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

MARIO POLETTI

# Anelli $p$-adici e loro rappresentazioni

*Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3^e série*, tome 25, n^o 1 (1971), p. 25-39

<http://www.numdam.org/item?id=ASNSP_1971_3_25_1_25_0>

# ANELLI $p$-ADICI E LORO RAPPRESENTAZIONI

MARIO POLETTI (1)

I vettori di Witt sono strumenti ben noti ai cultori della teoria delle varietà gruppali e delle teorie ad essa collegate.

Parte della loro importanza consiste nel fatto che permettono di dotare l'insieme delle successioni di elementi di un anello perfetto di caratteristica $p$ (cfr. **1**) di operazioni eseguibili tramite funzioni razionali sulle componenti, che lo rendono un anello $p$-adico (cfr. **2**) di residuo mod $(p)$ l'anello dato; rendendo inoltre razionale anche l'operazione di passaggio al quoziente.

A rigore l'insieme delle successioni di elementi di un qualsiasi anello di caratteristica $p$ è dotabile delle operazioni citate. La restrizione agli anelli perfetti è resa naturale dal fatto che un anello $R$ avente tutte le proprieta di un anello $p$-adico eccettuata eventualmente la perfettezza di $R/(p)$, è isomorfo all'anello dei vettori di Witt a coefficienti in $R/(p)$ se e solo se $R/(p)$ è perfetto (cfr. l'appendice).

Per quanto riguarda la definizione di operazioni che godano delle proprietà dette, sono in uso due tecniche: una di Witt e una di Lazard (cfr. [1], risp. II-6, II-5).

La prima tra tali tecniche, pur essendo costruttiva, si presenta ermetica, e solo a posteriori è possibile verificare la sua adeguatezza allo scopo.

La seconda, pur definendo formalmente le operazioni naturali atte all'uopo, nulla dice sulla costruzione effettiva delle medesime.

Tale costruzione è data nel presente lavoro. Il lemma 4.2 è lo strumento fondamentale; la costruzione delle operazioni in questione si riduce, grazie ad esso, all'esecuzione di alcuni calcoli naturali e alla sistemazione grafica del loro risultato.

Le operazioni definite da Witt e quelle definite da Lazard non sono

---

Pervenuto alla Redazione il 9 Nov. 1970.

(1) Lavoro eseguito nell'ambito dei raggruppamenti di ricerca del C. N. R.

le sole verificanti le proprietà citate. In 7. vengono determinate tutte le operazioni di tale tipo.

Accanto ai vettori di Witt si sono allineati più recentemente i bivettori di Witt (cfr. [2], cap. li 1 e 2). Le operazioni tra questi ultimi sono attualmente definite in modo apparentemente ancora più ermetico di quelle tra vettori di Witt.

Tenuto conto del fatto che l'insieme dei bivettori speciali (cfr. [2], cap. 2, n$^0$ 8.) a componenti in un anello perfetto di caratteristica $p$, costituisce un'algebra sui razionali dotata di proprietà analoghe a quelle degli anelli $p$ adici, la tecnica adottata in questo lavoro per i vettori di Witt, sembra applicabile anche ai bivettori di Witt. È quanto ci proponiamo di fare in un successivo lavoro.

In quanto segue $p$ è un primo positivo, $\mathbf{F}_p$ è il corpo fondamentale di caratteristica $p$, $\mathbf{Z}$ è l'anello degli interi, $\mathbf{N}$ e l'insieme degli interi non negativi.

Se $k$ è un anello di caratteristica $p$, il suo endomorfismo di Frobenius si indicherà con $\pi$.

**1.** Un anello di caratteristica $p$ il cui endomorfismo di Frobenius sia un automorfismo, si dirà *perfetto*. La categoria degli anelli perfetti (della detta caratteristica $p$) si indicherà con $\mathfrak{P}$.

Se $S$ è il functore canonico di $\mathfrak{P}$ nella categoria degli insiemi, ed $I$ è un insieme qualsiasi, è subito visto (con significato ovvio dei simboli) che i morfismi functoriali di $S^I$ in $S$ (ossia le funzioni razionali sulle $I$ uple) costituiscono un anello perfetto di caratteristica $p$, canonicamente isomorfo all'anello $\mathbf{F}_p\,[X_i^{p^{-\infty}}]$ dei $p^{-\infty}$-polinomi nella famigla $(X_i)_{i\,\in\,I}$ di indeterminate a coefficienti in $\mathbf{F}_p$ (cfr. [1], II-5).

Se $h \in \mathbf{F}_p\,[X_i^{p^{-\infty}}]$, si ha $h = h\,(X_i)$; se poi $(a_i)_{i\,\in\,I}$ è una famiglia di elementi di un anello perfetto $k$ di caratteristica $p$, è chiaro chi sia l'elemento $h\,(a_i)$ di $k$.

**2.** Un anello $R$ di caratteristica 0, in cui $p$, non sia nè unità nè divisore di zero, che risulti separato e completo rispetto alla topologia $p$-adica (ossia rispetto alla topologia avente per sistema fondamentale di intorni di 0 le potenze di $(p)$), e tale che $R/(p)$ sia perfetto, si dirà *p-adico*. L'omomorfismo naturale di $R$ su tutto $R/(p)$ si indicherà con $\varrho$.

Se $R$ è un tale anello, è ben noto che $\bigcap_{n=0}^{\infty} R^{p^n}$ è l'unico suo sottinsieme moltiplicativamente chiuso la restrizione al quale di $\varrho$ sia bigettiva (cfr. [1], II-4, prop. 8) Se $a \in R$, l'unico elemento di $\bigcap_{n=0}^{\infty} R^{p^n}$ avente per re-

siduo $\varrho\, a$, si dirà il *rappresentante moltiplicativo* di $a$, e si indicherà con *molt* $a$; l'insieme $\bigcap_{n=0}^{\infty} R p^n$ si indicherà quindi con *molt* $R$.

È altresì ben noto (cfr. [1], II-5) che ogni elemento $a$ di $R$ può porsi nella forma $a = \sum_{i=0}^{\infty} a_i p^i$, ove gli $a_i$ sono elementi di *molt* $R$ univocamente determinati, che diremo le *componenti moltiplicative* di $a$.

Indichiamo con $\mathfrak{A}$ la categoria degli anelli $p$ adici; i morfismi essendo gli omomorfismi di anello. Sia $f: R \to S$ un tale morfismo; $f$ è continuo rispetto alle topologie $p$ adiche di $R$ e di $S$; inoltre $f(molt\ R) \subseteq molt\ S$.

Sia $S$ il functore canonico di $\mathfrak{A}$ nella categoria degli insiemi, $M$ quello di $\mathfrak{A}$ nella categoria degli insiemi che ad ogni anello $p$ adico $R$ associa l'insieme *molt* $R$, ed $I$ un insieme qualsiasi. È subito visto che i morfismi functoriali di $M^I$ in $S$ costituiscono un anello $p$-adico canonicamente isomorfo al completamento $p$-adico $\mathbf{Z}[X_i^{p^{-\infty}}]^{(p)}$ dell'anello $\mathbf{Z}[X_i^{p^{-\infty}}]$ dei $p^{-\infty}$-polinomi nella famiglia $(X_i)_{i \in I}$ di indeterminate a coefficienti in $\mathbf{Z}$ (cfr. [1], II-5). Il residuo modulo $(p)$ di $\mathbf{Z}[X_i^{p^{-\infty}}]^{(p)}$ è ovviamente $\mathbf{F}_p[X_i^{p^{-\infty}}]$.

