SOVRAANELLI DI UN CORPO E PROLUNGAMENTI DI GALOIS (*)

di ALDO VOLPI (a Livorno) (**)

SOMMARIO. - *Si presenta una classificazione analitica dei prolungamenti di Galois di un corpo k di caratteristica positiva. Tale classificazione è basata su proprietà dell'endomorfismo di Frobenius. Lo strumento principale consiste nello studio di "moltiplicatori", in sovraanelli di k, visti come endomorfismi di spazio vettoriale.*

SUMMARY. - *An analytic classification of Galois extensions of a field k, of positive characteristic, is introduced. Such classification is based on proprieties of Frobenius endomorphism. The main tool consists in the study of "multiplicators", in overrings of k, viewed as vector space endomorphisms.*

Dato un corpo k e un sovraanello commutativo V, di dimensione finita su k, esiste un sottoanello di $\mathrm{End}_k V$ ad esso isomorfo, che potremmo chiamare l'anello dei "moltiplicatori". Se V è un prolungamento di Galois (cioè finito, separabile, normale) di k, e $v \in V$ è un elemento i cui coniugati costituiscono una base di V, allora il sottocorpo di $\mathrm{End}_k V$ isomorfo a V è descrivibile in funzione dell'endomorfismo "moltiplicazione per v" e degli automorfismi appartenenti al gruppo di Galois G di V su k.

Traendo spunto da tali considerazioni, e fissati opportunamente, in uno spazio vettoriale V su k, un gruppo $G \subseteq \mathrm{Aut}_k V$ e $v \in V$, si definiscono particolari strutture di anello in V, dette (k, G, v)-anelli. Si forniscono condizioni necessarie e sufficienti affinché, dato un elemento $\varphi \in \mathrm{Aut}_k V$, esista una struttura di (k, G, v)–anello in V, tale che φ sia la "moltiplicazione per v", e si definisce esplicitamente la "moltiplicazione" in V, in funzione di G, v, φ.

Nel caso in cui k abbia caratteristica positiva, ogni struttura di pro-

---

(*) Pervenuto in Redazione il 20 dicembre 1989.

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

lungamento di Galois di k, con gruppo di Galois G, oltre ad essere un (k, G, v)-anello, è anche uno "pseudoprolungamento" di k (cfr. [4]).

Ai fini di una classificazione dei prolungamenti di Galois di k assume quindi particolare interesse lo studio dell'intersezione della classe delle strutture di (k, G, v)-anello, con la classe delle strutture di pseudoprolungamento di k. In tal senso il risultato principale ottenuto nel presente lavoro è quello enunciato nel teorema 3.3.

Come detto nell'introduzione di [4], sussiste la possibilità di classificare i prolungamenti di Galois di k con classi di semisimiglianza di matrici associate all'endomorfismo di Frobenius π. Infatti M. Poletti ha dimostrato (cfr. teoremi 2.1 di [1] e 3.4 di [2]) che se due tali prolungamenti sono π-isomorfi (cioè se esiste una applicazione dall'uno nell'altro k-lineare, biiettiva e che commuta con π), allora essi sono isomorfi.

Nel teorema 3.4 del presente lavoro si fornisce una risposta al problema rimasto aperto in [4]; si determina, cioè, un elenco di condizioni analitiche necessarie e sufficienti affinché una classe di semisimiglianza di matrici ad elementi in k individui almeno una struttura di prolungamento di Galois di k. Inoltre, nota una di tali strutture, si descrivono le eventuali altre strutture dello stesso tipo.

CAPITOLO 1

Sia k un corpo, N un suo prolungamento di Galois, e sia $G = \mathcal{G}(N/k) = \{\sigma_1, \ldots, \sigma_n\}$ il gruppo di Galois di N su k. Supponiamo che σ_1 sia l'applicazione identica di N.

Sia inoltre $\omega_1 = \sigma_1(\omega), \ldots, \omega_n = \sigma_n(\omega)$ una base normale di N su K; G opera transitivamente su $\{\omega_1, \ldots, \omega_n\}$.

Poniamo $\lambda = \sum_{i=1}^{n} \omega_i$; risulta $\lambda \in k - \{0\}$.

In quel che segue indicheremo con $(N, +, \cdot)$ la suddetta struttura di prolungamento.

1.1. PROPOSIZIONE. *Per ogni $\tau \in Aut_k N$, tale che $\tau(1) = 1$, esiste una e una sola struttura $(N, +, *)$ di prolungamento di k, tale che τ sia un isomorfismo tra i prolungamenti $(N, +, \cdot)$ e $(N, +, *)$. Il gruppo di Galois di $(N, +, *)$ è $\tau \circ G \circ \tau^{-1}$.*

Dim. Per ogni $u, u' \in N$, definiamo:

$$u * u' = \tau(\tau^{-1}(u)\tau^{-1}(u'))\ ;$$

$(N, +, *)$ è l'unica struttura di prolungamento verificante la proprietà richiesta. L'ultimo asserto è evidente, c.v.d..

1.2. PROPOSIZIONE. *Due elementi $\tau, \rho \in Aut_k N$, tali che $\tau(1) = \rho(1) = 1$, individuano (nel senso della prop. precedente) una stessa struttura di prolungamento se e solo se $\tau^{-1} \circ \rho \in G$.*

Dim. Se τ e ρ individuano una stessa struttura è evidente che $\tau^{-1} \circ \rho$ è un automorfismo di $(N, +, \cdot)$.

