ENDOMORFISMO DI FROBENIUS E PSEUDOPROLUNGAMENTI DI UN CORPO(*)

di ALDO VOLPI (a Livorno)(**)

SOMMARIO.- *Si studiano i prolungamenti algebrici di un corpo in relazione alle proprietà dell'endomorfismo di Frobenius. Si introduce una struttura algebrica più debole di quella di prolungamento. Si estendono a tale struttura le nozioni di prolungamento separabile e di Galois; si descrivono alcune proprietà degli endomorfismi di tale struttura.*

SUMMARY.- *Algebraic extensions of a field are studied with respect to the proprieties of the endomorphism of Frobenius. An algebraic structure, weaker than that of algebraic extension, is introduced. The notions of separable and Galois extension are extended to that structure; some proprieties of endomorphisms of that structure are described.*

In [2] si definiscono i π-omomorfismi di un prolungamento finito di un corpo k di caratteristica positiva (applicazioni k-lineari che commutano con l'endomorfismo di Frobenius π), e se ne studiano alcune proprietà, ottenendo risultati particolarmente significativi soprattutto nel caso di prolungamenti separabili. Pur essendo in generale falso che il π-isomorfismo tra prolungamenti implichi l'isomorfismo (come visto in [3]), per alcune classi di prolungamenti tale implicazione risulta vera; in particolare in [1] si dimostra che è vera per prolungamenti di Galois.

Per tali prolungamenti sussiste quindi la possibilità di classificazione con classi di semisimiglianza di matrici ad elementi in k.

I problemi che si pongono al riguardo sono pertanto i seguenti:
i) riconoscere le classi di semisimiglianza associate a prolungamenti di Galois, ii) risalire da tali classi alla struttura di prolungamento.

Scopo del presente lavoro è quello di sostituire l'utilizzazione delle classi di semisimiglianza, in sé significative ed estetiche, ma poco maneggevoli, con lo studio di strutture algebriche più facilmente gestibili. In particolare si introduce una struttura algebrica più debole di quella di prolungamento, che abbiamo chiamato *pseudoprolungamento*.

(*) Pervenuto in Redazione il 29 novembre 1988.

(**) Indirizzo dell'Autore: Accademia Navale - 57100 Livorno (Italy).

Si dànno inoltre definizioni che estendono le nozioni di prolungamento separabile e di prolungamento di Galois agli pseudoprolungamenti. Si studiano gli endomorfismi di uno pseudoprolungamento di Galois e si forniscono i risultati ottenuti finora, riguardo alle proprietà dei π-endomorfismi di un prolungamento di Galois che valgono anche, mutatis mutandis, per gli endomorfismi di uno pseudoprolungamento di Galois.

Resta comunque aperto il problema di individuare quali pseudoprolungamenti sono isomorfi a prolungamenti, e di risalire, per tali pseudoprolungamenti, alla struttura di prolungamento.

In quanto segue p è un primo positivo, k è un corpo infinito di caratteristica p, $\bar{k}$ è una chiusura algebrica di k. Tutti i prolungamenti algebrici di k si intendono immersi in $\bar{k}$. $\mathcal{F}_p$ è il corpo fondamentale di caratteristica p; π è l'endomorfismo di Frobenius di $\bar{k}$.

CAPITOLO 1

Endomorfismo di Frobenius e p-polinomi

Sia X una indeterminata su k; si diranno *p-polinomi* su k gli elementi di $k[X]$ del tipo:

$$a_0X^{p^0} + a_1X^{p^1} + \ldots + a_rX^{p^r} .$$

Dato $\theta \in \bar{k}$, si dirà polinomio *p-minimo* di θ su k il generatore monico $f_\theta(X)$ dell'ideale di $k[X]$ generato dai p-polinomi aventi θ per radice. Dalla dimostrazione di 2.1 di [1] segue che $f_\theta(X)$ è un p-polinomio e che le radici di $f_\theta(X)$ formano uno spazio vettoriale su $\mathcal{F}_p$, generato dai coniugati di θ su k.

Nell'anello degli endomorfismi di gruppo di $\bar{k}$, consideriamo il sottoanello, che indicheremo con $k[\pi]$, degli endomorfismi p-polinomiali; cioè quegli endomorfismi $\tilde{\varphi}$ per i quali esiste un p-polinomio $\varphi(X)$ su k, tale che, per ogni $x \in \bar{k}$, $\tilde{\varphi}(x) = \varphi(x)$.

Ovviamente $\pi \in k[\pi]$, e ogni elemento di $k[\pi]$ si può scrivere nella forma:

$$a_0\pi_0 + \ldots + a_r\pi^r, \text{ con } a_0, \ldots, a_r \in k.$$

Si osservi che $k[\pi]$ è un dominio di integrità, non commutativo.

Ogni prolungamento algebrico di k risulta, in modo naturale, un $k[\pi]$-modulo sinistro.