Se $h \in \mathbf{Z}[X_i^{p^{-\infty}}]^{(p)}$, si ha $h = h(X_i)$; se poi $(a_i)_{i \in I}$ è una famiglia di elementi di *molt* $R$ è chiaro chi sia l'elemento $h(a_i)$ di $R$.

Concludiamo osservando che i morfismi functoriali di $M^I$ in $M$ costituiscono un insieme moltiplicativamente chiuso, canonicamente isomorfo a *molt* $\mathbf{Z}[X_i^{p^{-\infty}}]^{(p)}$.

**3.** In questo numero definiamo alcuni interi, analoghi ai coefficienti polinomiali, che permettono di calcolare esplicitamente i rappresentanti moltiplicativi di varii elementi di un anello $p$-adico.

Se $h, k_1, \dots, k_s$ sono interi non negativi tali che $k_1 + \dots + k_s = h$, poniamo $\binom{h}{k_1, \dots, k_s} = \frac{h!}{k_1! \dots k_s!}$.

3.1 LEMMA. *Siano* $n, k_1, \dots, k_s$ *interi non negativi tali che* $k_1 + \dots + k_s = p^n$.

*Si ha*

$$\binom{p^n}{k_1, \dots, k_s} \equiv \binom{pp^n}{pk_1, \dots, pk_s} \quad mod\ p^{n+1}.$$

DIM. Siano $X_1, \dots, X_s$ indeterminate su $\mathbf{Z}$. Essendo $(X_1 + \dots + X_s)^p \equiv (X_1^p + \dots + X_s^p)\ mod\ p$, si ha $(X_1 + \dots + X_s)^{p^{n+1}} \equiv (X_1^p + \dots + X_s^p)^{p^n}\ mod\ p^{n+1}$.

Ciò posto, l'asserto è conseguenza del fatto che il monomio $X_1^{pk_1} \dots X_s^{pk_s}$ compare nello sviluppo di $(X_1 + \dots + X_s)^{p^{n+1}}$ con coefficiente $\binom{pp^n}{pk_1, \dots, pk_s}$, e nello sviluppo di $(X_1^p + \dots + X_s^p)^{p^n}$ con coefficiente $\binom{p^n}{k_1, \dots, k_s}$, C.V.D..

Sia $\mathbf{Z}^{(p)}$ il completamento $p$-adico di $\mathbf{Z}$.

Siano $n, k_1, \dots, k_s$ interi non negativi tali che $k_1 + \dots + k_s = p^n$; per 3.1, in $\mathbf{Z}^{(p)}$ esiste $\left\{ \begin{matrix} p^n \\ k_1, \dots, k_s \end{matrix} \right\} = \lim_{m \to \infty} \binom{p^m p^n}{p^m k_1, \dots, p^m k_s}$. Poniamo $\left\{ \begin{matrix} p^n \\ k_1, \dots, k_s \end{matrix} \right\} = \sum_{i=0}^{\infty} \left\{ \begin{matrix} p^n \\ k_1, \dots, k_s \end{matrix} \right\}_i p^i$, ove gli elementi $\left\{ \begin{matrix} p^n \\ k_1, \dots, k_s \end{matrix} \right\}_i$ sono interi univocamente determinati dall'essere non negativi e minori di $p$.

3.2 LEMMA. *Stesse ipotesi di* 3.1. *In* $\mathbf{Z}^{(p)}$ *si ha*

$$\binom{p^n}{k_1, \dots, k_s} \equiv \left\{ \begin{matrix} p^n \\ k_1, \dots, k_s \end{matrix} \right\} \quad mod\ p^{n+1},$$

$$\binom{p^n}{k_1, \dots, k_s} \equiv \sum_{i=0}^{n} \left\{ \begin{matrix} p^n \\ k_1, \dots, k_s \end{matrix} \right\}_i p^i \quad mod.\ p^{n+1}.$$

DIM. Essendo $\left\{ \begin{matrix} p^n \\ k_1, \dots, k_s \end{matrix} \right\} = \binom{p^n}{k_1, \dots, k_s} + \left[ \binom{pp^n}{pk_1, \dots, pk_s} - \binom{p^n}{k_1, \dots, k_s} \right] + \dots$, il primo asserto è conseguenza di 3.1. Il secondo asserto segue dal primo e dalle definizioni, C.V.D..

3.3 LEMMA. *Stesse ipotesi di* 3.1, *con* $n \geq 1$. *Sia* $j$ *un intero con* $1 \leq j \leq n$. *Se esiste* $i$ *tale che* $k_i$ *non sia divisibile per* $p^j$, *si ha* $\binom{p^n}{k_1, \dots, k_s} \equiv 0$ *mod* $p^{n-j+1}$. *Inoltre* $\left\{ \begin{matrix} p^n \\ k_1, \dots, k_s \end{matrix} \right\}_t = 0$ *per ogni* $t$ *tale che* $0 \leq t \leq n - j$.

DIM. Sia $p^l$ la massima potenza di $p$ che divide $k_1, \dots, k_s$; si ha $0 \leq l < j \leq n$. Poniamo $m = n - l \neq 0$, $h_1 = k_1 p^{-l}, \dots, h_s = k_s p^{-l}$.

Siano $X_1, \dots, X_s$ indeterminate su $\mathbf{Z}$. Essendo $(X_1 + \dots + X_s)^p \equiv (X_1^p + \dots + X_s^p)$ *mod* $p$, si ha $(X_1 + \dots + X_s)^{p^m} \equiv (X_1^p + \dots + X_s^p)^{p^{m-1}}$ *mod* $p^m$. Siccome il monomio $X_1^{h_1} \dots X_s^{h_s}$, essendo almeno un $h_i$ non divisibile per $p$, non compare nello sviluppo di $(X_1^p + \dots + X_s^p)^{p^{m-1}}$, mentre compare nello sviluppo di $(X_1 + \dots + X_s)^{p^m}$ con coefficiente $\binom{p^m}{h_1, \dots, h_s}$, si

ha $\binom{p^m}{h_1, \dots, h_s} \equiv 0 \mod p^m$. Essendo per 3.1 $\binom{p^m}{h_1, \dots, h_s} \equiv \binom{p^n}{k_1, \dots, k_s} \mod p^{m+1}$, si ha $\binom{p^n}{k_1, \dots, k_s} \equiv 0 \mod p^m$. L'ultima congruenza, essendo $m = n - l > n - j$ e quindi $m \geq n - j + 1$, dimostra il primo asserto del lemma; il secondo asserto è conseguenza immediata del primo, C.V.D..

**4.** Sia $R$ un anello $p$-adico. Se $(a_1, \dots, a_s)$ è una famiglia di elementi di *molt* $R$, ed $n$ un intero non negativo, porremo

$$4.1 \qquad (a_1, \dots a_s)^{\{n\}} = \Sigma \left\{ \begin{matrix} p^n \\ k_1, \dots, k_s \end{matrix} \right\}_n a_1^{k_1/p^n} \dots a_s^{k_s/p^n},$$

ove la sommatoria si intende estesa a tutte le famiglie $(k_1, \dots, k_s)$ di interi non negativi tali che $k_1 + \dots + k_s = p^n$.