Viceversa se esiste $\sigma \in G$ tale che $\tau^{-1} \circ \rho = \sigma$, allora, per ogni $u \in N$:

$$\tau(\tau^{-1}(u)\tau^{-1}(u')) = (\rho \circ \sigma^{-1})((\sigma \circ \rho^{-1})(u)(\sigma \circ \rho^{-1})(u')) =$$

$$(\rho \circ \sigma^{-1} \circ \sigma)(\rho^{-1}(u)\rho^{-1}(u')) = \rho(\rho^{-1}(u)\rho^{-1}(u'))\ .$$

Segue l'asserto, c.v.d..

1.3. COROLLARIO. *Per ogni struttura $(N, +, *)$ di prolungamento di k isomorfo a $(N, +, \cdot)$ esistono n isomorfismi di prolungamento da $(N, +, \cdot)$ in $(N, +, *)$.*

Dim. Detto τ un isomorfismo da $(N, +, \cdot)$ in $(N, +, *)$, ogni altro tale isomorfismo è del tipo $\tau \circ \sigma$, con $\sigma \in G$ (cfr. prop. precedente); perciò il numero di tali isomorfismi è n, c.v.d..

Sia $T = \{\tau \in \mathrm{Aut}_k N / \tau(\omega) = \omega,\ \tau \circ G \circ \tau^{-1} = G\}$.

1.4. PROPOSIZIONE. *Risulta:*

i) T è un sottogruppo di $Aut_k N$;

ii) per ogni $\tau \in T$, $\tau(1) = 1$.

Dim. È evidente che T è un sottomonoide di $\mathrm{Aut}_k N$. Inoltre per ogni $\tau \in T$ risulta $\tau^{-1}(\omega) = \omega$, e, per ogni $\sigma \in G$, esiste $\tilde{\sigma} \in G$ tale che $\sigma = \tau \circ \tilde{\sigma} \circ \tau^{-1}$; quindi $\tau^{-1} \circ \sigma(\tau^{-1})^{-1} = \tilde{\sigma}$. Ciò prova (i).

Risulta:

$$\tau(\lambda) = \tau\left(\sum_{i=1}^{n} \omega_i\right) = \sum_{i=1}^{n}(\tau \circ \sigma_i)(\omega) = \sum_{i=1}^{n}(\sigma_i \circ \tau)(\omega) = \sum_{i=1}^{n} \omega_i = \lambda\,.$$

Poiché $\lambda \in k - \{0\}$, tutti gli elementi di k sono elementi uniti di τ; ne segue l'asserto (ii), c.v.d..

Gli elementi di T inducono, nel senso della prop. 1.1, una struttura di prolungamento di Galois su N, con lo stesso gruppo di Galois G ed una stessa base normale $(\omega_1, \ldots, \omega_n)$.

T opera su $\{\omega_1, \ldots, \omega_n\}$; infatti, per ogni $i \in [1, n]$, esiste $j \in [1, n]$, tale che $\tau(\omega_i) = (\tau \circ \sigma_i)(\omega) = (\sigma_j \circ \tau)(\omega) = \omega_j$. È inoltre evidente che G opera transitivamente su $\{\omega_1, \ldots, \omega_n\}$.

Indichiamo con G' e T' i sottogruppi del gruppo simmetrico S_n che rappresentano, rispettivamente, G e T.

Risulta $G' = \{s_1, \ldots, s_n\}$, ove, per ogni $i \in [1, n]$, s_i è la permutazione tale che

$$\omega_{s_i(j)} = \sigma_i(\omega_j)\,,\ j = 1, \ldots, n\,.$$

Risulta inoltre:

$$T' = \{t \in S_n / t(1) = 1,\ t \circ G' \circ t^{-1} = G'\}\,.$$

Si osservi che $G \simeq G'$, $T \simeq T'$.

1.5. PROPOSIZIONE. *Le matrici associate ad elementi di T rispetto alla base $(\omega_1, \ldots, \omega_n)$ sono tutte e sole quelle che si ottengono dalla matrice identica effettuando una permutazione t delle colonne, ove $t \in T'$.*

La dimostrazione è immediata.

Diremo (ω, G)-*isomorfa* ad $(N, +, \cdot)$ una struttura $(N, +, *)$ di prolungamento di k, tale che esista un isomorfismo tra le due strutture che lasci fisso ω e tale che abbia lo stesso gruppo di Galois G.

1.6 PROPOSIZIONE. *Il numero delle strutture di prolungamento di k definibili in N e (ω, G)-isomorfe a $(N, +, \cdot)$ coincide con l'ordine del gruppo T.*

Dim. Se τ e ρ sono due elementi di T che inducono la stessa struttura, allora esiste $\sigma_i \in G$ tale che $\rho = \tau \circ \sigma_i$ (cfr. prop. 1.2); quindi $\omega = \rho(\omega) = \tau(\sigma_i(\omega))$.

Se fosse $i \neq 1$, risulterebbe $\tau(\omega_i) = \omega$, $\tau(\omega) \neq \omega$, $\tau \notin T$, contro l'ipotesi; dunque $\rho = \tau \circ \sigma_1 = \tau$.

Gli elementi di T risultano perciò in corrispondenza biunivoca con le strutture in esame, c.v.d..

Consideriamo l'applicazione $g : N \to \mathrm{End}_k N$, tale che, per ogni $x \in N$, $g(u)(x) = ux$; sia $\mathcal{N} = g(N)$.