1.1 TEOREMA. *Siano $f(X)$ e $g(X)$ p-polinomi e siano $\tilde{f}$, $\tilde{g}$ i corrispondenti elementi di $k[\pi]$. Se $g(X)$ divide $f(X)$, allora:*

i) esistono $a_1, \ldots, a_r \in k$ e interi non negativi $\lambda_1, \ldots, \lambda_r$ tali che:

$$f(X) = a_1 g(X)^{p^{\lambda_1}} + \ldots + a_r g(X)^{p^{\lambda_r}} ;$$

ii) $\tilde{g}$ è un divisore destro di $\tilde{f}$.

Dim. Possiamo supporre, senza ledere la generalità del ragionamento, che il coefficiente del termine di grado massimo di $g(X)$ sia 1.

Posto $f(X) = h(X)g(X)$, $\deg f(X) = p^{n_1}$, $\deg g(X) = p^m$, $\lambda_1 = n_1 - m$, a_1 = coefficiente di $X^{p^m(p^{\lambda_1-1})}$ in $h(X)$, $g_1(X) = a_1 g(X)\, g(X)^{p^{\lambda_1-1}}$, risulta che il p-polinomio $f(X) - g_1(X)$ è multiplo di $g(X)$ e $\deg (g(X) - g_1(X)) < \deg f(X)$.

Se $f(X) = g_1(X)$, la dimostrazione di (i) è conclusa; altrimenti, posto $\deg (f(X) - g_1(X)) = p^{n_2}$, $\lambda_2 = n_2 - m$, a_2 = coefficiente di $X^{p^m(p^{\lambda_2-1})}$ in $(f(X) - g_1(X)) / g(X)$, $g_2(X) = a_2 g(X)\, g(X)^{p^{\lambda_2-1}}$, risulta che $f(X) - g_1(X) - g_2(X)$ è un p-polinomio multiplo di $g(X)$, e $\deg (f(X) - g_1(X) - g_2(X)) < \deg (f(X) - g_1(X)) < \deg f(X)$.

Iterando il procedimento, per un certo r risulterà:

$$f(X) - g_1(X) - \ldots - g_r(X) = 0,$$

il che prova (i); (ii) è facile conseguenza di (i), c.v.d..

1.2 OSSERVAZIONE. *Se F è un prolungamento finito e separabile di k, allora F è un $k[\pi]$-modulo ciclico.*

Dim. Posto $s = [F : k]$, per il teorema 1.2 di [3], esiste un elemento $\theta \in F$, tale che $(\pi^0(\theta), \ldots, \pi^{s-1}(\theta))$ sia una base di F su k.

Allora θ è un generatore di F come $k[\pi]$-modulo, c.v.d..

Sia F come nel teorema precedente e sia θ un generatore di F come $k[\pi]$-modulo. La matrice M associata a π rispetto alla base $\mathcal{B} = (\pi^0(\theta), \ldots, \pi^{s-1}(\theta))$ di F, risulta del tipo:

$$M = \begin{pmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & \dots & 1 & a_{s-1} \end{pmatrix};$$

il polinomio p-minimo di θ lo possiamo scrivere così:

$$f_\theta(X) = X^{p^s} - a_{s-1}X^{p^{s-1}} - \dots - a_0 X^{p^0}.$$

Sia $x \equiv_{\mathcal{B}} (x_0, \dots, x_{s-1})$; risulta:

$$\pi(X) \equiv_{\mathcal{B}} M \begin{pmatrix} x_0^p \\ \cdot \\ \cdot \\ x_{s-1}^p \end{pmatrix}.$$

1.3 TEOREMA. *Siano* $(\alpha_0, \dots, \alpha_{s-1})$ *le coordinate di* 1 *rispetto a* $\mathcal{B}$, *e sia* $\gamma(X) = \alpha_0 X^{p^0} + \dots + \alpha_{s-1}X^{p^{s-1}}$. *Risulta:*

i) $\alpha_0 \neq 0$, $\alpha_{s-1} \neq 0$;

ii) $f_\theta(X) = \alpha_{s-1}^{-1}(\gamma(X)^p - \gamma(X))$.

Dim. Poiché 1 è unito rispetto a π, θ risulta radice del p-polinomio $\gamma(X)^p - \gamma(X)$, il cui grado non può essere inferiore a p^s; dunque $\alpha_{s-1} \neq 0$ e $f_\theta(X) = \alpha_{s-1}^{-1}(\gamma(X)^p - \gamma(X))$.

Se fosse $\alpha_0 = 0$, allora $D f_\theta(X) = 0$, e ciò è in contrasto con l'ipotesi che F sia separabile; dunque $\alpha_0 \neq 0$, c.v.d..

1.4 COROLLARIO. *Siano* $\tilde{f}_\theta$, $\tilde{\gamma}$, *gli elementi di* $k[\pi]$ *corrispondenti a* $f_\theta(X)$ *e* $\gamma(X)$ *rispettivamente. Allora* $\tilde{f}_\theta = \alpha_{s-1}^{-1}(\pi^1 - \pi^0) \circ \tilde{\gamma}$.