Dato un elemento $a$ di $R$ che sia somma di elementi di *molt* $R$, l'espressione « *definire* $a^{\{0\}}, a^{\{1\}}, \dots$ » sarà usata in luogo dell'espressione « *scegliere una famiglia* $(a_1, \dots, a_s)$ *di elementi di molt* $R$ *tale che* $a = a_1 + \dots + a_s$, *e porre* $a^{\{0\}} = (a_1, \dots, a_s)^{\{1\}}, a^{\{1\}} = (a_1, \dots, a_s)^{\{1\}}, \dots$ ».

Di un elemento del tipo detto è esplicitamente calcolabile il rappresentante moltiplicativo; sussiste infatti il seguente

4.2 LEMMA. *Sia $a$ un elemento di $R$ che sia somma di elementi di molt $R$. Comunque siano stati definiti $a^{\{0\}}, a^{\{1\}}, \dots$, si ha molt* $a = \sum_{l=0}^{\infty} a^{\{l\}} p^l$.

DIM. Sia $(a_1, \dots, a_s)$ una famiglia di elementi di *molt* $R$ tale che $a = a_1 + \dots + a_s$; per ogni $l \geq 0$ poniamo $a^{\{l\}} = (a_1, \dots, a_s)^{\{l\}}$.

Per ogni $m \geq 0$, posto $b_m = a_1^{1/p^m} + \dots + a_s^{1/p^m}$, si ha $\varrho b_m = (\varrho a)^{1/p^m}$; dall'ultima uguaglianza si deduce che *molt* $a = \lim_{m \to \infty} b_m^{p^m}$ (cfr. [1], II·4, dim. della prop. 8).

Per ogni $n \geq 0$ si ha

$$\sum_{l=0}^{\infty} a^{\{l\}} p^l = \sum_{l=0}^{n} a^{\{l\}} p^l + \sum_{l=n+1}^{\infty} a^{\{l\}} p^l =$$

$$= \sum_{l=0}^{n} \left( \sum_{k_1 + \dots + k_s = p^l} \left\{ \begin{matrix} p^l \\ k_1, \dots, k_s \end{matrix} \right\}_l a_1^{k_1/p^l} \dots a_s^{k_s/p^l} \right) p^l + \sum_{l=n+1}^{\infty} a^{\{l\}} p^l.$$

Essendo, per ogni $h \geq 0$,

$$\left\{ \begin{matrix} p^h p^l \\ p^h k_1, \dots, p^h k_s \end{matrix} \right\} = \left\{ \begin{matrix} p^l \\ k_1, \dots, k_s \end{matrix} \right\},$$

per ogni $i \geq 0$ si ha

$$\left\{ \begin{matrix} p^h\, p^l \\ p^h\, k_1\, , \ldots , p^h\, k_s \end{matrix} \right\}_i = \left\{ \begin{matrix} p^l \\ k_1\, , \ldots , k_s \end{matrix} \right\}_i ;$$

ne segue

$$\sum_{l=0}^{\infty} a^{\{l\}} p^l =$$

$$= \sum_{l=0}^{n} \left( \sum_{k_1 + \ldots + k_s = p^l} \left\{ \begin{matrix} p^{n-l}\, p^l \\ p^{n-l}\, k_1\, , \ldots , p^{n-l}\, k_s \end{matrix} \right\}_l a_1^{k_1 p^{n-l}/p^n} \ldots a_s^{k_s p^{n-l}/p^n} \right) p^l + \sum_{l=n+1}^{\infty} a^{\{l\}} p^l .$$

Per ogni $l$ tale che $0 \leq l \leq n$ si ha

$$\sum_{k_1 + \ldots + k_s = p^l} \left\{ \begin{matrix} p^{n-l}\, p^l \\ p^{n-l}\, k_1\, , \ldots , p^{n-l} k_s \end{matrix} \right\}_l a_1^{k_1 p^{n-l}/p^n} \ldots a_s^{k_s p^{n-l}/p^n} =$$

$$= \sum_{h_1 + \ldots + h_s = p^n} \left\{ \begin{matrix} p^n \\ h_1\, , \ldots , h_s \end{matrix} \right\}_l a_1^{h_1/p^n} \ldots a_s^{h_s/p^n} ;$$

infatti, se $l = n$ l'uguaglianza detta è banale, mentre nei rimanenti casi si prova osservando che l'insieme degli addendi di cui il secondo membro è somma, consta sia degli addendi di cui il primo membro è somma, sia degli elementi $\left\{ \begin{matrix} p^n \\ h_1\, , \ldots , h_s \end{matrix} \right\}_l a_1^{h_1/p^n} \ldots a_s^{h_s/p^n}$ con almeno un $h_i$ non divisibile per $p^{n-l}$, i quali ultimi, per il secondo asserto di 3.3, sono nulli.

Tenuto conto dell'ultima osservazione, si ha

$$\sum_{l=0}^{\infty} a^{\{l\}} p^l = \sum_{l=0}^{n} \left( \sum_{h_1 + \ldots + h_s = p^n} \left\{ \begin{matrix} p^n \\ h_1\, , \ldots , h_s \end{matrix} \right\}_l a_1^{h_1/p^n} \ldots a_s^{h_s/p^n} \right) p^l + \sum_{l=n+1}^{\infty} a^{\{l\}} p^l =$$

$$= \sum_{h_1 + \ldots + h_s = p^n} \left( \sum_{l=0}^{n} \left\{ \begin{matrix} p^n \\ h_1\, , \ldots , h_s \end{matrix} \right\}_l p^l \right) a_1^{h_1/p^n} \ldots a_s^{h_s/p^n} + p^{n+1} \left( \sum_{l=0}^{\infty} a^{\{n+l+1\}} p^l \right).$$

Tenuto quindi conto del secondo asserto di 3.2, si ha

$$\sum_{h_1 + \ldots + h_s = p^n} \left( \begin{matrix} p^n \\ h_1\, , \ldots , h_s \end{matrix} \right) a_1^{h_1/p^n} \ldots a_s^{h_s/p^n} \equiv \sum_{l=0}^{\infty} a^{\{l\}} p^l \ mod\ p^{n+1} ,$$

ossia

$$\sum_{l=0}^{\infty} a^{\{l\}} p^l \equiv b_n^{p^n} \ mod\ p^{n+1} ,$$

dal che segue l'asserto, C. V. D..