1.7 PROPOSIZIONE.

i) g è un isomorfismo di anelli da N su $\mathcal{N}$, tale che, per ogni $\alpha \in k$, $g(\alpha) = \alpha\sigma_1$;

ii) per ogni $\psi \in \mathcal{N}$, $g^{-1}(\psi) = \psi(1)$;

iii) gli elementi del gruppo di Galois di $\mathcal{N}$ su $k\sigma_1$ sono le applicazioni $\tilde{\sigma}_i$, $i = 1, \ldots, n$, tali che, per ogni $\psi \in \mathcal{N}$, $\tilde{\sigma}_i(\psi) = \sigma_i \circ \psi \circ \sigma_i^{-1}$.

Dim. Presi $u, u' \in N$ e posto $g(u) = \psi$, $g(u') = \psi'$, risulta, per ogni $x \in N$:

$$g(uu')(x) = uu'x = (\psi \circ \psi')(x) = (g(u) \circ g(u'))(x) \ ;$$

$$g(u + u')(x) = (u + u')x = \psi(x) + \psi'(x) = (g(u) + g(u'))(x);$$

$$\text{per ogni } \alpha \in k,\ g(\alpha)(x) = \alpha x = \alpha\sigma_1(x) \ .$$

Inoltre $g(u) = 0$ se e solo se $u = 0$; e con ciò si è provato (i).

L'asserto (ii) è evidente.

Per provare (iii) si osservi che un coniugato di un elemento $\psi = g(u) \in \mathcal{N}$ è immagine, tramite g, di un coniugato di u; poniamo perciò, per ogni $\psi \in \mathcal{N}$:

$$\tilde{\sigma}_i(\psi) = g(\sigma_i(g^{-1}(\psi))),\ i = 1, \ldots n.$$

Per ogni $x \in N$, risulta

$$\tilde{\sigma}_i(\psi)(x) = \sigma_i(u)x = \sigma_i(u\sigma_i^{-1}(x)) = (\sigma_i \circ \psi \circ \sigma_i^{-1})(x) \ ,$$

c.v.d. .

Sia $\tau \in Aut_k N$, tale che $\tau(1) = 1$, e sia $(N, +, *)$ la struttura associata nel senso della prop.1.1; sia $g^* : N \to \mathrm{End}_k N$ tale che $g^*(u)(x) = u * x$.

1.8. PROPOSIZIONE. *Posto* $\mathcal{M} = g^*(N)$, *risulta* $\mathcal{M} = \tau \circ \mathcal{N} \circ \tau^{-1}$.

Dim. Sia $u \in N$ e sia $g(\tau^{-1}(u)) = \psi$; per ogni $x \in N$, risulta:

$$g^*(u)(x) = u * x = \tau(\tau^{-1}(u)\tau^{-1}(x)) =$$

$$\tau(g(\tau^{-1}(u))(\tau^{-1}(x))) = (\tau \circ \psi \circ \tau^{-1})(x) ,$$

c.v.d. .

Nel seguito di questo capitolo supponiamo che la caratteristica di k sia un numero positivo p; indichiamo con $\mathbf{F}_p$ il corpo fondamentale di caratteristica p.

1.9. PROPOSIZIONE. *Se una struttura di prolungamento di Galois di k, definita in N, ha lo stesso endomorfismo di Frobenius di $(N, +, \cdot)$, allora è isomorfa a $(N, +, \cdot)$.*

Dim. L'applicazione identica di N risulta un isomorfismo di spazi vettoriali che commuta con l'endomorfismo di Frobenius. Dunque (cfr. teoremi 2.1 di [1] e 3.4 di [2]) le due strutture di prolungamento di k sono isomorfe, c.v.d. .

1.10. PROPOSIZIONE. *Se due strutture di prolungamento di Galois di k, definite in N, sono (ω, G)-isomorfe ed hanno lo stesso endomorfismo di Frobenius, allora coincidono.*

Dim. Sia τ un isomorfismo di prolungamenti tale che $\tau(\omega) = \omega$. Come noto (cfr. teorema 1.2 di [3]), $(\omega^{p^0}, \ldots, \omega^{p^{n-1}})$ è una base di N. Poiché risulta $\tau(\omega^{p^0}) = \omega^{p^0}, \ldots, \tau(\omega^{p^{n-1}}) = \omega^{p^{n-1}}$, τ è l'applicazione identica; ne segue l'asserto, c.v.d. .

1.11. TEOREMA. *Per ogni $\tau \in Aut_k N$ risultano equivalenti i seguenti asserti:*

i) τ è un isomorfismo di corpi da $(N,+,\cdot)$ in una struttura di corpo $(N,+,*)$ avente lo stesso endomorfismo di Frobenius π;

ii) esistono $\mu_1,\ldots,\mu_n \in \mathbf{F}_p$, tali che $\tau = \mu_1\sigma_1 + \ldots + \mu_n\sigma_n$.

Dim. Se vale (i) risulta $\tau \circ \pi = \pi \circ \tau$; quindi (cfr. [2]) τ è un π-endomorfismo di $(N,+,\cdot)$. Per il teorema 1.1 di [2] esistono $\mu_1,\ldots,\mu_n \in \mathbf{F}_p$ tali che $\tau = \mu_1\sigma_1 + \ldots + \mu_n\sigma_n$.

