Annali della
Scuola Normale Superiore di Pisa
Classe di Scienze

Mario Poletti
Aldo Volpi

π-omomorfismi e loro rappresentazione

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4e série, tome 8, nº 1 (1981), p. 119-155
<http://www.numdam.org/item?id=ASNSP_1981_4_8_1_119_0>

π-omomorfismi e loro rappresentazione.

MARIO POLETTI - ALDO VOLPI (*)

In [1], per ciascun prolungamento finito F di un corpo k di caratteristica positiva, viene introdotta un'iperalgebra locale R_F, le cui principali proprietà sono: i) il T_k-modulo canonico $\mathcal{V}D_F$ dei vettori canonici di Witt dell'iperalgebra D_F, duale di R_F, è isomorfo al T_k-modulo canonico *vect* F; ii) F, come prolungamento di k, è quoziente dell'algebra delle iperderivazioni 1-speciali invarianti di R_F.

In [2], per prolungamenti separabili, viene provato che l'isomorfismo tra iperalgebre R_F, R_H, equivale al π-isomorfismo di F, H.

Quanto ai legami tra π-isomorfismo e isomorfismo, il risultato più significativo ottenuto in [1], è che prolungamenti normali di k sono isomorfi se e solo se π-isomorfi; altre classi di prolungamenti per i quali il π-isomorfismo comporta l'isomorfismo, sono descritte in [2].

La caratterizzazione dei π-omomorfismi tra due prolungamenti è data in [2]; il presente lavoro descrive procedimenti analitici per caratterizzare tra essi gli eventuali π-isomorfismi. Le tecniche adottate si prestano in modo naturale allo studio (per un k perfetto) degli omomorfismi come T_k^*-moduli (qui detti π-omomorfismi) dei corpi dei bivettori a elementi nei prolungamenti finiti di k, ed alla caratterizzazione tra essi degli eventuali π-isomorfismi.

I risultati in merito ottenuti consentono di provare che, nell'ambito dei prolungamenti di ordine $\leqslant 6$, sia il π-isomorfismo tra i prolungamenti, sia il π-isomorfismo tra i bivettori, comportano l'isomorfismo tra i prolungamenti.

Per quanto concerne invece i prolungamenti di ordine $\geqslant 7$ (contro la congettura posta alla fine di [1]), i procedimenti analitici sviluppati con-

(*) Lavoro eseguito nell'ambito del Gruppo Nazionale per le Strutture Algebriche e Geometriche e loro Applicazioni, del C.N.R.

Pervenuto alla Redazione il 16 Febbraio 1980.

sentono di individuare tra essi prolungamenti non isomorfi, ma π-isomorfi, e prolungamenti non π-isomorfi, ma con i bivettori π-isomorfi.

I risultati detti consentono in particolare di concludere che, per prolungamenti di ordine $\leqslant 6$ di un corpo perfetto, l'isogenia delle iperalgebre comporta l'isomorfismo delle iperalgebre stesse, mentre per prolungamenti di ordine $\geqslant 7$ tale implicazione cessa di sussistere.

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

Se F è un corpo di caratteristica p, indicheremo con $\mathit{vect}\, F$ l'anello dei vettori infiniti di Witt a elementi in F; se F è perfetto, indicheremo con $\mathit{biv}\, F$ il corpo dei bivettori di Witt a elementi in F (cfr. [MA], cap. 2); in entrambi i casi, π denota l'endomorfismo di Frobenius.

Se F è un prolungamento finito di k, $\mathit{vect}\, F$ risulta un T_k-modulo (cfr. **1** di [2]); se k è perfetto, $\mathit{biv}\, F$ risulta un T_k^*-modulo (cfr. **2** di [2]).

Dati prolungamenti finiti F, H di k, le applicazioni $f\colon F \to H$, $f\colon \mathit{vect}\, F \to \mathit{vect}\, H$, e (se k è perfetto) $f\colon \mathit{biv}\, F \to \mathit{biv}\, H$, rispettivamente: k-, $\mathit{vect}\, k$-, $\mathit{biv}\, k$-lineari, e commutanti con π, si diranno *π-omomorfismi*; nel secondo e terzo caso, i π-omomorfismi sono gli omomorfismi rispettivamente di T_k-, T_k^*-moduli (cfr. **1, 2** di [2]).

$\boldsymbol{Z}$ è l'anello degli interi, $\boldsymbol{Q}$ è il corpo razionale, $\boldsymbol{F}_p$ è il corpo fondamentale di caratteristica p; $\boldsymbol{Z}_p = \mathit{vect}\, \boldsymbol{F}_p$ e $\boldsymbol{Q}_p = \mathit{biv}\, \boldsymbol{F}_p$ sono rispettivamente l'anello degli interi p-adici ed il corpo dei razionali p-adici.

Se A è un anello commutativo ed M un modulo su A, dati $m_1, m_2, \ldots \in M$, il modulo su A da essi generato si indicherà con $A\boldsymbol{I}m_1, m_2, \ldots \boldsymbol{I}$.

Prolungamento di Galois significa prolungamento finito, separabile, normale.

I gruppi di cui in **2** e **3** del cap. 3 sono stati determinati in base a un programma curato da G. Ghelardoni.

Capitolo 1

MATRICE RAPPRESENTATIVA DI UN π-OMOMORFISMO

1.

1.1 Lemma. *Sia $\theta \in \bar{k}$, $\theta \neq 0$, un elemento separabile su k; sia $s = [k(\theta):k]$, e siano $\theta_1, \ldots, \theta_s$ i coniugati di θ su k.*

Posto $t = \dim_{\boldsymbol{F}_p} \boldsymbol{F}_p \boldsymbol{I}\theta_1, \ldots, \theta_s \boldsymbol{I}$, gli elementi $\theta^{p^0}, \ldots, \theta^{p^{t-1}}$ costituiscono una base di $k\boldsymbol{I}\theta^{p^0}, \theta^{p^1}, \ldots \boldsymbol{I}$ come spazio vettoriale su k.

DIM. Sia $V = \boldsymbol{F}_p \boldsymbol{I}\theta_1, \ldots, \theta_s \boldsymbol{I}$; V ha p^t elementi. Posto $f(X) = \prod_{\eta \in V} (X - \eta)$, si ha $f(X) = a_0 X^{p^0} + a_1 X^{p^1} + \ldots + a_{t-1} X^{p^{t-1}} + X^{p^t}$ (cfr. l'appendice di [1]). Essendo θ separabile su k, i coefficienti di $f(X)$ sono separabili su k, in quanto elementi di $k(\theta_1, \ldots, \theta_s)$; per ogni $\sigma \in \mathcal{G}(\bar{k}/k)$ si ha $\sigma V = V$, pertanto $\sigma f(X) = f(X)$, e conseguentemente i coefficienti di $f(X)$ risultano anche puramente inseparabili su k; si conclude che $f(X) \in k[X]$. Essendo θ radice di $f(X)$, si ha allora che:

$$\theta^{p^t},\ \theta^{p^{t+1}},\ \ldots \in k\boldsymbol{I}\theta^{p^0},\ \ldots,\ \theta^{p^{t-1}}\boldsymbol{I}.$$

Dati infine $b_0, \ldots, b_{t-1} \in k$ tali che $b_0\theta^{p^0} + \ldots + b_{t-1}\theta^{p^{t-1}} = 0$, il polinomio $b_0 X^{p^0} + \ldots + b_{t-1} X^{p^{t-1}}$, avendo θ per radice, è annullato da tutti gli elementi di V, ed è pertanto multiplo di $f(X)$; ne segue: $b_0 = \ldots = b_{t-1} = 0$, C.V.D..

1.2 TEOREMA. *Sia F un prolungamento finito e separabile di k, e sia $s = [F:k]$. Dato $\theta \in F$, risultano equivalenti gli asserti:*

a) θ ha s coniugati su k, e tali coniugati sono linearmente indipendenti su $\boldsymbol{F}_p$,

b) $F = k\boldsymbol{I}\theta^{p^0}, \ldots, \theta^{p^{s-1}}\boldsymbol{I}$.

Si ha inoltre che esistono elementi di F verificanti la condizione a.

DIM. L'equivalenza degli asserti a, b è conseguenza pressochè banale di 1.1. Quanto all'ultimo asserto: sia N un prolungamento di Galois di k, contenente F, sia $\mathcal{G}(N/k) = \{\sigma_1, \ldots, \sigma_n\}$, e sia $\omega \in N$ tale che $\sigma_1\omega, \ldots, \sigma_n\omega$ risulti una base di N su k (cfr. [3], teorema 20, pag. 229). Posto $\theta = T_{N/F}\omega$, si ha $\theta \in F$; dette inoltre $\mathcal{F}_1, \ldots, \mathcal{F}_s$ le classi laterali sinistre di $\mathcal{G}(N/F)$ in $\mathcal{G}(N/k)$, i coniugati di θ su k risultano: $\theta_i = \sum_{\sigma \in \mathcal{F}_i} \sigma\omega$, $i = 1, \ldots, s$. Per la scelta di ω, tali coniugati sono in numero di s; sono inoltre indipendenti su k, ed in particolare su $\boldsymbol{F}_p$, C.V.D..