1.5 COROLLARIO. *Il risultato enunciato nel teorema* 1.3 *per* 1, *vale per ogni elemento di* $\mathcal{F}_p - \{0\}$.

1.6 COROLLARIO. *Risulta:*

$$a_0 = \frac{\alpha_0}{\alpha_{s-1}^p},\ a_1 = \frac{\alpha_1 - \alpha_0^p}{\alpha_{s-1}^p},\ \ldots,\ a_{s-1} = \frac{\alpha_{s-1} - \alpha_{s-2}^p}{\alpha_{s-1}^p}.$$

1.7 TEOREMA. *L'ultima coordinata, rispetto a $\mathcal{B}$, di ogni elemento di $\mathcal{F}_p$ è radice del p-polinomio:*

$$g(X) = X^{p^0} - a_{s-1}^{p^0} X^{p^1} - \ldots - a_0^{p^{s-1}} X^{p^s};$$

g(X) non ha altre radici in k.

Dim. Sia $\eta \equiv_{\mathcal{B}} (\beta_0, \ldots, \beta_{s-1})$ un elemento di $\mathcal{F}_p$; poiché $\pi(\eta) = \eta$, risulta:

$$M \begin{pmatrix} \beta_0^p \\ \cdot \\ \cdot \\ \cdot \\ \beta_{s-1}^p \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \cdot \\ \cdot \\ \cdot \\ \beta_{s-1} \end{pmatrix}.$$

Ne segue che β_{s-1} è una radice di $g(X)$.
Sia ora $\beta'_{s-1} \in k$ una radice di $g(X)$; risulta:

$$\beta'_{s-1} - a_{s-1}\beta'^p_{s-1} = a_{s-2}^p \beta'^{p^2}_{s-1} + \ldots + a_0^{p^{s-1}} \beta'^{p^s}_{s-1},$$

che, essendo una p-potenza possiamo porre $= \beta'^p_{s-2}$.

Iterando il procedimento, si determina una s-upla $(\beta'_0, \ldots, \beta'_{s-1})$ che individua un elemento unito rispetto a π.

Poiché gli elementi di F uniti rispetto a π, cioè le radici di $X^p - X$, sono solo gli elementi di $\mathcal{F}_p$, la dimostrazione è conclusa, c.v.d..

1.8 TEOREMA. *Sia μ la somma dei coniugati di θ su k. Allora $f_\theta(X)$ risulta divisibile per il p-polinomio (a coefficienti in k):*

$$\rho(X) = X^p - \mu^{p-1} X.$$

Dim. Per ogni σ appartenente al gruppo di Galois $G(\bar{k}/k)$, risulta $\sigma\mu = \mu$; dunque μ, in quanto separabile e puramente inseparabile su k, è un elemento di k.

Il polinomio $\prod_{\lambda \in \mathcal{F}_p} (X - \lambda\mu)$ è un p-polinomio (in conseguenza del lemma in appendice di [1]) ed è uguale a $\rho(X)$.

Quindi, poiché le radici di $f_\theta(X)$ formano uno spazio vettoriale su $\mathcal{F}_p$, $\rho(X)$ divide $f_\theta(X)$, c.v.d..

CAPITOLO 2

Pseudoprolungamenti di un corpo

Sia V uno spazio vettoriale su k; un endomorfismo di gruppo $P : V \to V$ si dirà *semilineare* se per ogni $u \in V$ e $\alpha \in k$, risulta:

$$P(\alpha u) = \alpha^p P(u).$$

Un endomorfismo semilineare si dirà *non degenere* se trasforma sistemi di vettori linearmente indipendenti in sistemi linearmente indipendenti.

2.1 TEOREMA. *Sia P un endomorfismo semilineare. Se P è non degenere, allora è iniettivo. Se k è perfetto e P è iniettivo, allora P è non degenere.*

Dim. Sia P non degenere e $u \in V$; se $P(u) = 0$, allora il sistema di vettori costituito dal solo vettore u è linearmente dipendente, cioè $u = 0$; ne segue $\ker P = \{0\}$.

Viceversa se $\ker P = \{0\}$ e se k è perfetto, consideriamo $u_1, \ldots, u_r \in V$ e $\beta_1, \ldots, \beta_r \in k$. Le seguenti uguaglianze sono equivalenti:

$$\beta_1 P(u_1) + \ldots + \beta_r P(u_r) = 0,$$

$$P\left(\beta_1^{1/p} u_1 + \ldots + \beta_r^{1/p} u_r\right) = 0;$$

ne segue che P è non degenere, c.v.d..

2.2 OSSERVAZIONE. *Gli elementi uniti di un endomorfismo semilineare formano uno spazio vettoriale su $\mathcal{F}_p$.*

Dim. Ovvia conseguenza della definizione di endomorfismo semilineare, c.v.d..

Si dirà *pseudoprolungamento* di k una coppia (V,P) formata da uno spazio vettoriale V su k e da un endomorfismo semilineare iniettivo P, tale che lo spazio vettoriale su $\mathcal{F}_p$ degli elementi uniti rispetto a P abbia dimensione 1.

Lo pseudoprolungamento si dirà *finito*, se V è di dimensione finita su k.

Si osservi che, preso un elemento $\eta \neq 0$, unito rispetto a P, l'applicazione di k in $< \eta >_k$, che ad ogni $x \in k$ associa $x\eta$ è biiettiva. Nel seguito, per ogni pseudoprolungamento, supporremo di aver fissato un tale η, che chiameremo *identità* dello pseudoprolungamento; l'applicazione biiettiva suddetta induce una struttura di corpo, che indicheremo con $\tilde{k}$, su $<\eta>_k$.