Viceversa supponiamo che τ verifichi (ii). Per ogni $u, u' \in N$ definiamo: $u * u' = \tau(\tau^{-1}(u)\tau^{-1}(u'))$. È evidente che $(N,+,*)$è un corpo e che τ è un isomorfismo da $(N,+,\cdot)$ in $(N,+,*)$. Indichiamo con π^* l'endomorfismo di Frobenius di $(N,+,*)$. Risulta $\tau \circ \pi = \pi^* \circ \tau$; poiché τ è un π-endomorfismo di $(N,+,\cdot)$ (cfr. il già citato teorema 1.1 di [2]), risulta $\tau \circ \pi = \pi \circ \tau$. Quindi $\pi = \pi^*$, c.v.d..

1.12. COROLLARIO. *Il numero delle strutture $(N,+,*)$ di prolungamento di un sottocorpo $\tilde{k}$ isomorfo a k, tali che $(N,+,*)$ e $(N,+,\cdot)$ abbiano lo stesso endomorfismo di Frobenius è finito.*

1.13. COROLLARIO. *Se $\tau \in Aut_k N$ verifica una delle condizioni equivalenti del teorema 1.11, allora l'identità di $(N,+,*)$ è un elemento del sottocorpo fondamentale di k.*

Dim. Posto $\tau = \mu_1\sigma_1 + \ldots + \mu_n\sigma_n$ con $\mu_1 \ldots \mu_n \in \mathbf{F}_p$, l'identità di $(N,+,*)$ è $\tau(1) = \mu_1 + \ldots + \mu_n$, c.v.d..

1.14. COROLLARIO. *Sia τ come in 1.13; l'insieme degli elementi del corpo $\tilde{k} = \tau(k)$ coincide con l'insieme degli elementi di k.*

CAPITOLO 2

Sia k un corpo e sia V un sovraanello di k di dimensione finita n su k. Sia $G = \{\sigma_1,\ldots,\sigma_n\}$ un gruppo di automorfismi di anello di V, che siano l'identità su k; sia σ_1 l'applicazione identica di V.

Supponiamo che:

i) esista $v \in V$ tale che $\sigma_1(v) = v_1, \ldots, \sigma_n(v) = v_n$ costituiscano una base di V come spazio vettoriale su k;

ii) $\sum_{i=1}^{n} v_i \in k - \{0\}$.

In tal caso V si dirà un (k, G, v)-anello.

Poniamo $\lambda = \sum_{i=1}^{n} v_i$.

2.1. PROPOSIZIONE. *Il sottoanello di stabilità di G in V è k.*

Dim. Preso $u = \sum_{i=1}^{n} \alpha_i v_i$, se esistono coefficienti $\alpha_i, \alpha_j \in k$ tali che $\alpha_i \neq \alpha_j$, allora $(\sigma_j \circ \sigma_i^{-1})(u) \neq u$. Ne segue che il sottoanello di stabilità di G è generato, su k, da $\lambda \in k$, c.v.d..

Si osservi che se N è un prolungamento di Galois di k con gruppo di Galois $\mathcal{G}(N/k)$ e se ω è un elemento i cui coniugati costituiscano una base normale di N su k, allora N è un $(k, \mathcal{G}(N/k), \omega)$-anello commutativo.

Sia V un (k, G, v)-anello commutativo.

Sia $\varphi : V \to V$, tale che, per ogni $x \in V$, $\varphi(x) = vx$. Risulta: $\varphi \in \mathrm{End}_k V$.

2.2. PROPOSIZIONE. *Risulta:*

a) $\varphi(\sum_{i=1}^{n} v_i) = \lambda v_1$;

b) $\sum_{i=1}^{n} \sigma_i \circ \varphi \circ \sigma_i^{-1} = \lambda \sigma_1$;

c) $\sigma_i \circ \varphi \circ \sigma_i^{-1} \circ \varphi = \varphi \circ \sigma_i \circ \varphi \circ \sigma_i^{-1}, i = 1, \ldots n$.

Dim. (a) è evidente.

Per ogni $x \in V$ risulta:

$$\left(\sum_{i=1}^{n} \sigma_i \circ \varphi \circ \sigma_i^{-1}\right)(x) = \sum_{i=1}^{n} \sigma_i(v\sigma_i^{-1}(x)) = \sum_{i=1}^{n} \sigma_i(v)x = \lambda x\,,$$

e ciò prova (b).

Per provare (c), osserviamo che, per ogni $x \in V$ e per $i = 1, \ldots, n$ risulta:

$$(\sigma_i \circ \varphi \circ \sigma_i^{-1} \circ \varphi)(x) = \sigma_i(v\sigma_i^{-1}(vx)) = v_i v x =$$

$$vv_i x = v(\sigma_i(v\sigma_i^{-1}(x))) = (\varphi \circ \sigma_i \circ \varphi \circ \sigma_i^{-1})(x) .$$

c.v.d. .

Supponiamo ora che V sia uno spazio vettoriale su k, di dimensione finita n; sia $(v_1, \dots, v_n)$ una base di V.

Consideriamo un gruppo $G = \{\sigma_1, \dots \sigma_n\} \subset \mathrm{Aut}_k V$ che operi transitivamente su $\{v_1, \dots, v_n\}$.

Supponiamo che esista $\varphi \in \mathrm{Aut}_k V$ e $\lambda \in k - \{0\}$, tali che valgano le uguaglianza (a),(b),(c) della prop. 2.2. Poniamo $\eta = \varphi^{-1}(v_1)$.