2. In questo numero supponiamo k perfetto.

Se N è un qualsiasi prolungamento di Galois di k, posto $G = \mathcal{G}(N/k) = \{\sigma_1, \ldots, \sigma_n\}$, e posto $\tilde{\sigma}_i(\ldots, a_{-1}; a_0, a_1, \ldots) = (\ldots, \sigma_i a_{-1}; \sigma_i a_0, \sigma_i a_1, \ldots)$, l'insieme $\tilde{G} = \{\tilde{\sigma}_1, \ldots, \tilde{\sigma}_n\}$ risulta un gruppo di automorfismi di *biv* N, gruppo canonicamente isomorfo a G. Il sottocorpo costituito dagli elementi di *biv* N, stabili rispetto a $\tilde{G}$, è ovviamente *biv* k; in particolare *biv* N è un prolungamento di Galois di *biv* k, e $\mathcal{G}(\textit{biv } N/\textit{biv } k) = \tilde{G}$. I gruppi G e $\tilde{G}$ verranno sistematicamente identificati.

1.3 OSSERVAZIONE. *Sia* $\nu = (\ldots, a_{-1}; a_0, a_1, \ldots) \in biv\,\bar{k}$; *risultano equivalenti gli asserti*:

a) ν *è algebrico su* $biv\,k$,

b) $k(\ldots, a_{-1}, a_0, a_1, \ldots)$ *è un prolungamento finito di* k.

DIM. *a*) $\Rightarrow$ *b*). Qualora $k(\ldots, a_{-1}, a_0, a_1, \ldots)$ non fosse finito su k, tenuto presente che solo un numero finito di a_i, con $i < 0$, è non nullo, per $r = 0, 1, \ldots$ esisterebbero $\sigma_r \in \mathcal{G}(\bar{k}/k)$, $n_r > 0$, tali che:

$$\ldots, \sigma_0(a_{-1}) = a_{-1}, \ \sigma_0(a_0) = a_0, \ \sigma_0(a_{n_0}) \neq a_{n_0},$$

$$\ldots, \sigma_r(a_{-1}) = a_{-1}, \ \sigma_r(a_0) = a_0, \ \ldots, \ \sigma_r(a_{n_{r-1}}) = a_{n_{r-1}}, \ \sigma_r(a_{n_r}) \neq a_{n_r}.$$

Considerando allora $\sigma_0, \sigma_1, \ldots$ come automorfismi di $biv\,\bar{k}$ su $biv\,k$, gli elementi $\sigma_0\nu, \sigma_1\nu, \ldots$ risulterebbero a due a due distinti, contro l'ipotesi che ν sia algebrico su $biv\,k$.

b) $\Rightarrow$ *a*). Sia N un prolungamento di Galois di k, contenente $k(\ldots, a_{-1}, a_0, a_1, \ldots)$; $biv\,N$ è algebrico su $biv\,k$ (cfr. le considerazioni introduttive di questo numero), ed ovviamente $\nu \in biv\,N$, C.V.D..

1.4 OSSERVAZIONE. *Detta* $biv_a\,k$ *la chiusura algebrica di* $biv\,k$ *in* $biv\,\bar{k}$, *sussistono gli asserti*:

a) $biv_a\,k$ *è normale su* $biv\,k$,

b) *se* K *è un prolungamento finito di* $biv\,k$ *in* $biv_a\,k$, *esiste un prolungamento finito* F *di* k *tale che* $K = biv\,F$,

c) *se* K *è un prolungamento di* $biv\,k$ *in* $biv_a\,k$, *risulta* $\pi K = K$; *in particolare* $\pi(biv_a\,k) = biv_a\,k$.

DIM. *b*) Esiste $\nu \in K$ tale che $K = (biv\,k)(\nu)$ (cfr. [3], teorema 14, pag. 185); per *b* di 1.3, esiste N di Galois su k tale che $K \subset biv\,N$; l'asserto segue allora dall'essere $biv\,N$ di Galois su $biv\,k$, e dall'essere $\mathcal{G}(biv\,N/biv\,k) = \mathcal{G}(N/k)$.

a) Segue dal fatto, appena dimostrato, che ciascun prolungamento finito di $biv\,k$ in $biv_a\,k$ è sottocorpo di un prolungamento normale di $biv\,k$ in $biv_a\,k$.

c) Sia $\nu \in K$; per *b* esiste un prolungamento F di k tale che $(biv\,k)(\nu) = biv\,F$; essendo $\pi\nu, \pi^{-1}\nu \in biv\,F \subset K$, si ha l'asserto, C.V.D.

Detto K un prolungamento di $biv\, k$ in $biv_a k$, indicheremo con Π_K l'anello ottenuto dal K-modulo sinistro dei polinomi formali nelle potenze non negative di π, a coefficienti (a sinistra) in K, ponendo $\pi a = a^\pi \pi$. Gli elementi di Π_K si diranno *π-polinomi* a coefficienti in K; il grado di un π-polinomio è il massimo degli esponenti delle potenze di π che vi figurano con coefficiente non nullo.

$biv\, \bar{k}$, nonchè qualsiasi prolungamento K di $biv\, k$ in $biv_a k$ (cfr. c di 1.4), risultano in modo canonico moduli sinistri su $\Pi_{biv\, k}$.

Dato $v \in biv_a k$, essendo (cfr. c di 1.4) $v^{\pi^0}, v^{\pi^1}, \ldots \in (biv\, k)(v)$, esistono π-polinomi non nulli $a_0\pi^0 + a_1\pi^1 + \ldots + a_h\pi^h \in \Pi_{biv\, k}$ che annullano v, ossia tali che: $a_0 v^{\pi^0} + a_1 v^{\pi^1} + \ldots + a_h v^{\pi^h} = 0$; quello tra essi di minimo grado, univocamente determinato a meno di un fattore moltiplicativo in $biv\, k$, si dirà il *π-polinomio minimo* di v su $biv\, k$.

1.5 Lemma. *Sia $v \in biv_a k$; sia $s = [(biv\, k)(v) : biv\, k]$, e siano $v_1, \ldots, v_s$ i coniugati di v su $biv\, k$* (cfr. a di 1.4).

Posto $t = \dim_{Q_p} Q_p \boldsymbol{I} v_1, \ldots, v_s \boldsymbol{I}$, sussistono gli asserti:

a) il π-polinomio minimo di v su $biv\, k$, ha grado t,

b) detto $\varphi(\pi) = b_0\pi^0 + \ldots + b_{t-1}\pi^{t-1} - \pi^t$ tale π-polinomio, l'insieme degli elementi di $biv\, \bar{k}$ annullati da $\varphi(\pi)$, risulta essere $Q_p \boldsymbol{I} v_1, \ldots, v_s \boldsymbol{I}$.

Dim. Se $v = 0$, l'asserto è banale. Supponiamo quindi $v \neq 0$; variando eventualmente gli indici, possiamo inoltre supporre che $v_1, \ldots, v_t$ sia una base di $Q_p \boldsymbol{I} v_1, \ldots, v_s \boldsymbol{I}$. In tale caso, per $1 \leqslant l \leqslant t$, risulta:

$$\det\begin{pmatrix} v_1^{\pi^0} & \ldots & v_1^{\pi^{l-1}} \\ \vdots & \ldots & \vdots \\ v_l^{\pi_0} & \ldots & v_l^{\pi^{l-1}} \end{pmatrix} \neq 0 ,$$

infatti: per $l = 1$ l'asserto è ovvio, essendo $v \neq 0$; supponendo quindi l'asserto provato per $l = 1, \ldots, m$, con $m < t$, se risultasse

$$\det\begin{pmatrix} v_1^{\pi^0} & \ldots & v_1^{\pi^m} \\ \vdots & \ldots & \vdots \\ v_{m+1}^{\pi_0} & \ldots & v_{m+1}^{\pi^m} \end{pmatrix} = 0 ,$$

per l'ipotesi induttiva esisterebbero $\lambda_1, \dots, \lambda_m \in biv\,\bar{k}$ tali che:

$$\nu_{m+1}^{\pi_0} = \sum_{r=1}^{m} \lambda_r \nu_r^{\pi^0}, \; \nu_{m+1}^{\pi^1} = \sum_{r=1}^{m} \lambda_r \nu_r^{\pi^1}, \; \dots, \; \nu_{m+1}^{\pi^m} = \sum_{r=1}^{m} \lambda_r \nu_r^{\pi^m};$$

trasformando con π i membri di ciascuna delle prime m uguaglianze e sottraendo i membri della uguaglianza successiva, si otterrebbe:

$$\,^t\!\begin{pmatrix} \nu_1^{\pi^0} & \dots & \nu_1^{\pi^{m-1}} \\ \vdots & \dots & \vdots \\ \nu_m^{\pi^0} & \dots & \nu_m^{\pi^{m-1}} \end{pmatrix}^{\pi} \begin{pmatrix} \lambda_1^\pi - \lambda_1 \\ \vdots \\ \lambda_m^\pi - \lambda_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

e quindi, per l'ipotesi induttiva, si avrebbe $\lambda_1^\pi = \lambda_1, \dots, \lambda_m^\pi = \lambda_m$, ossia $\lambda_1, \dots, \lambda_m \in \boldsymbol{Q}_p$, contro l'ipotesi che $\nu_{m+1} \notin \boldsymbol{Q}_p \boldsymbol{I} \nu_1, \dots, \nu_m \boldsymbol{I}$.