Siano $a, b$ elementi di $R$, e ne siano $a_0, a_1, \ldots, b_0, b_1, \ldots$ le rispettive componenti moltiplicative. Tenuto conto che

$$a + b = \sum_{i=0}^{\infty} (a_i + b_i)\, p^i, \text{ e che } ab = \sum_{i=0}^{\infty} \left( \sum_{r+s=i} a_r b_s \right) p^i;$$

il calcolo esplicito delle componenti moltiplicative di $a + b$ e di $ab$ è fornito dal seguente

4.3 TEOREMA. *Siano $x_0, x_1, \ldots$ elementi di $R$ ciascuno dei quali sia somma di elementi di molt $R$.*

*Siano $X_0, X_1, \ldots$ elementi di $R$ definiti induttivamente come segue:*

*poniamo $X_0 = x_0$, e, per ogni $n \geq 1$, definiti $X_{n-1}^{\{0\}}, X_{n-1}^{\{1\}}, \ldots,$*

*se $p = 2$ poniamo $X_n = x_n + \sum_{s=0}^{n-1} \left( \sum_{t=1}^{n-s} X_s^{\{t\}} \right)$,*

*se $p \neq 2$ poniamo $X_n = x_n - \sum_{s=0}^{n-1} X_s^{\{n-s\}}$.*

*Comunque per ogni $n$ siano stati definiti $X_n^{\{0\}}, X_n^{\{1\}}, \ldots,$ si ha*

$$\sum_{i=0}^{\infty} x_i\, p^i = \sum_{i=0}^{\infty} (molt\ X_i)\, p^i,$$

*e inoltre*

$$molt\ X_i = \sum_{i=0}^{\infty} X_i^{\{l\}} p^l.$$

DIM. Tenuto conto di 4.2, per dimostrare l'asserto è sufficiente provare che per ogni $n \geq 0$ si ha $\sum_{i=0}^{\infty} x_i\, p^i \equiv \sum_{i=0}^{n} \left( \sum_{l=0}^{\infty} X_i^{\{l\}} p^l \right) p^i \ mod\ p^{n+1}$. Condizione sufficiente al sussistere di tale relazione è che per ogni $n \geq 0$ si abbia $\sum_{i=0}^{n} \left( \sum_{l=0}^{n-i} X_i^{\{l\}} p^l \right) p^i \equiv \sum_{i=0}^{n} x_i\, p^i \ mod\ p^{n+1}$. Tale ultima congruenza sussiste dato che:

se $p = 2$ si ha $\sum_{i=0}^{n} \left( \sum_{l=0}^{n-i} X_i^{\{l\}} p^l \right) p^i - \sum_{i=0}^{n} x_i\, p^i =$

$$= \sum_{i=0}^{n} \left( \sum_{i=0}^{n-i} X_i^{\{l\}} p^l \right) p^i - X_0 - \sum_{i=1}^{n} \left( X_i - \sum_{s=0}^{i-1} \left( \sum_{t=1}^{i-s} X_s^{\{t\}} \right) \right) p^i =$$

$$= \sum_{w=0}^{n-1} \left( \sum_{l=0}^{n-w} X_w^{\{l\}} p^{w+l} - X_w\, p^w + \sum_{i=w+1}^{n} \left( \sum_{t=1}^{i-w} X_w^{\{t\}} \right) p^i \right) =$$

$$= \sum_{w=0}^{n-1} \left( \sum_{l=1}^{n-w} X_w^{\{l\}} p^{w+l} + \sum_{j=1}^{n-w} \left( \sum_{t=1}^{j} X_w^{\{t\}} \right) p^{w+j} \right) =$$

$$= \sum_{w=0}^{n-1} \left( \sum_{l=1}^{n-w} X_w^{\{l\}} p^{w+l} + \sum_{t=1}^{n-w} \left( \sum_{j=t}^{n-w} p^{w+j} \right) X_w^{\{t\}} \right) =$$

$$= \sum_{w=0}^{n-1} \left( \sum_{l=1}^{n-w} \left( p^{w+l} + \sum_{j=l}^{n-w} p^{w+j} \right) X_w^{\{l\}} \right) =$$

$$= \sum_{w=0}^{n-1} \left( p^{n+1} \sum_{l=1}^{n-w} X_w^{\{l\}} \right) \equiv 0 \mod p^{n+1};$$

se $p \neq 2$ si ha $\sum_{i=0}^{n} \left( \sum_{l=0}^{n-i} X_i^{\{l\}} p^l \right) p^i - \sum_{i=0}^{n} x_i p^i =$

$$= \sum_{i=0}^{n} \left( \sum_{l=0}^{n-i} X_i^{\{l\}} p^l \right) p^i - \sum_{i=0}^{n} \left( \sum_{s=0}^{i} X_s^{\{i-s\}} \right) p^i =$$

$$= \sum_{i=0}^{n} \left( \sum_{l=0}^{n-i} X_i^{\{l\}} p^l \right) p^i - \sum_{s=0}^{n} \left( \sum_{i=s}^{n} X_s^{\{i-s\}} p^{i-s} \right) p^s =$$

$$= \sum_{i=0}^{n} \left( \sum_{l=0}^{n-i} X_i^{\{l\}} p^l \right) p^i - \sum_{s=0}^{n} \left( \sum_{t=0}^{n-s} X_s^{\{t\}} p^t \right) p^s = 0, \qquad \text{C. V. D..}$$

**5.** Sia $V$ il functore di $\mathbb{P}$ (cfr. **1.**) nella categoria degli insiemi che ad ogni oggetto $k$ di $\mathbb{P}$ associa l'insieme delle applicazioni di $\mathbf{N}$ in $k$, con la definizione ovvia sui morfismi.

Poniamo $H = \mathbf{F}_p[X_i^{p^{-\infty}}]$, $i \in \mathbf{N}$.

Dato un endomorfismo $u$ di $H$, e posto $u(X_n) = u_n(X_i)$, indichiamo con $u^*$ l'endomorfismo functoriale di $V$ definito da $u^*(b) = u^*(b_i) = (u_0(b_i), u_1(b_i), \ldots)$.

Dato un omomorfismo $\mathbf{T}$ di $H$ in $H \bigotimes H$, e posto $\mathbf{T}(X_n) = T_n(1 \bigotimes X_i; X_i \bigotimes 1)$, indichiamo con $\mathbf{T}^*$ il morfismo functoriale di $V \times V$ in $V$ definito da $\mathbf{T}^*(b, b') = \mathbf{T}^*((b_i), (b_i')) = (T_0(b_i; b_i'), T_1(b_i; b_i'), \ldots)$. In tale modo le immagini degli oggetti di $\mathbb{P}$ tramite $V$ risultano dotate di legge di composizione interna. Rispetto a tale legge i trasformati dei morfismi di $\mathbb{P}$ risultano omomorfismi.

**6.** Se $R$ è un anello $p$-adico, indichiamo con $v : R \to V_Q R$ l'applicazione che ad ogni $a \in R$ associa $(\varrho a_0, \varrho a_1, \ldots)$, ove $a_0, a_1, \ldots$ sono le componenti moltiplicative di $a$.

La costruzione delle operazioni naturali che rendono ciascun $V_Q R$ un anello $p$-adico isomorfo ad $R$, ossia delle operazioni indotte da $v$ in $V_Q R$ (cfr. [1], II-5, prop. 9), è data dal seguente

6.1 THEOREMA. *Esiste una ed una sola coppia* $(\mathbf{S}, \mathbf{P})$ *di omomorfismi di* $H$ *in* $H \bigotimes H$ *tale che per ogni anello p-adico* $R$ *l'applicazione* $v$ *sia un isomorfismo di* $(R\,;+\,,\cdot)$ *su tutto* $(V_\varrho R\,;\mathbf{S}^*, \mathbf{P}^*)$.