2.3. PROPOSIZIONE. *Risulta*

i) $\eta = \lambda^{-1} \sum_{i=1}^{n} v_i$;

ii) per ogni $\sigma \in G$, $\sigma(\eta) = \eta$.

Dim. Da (a) segue che $\sum_{i=1}^{n} v_i = \lambda\varphi^{-1}(v_1) = \lambda\eta$, da cui i due asserti, c.v.d. .

Poniamo $\varphi_i = \sigma_i \circ \varphi \circ \sigma_i^{-1}$, $i = 1, \dots n$; risulta $\varphi(\eta) = v_i$.

2.4. PROPOSIZIONE. *Gli automorfismi* $\varphi_1, \dots, \varphi_n$ *commutano tra loro.*

Dim. Consideriamo le uguaglianze (c) e un $\sigma_h \in G$. Risulta:

$$\sigma_h \circ \sigma_i \circ \varphi \circ \sigma_i^{-1} \circ \varphi \circ \sigma_h^{-1} = \sigma_h \circ \varphi \circ \sigma_i \circ \varphi \circ \sigma_i^{-1} \circ \sigma_h^{-1} ,$$

$$(\sigma_h \circ \sigma_i) \circ \varphi \circ (\sigma_h \circ \sigma_i)^{-1} \circ \varphi_h = \varphi_h \circ (\sigma_h \circ \sigma_i) \circ \varphi \circ (\sigma_h \circ \sigma_i)^{-1};$$

l'asserto segue allora dal fatto che per ogni σ_j e per ogni σ_h, esiste σ_i tale che: $\sigma_j = \sigma_h \circ \sigma_i$, c.v.d. .

Definiamo un'operazione interna $*$ in V:

$$v_i * v_j = \varphi_i(v_j), \; i, j = 1, \dots, n,$$

$$\left(\sum_{i=1}^{n} \alpha_i v_i\right) * \left(\sum_{j=1}^{n} \beta_j v_j\right) = \sum_{\substack{1\leq i\leq n\\ 1\leq j\leq n}} \alpha_i\beta_j(v_i * v_j) \ ,$$

ove $\alpha_1, \ldots, \alpha_n$, $\beta_1 \ldots, \beta_n$ sono elementi di k.

2.5. TEOREMA. *$(V, +, *)$ è un $(k\eta, G, v_1)$-anello commutativo, con identità η.*

Dim. Per verificare le proprietà commutativa e associativa è sufficiente limitarsi a considerare gli elementi $v_1, \ldots, v_n$. Per $i, j, h \in [1, n]$, risulta:

$$v_i * v_j = \varphi_i(v_j) = (\varphi_i \circ \varphi_j)(\eta) = (\varphi_j \circ \varphi_i)(\eta) = \varphi_j(v_i) = v_j * v_i;$$

$$(v_i * v_j) * v_h = v_h * (v_i * v_j) = (\varphi_h \circ \varphi_i \circ \varphi_j)(\eta) =$$

$$(\varphi_i \circ \varphi_j \circ \varphi_h)(\eta) = v_i * (v_j * v_h) \ .$$

Quindi $(V, +, *)$ è un anello commutativo.

Poiché $v_i * \eta = \varphi_i(\eta) = v_i$, $i = 1, \ldots, n$, η è l'identità dell'anello.

Per ogni $\sigma_h \in G$, risulta:

$$\sigma_h(v_i * v_j) = (\sigma_h \circ \varphi_i \circ \sigma_j)(v_1) = (\sigma_i \circ \sigma_i \circ \varphi \circ \sigma_h^{-1} \circ \sigma_h^{-1} \circ \sigma_h \circ \sigma_j)(v_1) =$$

$$(\sigma_h \circ \sigma_i)(v_1) * (\sigma_h \circ \sigma_j)(v_1) = \sigma_h(v_i) * \sigma_h(v_j) \ .$$

Ne segue che gli elementi del gruppo G sono automorfismi dell'anello $(V, +, *)$.

Per la prop. 2.3 risulta $\sum_{i=1}^{n} v_i \in k\eta - \{0\}$, e gli elementi di G sono l'identità su $k\eta$.

Quindi $(V, +, *)$ è un $(k\eta, G, v_1)$-anello, c.v.d..

Consideriamo l'applicazione $g : V \to \mathrm{End}_k V$, tale che, per ogni $x \in V$, $g(u)(x) = u * x$; sia $\mathcal{N} = g(V)$.

2.6. PROPOSIZIONE.

i) g è un isomorfismo di anelli di V su $\mathcal{N}$, tale che, per ogni $\alpha \in k$, $g(\alpha\eta) = \alpha\sigma_1$;

ii) per ogni $\psi \in \mathcal{N}$, $g^{-1}(\psi) = \psi(\eta)$;
iii) $(\varphi_1, \dots, \varphi_n)$ *è una base di* $\mathcal{N}$ *come spazio vettoriale su* k.

Dim. Le verifiche dei primi due asserti sono analoghe a quelle della prop. 1.7.

Per (iii) si osservi che $\varphi_1 = g(v_1), \dots, \varphi_n = g(v_n)$; essendo g iniettivo, $\varphi_1, \dots, \varphi_n$ sono linearmente indipendenti, c.v.d..

Sia $\tilde{G} = \{\tilde{\sigma}_1, \dots, \tilde{\sigma}_n\}$ il gruppo di automorfismi di $\mathcal{N}$ tali che per ogni $\psi \in \mathcal{N}$, $\tilde{\sigma}_i(\psi) = \sigma_i \circ \psi \circ \sigma_i^{-1}$, $i = 1, \dots, n$.