Dette $X_0, \dots, X_t$ indeterminate, si consideri la matrice $(t+1)\times(t+1)$

$$A(X_0, \dots, X_t) = \begin{pmatrix} X_0 & \dots & X_t \\ \nu_1^{\pi^0} & \dots & \nu_1^{\pi^t} \\ \vdots & \dots & \vdots \\ \nu_t^{\pi^0} & \dots & \nu_t^{\pi^t} \end{pmatrix};$$

ciò posto, si consideri il π-polinomio $f(\pi) = a_0\pi^0 + \dots + a_t\pi^t$, ove a_i è l'aggiunto di X_i in $A(X_0, \dots, X_t)$. Per le osservazioni precedenti, si ha $a_t \neq 0$; inoltre, dato $\eta \in biv\,\bar{k}$, risulta:

$$f(\pi)\eta = \det A(\eta^{\pi^0}, \dots, \eta^{\pi^t}).$$

Dato $\sigma \in \mathcal{G}(\bar{k}/k)$, esistono $\alpha_{rs} \in \boldsymbol{Q}_p$ (dipendenti da σ) tali che

$$\begin{pmatrix} \sigma\nu_1 \\ \vdots \\ \sigma\nu_t \end{pmatrix} = (\alpha_{rs}) \begin{pmatrix} \nu_1 \\ \vdots \\ \nu_t \end{pmatrix}$$

e quindi, tenuto conto che $\alpha_{rs} \in \boldsymbol{Q}_p$, tali che

$$\begin{pmatrix} \sigma\nu_1^{\pi^j} \\ \vdots \\ \sigma\nu_t^{\pi^j} \end{pmatrix} = (\alpha_{rs}) \begin{pmatrix} \nu_1^{\pi^j} \\ \vdots \\ \nu_t^{\pi^j} \end{pmatrix};$$

posto allora $\alpha_\sigma = \det(\alpha_{rs})$, per $i = 0, \dots, t$ risulta $\sigma a_i = \alpha_\sigma a_i$.

Tenuto conto dell'ultima osservazione, il π-polinomio $\varphi(\pi) = b_0\pi^0 + \dots + b_{t-1}\pi^{t-1} - \pi^t = -a_t^{-1} f(\pi)$ è a coefficienti in $biv\, k$; tenuto inoltre conto del modo di operare di $f(\pi), \varphi(\pi)$ annulla $v_1, \dots, v_t$, conseguentemente annulla tutti gli elementi di $\boldsymbol{Q}_p \boldsymbol{I} v_1, \dots, v_s \boldsymbol{I}$ ed in particolare annulla v.

Se esistesse un π-polinomio $c_0\pi^0 + \dots + c_{h-1}\pi^{h-1} - \pi^h$, con $h < t$, a coefficienti in $biv\, k$, che annullasse v, risulterebbe $v^{\pi^h} = c_0 v^{\pi^0} + \dots + c_{h-1} v^{\pi^{h-1}}$, ed essendo $c_0, \dots, c_{h-1} \in biv\, k$, per $i = 1, \dots, s$ si avrebbe $v_i^{\pi^h} = c_0 v_i^{\pi^0} + \dots + c_{h-1} v_i^{\pi^{h-1}}$, e quindi

$$\det \begin{pmatrix} v_1^{\pi^0} & \dots & v_1^{\pi^{h-1}} & v_1^{\pi^h} \\ \vdots & \dots & \vdots & \vdots \\ v_{h+1}^{\pi^0} & \dots & v_{h+1}^{\pi^{h-1}} & v_{h+1}^{\pi^h} \end{pmatrix} = 0\,, \qquad \text{con } h+1 \leqslant t\,,$$

contro l'asserto introduttivo di questa dimostrazione; pertanto $\varphi(\pi)$ è il π-polinomio minimo di v su $biv\, k$.

Sia infine $\omega \in biv\, \bar{k}$ un elemento annullato da $\varphi(\pi)$; essendo $\det A(\omega^{\pi^0}, \dots, \omega^{\pi^t}) = 0$, ed essendo $a_t \neq 0$, esistono $\lambda_1, \dots, \lambda_t \in biv\, \bar{k}$ tali che:

$$\omega^{\pi^0} = \sum_{r=1}^{t} \lambda_r v_r^{\pi^0}, \dots, \omega^{\pi^t} = \sum_{r=1}^{t} \lambda_r v_r^{\pi^t};$$

trasformando con π i membri di ciascuna delle prime t uguaglianze, e sottraendo i membri della uguaglianza successiva, si ottiene

$${}^t\begin{pmatrix} v_1^{\pi^0} & \dots & v_1^{\pi^{t-1}} \\ \vdots & \dots & \vdots \\ v_t^{\pi^0} & \dots & v_t^{\pi^{t-1}} \end{pmatrix}^{\pi} \begin{pmatrix} \lambda_1^\pi - \lambda_1 \\ \vdots \\ \lambda_t^\pi - \lambda_t \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

e quindi, essendo $a_t \neq 0$, $\lambda_1^\pi = \lambda_1, \dots, \lambda_t^\pi = \lambda_t$, ossia $\lambda_1, \dots, \lambda_t \in \boldsymbol{Q}_p$; si conclude che $\omega \in \boldsymbol{Q}_p \boldsymbol{I} v_1, \dots, v_s \boldsymbol{I}$, C.V.D..

1.6 Lemma. *Sia $v \in biv_a k$, $v \neq 0$; sia $s = [(biv\, k)(v) : biv\, k]$, e siano $v_1, \dots, v_s$ i coniugati di v su $biv\, k$* (cfr. *a* di 1.4).

Posto $t = \dim_{\boldsymbol{Q}_p} \boldsymbol{Q}_p \boldsymbol{I} v_1, \dots, v_s \boldsymbol{I}$, gli elementi $v^{\pi^0}, \dots, v^{\pi^{t-1}}$ costituiscono una base di $(biv\, k) \boldsymbol{I} v^{\pi^0}, v^{\pi^1}, \dots \boldsymbol{I}$ come spazio vettoriale su $biv\, k$.

Dim. L'asserto è conseguenza pressochè immediata di *a* di 1.5, C.V.D..

1.7 Teorema. *Sia F un prolungamento finito di k, e sia $s = [F : k] = [biv\, F : biv\, k]$. Dato $v \in biv\, F$, risultano equivalenti gli asserti:*

a) *ν ha s coniugati su biv k, e tali coniugati sono linearmente indipendenti su $\boldsymbol{Q}_p$,*

b) *biv F = (biv k) $\boldsymbol{I}\nu^{\pi^0}, \ldots, \nu^{\pi^{s-1}}\boldsymbol{I}$.*

Si ha inoltre che esistono elementi di biv F verificanti la condizione a.

DIM. Tenuto conto di *c* di 1.4, l'equivalenza di *a* e *b* è conseguenza pressochè immediata di 1.6. Quanto all'ultimo asserto, per 1.2 esiste $\theta \in F$ con s coniugati su k, linearmente indipendenti su $\boldsymbol{F}_p$; si verifica facilmente che $\{\theta\} \in biv\, F$ ha s coniugati su *biv* k, e che tali coniugati sono linearmente indipendenti su $\boldsymbol{Q}_p$, C.V.D..

3. Siano F, H prolungamenti finiti separabili di k, tali che $[F:k] = [H:k] = s$.

Sia N un prolungamento di Galois di k, contenente F ed H, e ne sia $G = \mathcal{G}(N/k)$ il gruppo di Galois. Qualora venga specificato che k debba intendersi perfetto, come precisato in **2.**, identificheremo $\mathcal{G}(biv\, N/biv\, k)$ con G.

Posto $\mathcal{F} = \mathcal{G}(N/F)$, $\mathcal{H} = \mathcal{G}(N/H)$, siano $\mathcal{F}_1 = \mathcal{F}, \ldots, \mathcal{F}_s$ e $\mathcal{H}_1 = \mathcal{H}, \ldots, \mathcal{H}_s$ le classi laterali sinistre rispettivamente di $\mathcal{F}$ ed $\mathcal{H}$ in G.