Il sottocorpo $\tilde{\mathcal{F}}_p$ di $\tilde{k}$, costituito dagli elementi uniti rispetto a P, è ovviamente isomorfo al corpo fondamentale $\mathcal{F}_p$.

E' evidente che la restrizione di P a $\tilde{k}$ coincide con l'endomorfismo di Frobenius di k.

Indichiamo con $k[t;p]$ l'anello avente per sostegno l'insieme dei polinomi formali in t, a coefficienti a sinistra,

$$\delta(t) = \delta_0 + \delta_1 t + \ldots + \delta_r t^r,$$

ove t è una indeterminata, e $\delta_0, \ldots, \delta_r \in k$; le operazioni sono l'usuale addizione e la moltiplicazione tale che:

$$(\alpha t^i)\,(\beta t^j) = \alpha \beta^{p^i} t^{i+j}.$$

Come noto (cfr. [4], cap. 3), un tale anello è un dominio di integrità, non commutativo; inoltre, se l'endomorfismo di Frobenius di k è un automorfismo (cioè se k è perfetto), allora $k[t;p]$ è a ideali principali.

Comunque, anche se k non è perfetto, è facile verificare che gli ideali sinistri sono principali, e che, se $\delta(t)$ e $\delta'(t)$ generano lo stesso ideale sinistro, allora esiste $\alpha \in k$ tale che $\delta'(t) = \alpha\,\delta(t)$.

Gli elementi di $k[t;p]$ si chiameranno *(t;p)-polinomi.*

Associando ad ogni $(t;p)$-polinomio $\delta(t) = \delta_0 + \ldots + \delta_r t^r$ l'endomorfismo di gruppo $\delta(P) = \delta_0 P^0 + \ldots + \delta_r P^r$, otteniamo una rappresentazione di $k[t;p]$ in V, e V è un $k[t;p]$-modulo sinistro.

Ogni endomorfismo del tipo $\delta(P)$ si può chiamare un *endomorfismo (t;p)-polinomiale.*

Diremo che lo pseudoprolungamento (V,P) è *ciclico*, se V è ciclico come $k[t;p]$-modulo.

Diremo che (V,P) è *algebrico* su k se per ogni $x \in V$ esiste un $(t;p)$-polinomio non nullo $\delta(t)$, tale che $x \in \ker \delta(P)$.

E' evidente che se (V,P) è finito allora è algebrico.

Sia (V,P) algebrico su k e sia $x \in V$; i $(t;p)$-polinomi $\delta(t)$ tali che $x \in \ker \delta(P)$ formano ovviamente un ideale sinistro. Il generatore monico $\varepsilon(t) = t^s + a_{s-1}t^{s-1} + \ldots + a_0$ di tale ideale si dirà il *$(t;p)$-polinomio minimo* di x su k. Se $a_0 \neq 0$, diremo che x è *separabile* su k; (V,P) si dirà *separabile* se ogni elemento di V è separabile su k.

2.3 TEOREMA. *Sia (V,P) uno pseudoprolungamento finito di k. Risulta:*
i) se P è non degenere, allora (V,P) è separabile;
ii) se (V,P) è ciclico e separabile allora P è non degenere.

Dim. Sia $x \in V$ e $\varepsilon(t) = t^s + a_{s-1}t^{s-1} + \ldots + a_0$ il $(t;p)$-polinomio minimo di x; $P^0(x), \ldots, P^{s-1}(x)$ sono linearmente indipendenti. Se P è non degenere $P^1(x), \ldots, P^s(x)$ sono linearmente indipendenti, perciò $a_0 \neq 0$, e ciò prova (i).

Sia ora v un generatore di V e $n = \dim_k V$; siano $u_1, \ldots, u_r \in V$ linearmente indipendenti. Esistono $(t;p)$-polinomi $\delta_1(t), \ldots, \delta_r(t)$, linearmente indipendenti, di grado $< n$, tali che:

$$u_1 = \delta_1(P)v, \ldots, u_r = \delta_r(P)v.$$

Supponiamo per assurdo che esistano $\lambda_1, \ldots, \lambda_r \in k$, non tutti nulli, tali che:

$$\lambda_1 P(u_1) + \ldots + \lambda_r P(u_r) = 0,$$

cioè:

$$(\lambda_1 P\delta_1(P) + \ldots + \lambda_r P\delta_r(P))v = 0.$$

Per ogni $i \in [0,s-1]$ esistono $\lambda, \alpha \in k$, tali che $\lambda\alpha$ e $\lambda\alpha^p$ sono, rispettivamente, il coefficiente di t^i in $\delta(t) = \lambda_1 \delta_1(t) + \ldots + \lambda_r \delta_r(t)$, e il coefficiente di t^{i+1} in $\delta'(t) = \lambda_1 t\delta_1(t) + \ldots + \lambda_r t\delta_r(t)$. Poiché $\delta(t)$ non è identicamente nullo (altrimenti $u_1, \ldots, u_r$ sarebbero linearmente dipendenti), non è identicamente nullo nemmeno $\delta'(t)$.