2.7. OSSERVAZIONE. $\mathcal{N}$ è un $(k\sigma_1, \tilde{G}, \varphi)$-anello.

Nel seguito avrà particolare interesse il caso in cui l'anello V sia generato dalle potenze di v_1 : $V = k[v_1], \mathcal{N} = k\sigma_1[\varphi]$.

In tal caso il polinomio minimo $p(X)$ di v_1 su k è il polinomio caratteristico di φ.

Posto che $p(X) = q_1(X)^{r_1} \dots q_s(X)^{r_s}$ sia una scomposizione in fattori primi di $p(X)$, risulta, come noto (cfr. [5] cap.1, §11):

$$V \simeq k[X]/(p(X)) \simeq \prod_{i=1}^{s} k[X]/(q_i(X)^{r_i}) \,. \tag{2.8}$$

CAPITOLO 3

In questo capitolo p è un primo positivo, k è un corpo infinito di caratteristica p; $\mathbf{F}_p$ è il corpo fondamentale di caratteristica p.

In [4], dato uno spazio vettoriale V su k e un endomorfismo semilineare P di V (cioè un endomorfismo di gruppo di V, tale che, per ogni $u \in V$ e $\alpha \in k$, risulti $P(\alpha u) = \alpha^p P(u)$), la coppia (V, P) si dice uno *pseudoprolungamento di* k se P è iniettivo ed ha p elementi uniti. Lo pseudoprolungamento si dice *finito* se V ha dimensione finita su k; si dice *ciclico* se esiste un *generatore*, cioè un elemento u tale che $(P^i(u))_{i \in \mathbf{N}}$ generi V come spazio vettoriale su k. Uno pseudoprolungamento finito e ciclico è *separabile* se e solo se P è non degenere (cfr. teorema 2.3 di [4]),

cioè se P trasforma sistemi di vettori linearmente indipendenti in sistemi linearmente indipendenti.

3.1. LEMMA. *Sia* (V, P) *uno pseudoprolungamento finito di* k *e sia* $(v_1, \ldots, v_n)$ *una base di* V*; se* $P(v_1), \ldots, P(v_n)$ *sono linearmente indipendenti, allora* P *è non degenere.*

Dim. Si consideri un qualsiasi sistema di vettori linearmente indipendenti di V e lo si completi a una base di V : $(u_1, \ldots, u_n)$.

Sia δ il determinante della matrice A tale che:

$$(u_1 \ldots u_n) = (v_1 \ldots v_n) A \, ;$$

risulta $\delta \in k - \{0\}$.

Sia B la matrice tale che:

$$(P(u_1) \ldots P(u_n)) = (P(v_1) \ldots P(v_n)) B \, .$$

Gli elementi di B sono le potenze p-esime dei corrispondenti elementi di A; dunque il determinante di B è $\delta^p \neq 0$. Ne segue l'asserto, c.v.d..

Conservando le notazioni del capitolo 2, supponiamo che V sia un (k, G, v)-anello, η sia l'identità di V e π l'endomorfismo di Frobenius di V; sia $G = \{\sigma_1, \ldots, \sigma_n\}$ e $v_1 = \sigma_1(v), \ldots, v_n = \sigma_n(v)$. Tenuto conto del lemma precedente, risulta evidente la seguente proposizione.

3.2. PROPOSIZIONE. (V, π) *è uno pseudoprolungamento di* k*, ciclico generato da* v*, e separabile, se e solo se valgono le seguenti condizioni:*

i) gli elementi uniti rispetto a π *siano solo quelli appartenenti a* $\mathbf{F}_p\eta$*;*

ii) $\pi^0(v), \ldots, \pi^{n-1}(v)$ *siano linearmente indipendenti su* k*;*

iii) $\pi(v_1), \ldots, \pi(v_n)$ *siano linearmente indipendenti su* k*.*

3.3. TEOREMA. *Un* (k, G, v)*-anello* V*, tale che* (V, π) *sia uno pseudoprolungamento di* k *ciclico, generato da* v*, e separabile, è un prolungamento di Galois di* $k\eta$*.*

Dim. Poiché (V, π) è ciclico, V è generato dalle potenze di v. Con le notazioni del cap. 2, risulta (cfr. 2.8):

$$V \simeq \prod_{i=1}^{s} k[X]/(q_i(X)^{r_i}) .$$

Se fosse $s > 1$, allora la s-upla $(1, 0, \ldots, 0)$ individuerebbe un elemento idempotente di V non appartenente ad $\mathbf{F}_p\eta$; in particolare tale elemento sarebbe radice di $X^p - X$. Ciò è in contrasto con l'ipotesi che (V, π) sia uno pseudoprolungamento di k; dunque $s = 1$.

Se fosse $r_1 > 1$, allora $q_1(v)$ risulterebbe non nullo e nilpotente; esisterebbe quindi un intero positivo h tale che $q_1(v)^{p^h} = 0$. Ciò contrasta con il fatto che π sia non degenere. Dunque il polinomio minimo di v su k è irriducibile; ne segue l'asserto. c.v.d..

Tenuto conto del teorema precedente, si vuole ora individuare un elenco di condizioni analitiche affinché un endomorfismo semilineare P di uno spazio vettoriale V, di dimensione finita n su k, sia l'endomorfismo di Frobenius di una struttura di prolungamento di Galois di un sottocorpo isomorfo a k.