*Siano* $S_0', S_1', \ldots, P_0', P_1', \ldots$ *due successioni di elementi di* $\mathbf{Z}[X_0^{p^{-\infty}}, X_1^{p^{-\infty}}, \ldots\,; Y_0^{p^{-\infty}}, Y_1^{p^{-\infty}}, \ldots]^{(p)}$, *definite induttivamente come segue*:

*poniamo* $S_0' = X_0 + Y_0$, $P_0' = X_0 Y_0$, *e per ogni* $n \geq 1$, *definiti gli elementi* $S_{n-1}^{\langle\{0\}\rangle}, S_{n-1}^{\langle\{1\}\rangle}, \ldots, P_{n-1}^{\langle\{0\}\rangle}, P_{n-1}^{\langle\{1\}\rangle}, \ldots$,

*se* $p = 2$ *poniamo*

$$S_n' = X_n + Y_n + \sum_{s=0}^{n-1} \left( \sum_{t=1}^{n-s} S_s^{\langle\{t\}\rangle} \right)$$

$$P_n' = \sum_{i=0}^{n} X_i Y_{n-i} + \sum_{s=0}^{n-1} \left( \sum_{t=1}^{n-s} P_s^{\langle\{t\}\rangle} \right),$$

*se* $p \neq 2$ *poniamo*

$$S_n' = X_n + Y_n - \sum_{s=0}^{n-1} S_s^{\langle\{n-s\}\rangle}$$

$$P_n' = \sum_{i=0}^{n} X_i\, Y_{n-i} \sum_{s=0}^{n-1} P_s^{\langle\{n-s\}\rangle}.$$

*Comunque per ogni* $m \geq 0$ *siano stati definiti* $S_m^{\langle\{0\}\rangle}, S_m^{\langle\{1\}\rangle}, \ldots, P_m^{\langle\{0\}\rangle}, P_m^{\langle\{1\}\rangle}, \ldots$; *per ogni* $n \geq 0$ *si ha*

$$S_n(1 \bigotimes X_i\,;\, X_i \bigotimes 1) = \varrho S_n'(1 \bigotimes X_i\,;\, X_i \bigotimes 1)$$

$$P_n(1 \bigotimes X_i\,;\, X_i \bigotimes 1) = \varrho P_n'(1 \bigotimes X_i\,;\, X_i \bigotimes 1).$$

DIM. Indichiamo con $(\mathbf{S}, \mathbf{P})$ la coppia di omomorfismi di $H$ in $H \bigotimes H$ definita dall'essere per ogni $n \geq 0$:

$$\mathbf{S}(X_n) = \varrho S_n'(1 \bigotimes X_i\,;\, X_i \bigotimes 1), \quad \mathbf{P}(X_n) = \varrho P_n'(1 \bigotimes X_i\,;\, X_i \bigotimes 1).$$

Sia $R$ un anello $p$-adico; l'applicazione $v: R \longrightarrow V_\varrho R$ è bigettiva (cfr. **2.**). Dati inoltre $a_1, a_2 \in R$, e dette $a_{10}, a_{11}, \ldots, a_{20}, a_{21}, \ldots$ le loro componenti moltiplicative, tenuto conto di 4.3, si ha

$$v(a_1 + a_2) = v\left( \sum_{i=0}^{\infty} (a_{1i} + a_{2i})\, p^i \right) =$$

$$= v\left( \sum_{i=0}^{\infty} \left( \sum_{t=0}^{\infty} S_i^{\langle\{t\}\rangle}(a_{1j}\,;\, a_{2j})\, p^t \right) p^i \right) = (\varrho S_0'(\varrho a_{1j}\,;\, \varrho a_{2j}),$$

$\varrho\, S_1'(\varrho\, a_{1j}\,;\, \varrho\, a_{2j}), \ldots) = \mathbf{S}^*\ (v\,(a_1),\, v\,(a_2))$, e analogamente si ha $v(a_1\, a_2) = \mathbf{P}^*\,(v\,(a_1),\, v\,(a_2))$. Quanto precede prova che $v$ è un isomorfismo di $(R;+,\cdot)$ su tutto $(V\varrho R\,;\, \mathbf{S}^*, \mathbf{P}^*)$.

Viceversa sia $(\mathbf{T}, \mathbf{K})$ una coppia di omomorfismi di $H$ in $H \bigotimes H$, tale che per ogni anello $p$-adico $R$ l'applicazione $v$ sia un isomorfismo di $(R;+,\cdot)$ su tutto $(V\varrho R\,;\, \mathbf{T}^*, \mathbf{K}^*)$. Rispetto all'anello $p$-adico $\mathbf{Z}\,[X_i^{p^{-\infty}}\,;\, Y_i^{p^{-\infty}}]^{(p)}$, tenuto conto di 4.3, si ha

$$(T_0\,(X_i\,;\, Y_i),\, T_1\,(X_i\,;\, Y_i), \ldots) = \mathbf{T}^*\,((X_0\,, X_1\,, \ldots), (Y_0\,, Y_1\,, \ldots)) =$$

$$= \mathbf{T}^*\left(v\left(\sum_{i=0}^{\infty} X_i p^i\right),\ v\left(\sum_{i=0}^{\infty} Y_i\, p^i\right)\right) = v\left(\sum_{i=0}^{\infty} X_i\, p^i + \sum_{i=0}^{\infty} Y_i\, p^i\right) =$$

$$= v\left(\sum_{i=0}^{\infty}\left(\sum_{t=0}^{\infty} S_i^{(t)}\,(X_j\,;\, Y_j)\, p^t\right) p^i\right) = (\varrho S_0'\,(X_i\,;\, Y_i),\, \varrho S_1'\,(X_i\,;\, Y_i), \ldots).$$

Le considerazioni precedenti provano che per ogni $n \geq 0$ si ha $T_n\,(1 \bigotimes X_i\,;\, X_i \oplus 1) = \varrho\, S_n'\,(1 \bigotimes X_i\,;\, X_i \bigotimes 1)$, ossia che $\mathbf{T} = \mathbf{S}$. In modo analogo si prova che $\mathbf{K} = \mathbf{P}$, C. V. D..

**7.** Nel numero precedente è stata studiata una particolare coppia di funzioni razionali (cfr. **5.** e **1.**) tali da dotare ogni $Vk$, con $k$ anello perfetto di caratteristica $p$, della struttura di anello $p$-adico di residuo $k$, in modo tale che anche l'operazione di passaggio a quoziente sia espressa da una funzione razionale (nel caso studiato tale funzione è $X_0$).

Le considerazioni seguenti contengono la caratterizzazione di tutte le coppie di funzioni razionali verificanti le dette proprietà, e la caratterizzazione di tutti gli isomorfismi razionali tra strutture indotte da tali funzioni.