Visto che $\delta'(P)v = 0$, si deduce che il grado di $\delta'(t)$ è n; esiste allora $\alpha \in k$ tale che $\alpha\,\delta'(t)$ è il $(t;p)$-polinomio minimo di v; e ciò è in contrasto con l'ipotesi che (V,P) sia separabile, perché il coefficiente di t^0 in $\delta'(t)$ è 0, c.v.d..

Un $(t;p)$-polinomio $\delta(t)$ si dirà *limitato* se $\ker \delta(P)$ è un insieme finito. Si noti che $\ker \delta(P)$ è uno spazio vettoriale su $\mathcal{F}_p$.

2.4 LEMMA. *Siano $\delta(t)$, $\varepsilon(t)$, $\varepsilon'(t)$ $(t;p)$-polinomi limitati, tali che $\delta(P) = \varepsilon(P) \circ \varepsilon'(P)$ e $\ker \varepsilon(P) \subseteq \varepsilon'(P)V$; allora:*

$$\dim_{\mathcal{F}_p} \ker \delta(P) = \dim_{\mathcal{F}_p} \ker \varepsilon(P) + \dim_{\mathcal{F}_p} \ker \varepsilon'(P) .$$

Dim. L'applicazione iniettiva che associa ad ogni elemento $v + \ker \varepsilon'(P)$ di $\ker \delta(P) / \ker \varepsilon'(P)$, l'elemento $u = \varepsilon'(P)v$ di $\varepsilon'(P)V$, ha come insieme dei valori $\ker \varepsilon(P)$.

Dunque se $\ker \delta(P)$ ha p^s elementi e $\ker \varepsilon(P)$ ha p^t elementi, allora $\ker \varepsilon'(P)$ ha p^{s-t} elementi, donde la tesi, c.v.d..

Diremo che uno pseudoprolungamento (V,P) è *di Galois* se è finito, ciclico, separabile, e se, per ogni generatore v, detto $\psi(t)$ il $(t;p)$-polinomio minimo di v, risulta:

$$\dim_{\mathcal{F}_p} \ker \psi(P) = \dim_k V .$$

2.5 TEOREMA. *Sia (V,P) uno pseudoprolungamento di k, finito, ciclico e separabile; sia $n = \dim_k V$; (V,P) è di Galois se e solo se per ogni generatore v di (V,P), detto $\gamma(t)$ il $(t;p)$-polinomio, di grado $< n$, tale che l'identità di (V,P) sia $\eta = \gamma(P)v$, risulta:*

$$\dim_{\mathcal{F}_p} \ker \gamma(P) = n-1 .$$

Dim. Per ogni generatore v di (V,P), consideriamo il $(t;p)$-polinomio $\psi(t) = (t-1)\gamma(t)$; risulta $v \in \ker \psi(P)$. Ne segue che $\psi(t)$ è k- proporzionale al $(t;p)$-polinomio minimo di v.

Tenendo presente che, per definizione di pseudoprolungamento, $\ker (P^1 - P^0)$ ha dimensione 1 su $\mathcal{F}_p$, che $\eta = \gamma(P)v$, e che $\eta \in \ker (P^1 - P^0)$, risulta: $\ker (P^1 - P^0) \subseteq \gamma(P)V$.

Allora, per il lemma 2.4:

$$\dim_{\mathcal{F}_p} \ker \psi(P) = 1 + \dim_{\mathcal{F}_p} \ker \gamma(P) .$$

Ne segue che (V,P) è di Galois se e solo se $\dim_{\mathcal{F}_p} \ker \gamma(P) = n-1$, c.v.d..

2.6 TEOREMA. *Sia F un prolungamento algebrico di k, e sia π l'endomorfismo di Frobenius di F; risulta:*

i) (F,π) è uno pseudoprolungamento algebrico di k;

ii) F è finito come prolungamento se e solo se (F,π) è finito come pseudoprolungamento;

iii) F è separabile come prolungamento se e solo se (F,π) è separabile come pseudoprolungamento;

iv) F è di Galois come prolungamento se e solo se (F,π) è di Galois come pseudoprolungamento.

Dim. (i) e (ii) sono evidenti; (iii) segue dal fatto che, per ogni $x \in F$, $X^{p^s} + a_{s-1} X^{p^{s-1}} + \ldots + a_0 X^{p^0}$ è il p-polinomio minimo di x se e solo se $t^s + a_{s-1}t^{s-1} + \ldots + a_0$ è il $(t;p)$-polinomio minimo di x, e, d'altra parte, $a_0 \neq 0$ se e solo se il p-polinomio minimo non ha radici multiple.

Vediamo (iv): se F è di Galois come prolungamento allora, per (ii) e (iii), (F,π) è finito e separabile come pseudoprolungamento. Inoltre dal teorema 1.2 di [3] segue facilmente che (F,π) è ciclico e che, per ogni generatore θ, la dimensione dello spazio vettoriale su $\mathcal{F}_p$ costituito dalle radici del p-polinomio minimo di θ è uguale alla dimensione di F come spazio vettoriale su k: dunque (F,π) è uno pseudoprolungamento di Galois di k.