Sia M una matrice associata a P rispetto a una base $\mathcal{B}$; per ogni $u \equiv_{\mathcal{B}} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ appartenente a V, risulta: $P(u) \equiv_{\mathcal{B}} M \begin{pmatrix} \alpha_1^p \\ \vdots \\ \alpha_n^p \end{pmatrix}$.

Due matrici A, B quadrate e dello stesso ordine, si diranno semisimili se esiste una matrice C dello stesso tipo, non degenere, tale che $B = C^{-1}AC^{\pi}$, ove C^{π} è la matrice ottenuta da C elevando ogni elemento alla p-esima potenza. Le matrici associate ad uno stesso endomorfismo semilineare costituiscono una classe di semisimiglianza.

3.4 TEOREMA. *Sia V uno spazio vettoriale di dimensione finita n su k; sia P un endomorfismo semilineare di V. Affinché in V esista almeno una struttura di corpo che sia un prolungamento di Galois di un sottocorpo isomorfo a k, e tale che P sia l'endomorfismo di Frobenius, è necessario e sufficiente che nella classe di semisimiglianza delle matrici associate a P esista una matrice M, tale che:*

i) M sia non degenere;

ii) *la somma ν degli elementi della prima colonna di M appartenga a $k^{p-1} - \{0\}$;*

iii) *esista un sottogruppo $G' = \{s_1, \dots s_n\}$ di S_n, che operi transitivamente su $\{1, \dots, n\}$ e tale che le colonne di M siano permutazioni della prima colonna tramite elementi di G';*

iv) *le n-uple non nulle $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in k^n$, tali che $M \begin{pmatrix} \alpha_1^p \\ \vdots \\ \alpha_n^p \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ siano solo quelle del tipo $\begin{pmatrix} \lambda^{-1} \\ \vdots \\ \lambda^{-1} \end{pmatrix}$, con $\lambda^{p-1} = \nu$;*

v) *le prime colonne di $M^0, \dots, M^{n-1}$ siano linearmente indipendenti;*

vi) *esista una matrice Φ, di tipo $n \times n$, non degenere, ad elementi in k, tale che, $\Phi \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, con λ come in (iv);*

vii) *detta C_i la matrice le cui colonne sono ottenute dalla n-upla $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ tramite le permutazioni $s_i \circ s_h$, per $h = 1, \dots, n$, risulti:*

$$\sum_{i=1}^{n} C_i \Phi C_i^{-1} = \lambda I \text{ (ove } I \text{ è la matrice identica)} ;$$

viii) *sia $C_i \Phi C_i^{-1} \Phi = \Phi C_i \Phi C_i^{-1}$, $i = 1, \dots, n$;*

ix) *la prima colonna della matrice Φ^{p-1} sia uguale alla prima colonna di M.*

Dim. Verifichiamo che le condizioni elencate sono necessarie. Sia η l'identità di una struttura di corpo in V; tale struttura sia un prolungamento di Galois di $k\eta$, tale che P sia l'endomorfismo di Frobenius.

Sia $G = \{\sigma_1, \dots, \sigma_n\}$ il gruppo di Galois di V su $k\eta$ e sia $\mathcal{B} = (v_1 = \sigma_1(v_1), \dots, v_n = \sigma_n(v_1))$ una base normale di V. Sia M la matrice associata a P rispetto a $\mathcal{B}$.

Essendo V separabile, P è non degenere; vale quindi la condizione (i).

Poiché $\sum_{i=1}^{n} v_i$ appartiene all'anello di stabilità di G, esiste $\lambda \in k-\{0\}$, tale che $\sum_{i=1}^{n} v_i = \lambda\eta$.

Il gruppo G opera transitivamente su $\{v_1, \ldots, v_n\}$; sia $G' = \{s_1, \ldots, s_n\}$ il sottogruppo di S_n che rappresenta G.

La condizione (iii) è allora conseguenza delle seguenti uguaglianze:

$$P(v_i) = P(\sigma_i(v_1)) = \sigma_i(P(v_1)), \quad i = 1, \ldots, n.$$

In particolare se $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ è la prima colonna della matrice M, allora $M = \left(\alpha_{s_j^{-1}(i)}\right)_{\substack{1\le i\le n \\ 1\le j\le n}}$

Sia $\nu = \alpha_1 + \ldots + \alpha_n$.

Poiché $\eta = P(\eta)$, risulta $\lambda^{-1}\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \lambda^{-p} M \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$; perciò $\lambda^{-1} = \lambda^{-p}\nu$. Ne segue la condizione (ii).

La condizione (iv) discende dal fatto che gli elementi uniti di P sono solo quelli appartenenti a $\mathbb{F}_p\eta$.

Si osservi che $P^i(v_1) \equiv_{\mathcal{B}} M^i \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $i \in \mathbb{N}$; la condizione (v) segue allora dal teorema 1.2 di [3].

Poiché V è un $(k\eta, G, v_1)$-anello, le condizioni (vi), (vii), (viii) sono conseguenza della proposizione 2.2.

La condizione (ix) segue da:

$$v_1^p \equiv_{\mathcal{B}} \Phi^{p-1}\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad P(v_1) \equiv_{\mathcal{B}} M\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \; v_1^p = P(v_1)\,.$$

Verifichiamo che le condizioni elencate sono anche sufficienti.