1.8 TEOREMA. *Sia $f\colon F \to H$ un π-omomorfismo. Sussistono gli asserti:*

a) *esiste una ed una sola matrice $A = (a_{ij})$, di tipo $s \times s$, ad elementi in $\boldsymbol{F}_p$, tale che, per ogni $\theta \in F$, e per ogni scelta di rappresentanti $\sigma_1, \ldots, \sigma_s$ e $\xi_1, \ldots, \xi_s$ rispettivamente di $\mathcal{F}_1, \ldots, \mathcal{F}_s$ e $\mathcal{H}_1, \ldots, \mathcal{H}_s$, risulti:*

$$\begin{pmatrix} \xi_1 f(\theta) \\ \vdots \\ \xi_s f(\theta) \end{pmatrix} = A \begin{pmatrix} \sigma_1\theta \\ \vdots \\ \sigma_s\theta \end{pmatrix};$$

b) *per tale A, ogniqualvolta $\mathcal{H}_i^{-1}\mathcal{F}_j = \mathcal{H}_\lambda^{-1}\mathcal{F}_\mu$, risulta $a_{ij} = a_{\lambda\mu}$.*

DIM. Sia $\theta \in F$ un elemento con s coniugati su k, linearmente indipendenti su $\boldsymbol{F}_p$ (cfr. 1.2), e sia $\sigma_1, \ldots, \sigma_s$, $\xi_1, \ldots, \xi_s$ una scelta di rappresentanti di $\mathcal{F}_1, \ldots, \mathcal{F}_s$, $\mathcal{H}_1, \ldots, \mathcal{H}_s$. Per 3.1 di [2], esistono $b_1, \ldots, b_s \in \boldsymbol{F}_p$ tali che: $f(\theta) = b_1\sigma_1\theta + \ldots + b_s\sigma_s\theta$; inoltre, ogniqualvolta esiste $\xi \in \mathcal{H}$ tale che $\xi\mathcal{F}_i = \mathcal{F}_j$, risulta $b_i = b_j$.

Per $i = 1, \ldots, s$, detta $\varrho_i \in S_s$ la permutazione definita da $\xi_i^{-1}\mathcal{F}_j = \mathcal{F}_{\varrho_i(j)}$, si ha: $f(\theta) = b_{\varrho_i(1)}\xi_i^{-1}\sigma_1\theta + \ldots + b_{\varrho_i(s)}\xi_i^{-1}\sigma_s\theta$. Detta quindi $A = (a_{ij})$ la matrice $s \times s$, ad elementi in $\boldsymbol{F}_p$, tale che $a_{ij} = b_{\varrho_i(j)}$, si ha:

$$\begin{pmatrix} \xi_1 f(\theta) \\ \vdots \\ \xi_s f(\theta) \end{pmatrix} = A \begin{pmatrix} \sigma_1 \theta \\ \vdots \\ \sigma_s \theta \end{pmatrix};$$

inoltre, essendo $\sigma_1\theta, \ldots, \sigma_s\theta$ linearmente indipendenti su $\boldsymbol{F}_p$, A è l'unica matrice ad elementi in $\boldsymbol{F}_p$ verificante tale relazione per la scelta effettuata di θ e di $\sigma_1, \ldots, \sigma_s$, $\xi_1, \ldots, \xi_s$.

La matrice A soddisfa le condizioni richieste in a, infatti: dati $\theta' \in F$, e rappresentanti $\sigma'_1, \ldots, \sigma'_s$, $\xi'_1, \ldots, \xi'_s$ di $\mathcal{F}_1, \ldots, \mathcal{F}_s$, $\mathcal{H}_1, \ldots, \mathcal{H}_s$, essendo $\xi'_i f(\theta) = \xi_i f(\theta)$, $\sigma'_i\theta = \sigma_i\theta$, si ha intanto:

$$\begin{pmatrix} \xi'_1 f(\theta) \\ \vdots \\ \xi'_s f(\theta) \end{pmatrix} = A \begin{pmatrix} \sigma'_1 \theta \\ \vdots \\ \sigma'_s \theta \end{pmatrix};$$

tenuto quindi conto che $\theta' = c_0\theta^{p^0} + \ldots + c_{s-1}\theta^{p^{s-1}}$, con $c_0, \ldots, c_{s-1} \in k$ (cfr. 1.2), che f è un π-omomorfismo, e che A è a coefficienti in $\boldsymbol{F}_p$, si conclude facilmente che:

$$\begin{pmatrix} \xi'_1 f(\theta') \\ \vdots \\ \xi'_s f(\theta') \end{pmatrix} = A \begin{pmatrix} \sigma'_1 \theta' \\ \vdots \\ \sigma'_s \theta' \end{pmatrix}.$$

La matrice A verifica le proprietà di cui in b, infatti: se $\mathcal{H}_i^{-1}\mathcal{F}_j = \mathcal{H}_\lambda^{-1}\mathcal{F}_\mu$, si ha $\mathcal{H}\xi_i^{-1}\mathcal{F}_j = \mathcal{H}\xi_\lambda^{-1}\mathcal{F}_\mu$, ossia $\mathcal{H}\mathcal{F}_{\varrho_i(j)} = \mathcal{H}\mathcal{F}_{\varrho_\lambda(\mu)}$; ne segue facilmente che esiste $\xi \in \mathcal{H}$ tale che $\xi\mathcal{F}_{\varrho_i(j)} = \mathcal{F}_{\varrho_\lambda(\mu)}$, pertanto $b_{\varrho_i(j)} = b_{\varrho_\lambda(\mu)}$, e quindi $a_{ij} = a_{\lambda\mu}$, C.V.D..

Sia $f: F \to H$ un π-omomorfismo, e sia A la matrice che lo rappresenta, nel senso precisato in 1.8, rispetto ad N e ad $\mathcal{F}_1, \ldots, \mathcal{F}_s$, $\mathcal{H}_1, \ldots, \mathcal{H}_s$. Una volta nota la prima riga $(a_{11}, \ldots, a_{1s})$ di A, tenuto conto che $\{\mathcal{H}_1^{-1}\mathcal{F}_1, \ldots, \ldots, \mathcal{H}_1^{-1}\mathcal{F}_s\} = \ldots = \{\mathcal{H}_s^{-1}\mathcal{F}_1, \ldots, \mathcal{H}_s^{-1}\mathcal{F}_s\}$, l'asserto b di 1.8 consente di determinare le rimanenti righe di A.

Se N' è un secondo prolungamento normale di k, contenente F ed H, la matrice A' che rappresenta $f: F \to H$ rispetto ad N' e ad una qualsiasi attribuzione di indici alle classi laterali sinistre di $\mathcal{G}(N'/F)$ e di $\mathcal{G}(N'/H)$ in $\mathcal{G}(N'/k)$, coincide con A, a meno di permutazioni sulle colonne e sulle righe.

1.9 TEOREMA. *Sia* $A = (a_{ij})$ *una matrice* $s \times s$, *ad elementi in* $\boldsymbol{F}_p$, *tale che, ogniqualvolta* $\mathcal{H}_i^{-1} \mathcal{F}_j = \mathcal{H}_\lambda^{-1} \mathcal{F}_\mu$, *risulti* $a_{ij} = a_{\lambda\mu}$.

Esiste uno ed un solo π*-omomorfismo* $f\colon F \to H$, *avente* A *come matrice rappresentativa rispetto ad* N *e ad* $\mathcal{F}_1, \ldots, \mathcal{F}_s$, $\mathcal{H}_1, \ldots, \mathcal{H}_s$.

DIM. Ogniqualvolta esiste $\xi \in \mathcal{H}$ tale che $\xi \mathcal{F}_i = \mathcal{F}_j$, risulta $\mathcal{H}_1^{-1} \mathcal{F}_i = \mathcal{H}_1^{-1} \mathcal{F}_j$ (si ricordi che $\mathcal{H}_1 = \mathcal{H}$), e quindi $a_{1i} = a_{1j}$; per 3.1 di [2], l'applicazione $a_{11}\sigma_1 + \ldots + a_{1s}\sigma_s$, ove $\sigma_1, \ldots, \sigma_s$ sono rappresentanti di $\mathcal{F}_1, \ldots, \mathcal{F}_s$, è pertanto un π-omomorfismo di F in H, indipendente dalla particolare scelta di $\sigma_1, \ldots, \sigma_s$. Detto $f\colon F \to H$ tale π-omomorfismo, ed A' la matrice che lo rappresenta rispetto ad N e ad $\mathcal{F}_1, \ldots, \mathcal{F}_s$, $\mathcal{H}_1, \ldots, \mathcal{H}_s$, tenuto conto che la prima riga di A' coincide con la prima riga di A, per b di 1.8 e per le ipotesi poste, risulta $A' = A$.

L'unicità di f è banale, C.V.D..

1.10 TEOREMA. *Sia* $f\colon F \to H$ *un* π*-omomorfismo, e sia* A *la matrice che lo rappresenta rispetto ad* N *e ad* $\mathcal{F}_1, \ldots, \mathcal{F}_s$, $\mathcal{H}_1, \ldots, \mathcal{H}_s$. *Risultano equivalenti gli asserti*:

a) $f\colon F \to H$ *è un* π*-isomorfismo*,

b) $\det A \neq 0$.