Dato un automorfismo $u$ di $H$, indicheremo con $(\mathbf{S}_u\,, \mathbf{P}_u)$ la coppia di omomorfismi di $H$ in $H \bigotimes H$ che rendono commutativi i seguenti diagrammi:

$$\begin{array}{ccc} H & \xrightarrow{\ \mathbf{S}\ } & H \bigotimes H \\ {\scriptstyle u}\uparrow & & \uparrow{\scriptstyle u \bigotimes u} \\ H & \xrightarrow[\ \mathbf{S}_u\ ]{} & H \bigotimes H \end{array}, \qquad \begin{array}{ccc} H & \xrightarrow{\ \mathbf{P}\ } & H \bigotimes H \\ {\scriptstyle u}\uparrow & & \uparrow{\scriptstyle u \bigotimes u} \\ H & \xrightarrow[\ \mathbf{P}_u\ ]{} & H \bigotimes H \end{array}.$$

**7.1** TEOREMA. *Al variare di $u$ tra gli automorfismi di $H$, le $(\mathbf{S}_u\,, \mathbf{P}_u)$ sono le sole coppie di omomorfismi di $H$ in $H \bigotimes H$ verificanti le proprietà seguenti :*

*a) dato comunque un anello perfetto k di caratteristica p,* $(Vk; \mathbf{S}_u^*, \mathbf{P}_u^*)$ *è un anello p adico di residuo k,*

*b) esiste* $h \in H$ *tale che, dato comunque un anello perfetto k di caratteristica p, l'applicazione h risulti un omomorfismo di* $(Vk; \mathbf{S}_u^*, \mathbf{P}_u^*)$ *su tutto* $(k; +, .)$, *di nucleo* $(p)$.

DIM. In quanto segue indicheremo una successione $(a_0, a_1, ...)$ con il simbolo $(a_i/i \geq 0)$.

Sia $u$ un automorfismo di $H$. Per ogni $n \geq 0$ si ha $(u \bigotimes u)\, \mathbf{S}_u\, (X_n) = \mathbf{S}\, u(X_n)$, $(u \bigotimes u)\, S_{u,n}(1 \bigotimes X_j;\ X_j \bigotimes 1/j \geq 0) = \mathbf{S} u_n\, (X_j/j \geq 0)$, $S_{u,n}((u \bigotimes u)(1 \bigotimes X_j);$ $(u \oplus u)\, (X_j \bigotimes 1)/j \geq 0) = u_n\, (\mathbf{S}\, (X_j)/j \geq 0)$, e quindi $S_{u,n}(u_j (1 \bigotimes X_i/i \geq 0);$ $u_j (X_i \bigotimes 1/i \geq 0)/j \geq 0) = u_n\, (S_j (1 \bigotimes X_i;\ X_i \bigotimes 1/i \geq 0)/j \geq 0)$. In modo analogo si prova che per ogni $n \geq 0$ si ha $P_{u,n}(u_j (1 \bigotimes X_i/i \geq 0); u_j (X_i \bigotimes 1/i \geq 0)/$ $/j \geq 0) = u_n\, (P_j (1 \bigotimes X_i;\ X_i \bigotimes 1/i \geq 0)/j \geq 0)$.

Quanto precede prova che per ogni anello perfetto $k$ di caratteristica $p$, e per ogni coppia $(b, b')$ di elementi di $Vk$, si ha $u^*\, \mathbf{S}^*(b, b') = \mathbf{S}_u^*\, (u^*(b),$ $u^*(b'))$, $u^*\, \mathbf{P}^*(b, b') = \mathbf{P}_u^*\, (u^*\, (b), u^*\, (b'))$. Quindi, essendo $u$ un automorfismo di $H$, $u^*$ risulta un isomorfismo di $(Vk; \mathbf{S}^*, \mathbf{P}^*)$ su tutto $(Vk; \mathbf{S}_u^*, \mathbf{P}_u^*)$.

Si prova poi facilmente che $(Vk; \mathbf{S}^*, \mathbf{P}^*)$ è un anello $p$ adico, e che l'applicazione di $Vk$ in $k$ definita da $(b_i/i \geq 0) \longrightarrow b_0$ è un omomorfismo di $(Vk; \mathbf{S}^*, \mathbf{P}^*)$ su tutto $(k; +, .)$, di nucleo $(p)$.

Allora $(Vk; \mathbf{S}_u^*, \mathbf{P}_u^*)$, essendo isomorfo a $(Vk; \mathbf{S}^*, \mathbf{P}^*)$, è un anello $p$-adico di residuo isomorfo a $k$; posto inoltre $h\, (X_i/i \geq 0) = (u^{-1})_0\, (X_i/i \geq 0)$, l'applicazione $h$ risulta un omomorfismo di $(Vk; \mathbf{S}_u^*, \mathbf{P}_u^*)$ su tutto $(k; +, .)$ di nucleo $(p)$.

Sia viceversa $(\mathbf{T}, \mathbf{K})$ una coppia di omomorfismi di $H$ in $H \bigotimes H$ verificanti le proprietà *a*), *b*). Sia inoltre $h$ un elemento di $H$ verificante rispetto a $(\mathbf{T}, \mathbf{K})$ la condizione *b*).

Indichiamo con $(y_i\, (X)/i \geq 0)$ l'elemento di $molt\, (V\, (\mathbf{F}_p[X^{p^{-\infty}}]); \mathbf{T}^*, \mathbf{K}^*)$ tale che $h\, (y_i\, (X)/i \geq 0) = X$. Dato comunque un anello perfetto $k$ di caratteristica $p$, e un elemento $b$ di $k$, si ha che $(y_i(b)/i \geq 0) \in molt\, (Vk; \mathbf{T}^*, \mathbf{K}^*)$, e che $h\, (y_i\, (b)/i \geq 0) = b$; infatti, detto $g$ l'omomorfismo di $\mathbf{F}_p\, [X^{p^{-\infty}}]$ in $k$ definito da $g\, (X) = b$, e detta $\tilde{g}$ l'applicazione di $V\, (\mathbf{F}_p\, [X^{p^{-\infty}}])$ in $Vk$ definita da $\tilde{g}(a_i/i \geq 0) = (g a_i/i \geq 0)$, $\tilde{g}$ risulta un omomorfismo di $(V\, (\mathbf{F}_p\, [X^{p^{-\infty}}]);$ $\mathbf{T}^*, \mathbf{K}^*)$ in $(Vk; \mathbf{T}^*, \mathbf{K}^*)$.

Sia $(u_0\, (X_i/i \geq 0), u_1\, (X_i/i \geq 0), ...)$ l'elemento di $VH$ tale che in $(VH, \mathbf{T}^*, \mathbf{K}^*)$ si abbia $\sum_{i=0}^{\infty} (y_0\, (X_i), y_1\, (X_i), ...)\, p^i = (u_0\, (X_i/i \geq 0), u_1\, (X_i/i \geq 0), ...)$. Dati comunque un anello perfetto $k$ di caratteristica $p$, ed elementi $b_0, b_1, ...$ di $k$, in $(Vk; \mathbf{T}^*, \mathbf{K}^*)$ si ha $\sum_{i=0}^{\infty} (y_0\, (b_i), y_1\, (b_i), ...)\, p^i = (u_0\, (b_i/i \geq 0), u_1\, (b_i/i \geq 0), ...)$;

infatti, detto $g$ l'omomorfismo di $H$ in $k$ definito da $g(X_i) = b_i$, e detta $\tilde{g}$ l'applicazione di $VH$ in $Vk$ definita da $\tilde{g}(a_i/i \geq 0) = (ga_i/i \geq 0)$, $\tilde{g}$ risulta un omomorfismo di $(VH; \mathbf{T}^*, \mathbf{K}^*)$ in $(Vk; \mathbf{T}^*, \mathbf{K}^*)$.