Viceversa se (F,π) è di Galois come pseudoprolungamento, allora, per (ii) e (iii), F è finito e separabile come prolungamento. Sia $n = \dim_k F$; preso un generatore θ di (F,π), per il teorema 1.2 di [3], θ ha n coniugati su k, linearmente indipendenti su $\mathcal{F}_p$ e, a priori, appartenenti a una chiusura normale N di F. Siano

$$f_\theta(X) = X^{p^n} + a_{n-1} X^{p^{n-1}} + \ldots + a_0 X^{p^0},$$

$$\psi(t) = t^n + a_{n-1} t^{n-1} + \ldots + a_0,$$

rispettivamente il p-polinomio minimo e il $(t;p)$-polinomio minimo di θ su k. Poiché $\dim_{\mathcal{F}_p} \ker \psi(\pi) = n$, e poiché ogni elemento di $\ker \psi(\pi)$ è una radice, appartenente ad F, di $f_\theta(X)$, si deduce che $N = F$; dunque F è un prolungamento di Galois di k, c.v.d..

CAPITOLO 3

Endomorfismi di uno pseudoprolungamento

Sia (V,P) uno pseudoprolungamento di k; ogni endomorfismo τ di spazio vettoriale di V che commuta con P (cioè tale che $P\circ\tau = \tau\circ P$) si dirà un *endomorfismo dello pseudoprolungamento* (V,P).

L'insieme di tali endomorfismi si indicherà con $\mathcal{P}$; $\mathcal{P}$ è uno spazio vettoriale su $\mathcal{F}_p$.

3.1 OSSERVAZIONE. *Gli elementi di $\mathcal{P}$ commutano con gli endomorfismi $(t;p)$-polinomiali; cioè per ogni $\tau \in \mathcal{P}$, e per ogni $\delta(t) \in k[t;p]$, risulta $\tau\circ\delta(P) = \delta(P)\circ\tau$.*

3.2 OSSERVAZIONE. *Sia $\delta(t) \in k[t;p]$; se $z \in \ker \delta(P)$, allora, per ogni $\tau \in \mathcal{P}$, $\tau(z) \in \ker \delta(P)$.*

3.3 OSSERVAZIONE. *Per ogni $\tau \in \mathcal{P}$, $\tau(\eta) \in \tilde{\mathcal{F}}_p$.*

Dim. Poiché $\eta \in \ker (P^1 - P^0)$, allora, per 3.2, $\tau(\eta) \in \ker (P^1 - P^0)$; ne segue che esiste $\lambda \in \mathcal{F}_p$ tale che $\tau(\eta) = \lambda\eta$, c.v.d..

In quel che segue (V,P) è uno pseudoprolungamento di Galois di k, v è un generatore di (V,P), e $\psi(t) = t^n - a_{n-1}t^{n-1} - \ldots - a_0$ è il $(t;p)$-polinomio minimo di v.

Posto che $\eta = \gamma(P)v = (\gamma_0 P^0 + \ldots + \gamma_{n-1}P^{n-1})v$ sia l'identità di (V,P), si noti che, poiché $v \in \ker (P^1 - P^0)\circ\gamma(P)$, risulta $\gamma_{n-1} \neq 0$ e:

$$\psi(t) = \gamma_{n-1}^{-1}\,(t\text{-}1)\,\gamma(t).$$

Sia $< , > : V \times P \to V$ l'applicazione $\mathcal{F}_p$-bilineare tale che $<u,\tau> = \tau(u)$.

3.4 TEOREMA. *L'applicazione $<v, >$ è un $\mathcal{F}_p$- isomorfismo da $\mathcal{P}$ su $\ker \psi(P)$.*

Dim. Tenuto conto dell'oss. 3.2, per ogni $\tau \in \mathcal{P}$, risulta $<v,\tau> \in \ker \psi(P)$.

Sia ora z un qualunque elemento di $\ker \psi(P)$; l'applicazione lineare τ tale che

$$\tau(P^0 v) = P^0 z, \tau(P^1 v) = P^1 z, \ldots, \tau(P^{n-1} v) = P^{n-1} z,$$

è l'unico elemento di $\mathcal{P}$ tale che $\tau(v) = z$.

Controlliamo che τ commuta con P.

Per ogni $u \in V$, $u = \lambda_0 P^0 v + \ldots + \lambda_{n-1} P^{n-1} v$, risulta:

$$\tau(Pu) = \tau((\lambda_{n-1}^p a_0)v + (\lambda_{n-1}^p a_1 + \lambda_0^p)Pv + \ldots + (\lambda_{n-1}^p a_{n-1} + \lambda_{n-2}^p)P^{n-1} v) =$$

$$\lambda_{n-1}^p a_0 \tau(v) + (\lambda_{n-1}^p a_1 + \lambda_0^p)\tau(Pv) + \ldots + (\lambda_{n-1}^p a_{n-1} + \lambda_{n-2}^p)\tau(P^{n-1} v);$$

$$P\tau(u) = P(\lambda_0 \tau(v) + \lambda_1 P\tau(v) + \ldots + \lambda_{n-1} P^{n-1} \tau(v)) =$$

$$\lambda_0^p P\tau(v) + \ldots + \lambda_{n-2}^p P^{n-1} \tau(v) + \lambda_{n-1}^p P^n \tau(v).$$

Poiché $\tau(v) \in \ker \psi(P)$, risulta:

$$\lambda_{n-1}^p P^n \tau(v) = \lambda_{n-1}^p (a_0 P^0 \tau(v) + \ldots + a_{n-1} P^{n-1} \tau(v)).$$

Quindi $\tau(Pu) = P\tau(u)$, c.v.d..