DIM. Siano $\sigma_1, \ldots, \sigma_s, \xi_1, \ldots, \xi_s$ rappresentanti di $\mathcal{F}_1, \ldots, \mathcal{F}_s, \mathcal{H}_1, \ldots, \mathcal{H}_s$, e sia $\theta \in F$ tale che $\sigma_1\theta, \ldots, \sigma_s\theta$ siano linearmente indipendenti su $\boldsymbol{F}_p$ (cfr. 1.2). Per 1.2 si ha $F = k\boldsymbol{I}\theta^{p^0}, \ldots, \theta^{p^{s-1}}\boldsymbol{I}$; in particolare $fF = k\boldsymbol{I}f(\theta)^{p^0}, \ldots, f(\theta)^{p^{s-1}}\boldsymbol{I}$. $f\colon F \to H$ è pertanto un π-isomorfismo se e solo se $f(\theta)^{p^0}, \ldots, f(\theta)^{p^{s-1}}$ sono linearmente indipendenti su k, e quindi, per 1.2, se e solo se $\xi_1 f(\theta), \ldots, \xi_s f(\theta)$ sono linearmente indipendenti su $\boldsymbol{F}_p$. Osservando che in $\boldsymbol{F}_p\boldsymbol{I}\sigma_1\theta, \ldots, \sigma_s\theta\boldsymbol{I}$, ${}^tA$ è la matrice delle coordinate di $\xi_1 f(\theta), \ldots, \xi_s f(\theta)$ rispetto alla base $\sigma_1\theta, \ldots, \ldots, \sigma_s\theta$ (cfr. 1.8), si ha l'asserto, C.V.D..

1.11 TEOREMA. *Supponendo* k *perfetto, sia* $f\colon \operatorname{biv} F \to \operatorname{biv} H$ *un* π*-omomorfismo. Sussistono gli asserti*:

a) *esiste una ed una sola matrice* $A = (a_{ij})$, *di tipo* $s \times s$, *ad elementi in* $\boldsymbol{Q}_p$, *tale che, per ogni* $v \in \operatorname{biv} F$, *e per ogni scelta di rappresentanti* $\sigma_1, \ldots, \sigma_s$ *e* $\xi_1, \ldots, \xi_s$ *rispettivamente di* $\mathcal{F}_1, \ldots, \mathcal{F}_s$ *e* $\mathcal{H}_1, \ldots, \mathcal{H}_s$, *risulti*:

$$\begin{pmatrix} \xi_1 f(v) \\ \vdots \\ \xi_s f(v) \end{pmatrix} = A \begin{pmatrix} \sigma_1 v \\ \vdots \\ \sigma_s v \end{pmatrix};$$

b) *per tale* A, *ogniqualvolta* $\mathcal{H}_i^{-1} \mathcal{F}_j = \mathcal{H}_\lambda^{-1} \mathcal{F}_\mu$, *risulta* $a_{ij} = a_{\lambda\mu}$.

DIM. La dimostrazione di questo asserto, ove si tenga conto di 1.7 in luogo di 1.2, e di 3.2 di [2] in luogo di 3.1 di [2], è pressochè identica a quella di 1.8, C.V.D..

Dato un π-omomorfismo f: $biv\, F \to biv\, H$, per la matrice A che lo rappresenta rispetto ad N e ad $\mathcal{F}_1, \ldots, \mathcal{F}_s$, $\mathcal{H}_1, \ldots, \mathcal{H}_s$, nel senso precisato in 1.11, valgono considerazioni analoghe a quelle che seguono 1.8.

1.12 TEOREMA. *Sia $A = (a_{ij})$ una matrice $s \times s$, ad elementi in $\boldsymbol{Q}_p$, tale che, ogniqualvolta $\mathcal{H}_i^{-1}\mathcal{F}_j = \mathcal{H}_\lambda^{-1}\mathcal{F}_\mu$, risulti $a_{ij} = a_{\lambda\mu}$.*

Supponendo k perfetto, esiste uno ed un solo π-omomorfismo f: $biv\, F \to biv\, H$, avente A come matrice rappresentativa rispetto ad N e ad $\mathcal{F}_1, \ldots, \mathcal{F}_s$, $\mathcal{H}_1, \ldots, \mathcal{H}_s$.

DIM. La dimostrazione di questo asserto, ove si tenga conto di 3.2 di [2] in luogo di 3.1 di [1], e di b di 1.11 in luogo di b di 1.8, è pressochè identica a quella di 1.9, C.V.D..

1.13 TEOREMA. *Supponendo k perfetto, sia f: $biv\, F \to biv\, H$ un π-omomorfismo, e sia A la matrice che lo rappresenta rispetto ad N e ad $\mathcal{F}_1, \ldots, \mathcal{F}_s$, $\mathcal{H}_1, \ldots, \mathcal{H}_s$. Risultano equivalenti gli asserti:*

a) f: $biv\, F \to biv\, H$ *è un π-isomorfismo,*

b) $\det A \neq 0$.

DIM. La dimostrazione di questo asserto, ove si tenga conto di 1.7 e di 1.11 in luogo rispettivamente di 1.2 e di 1.8, è pressochè identica a quella di 1.10, C.V.D..

1.14 TEOREMA. *Si considerino gli elementi dell'insieme $\{\mathcal{H}_i^{-1}\mathcal{F}_j\colon i, j = 1, \ldots, s\}$ come indeterminate su $\boldsymbol{Q}$, cosicchè $(\mathcal{H}_i^{-1}\mathcal{F}_j)$ risulta una matrice a elementi in $\boldsymbol{Q}(\mathcal{H}_i^{-1}\mathcal{F}_j\colon i, j = 1, \ldots, s)$. Risultano equivalenti gli asserti:*

a) F ed H sono π-isomorfi,

b) esiste una specializzazione degli $\mathcal{H}_i^{-1}\mathcal{F}_j$ in $\boldsymbol{F}_p$, sulla quale $\det(\mathcal{H}_i^{-1}\mathcal{F}_j)$ *non si annulla.*

Supponendo k perfetto, risultano inoltre equivalenti gli asserti:

a′) $biv\, F$ e $biv\, H$ sono π-isomorfi,

b′) $\det(\mathcal{H}_i^{-1}\mathcal{F}_j) \neq 0$.

DIM. Per b di 1.8 e per 1.10, a implica b; per 1.9 e per 1.10, b implica a. Per b di 1.11 e per 1.13, a' implica b'; tenuto conto che $\boldsymbol{Q}_p$ è un corpo infinito, per 1.12 e per 1.13, b' implica a', C.V.D..

Se F ed H sono π-isomorfi, le loro chiusure normali su k, qualora immerse in N, coincidono (cfr. 2.1 di [1]); sussiste inoltre la seguente:

1.15 OSSERVAZIONE. *Supponendo k perfetto, se biv F e biv H sono π-isomorfi, le loro chiusure normali su biv k, qualora immerse in biv N, coincidono.*

DIM. Siano $\sigma_1, \ldots, \sigma_s, \xi_1, \ldots, \xi_s$ rappresentanti di $\mathcal{F}_1, \ldots, \mathcal{F}_s, \mathcal{H}_1, \ldots, \mathcal{H}_s$, e sia $\nu \in \textit{biv}\, F$ con $\sigma_1\nu, \ldots, \sigma_s\nu$ linearmente indipendenti su $\boldsymbol{Q}_p$ (cfr. 1.7). Essendo $\sigma_1\nu, \ldots, \sigma_s\nu$ a due a due distinti, si ha $\textit{biv}\, F = (\textit{biv}\, k)(\nu)$; inoltre la chiusura normale di $\textit{biv}\, F$ su $\textit{biv}\, k$ è $(\textit{biv}\, k)(\sigma_1\nu, \ldots, \sigma_s\nu)$.

Detta A la matrice che rappresenta f rispetto ad N e ad $\mathcal{F}_1, \ldots, \mathcal{F}_s$, $\mathcal{H}_1, \ldots, \mathcal{H}_s$, essendo $\det A \neq 0$ (cfr. 1.13), si ha $\boldsymbol{Q}_p \boldsymbol{I}\xi_1 f(\nu), \ldots, \xi_s f(\nu)\boldsymbol{I} = \boldsymbol{Q}_p \boldsymbol{I}\sigma_1\nu, \ldots, \sigma_s\nu\boldsymbol{I}$ (cfr. 1.11); in particolare risulta: $(\textit{biv}\, k)(\xi_1 f(\nu), \ldots, \xi_s f(\nu)) = (\textit{biv}\, k)(\sigma_1\nu, \ldots, \sigma_s\nu)$. L'asserto si ottiene allora osservando che $\xi_1 f(\nu), \ldots, \xi_s f(\nu)$ sono a due a due distinti, e quindi che $\textit{biv}\, H = (\textit{biv}\, k)(f(\nu))$, e che la chiusura normale di $\textit{biv}\, H$ su $\textit{biv}\, k$ è $(\textit{biv}\, k)(\xi_1 f(\nu), \ldots, \xi_s f(\nu))$, C.V.D..

CAPITOLO 2

π-MATRICI

1. Una matrice $A = (a_{ij})$, di tipo $s \times s$, ad elementi in un prolungamento di $\boldsymbol{Q}$, si dirà una *π-matrice*, se esistono: un gruppo finito G, due suoi sottogruppi $\mathcal{F}$, $\mathcal{H}$ di indice s, ed attribuzioni di indici $\mathcal{F}_1 = \mathcal{F}, \mathcal{F}_2, \ldots, \mathcal{F}_s$, e $\mathcal{H}_1 = \mathcal{H}, \mathcal{H}_2, \ldots, \mathcal{H}_s$ alle classi laterali sinistre di $\mathcal{F}$ ed $\mathcal{H}$ in G, tali che:

a) la matrice $(\mathcal{H}_i^{-1}\mathcal{F}_j)$ sia a righe e colonne a due a due distinte (qui l'insieme $\{\mathcal{H}_i^{-1}\mathcal{F}_j\colon i, j = 1, \ldots, s\}$ è considerato come un sistema di indeterminate su $\boldsymbol{Q}$),

b) A sia specializzazione banale di $(\mathcal{H}_i^{-1}\mathcal{F}_j)$ (nel senso che esiste un isomorfismo f di $\boldsymbol{Q}(\mathcal{H}_i^{-1}\mathcal{F}_j\colon i, j = 1, \ldots, s)$ tale che $f(\mathcal{H}_i^{-1}\mathcal{F}_j) = a_{ij}$).