Sia $\mathcal{B} = (v_1, \ldots, v_n)$ una base rispetto alla quale la matrice M è associata a P. Sia $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ la prima colonna di M e sia $\nu = \alpha_1 + \ldots + \alpha_n$.

Per la condizione (iv) gli elementi uniti di P sono solo quelli del tipo $\lambda^{-1}\sum_{i=1}^{n} v_i$, con λ radice del polinomio $X^p - \nu X$. Vista la condizione su ν specificata in (ii), tale polinomio ha p radici in k.

Tenuto conto anche della condizione (i), risulta che (V, P) è uno pseudoprolungamento separabile di k.

La condizione (v) implica che V è generato da $P^0(v_1), \dots, P^{n-1}(v_1)$; dunque (V, P) è ciclico, generato da v_1.

Per (iii) esiste un gruppo $G' = \{s_1, \dots, s_n\}$ che opera transitivamente su $\{1, \dots, n\}$ e tale che:

$$M = \left(\alpha_{s_j^{-1}(i)}\right)_{\substack{1\le i\le n\\ 1\le j\le n}} .$$

Il gruppo $G = \{\sigma_1, \dots, \sigma_n\}$ di automorfismi di spazio vettoriale che opera transitivamente su $\{v_1, \dots, v_n\}$, rappresentato da G', è formato da elementi che commutano con P. Infatti, per ogni $i, j \in [1, n]$, posto $\sigma_h = \sigma_i \circ \sigma_j$, risulta:

$$(P \circ \sigma_i)(v_j) = P(v_h) = \sum_{i=1}^{n} \alpha_i v_{s_j(i)} ;$$

$$(\sigma_i \circ P)(v_j) = \sigma_j\left(\sum_{i=1}^{n} \alpha_i v_{s_h(i)}\right) = \sum_{i=1}^{n} \alpha_i v_{s_h(i)} .$$

Le matrici C_i descritte in (vii) risultano matrici associate agli elementi di G, rispetto alla base $\mathcal{B}$.

Dunque le condizioni (vi), (vii), (viii) implicano che esiste in V una struttura di $(k\eta, G, v_1)$-anello commutativo, con identità $\eta = \lambda^{-1}\sum_{i=1}^{n} v_i$ (cfr. teorema 2.5).

La condizione (ix) implica $v_1^p = P(v_1)$; allora, per ogni $u \in V$, $u = \sum_{i=1}^{n} \alpha_i v_i$, risulta:

$$u^p = \sum_{i=1}^{n} \alpha_i^p \sigma_i(v_1^p) = \sum_{i=1}^{n} \alpha_i^p \sigma_i \circ P(v_1) = \sum_{i=1}^{n} \alpha_i^p P(v_i) = P(u) .$$

Perciò P è l'endomorfismo di Frobenius dell'anello V. Allora per il teorema 3.3, V è un prolungamento di Galois di $k\eta$, c.v.d..

Supponiamo che esistano matrici M e Φ come descritte nel teorema precedente; sia $(V, +, \cdot)$ la struttura di prolungamento di $k\eta$ individuata da Φ (ove η è l'identità di V).

3.5. TEOREMA. *Se una matrice Ψ verifica le condizioni (vi), (vii), (viii), (ix) enunciate per Φ nel teorema 3.4, allora esistono $\mu_1, \ldots, \mu_n \in \mathbf{F}_p$, tali che, posto*

$$A = \sum_{i=1}^{n} \mu_i C_i ,$$

$$\Phi_i = C_i \Phi C_i^{-1}, \; i = 1, \ldots, n ,$$

risulti A non degenere e:

$$\Psi = \sum_{i=1}^{n} \mu_i A^{-1} \Phi_i A .$$

Dim. Sia $\mathcal{B} = (v_i, \ldots, v_n)$ una base rispetto alla quale la matrice M sia associata a P; sia $(V, +, *)$ la struttura di prolungamento di $k\eta$ individuata da Ψ.

Poiché le due strutture $(V, +, \cdot)$, $(V, +, *)$ hanno lo stesso endomorfismo di Frobenius P, anche l'insieme del P-endomorfismi è lo stesso.

Considerato un isomorfismo τ dalla seconda struttura nella prima, la matrice A associata a τ rispetto a $\mathcal{B}$ è del tipo (cfr. 1.11):

$$A = \sum_{i=1}^{n} \mu_i C_i, \text{ con } \mu_1, \ldots, \mu_n \in \mathbf{F}_p .$$

Poiché la prima colonna di A è $\begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}$, risulta $\tau(v_1) = \mu_1 v_1 + \ldots +$

$\mu_n v_n$. Quindi per ogni $u \in V$, posto $u \equiv_{\mathcal{B}} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$, risulta:

$$\tau(v_1)u \equiv_{\mathcal{B}} (\mu_1\Phi_1 + \ldots + \mu_n\Phi_n) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} .$$

D'altra parte, poiché $\tau(v_1)u = \tau(v_1 * \tau^{-1}(u))$, si ha anche:

$$\tau(v_1)u \equiv_{\mathcal{B}} A\Psi A^{-1} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} .$$

Confrontando i due risultati si ottiene l'asserto, c.v.d..

BIBLIOGRAFIA

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

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

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

[4] VOLPI A., *Endomorfismo di Frobenius e pseudoprolungamenti di un corpo*, Rendiconti Ist. Mat. Univ. Trieste, *20*, (1988), 241.

[5] BOURBAKI N., *Algebre*, Capp. 1-3 Hermann, Paris (1970).