3.5 COROLLARIO. *Risulta:* $\dim_{\mathcal{F}_p} \mathcal{P} = n$.

3.6 OSSERVAZIONE. *Sia* $S = \{\tau \in \mathcal{P} : <\eta,\tau> = 0\}$, *risulta:*

$$<v,S> = \ker \gamma(P).$$

Dim. Se $z \in <v,S>$, allora esiste $\tau \in S$ tale che $z = <v,\tau>$; quindi $\gamma(P)z = \gamma(P)<v,\tau> = <\gamma(P)v,\tau> = 0$. Viceversa se $z \in \ker \gamma(P)$, considerato l'elemento τ di $\mathcal{P}$ tale che $<v,\tau> = z$, risulta:

$$<\eta,\tau> = <\gamma(P)v,\tau> = \gamma(P)<v,\tau> = \gamma(P)z = 0,$$

c.v.d..

Indichiamo con $\mathcal{F}$ l'insieme degli elementi di $\mathcal{P}$ che lasciano fisso η (e perciò $\tilde{k}$).

3.7 OSSERVAZIONE. *Risulta:*

i) $\mathcal{F} = \mathrm{id} + S$;

ii) $<v,\mathcal{F}> = v + \ker \gamma(P)$.

3.8 TEOREMA. *Sia $\mathcal{T}$ l'ideale sinistro di k[t;p] costituito dai (t;p)-polinomi $\delta(t)$ tali che* $\ker \gamma(P) \subseteq \ker \delta(P)$.

I seguenti asserti sono equivalenti:

i) gli elementi di V lasciati fissi da $\mathcal{F}$ sono solo quelli appartenenti a $\tilde{k}$;

ii) $\gamma(t)$ genera $\mathcal{T}$

Dim. Come osservato nel cap. 2, gli ideali sinistri di $k[t;p]$ sono principali; se $\gamma(t)$ non genera $\mathcal{T}$ allora, preso un generatore $\varepsilon(t) = \varepsilon_0 t^0 + \ldots + \varepsilon_{n-1} t^{n-1}$, le n-uple $(\gamma_0, \ldots, \gamma_{n-1})$, $(\varepsilon_0, \ldots, \varepsilon_{n-1})$ risultano linearmente indipendenti.

Allora $\varepsilon(P)v \notin \tilde{k}$ e, poiché $\ker \gamma(P) \subseteq \ker \varepsilon(P)$, $\varepsilon(P)v$ è lasciato fisso da $\mathcal{F}$.

Viceversa, se $\gamma(t)$ genera $\mathcal{T}$ si consideri un elemento

$$z = (\alpha_0 P^0 + \ldots + \alpha_{n-1} P^{n-1})v,$$

lasciato fisso da $\mathcal{F}$. Risulta:

$$\ker \gamma(P) \subseteq \ker (\alpha_0 P^0 + \ldots + \alpha_{n-1} P^{n-1}),$$

e perciò:

$$\alpha_0 t^0 + \ldots + \alpha_{n-1} t^{n-1} = \lambda \gamma(t),$$

ove $\lambda \in k$ (essendo il grado di $\gamma(t)$ uguale a n-1).

Quindi $z = \lambda\eta \in \tilde{k}$, c.v.d..

3.9 TEOREMA. *$\mathcal{F}$ genera $\mathcal{P}$ come spazio vettoriale su $\mathcal{F}_p$.*

Dim. Sia $\tau \in \mathcal{P}$; per l'oss. 3.3, esiste $\lambda \in \mathcal{F}_p$ tale che $\tau(\eta) = \lambda\eta$.

Se $\lambda \neq 0$, si può scrivere $\tau = \lambda(\lambda^{-1}\tau)$, e $\lambda^{-1}\tau \in \mathcal{F}$; se $\lambda = 0$, si può scrivere $\tau = \mathrm{id} - (\mathrm{id} - \tau)$, e id, id-$\tau \in \mathcal{F}$, c.v.d..

3.10 OSSERVAZIONE. *Un endomorfismo τ di (V,P) è biiettivo (cioè è un automorfismo di (V,P)) se e solo se $\tau(v)$ è un generatore di (V,P).*

Dim. Infatti τ è biiettivo se e solo se trasforma la base

$$(P^0 v, \ldots, P^{n-1} v)$$

di V, in una base di V:

$$(P^0\tau(v), \dots, P^{n-1}\tau(v)).$$

Il che equivale a dire che $\tau(v)$ è un generatore di (V,P), c.v.d..

Sia $\mathcal{H}$ il gruppo degli automorfismi di (V,P) che lasciano fisso $\tilde{k}$ $(\mathcal{H} \subseteq \mathcal{F})$.