In tale caso, tutte le matrici che si ottengono permutando le righe e le colonne di A, risultano π-matrici (*infatti*: Date $f, h \in S_s$, si ponga: $\mathcal{F}_j = \sigma_j\mathcal{F}$, $\mathcal{H}_i = \xi_i\mathcal{H}$, $\tilde{\mathcal{F}} = \sigma_{f(1)}\mathcal{F}\sigma_{f(1)}^{-1}$, $\tilde{\mathcal{H}} = \xi_{h(1)}\mathcal{H}\xi_{h(1)}^{-1}$, $\tilde{\sigma}_j = \sigma_{f(j)}\sigma_{f(1)}^{-1}$, $\tilde{\xi}_i = \xi_{h(i)}\xi_{h(1)}^{-1}$. Si verifica che: $\tilde{\sigma}_1\tilde{\mathcal{F}} = \tilde{\mathcal{F}}, \tilde{\sigma}_2\tilde{\mathcal{F}}, \ldots, \tilde{\sigma}_s\tilde{\mathcal{F}}$ e $\tilde{\xi}_1\tilde{\mathcal{H}} = \tilde{\mathcal{H}}, \tilde{\xi}_2\tilde{\mathcal{H}}, \ldots, \tilde{\xi}_s\tilde{\mathcal{H}}$ sono le classi laterali sinistre rispettivamente di $\tilde{\mathcal{F}}$ e $\tilde{\mathcal{H}}$ in G. Essendo $(\tilde{\mathcal{H}}\tilde{\xi}_i^{-1}\tilde{\sigma}_j\tilde{\mathcal{F}}) = (\xi_{h(i)}\mathcal{H}\xi_{h(1)}\sigma_{f(j)}\mathcal{F}\sigma_{h(1)}^{-1})$, la matrice $(\tilde{\mathcal{H}}\tilde{\xi}_i^{-1}\tilde{\sigma}_j\tilde{\mathcal{F}})$ si specializza banalmente in $(\mathcal{H}\xi_{h(i)}^{-1}\sigma_{f(j)}\mathcal{F})$ e quindi in $(a_{h(i),f(j)})$.)

2.1 TEOREMA. *Sia A una π-matrice di tipo $s \times s$. A verifica le seguenti condizioni*:

2.2 *A è a righe e colonne a due a due distinte,*

2.3 *esistono indeterminate $b_1, \ldots, b_r$ su $\boldsymbol{Q}$, e interi positivi $s_1, \ldots, s_r$, con $s_1 + \ldots + s_r = s$, tali che, posto:*

$$\boldsymbol{b} = (\underbrace{b_1, \ldots, b_1}_{s_1 \text{ volte}}, \ldots \ldots, \underbrace{b_r, \ldots, b_r}_{s_r \text{ volte}}),$$

le righe e le colonne di A sono permutazioni rispettivamente di $\boldsymbol{b}$ e di ${}^t\boldsymbol{b}$.

DIM. Siano $G, \mathcal{F}, \mathcal{H}, \mathcal{F}_1, \ldots, \mathcal{F}_s, \mathcal{H}_1, \ldots, \mathcal{H}_s$ verificanti per A le condizioni a, b; è sufficiente provare l'asserto per la matrice $(\mathcal{H}_i^{-1} \mathcal{F}_j)$. L'asserto 2.2 è allora ovvio. Quanto a 2.3, sussistono le considerazioni seguenti.

Siano $b_1, \ldots, b_r$ (ove $h \neq t$ implica $b_h \neq b_t$) gli elementi dell'insieme $\{\mathcal{H}\eta\mathcal{F} : \eta \in G\}$; ovviamente $\boldsymbol{Q}(b_1, \ldots, b_r) = \boldsymbol{Q}(\mathcal{H}_i^{-1} \mathcal{F}_j)$, pertanto $b_1, \ldots, b_r$ sono un sistema di indeterminate su $\boldsymbol{Q}$. Essendo $\mathcal{F}$ ed $\mathcal{H}$ equipotenti, ciascun b_t è unione di un ugual numero s_t di classi laterali sia sinistre di $\mathcal{F}$, che destre di $\mathcal{H}$; tenuto conto che $b_1, \ldots, b_r$ è una partizione di G, si ha allora: $s_1 + \ldots + s_r = s$. Si ponga $\boldsymbol{b} = (b_1, \ldots, b_1, \ldots \ldots, b_r, \ldots, b_r)$, ove ciascun b_t è ripetuto s_t volte.

Si consideri quindi la i-esima riga $(\mathcal{H}_i^{-1} \mathcal{F}_1, \ldots, \mathcal{H}_i^{-1} \mathcal{F}_s)$ di $(\mathcal{H}_i^{-1} \mathcal{F}_j)$, e sia ξ_i tale che $\mathcal{H}_i = \xi_i \mathcal{H}$. Per ciascun b_t si ha $\mathcal{H}_i^{-1} \mathcal{F}_j = b_t$ se e solo se $\mathcal{H}\xi_i^{-1} \mathcal{F}_j = b_t$, se e solo se $\xi_i^{-1} \mathcal{F}_j \subseteq b_t$, se e solo se $\mathcal{F}_j \subseteq \xi_i b_t$, se e solo se $\mathcal{F}_j$ è una delle s_t classi laterali sinistre di $\mathcal{F}$ in cui è ripartibile $\xi_i b_t$. Ne segue che ciascun b_t compare s_t volte nella i-esima riga di $(\mathcal{H}_i^{-1} \mathcal{F}_j)$; tale riga è pertanto permutazione di $\boldsymbol{b}$.

Con criterio analogo si prova che la j-esima colonna di $(\mathcal{H}_i^{-1} \mathcal{F}_j)$ è permutazione di ${}^t\boldsymbol{b}$, C.V.D..

2. Sia $A = (a_{ij})$ una matrice $s \times s$, ad elementi in un prolungamento di $\boldsymbol{Q}$, verificante le condizioni 2.2, 2.3.

Posto: $A = (\hat{A}_1, \ldots, \hat{A}_s) = \begin{pmatrix} \bar{A}_1 \\ \vdots \\ \bar{A}_s \end{pmatrix}$, ove $\hat{A}_j$ denota la j-esima colonna di A, ed $\bar{A}_i$ la i-esima riga, si considerino i seguenti sottinsiemi di S_s:

$\hat{\mathcal{A}} = \{\sigma \in S_s$: *l'insieme delle righe di* $(\hat{A}_{\sigma(1)}, \ldots, \hat{A}_{\sigma(s)})$ *coincide con l'insieme delle righe di* $A\}$,

$\bar{\mathcal{A}} = \left\{\sigma \in S_s\right.$: *l'insieme delle colonne di* $\begin{pmatrix} \bar{A}_{\sigma(1)} \\ \vdots \\ \bar{A}_{\sigma(s)} \end{pmatrix}$ *coincide con l'insieme delle colonne di* $\left. A \right\}$.

Data $\sigma \in \hat{\mathcal{A}}$, esiste una ed una sola $\sigma^0 \in S_s$ tale che:

$$(\hat{A}_{\sigma(1)}, \ldots, \hat{A}_{\sigma(s)}) = \begin{pmatrix} \bar{A}_{\sigma^0(1)} \\ \vdots \\ \bar{A}_{\sigma^0(s)} \end{pmatrix};$$

ovviamente $\sigma^0 \in \overline{\mathcal{A}}$. Data $\sigma \in \overline{\mathcal{A}}$, esiste una ed una sola $\sigma^* \in S_s$ tale che:

$$\begin{pmatrix} \bar{A}_{\sigma(1)} \\ \vdots \\ \bar{A}_{\sigma(s)} \end{pmatrix} = (\hat{A}_{\sigma^*(1)}, \ldots, \hat{A}_{\sigma^*(s)});$$

ovviamente $\sigma^* \in \hat{\mathcal{A}}$.

2.4 Osservazione. *$\hat{\mathcal{A}}$ e $\overline{\mathcal{A}}$ sono sottogruppi di S_s. Le applicazioni $^0\colon \hat{\mathcal{A}} \to \overline{\mathcal{A}}$, $^*\colon \overline{\mathcal{A}} \to \hat{\mathcal{A}}$ sono antiisomorfismi l'uno inverso dell'altro.*

Dim. Dato $\sigma \in S_s$, si verifica direttamente che $\sigma \in \hat{\mathcal{A}}$ (risp.: $\sigma \in \overline{\mathcal{A}}$), se e solo se esiste $\sigma' \in S_s$ tale che, per ogni i, j, risulti $a_{i,\sigma(j)} = a_{\sigma'(i),j}$ (risp.: $a_{\sigma(i),j} = a_{i,\sigma'(j)}$); in tal caso, ovviamente, $\sigma' = \sigma^0$ (risp.: $\sigma' = \sigma^*$).