A questo punto, se teniamo conto che per ogni elemento $(b_i/i \geq 0)$ di $Vk$, in $(Vk; \mathbf{S}^*, \mathbf{P}^*)$ si ha $(b_i/i \geq 0) = \sum_{i=0}^{\infty} (b_i, 0, 0, ...) p^i$, e che $(b_i, 0, 0, ...) \in \in molt(Vk; \mathbf{S}^*, \mathbf{P}^*)$ ed ha $b_i$ per residuo in $k$; da 6.1 (cfr. anche [1], II-5, Prop. 10 e il suo Cor.) segue che l'applicazione di $Vk$ in $Vk$ definita da $(b_i/i \geq 0) \longrightarrow (u_0(b_i/i \geq 0), u_1(b_i/i \geq 0), ...)$ è un *isomorfismo di* $(Vk; \mathbf{S}^*, \mathbf{P}^*)$ *su tutto* $(Vk; \mathbf{T}^*, \mathbf{K}^*)$.

Sia adesso $u$ l'endomorfismo di $X$ definito ponendo $u(X_n) = u_n(X_i/i \geq 0)$ Dalle precedenti considerazioni si deduce in particolare che per ogni anello perfetto $k$ di caratteristica $p$, l'applicazione $u^*: Vk \longrightarrow Vk$ è una bigezione.

Allora, essendo in particolare l'applicazione $u^*: VH \longrightarrow VH$ surgettiva, esiste $(z_0(X_i/i \geq 0), z_1(X_i/i \geq 0), ...)$ tale che $u^*(z_0(X_i/i \geq 0), z_1(X_i/i \geq 0), ...) = = (X_i/i \geq 0)$. Sia $z$ l'endomorfismo di $H$ definito ponendo $z(X_n) = z_n(X_i/i \geq 0)$. Si ha $zu(X_n) = zu_n(X_i/i \geq 0) = u_n(zX_i/i \geq 0) = u_n(z_0(X_i/i \geq 0), z_1(X_i/i \geq 0), ...) = = X_n$. Se ne deduce che $zu$ è l'applicazione identica di $H$, e quindi che $u$ è iniettiva; in particolare $z$ è surgettiva.

Consideriamo $z^*$. Per ogni anello perfetto $k$ di caratteristica $p$, $(zu)^* = = u^* z^*$ è l'applicazione identica di $Vk$; siccome $u^*$ è bigettiva, allora anche $z^*$ è bigettiva. Quindi, come fatto per $u$, si prova che $z$ è iniettiva.

Siccome $z$ è anche surgettiva, $z$ è un automorfismo. Allora, siccome $zu$ è l'applicazione identica di $H$, si ha che pure $u$ è un automorfismo.

A questo punto è immediato che $(\mathbf{T}, \mathbf{K}) = (\mathbf{S}_u, \mathbf{P}_u)$, C. V. D..

7.2 COROLLARIO. *Siano $u$, $v$ automorfismi di $H$. Si ha $(\mathbf{S}_u, \mathbf{P}_u) = (\mathbf{S}_v, \mathbf{P}_v)$ se e solo se esiste $n \in \mathbf{Z}$ tale che $uv^{-1} = \pi^n$.*

DIM. Siano $u, v$ automorfismi di $H$ tali che $(\mathbf{S}_u, \mathbf{P}_u) = (\mathbf{S}_v, \mathbf{P}_v)$; poniamo $w = uv^{-1}$. Dalla dimostrazione di 7.1 segue che dato comunque un anello perfetto $k$ di caratteristica $p$, le applicazioni $u^*$, $v^*$ di $Vk$ in $Vk$ sono isomorfismi di $(Vk; \mathbf{S}^*, \mathbf{P}^*)$ rispettivamente su tutto $(Vk; \mathbf{S}_u^*, \mathbf{P}_u^*)$ e su tutto $(Vk; \mathbf{S}_v^*, \mathbf{P}_v^*)$.

Dato che $w^* = (v^*)^{-1} u^*$, e che $(Vk; \mathbf{S}_u^*, \mathbf{P}_u^*) = (Vk; \mathbf{S}_v^*, \mathbf{P}_v^*)$, si ha che l'applicazione $w^*$ di $Vk$ in $Vk$ è un automorfismo di $(Vk; \mathbf{S}^*, \mathbf{P}^*)$.

L'applicazione di $Vk$ in $k$ definita da $(b_i/i \geq 0) \longrightarrow b_0$ è un omomorfismo di $(Vk; \mathbf{S}^*, \mathbf{P}^*)$ su tutto $(k; +, .)$ di nucleo $(p)$; tenuto conto di ciò e delle precedenti osservazioni, si ha che l'applicazione di $k$ in $k$ definita da $c \longrightarrow \longrightarrow w_0(c, b_1, b_2, ...)$ è un automorfismo di $k$ indipendente dalla scelta di $b_1, b_2, ....$ Esiste allora un elemento $y(X) \in \mathbf{F}_p[X^{p^{-\infty}}]$ tale che $w_0(c, b_1, b_2, ...) = y(c)$.

Poniamo $y(X) = \Sigma\, n_q\, X^q$, ove la sommatoria si intende estesa a tutti i $q$ del tipo $mp^{-n}$, con $m$ ed $n$ interi non negativi, ed ove gli $n_q$ sono elementi di $\mathbf{F}_p$ quasi tutti nulli.

In $\mathbf{F}_p\,[X^{p^{-\infty}}, Y^{p^{-\infty}}]$ si deve avere $y(XY) = y(X)\,y(Y)$, cioè $\Sigma\, n_q\,(XY)^q = (\Sigma\, n_q\, X^q)\,(\Sigma\, n_q\, Y^q)$; allora, se $q \neq q'$ si ha $n_q\, n_{q'} = 0$, mentre per ogni $q$ si ha $n_q\, n_q = n_q$. Siccome $y(X) \neq 0$, esiste $\tilde{q}$ tale che $n_{\tilde{q}} \neq 0$, e tale $\tilde{q}$ è unico.

Si ha $\tilde{q} \neq 0$. Altrimenti si avrebbe $y(X) \in \mathbf{F}_p$, cosa ovviamente impossibile.

Le precedenti osservazioni provano che $y(X) = X^{\tilde{q}}$.

Poniamo $\tilde{q} = mp^n$, ove $m$ è un intero positivo primo con $p$, ed $n$ è un intero.

In $\mathbf{F}_p\,[X^{p^{-\infty}}]$ si deve avere $(X+1)^{\tilde{q}} = X^{\tilde{q}} + 1^{\tilde{q}}$, ossia $(X+1)^{mp^n} = X^{mp^n} + 1^{mp^n} = (X^m + 1^m)^{p^n}$. Allora in $\mathbf{F}_p[X]$ si ha $(X+1)^m = X^m + 1^m$; derivando ambo i membri di questa uguaglianza si ottiene $m\,(X+1)^{m-1} = m\,X^{m-1}$. Siccome $m$ è primo rispetto a $p$, si conclude che $m = 1$. Allora $\tilde{q} = p^n$, e quindi $y(X) = X^{p^n}$.