3.11 LEMMA. *Sia $\tau \in \mathcal{P}$; se esiste $\lambda \in \mathcal{F}_p - \{0\}$ non autovalore di τ, allora τ è combinazione lineare su $\mathcal{F}_p$ di elementi di $\mathcal{H}$.*

Dim. Preso $\lambda \in \mathcal{F}_p - \{0\}$, non autovalore di τ, risulta $\ker(\tau - \lambda\,\mathrm{id}) = \{0\}$. Quindi τ è uguale alla somma di due elementi di $\mathcal{H}$: $\tau - \lambda\,\mathrm{id}$, $\lambda\,\mathrm{id}$, c.v.d..

3.12 TEOREMA. *Sia $p > 2$; $\mathcal{H}$ genera $\mathcal{P}$ come spazio vettoriale su $\mathcal{F}_p$.*

Dim. Sia $\tau \in \mathcal{P}$; vogliamo verificare che τ è combinazione lineare su $\mathcal{F}_p$ di elementi di $\mathcal{H}$ Supponiamo che ogni elemento di $\mathcal{F}_p - \{0\}$ sia autovalore di τ (in caso contrario la conclusione è immediata conseguenza del lemma 3.11).

Siano $A_1(\tau), \dots, A_{p-1}(\tau)$ gli autospazi di τ, relativi agli autovalori 1, ..., p-1, rispettivamente, e sia $A_0(\tau) = \ker\tau$; $A_0(\tau) + \dots + A_{p-1}(\tau)$ è una somma diretta.

Consideriamo l'endomorfismo τ^{p-1}; risulta:

$$A_0(\tau^{p-1}) \supseteq A_0(\tau),$$

$$A_1(\tau^{p-1}) \supseteq A_1(\tau) \oplus \dots \oplus A_{p-1}(\tau),$$

e quindi $\dim A_1(\tau^{p-1}) > \dim A_1(\tau)$.

Se 2 è un autovalore di τ^{p-1}, si considera $\tau^{(p-1)^2}$; risulta:

$$A_0(\tau^{(p-1)^2}) \supseteq A_0(\tau^{p-1}),$$

$$A_1(\tau^{(p-1)^2}) \supseteq A_1(\tau^{p-1}) \oplus \dots \oplus A_{p-1}(\tau^{p-1}),$$

e quindi $\dim A_1(\tau^{(p-1)^2}) > \dim A_1(\tau^{p-1})$.

Iterando il procedimento e tenendo conto che la dimensione di V è finita, si può concludere che esiste un r_0 tale che 2 non è autovalore di $\tau^{(p-1)^{r_0}}$.

Posto $\sigma_1 = \tau - \tau^{(p-1)^{r_0}}$, risulta: $\ker \sigma_1 \supseteq A_0(\tau) \oplus A_1(\tau)$.

Se esiste un elemento di $\mathcal{F}_p - \{0\}$ non autovalore di σ_1, allora $\tau = \tau^{(p-1)^{r_0}} + \sigma_1$ è combinazione lineare su $\mathcal{F}_p$ di elementi di $\mathcal{H}$ (per il lemma 3.11).

In caso contrario esiste r_1 tale che 2 non è autovalore di $\sigma_1^{(p-1)^{r_1}}$ e, posto $\sigma_2 = \sigma_1 - \sigma_1^{(p-1)^{r_1}}$, risulta:

$$\ker \sigma_2 \supseteq A_0(\sigma_1) \oplus A_1(\sigma_1).$$

Inoltre, poiché $A_0(\sigma_1) \supseteq A_0(\tau) \oplus A_1(\tau)$ e $A_1(\sigma_1) \neq \{0\}$, risulta:

$$\dim A_0(\sigma_1) \oplus A_1(\sigma_1) > \dim A_0(\tau) \oplus A_1(\tau).$$

Se esiste un elemento di $\mathcal{F}_p - \{0\}$ non autovalore di σ_2, allora $\tau = \tau^{(p-1)^{r_0}} + \sigma_1^{(p-1)^{r_1}} + \sigma_2$ è combinazione lineare su $\mathcal{F}_p$ di elementi di $\mathcal{H}$ (per il lemma 3.11).

Iterando il procedimento e tenendo presente che V è di dimensione finita, si conclude che ogni elemento $\tau \in \mathcal{P}$ è combinazione lineare su $\mathcal{F}_p$ di elementi di $\mathcal{H}$ c.v.d..

BIBLIOGRAFIA

[1] M. POLETTI, *Prolungamenti finiti di un corpo e iperalgebre*, Ist. Naz. Alta Mat., Symposia Math., *15* (1975), pg. 461.

[2] M. POLETTI, *Prolungamenti finiti di un corpo ed algebre gruppali*, Ann. Mat. pura e appl., (IV) *115* (1977), pg. 381.

[3] M. POLETTI and A. VOLPI, *π-omomorfismi e loro rappresentazione*, Ann. Scuola Norm. Sup. Pisa, (IV) *8* n.1 (1981), pg. 119.

[4] N. JACOBSON, *The theory of rings*, American Math. Soc., 1943.