Dati quindi $\varrho, \sigma \in \hat{\mathcal{A}}$, per ogni i, j, risulta: $a_{i,\varrho\sigma(j)} = a_{\varrho^0(i),\sigma(j)} = a_{\sigma^0\varrho^0(i),j}$; pertanto: $\varrho\sigma \in \hat{\mathcal{A}}$, $(\varrho\sigma)^0 = \sigma^0\varrho^0$. Analogamente, dati $\varrho, \sigma \in \overline{\mathcal{A}}$, si prova che: $\varrho\sigma \in \overline{\mathcal{A}}$, $(\varrho\sigma)^* = \sigma^*\varrho^*$. Tenuto conto che ^{0} e * sono applicazioni l'una inversa dell'altra, si ha l'asserto, C.V.D..

Poniamo infine: $\mathcal{C} = \{\sigma \in \hat{\mathcal{A}} : \sigma(1) = 1\}$, $\mathcal{R} = \{\sigma \in \hat{\mathcal{A}} : \sigma^0(1) = 1\}$. $\mathcal{C}$ ed $\mathcal{R}$ sono sottogruppi di $\hat{\mathcal{A}}$, e precisamente quelli costituiti dagli elementi di $\hat{\mathcal{A}}$ che lasciano invariata la prima colonna e, rispettivamente, la prima riga di A.

3. Sia A una π-matrice di tipo $s \times s$, e siano (cfr. 2.1) $\hat{\mathcal{A}}$, $\hat{\mathcal{A}}$, $\mathcal{C}$, $\mathcal{R}$ i gruppi legati ad A nel modo descritto in **2.**

Siano inoltre: G un gruppo finito; $\mathcal{F}$ ed $\mathcal{H}$ sottogruppi di G di indice s, tali che, dette $\mathcal{F}_1 = \mathcal{F}, \ldots, \mathcal{F}_s$, ed $\mathcal{H}_1 = \mathcal{H}, \ldots, \mathcal{H}_s$ le classi laterali sinistre di $\mathcal{F}$ ed $\mathcal{H}$ in G, la matrice A sia specializzazione banale di $(\mathcal{H}_i^{-1}\mathcal{F}_j)$.

Dato $\eta \in G$, indichiamo con $\hat{\eta}$ l'elemento di S_s tale che $\eta\mathcal{F}_i = \mathcal{F}_{\hat{\eta}(i)}$, ed indichiamo con $\bar{\eta}$ l'elemento di S_s tale che $\eta^{-1}\mathcal{H}_i = \mathcal{H}_{\bar{\eta}(i)}$; ovviamente:

$$(\hat{A}_{\hat{\eta}(1)}, \ldots, \hat{A}_{\hat{\eta}(s)}) = \begin{pmatrix} \bar{A}_{\bar{\eta}(1)} \\ \vdots \\ \bar{A}_{\bar{\eta}(s)} \end{pmatrix},$$

in particolare: $\hat{\eta} \in \hat{\mathcal{A}}$, $\bar{\eta} \in \overline{\mathcal{A}}$.

2.5 OSSERVAZIONE. *Sussistono gli asserti:*

a) $\hat{}: G \to \hat{\mathcal{A}}$ *è un omomorfismo*; $\ker \hat{} = \bigcap_{i=1}^{s} (\mathcal{F}_i \mathcal{F}_i^{-1})$;

b) $\bar{}: G \to \overline{\mathcal{A}}$ *è un antiomomorfismo*; $\ker \bar{} = \bigcap_{i=1}^{s} (\mathcal{H}_i \mathcal{H}_i^{-1})$;

c) $\ker \hat{} = \ker \bar{}$.

DIM. Gli asserti *a* e *b* si verificano direttamente. Tenuto conto che, per $\eta \in G$, risulta $\bar{\eta} = (\hat{\eta})^0$, $\hat{\eta} = (\bar{\eta})^*$ (cfr. la definizione di $\hat{\eta}, \bar{\eta}$), l'asserto *c* segue da 2.4, C.V.D..

Le immagini $\hat{G}$ e $\overline{G}$ di G tramite $\hat{}$ e $\bar{}$, sono sottogruppi rispettivamente di $\hat{\mathcal{A}}$ e di $\overline{\mathcal{A}}$;

tenuto inoltre conto che $\mathcal{F}_1 = \mathcal{F}$, $\mathcal{H}_1 = \mathcal{H}$, le immagini $\hat{\mathcal{F}}$ ed $\hat{\mathcal{H}}$ di $\mathcal{F}$ ed $\mathcal{H}$ tramite $\hat{}$, risultano sottogruppi rispettivamente di $\mathfrak{C}$ e di $\mathfrak{R}$.

2.6 TEOREMA. *Sussistono gli asserti:*

a) $\hat{G}$ *ed* $\hat{\mathcal{A}}$ *operano transitivamente sulle colonne di* A;

b) $\overline{G}$ *ed* $\overline{\mathcal{A}}$ *operano transitivamente sulle righe di* A.

DIM. La transitività di $\hat{G}$ e $\overline{G}$ segue dalla transitività di G come gruppo di operatori sia su $\{\mathcal{F}_1, \dots, \mathcal{F}_s\}$ che su $\{\mathcal{H}_1, \dots, \mathcal{H}_s\}$. La transitività di $\hat{\mathcal{A}}$ ed $\overline{\mathcal{A}}$, segue dall'essere $\hat{\mathcal{A}}$ e $\overline{\mathcal{A}}$ sovragruppi rispettivamente di $\hat{G}$ e $\overline{G}$, C.V.D..

2.7 TEOREMA.

i) *Siano* $\hat{A}_\lambda, \hat{A}_\mu$ *due colonne di* A, *tali che* $a_{1\lambda} = a_{1\mu}$; *esiste* $\sigma \in \hat{\mathcal{H}}$ (*in particolare*: $\sigma \in \mathfrak{R}$) *tale che*: $\sigma(\lambda) = \mu$;

ii) *Siano* $\overline{A}_\lambda, \overline{A}_\mu$ *due righe di* A, *tali che* $a_{\lambda 1} = a_{\mu 1}$; *esiste* $\sigma \in \hat{\mathcal{F}}$ (*in particolare*: $\sigma \in \mathfrak{C}$) *tale che*: $\sigma^0(\lambda) = \mu$.

DIM. i) Essendo $a_{1\lambda} = a_{1\mu}$, si ha $\mathcal{H}_1^{-1}\mathcal{F}_\mu = \mathcal{H}_1^{-1}\mathcal{F}_\mu$, ossia $\mathcal{H}\mathcal{F}_\lambda = \mathcal{H}\mathcal{F}_\mu$ (si ricordi che $\mathcal{H}_1 = \mathcal{H}$); esiste pertanto $\eta \in \mathcal{H}$ tale che $\eta\mathcal{F}_\lambda = \mathcal{F}_\mu$; allora: $\hat{\eta} \in \in \hat{\mathcal{H}} \subset \hat{\mathfrak{R}}$, e $\hat{\eta}(\lambda) = \mu$.

ii) Essendo $a_{\lambda 1} = a_{\mu 1}$, si ha $\mathcal{H}_\lambda^{-1}\mathcal{F}_1 = \mathcal{H}_\mu^{-1}\mathcal{F}_1$, ossia $\mathcal{H}_\lambda^{-1}\mathcal{F} = \mathcal{H}_\mu^{-1}\mathcal{F}$ (si ricordi che $\mathcal{F}_1 = \mathcal{F}$); esiste pertanto $\eta \in \mathcal{F}$ tale che $\mathcal{H}_\lambda^{-1}\eta = \mathcal{H}_\mu^{-1}$, ossia tale che $\eta^{-1}\mathcal{H}_\lambda = \mathcal{H}_\mu$; allora $\hat{\eta} \in \hat{\mathcal{F}} \subset \hat{\mathfrak{C}}$, e $(\hat{\eta})^0(\lambda) = \bar{\eta}(\lambda) = \mu$, C.V.D..

4. Sia $A = (a_{ij})$ una matrice $s \times s$ ad elementi in un prolungamento di $\boldsymbol{Q}$, verificante le condizioni 2.2, 2.3, necessarie a che A sia una π-matrice, e siano $\hat{\mathcal{A}}, \overline{\mathcal{A}}, \mathfrak{C}, \mathfrak{R}$ i gruppi legati ad A nel modo descritto in **2.**.