Sia $c \in k$ Siccome $(c, 0, \ldots) \in molt\ (Vk;\ \mathbf{S}^*, \mathbf{P}^*)$, allora $\mathrm{w}^*(c, 0, \ldots) \in \in molt\ (Vk;\ \mathbf{S}^*, \mathbf{P}^*)$; esiste quindi $d \in k$ tale che $\mathrm{w}^*(c, 0, \ldots) = (d, 0, \ldots)$. Siccome inoltre $\mathrm{w}^*(c, 0, \ldots) = (\mathrm{w}_0(c, 0, \ldots), \mathrm{w}_1(c, 0, \ldots), \ldots)$, si ha $\mathrm{w}^*(c, 0, \ldots) = (y(c), 0, \ldots) = (c^{p^n}, 0, \ldots)$.

Tenuto conto di ciò, siccome $\mathrm{w}^*(b_i/i \geq 0) = \mathrm{w}^* \sum_{i=0}^{\infty} (b_i, 0, \ldots)\, p^i = \sum_{i=0}^{\infty} \mathrm{w}^*(b_i, 0, \ldots)\, p^i = \sum_{i=0}^{\infty} (b_i^{p^n}, 0, \ldots)\, p^i = (b_0^{p^n}, b_1^{p^n}, \ldots)$, si conclude che $\mathrm{w}^* = (\pi^n)^*$, ossia che $uv^{-1} = \pi^n$.

Viceversa, siano $n$ un intero, ed $u$, $v$ automorfismi di $H$ tali che $uv^{-1} = \pi^n$. Siccome i diagrammi

$$\begin{array}{ccc} H & \xrightarrow{\mathbf{S}} & H \otimes H \\ {\scriptstyle v}\uparrow & & \uparrow{\scriptstyle v \otimes v} \\ H & \xrightarrow[\mathbf{S}_v]{} & H \otimes H \end{array} \qquad \begin{array}{ccc} H & \xrightarrow{\mathbf{S}} & H \otimes H \\ {\scriptstyle \pi^n}\uparrow & & \uparrow{\scriptstyle \pi^n \otimes \pi^n} \\ H & \xrightarrow[\mathbf{S}]{} & H \otimes H \end{array}$$

sono commutativi, allora il diagramma

$$\begin{array}{ccc} H & \xrightarrow{\mathbf{S}} & H \otimes H \\ {\scriptstyle \pi^n v}\uparrow & & \uparrow{\scriptstyle (\pi^n v) \otimes (\pi^n v)} \\ H & \xrightarrow[\mathbf{S}_v]{} & H \otimes H \end{array}$$

è commutativo. Allora $\mathbf{S}_v = \mathbf{S}_{\pi^{n_v}}$, ed essendo $\pi^n v = u$, si ha $\mathbf{S}_v = \mathbf{S}_u$ Analogamente si prova che $\mathbf{P}_v = \mathbf{P}_u$, C.V.D..

7.3. TEOREMA. *Siano $u, v$ automorfismi di $H$. Al variare di $n$ in $\mathbf{Z}$, gli endomorfismi $u^{-1}\pi^n v$ di $H$ sono i soli tali che, dato comunque un anello perfetto $k$ di caratteristica $p$, l'applicazione $(u^{-1}\pi^n v)^* : Vk \to Vk$ sia un isomorfismo di $(Vk; \mathbf{S}_u^*, \mathbf{P}_u^*)$ su tutto $(Vk; \mathbf{S}_v^*, \mathbf{P}_v^*)$.*

DIM. Sia $w$ un endomorfismo di $H$ tale che, dato comunque un anello perfetto $k$ di caratteristica $p$, l'applicazione $w^*$ sia un isomorfismo di $(Vk; \mathbf{S}_u^*, \mathbf{P}_u^*)$ su tutto $(Vk; \mathbf{S}_v^*, \mathbf{P}_v^*)$. Allora $w$ è un automorfismo di $H$ (cfr. la dim. di 7.1), inoltre l'applicazione $(v^{-1})^* w^* u^* = (uwv^{-1})^*$ è un automorfismo di $(Vk; \mathbf{S}^*, \mathbf{P}^*)$.

Dalla dimostrazione di 7.2 segue che esiste $n \in \mathbf{Z}$ tale che $uwv^{-1} = \pi^n$. Si può quindi concludere che $w = u^{-1}\pi^n v$

Viceversa che ogni applicazione $(u^{-1}\pi^n v)^*$, con $n \in \mathbf{Z}$, sia un isomorfismo di $(Vk; \mathbf{S}_u^*; \mathbf{P}_u^*)$ su tutto $(Vk; \mathbf{S}_v^*, \mathbf{P}_v^*)$, con $k$ anello perfetto di caratteristica $p$, è pressoché ovvio, C. V. D..

## APPENDICE

*Sia $R$ un anello avente tutte le proprietà di un anello $p$-adico, eccettuata eventualmente la perfettezza di $R/(p) = \varrho R$, e sia $\mathcal{V}(\varrho R)$ l'anello dei vettori di Witt a componenti in $\varrho R$.*

*Allora $R$ è isomorfo a $\mathcal{V}(\varrho R)$ se e solo se $\varrho R$ è perfetto.*

DIM. Se $\varrho R$ è perfetto, è ben noto che $R$ è isomorfo a $\mathcal{V}(\varrho R)$ (cfr. [1], II 5, teor. 4, e II-6).

Supponiamo viceversa che $R$ sia isomorfo a $\mathcal{V}(\varrho R)$.

Allora *l'endomorfismo $\pi$ di $\varrho R$ è iniettivo.* Sia infatti $a$ un elemento di $\varrho R$ tale che $\pi a = 0$; si ha $p(a, 0, 0, ...) = (0, \pi a, 0, ...) = (0, 0, ...)$; allora siccome $p$ non è un divisore di zero in $R$ e quindi neppure in $\mathcal{V}(\varrho R)$, si ha $(a, 0, ...) = (0, 0, ...)$, e quindi $a = 0$.

Inoltre *l'endomorfismo $\pi$ di $\varrho R$ è surgettivo.* Altrimenti, esisterebbe un elemento $s$ di $\varrho R$, ma non di $\pi\varrho R$. In tale caso avremmo che $(0, s, 0, ...) \notin p\mathcal{V}(\varrho R)$, mentre $(0, s, 0, ...)^2 = (0, 0, s^{2p}, 0, ...) = p(0, s^2, 0, ...) \in p\mathcal{V}(\varrho R)$. Allora in $\varrho R \cong \mathcal{V}(\varrho R)/p\mathcal{V}(\varrho R)$ esisterebbero elementi non nulli di seconda, e quindi di $p$-esima potenza nulla, il che è assurdo essendo $\pi$ iniettivo,

C. V. D..

## BIBLIOGRAFIA

[1] SERRE, *Corps Locaux*. Hermann, Paris, 1962.

[2] BARSOTTI, *Metodi analitici per varietà abeliane in caratteristica positiva*. Cap. 1, 2; Ann. Sc. Norm. Sup., in 14, 1964, pg. 1.