$

se $h > 1$, ove la $\sum_{(e_1,\dots,e_h)}$ è estesa ai vettori di numeri interi non negativi tali che $\sum e_i = j$, $\sum ie_i = h$. Se si suppone $v(b_j) \geqslant j-1$ per $j \leqslant h-1$ (vero per $h=2$), si ha:
$v(b_h) \geqslant \min v(b_j) + e_1v(a_1) + \dots + e_hv(a_h) \geqslant j - 1 + e_1 0 + e_2 1 + \dots + e_h(h-1) = e_1 + 2e_2 + \dots + he_h - 1$ (il minimo è fatto sui monomi $b_ja_1 \dots a_h$ che compaiono nella formula che dà b_h). Dunque $v(b_h) \geqslant h-1$ per ogni h.

Sia ora $\zeta \in \Omega$, $v(\zeta) > -1$:

$$\lim_{h\to+\infty} v(b_h) + hv(\zeta) \geqslant \lim_{h\to+\infty} h\big(v(\zeta)+1\big) - 1 = +\infty\,;$$

dunque $\beta(\zeta)$ converge per ogni $\zeta \in \Omega$ con $v(\zeta) > -1$; ed ovviamente $v\big(\beta(\zeta)\big) > -1$; lo stesso dicasi per $\Psi(\zeta)$. Se, d'altra parte, $\zeta \in \Omega$ e $v(\zeta) = -1$, $\beta(\zeta)$ non può convergere: in caso contrario, infatti, la serie di $\beta(\zeta)$ dovrebbe convergere, come è noto, per ogni tale ζ, ed in particolare per $\zeta \in Q_p$ (per esempio $\zeta = p^{-1}$); ma allora il lemma 16 darebbe $\Psi\big(\beta(\zeta)\big) = \zeta$, e questo per $\zeta \in Q_p$ contradirebbe al 12. Concludendo si ha:

17) TEOREMA. *La serie reciproca $\beta(x)$ di $\Psi(x)$ è un elemento di $Z\{x]$ che converge per $\zeta \in \Omega$ se e solo se $v(\zeta) > -1$. In tal caso si ha*:

$$\Psi\big(\beta(\zeta)\big) = \zeta = \beta\big(\Psi(\zeta)\big)\,.$$

BIBLIOGRAFIA

[MA] I. BARSOTTI, *Metodi analitici per varietà abeliane in caratteristica positiva,* Capitoli 1, 2, Ann. Scuola Norm. Sup. Pisa, **18** (1964), p. 1.

[VP] I. BARSOTTI, *Varietà abeliane su corpi p-adici,* Parte I, Istituto Nazionale di Alta Matematica, Symposia Mathematica, **1** (1968), p. 109.

[1] B. DWORK, *On the zeta function of a hypersurface,* Publ. Math. I.H.E.S., **12** (1962).