2.8 TEOREMA. *Risultano equivalenti gli asserti:*

a) A *è una* π*-matrice,*

b) $\hat{\mathcal{A}}$ *ed* $\overline{\mathcal{A}}$ *operano transitivamente rispettivamente sulle colonne e sulle righe di* A*; inoltre, date comunque colonne* $\hat{A}_\lambda, \hat{A}_\mu$ *di* A*, tali che* $a_{1\lambda} = a_{1\mu}$*, esiste* $\sigma \in \mathfrak{R}$ *tale che:* $\sigma(\lambda) = \mu$*,*

c) $\hat{\mathcal{A}}$ *ed* $\overline{\mathcal{A}}$ *operano transitivamente rispettivamente sulle colonne e sulle righe di* A*; inoltre, date comunque righe* $\overline{A}_\lambda, \overline{A}_\mu$ *di* A*, tali che* $a_{\lambda 1} = a_{\mu 1}$*, esiste* $\sigma \in \mathcal{C}$ *tale che:* $\sigma^0(\lambda) = \mu$*.*

DIM. Supponiamo in primo luogo che $\hat{\mathcal{A}}$ ed $\overline{\mathcal{A}}$ operino transitivamente. In tale ipotesi esistono: $\sigma_1, \ldots, \sigma_s, \xi_1, \ldots, \xi_s \in \hat{\mathcal{A}}$ tali che: $\sigma_1(1) = 1$, $\sigma_2(1) = 2, \ldots, \sigma_s(1) = s$, $\xi_1^0(1) = 1$, $\xi_2^0(2) = 1, \ldots, \xi_s^0(s) = 1$; si ponga $\mathcal{C}_i = \sigma_i \mathcal{C}$, $\mathfrak{R}_i = \xi_i \mathfrak{R}$.

Si ha: $\mathcal{C}_i = \{\sigma \in \hat{\mathcal{A}} \colon \sigma(1) = i\}$, $\mathfrak{R}_i = \{\sigma \in \hat{\mathcal{A}} \colon \sigma^0(i) = 1\}$. Infatti: se $\varphi \in \mathcal{C}$, si ha $\sigma_i \varphi(1) = \sigma_i(1) = i$; mentre se $\sigma(1) = i$, si ha $\sigma_i^{-1}\sigma(1) = \sigma_i^{-1}(i) = 1$, onde $\sigma_i^{-1}\sigma \in \mathcal{C}$, ossia $\sigma \in \mathcal{C}_i$. Inoltre: se $\psi \in \mathfrak{R}$, si ha $(\xi_i \psi)^0(i) = \psi^0 \xi_i^0(i) = \psi^0(1) = 1$; mentre se $\sigma^0(i) = 1$, si ha $\sigma^0(\xi_i^0)^{-1}(1) = \sigma^0(i) = 1$, onde $(\xi_i^{-1}\sigma)^0(1) = 1$, pertanto $\xi_i^{-1}\sigma \in \mathfrak{R}$, ossia $\sigma \in \mathfrak{R}_i$.

Ne segue che $\mathcal{C}_1 = \mathcal{C}, \mathcal{C}_2, \ldots, \mathcal{C}_s$ costituiscono una partizione di $\hat{\mathcal{A}}$, e sono pertanto le classi laterali sinistre di $\mathcal{C}$ in $\hat{\mathcal{A}}$; analogamente $\mathfrak{R}_1 = \mathfrak{R}$, $\mathfrak{R}_2, \ldots, \mathfrak{R}_s$ risultano le classi laterali sinistre di $\mathfrak{R}$ in $\hat{\mathcal{A}}$.

Ogniqualvolta $\mathfrak{R}_i^{-1}\mathcal{C}_j = \mathfrak{R}_\lambda^{-1}\mathcal{C}_\mu$, si ha $\xi_i^{-1}\sigma_j \in \mathfrak{R}\xi_\lambda^{-1}\sigma_\mu \mathcal{C}$, onde esistono $\eta \in \mathfrak{R}$, $\varphi \in \mathcal{C}$ tali che $\xi_i^{-1}\sigma_j = \eta \xi_\lambda^{-1}\sigma_\mu \varphi$, e pertanto (cfr. le considerazioni introduttive della dim. di 2.4): $a_{ij} = a_{(\xi_i^0)^{-1}(1), \sigma_j(1)} = a_{1, \xi_i^{-1}\sigma_j(1)} = a_{1, \eta\xi_\lambda^{-1}\sigma_\mu\varphi(1)}\, a_{(\xi_\lambda^0)^{-1}\eta^0(1), \sigma_\mu\varphi(1)} = a_{(\xi_\lambda^0)^{-1}(1), \sigma_\mu(1)} = a_{\lambda\mu}$. Ne segue che la matrice A è specializzazione della matrice $(\mathfrak{R}_i^{-1}\mathcal{C}_j)$; in particolare $(\mathfrak{R}_i^{-1}\mathcal{C}_j)$ è a righe e colonne a due a due distinte.

b) $\Rightarrow$ *a)*. Tenuto conto di quanto precede, resta da dimostrare che, ogniqualvolta $a_{ij} = a_{\lambda\mu}$, risulta $\mathfrak{R}_i^{-1}\mathcal{C}_j = \mathfrak{R}_\lambda^{-1}\mathcal{C}_\mu$. Questo è il caso, infatti: se $a_{ij} = a_{\lambda\mu}$, si ha $a_{1, \xi_i^{-1}\sigma_j(1)} = a_{1, \xi_\lambda^{-1}\sigma_\mu(1)}$, pertanto le colonne $\hat{A}_{\xi_i^{-1}\sigma_j(1)}$ e $\hat{A}_{\xi_\lambda^{-1}\sigma_\mu(1)}$ di A, hanno lo stesso primo elemento; esiste allora $\sigma \in \mathfrak{R}$ tale che $\sigma\big(\xi_\lambda^{-1}\sigma_\mu(1)\big) = \xi_i^{-1}\sigma_j(1)$, onde $\sigma_j^{-1}\xi_i\sigma\xi_\lambda^{-1}\sigma_\mu(1) = 1$, ossia $\sigma_j^{-1}\xi_i\sigma\xi_\lambda^{-1}\sigma_\mu \in \mathcal{C}$; ne segue $\xi_\lambda^{-1}\sigma_\mu \in \sigma^{-1}\xi_i^{-1}\sigma_j\mathcal{C} \subset \mathfrak{R}\xi_i^{-1}\sigma_j\mathcal{C}$, e infine $\mathfrak{R}_\lambda^{-1}\mathcal{C}_\mu = \mathfrak{R}_i^{-1}\mathcal{C}_j$.

c) $\Rightarrow$ *a)*. Tenuto conto delle considerazioni introduttive, resta da dimostrare che, ogniqualvolta $a_{ij} = a_{\lambda\mu}$, risulta $\mathfrak{R}_i^{-1}\mathcal{C}_j = \mathfrak{R}_\lambda^{-1}\mathcal{C}_\mu$. Questo è il caso, infatti: se $a_{ij} = a_{\lambda\mu}$, si ha $a_{(\xi_i^{-1}\sigma_j)^0(1),1} = a_{(\xi_\lambda^{-1}\sigma_\mu)^0(1),1}$, pertanto le righe $\overline{A}_{(\xi_i^{-1}\sigma_j)^0(1)}$ e $\overline{A}_{(\xi_\lambda^{-1}\sigma_\mu)^0(1)}$ di A, hanno lo stesso primo elemento; esiste allora $\sigma \in \mathcal{C}$ tale che $\sigma^0\big((\xi_\lambda^{-1}\sigma_\mu)^0(1)\big) = (\xi_i^{-1}\sigma_j)(1)$, onde $(\xi_\lambda^{-1}\sigma_\mu\sigma)^0(1) = (\xi_i^{-1}\sigma_j)^0(1)$,

$(\xi_\lambda^{-1}\sigma_\mu\sigma\sigma_j^{-1}\xi_i)^0(1)=1$, ossia $\xi_\lambda^{-1}\sigma_\mu\sigma\sigma_j^{-1}\xi_i\in\mathfrak{K}$; ne segue $\xi_\lambda^{-1}\sigma_\mu\in\mathfrak{K}\xi_i^{-1}\sigma_j\sigma\subset$ $\subset\mathfrak{K}\xi_i^{-1}\sigma_j$, e infine $\mathfrak{K}_\lambda^{-1}\mathfrak{C}_\mu=\mathfrak{K}_i^{-1}\mathfrak{C}_j$.

Che $a)\Rightarrow b)$, e che $a)\Rightarrow c)$, segue da 2.6, 2.7, C.V.D..

5. Sia A una π-matrice di tipo $s\times s$, e siano $\hat{\mathfrak{A}}$, $\mathfrak{C}$, $\mathfrak{K}$ i gruppi legati ad A nel modo descritto in **2**.

Siano inoltre $\sigma_1,\dots,\sigma_s$, $\xi_1,\dots,\xi_s$ (certamente esistenti per b di 2.8) tali che: $\sigma_1(1)=1$, $\sigma_2(1)=2,\dots,\sigma_s(1)=s$, $\xi_1^0(1)=1$, $\xi_2^0(2)=1,\dots,\xi_s^0(s)=1$; e siano: $\mathfrak{C}_i=\sigma_i\mathfrak{C}$, $\mathfrak{K}_i=\xi_i\mathfrak{K}$.

2.9 Teorema. *Sussistono gli asserti:*

a) $\mathfrak{C}_1=\mathfrak{C}$, $\mathfrak{C}_2,\dots,\mathfrak{C}_s$, *ed* $\mathfrak{K}_1=\mathfrak{K}$, $\mathfrak{K}_2,\dots,\mathfrak{K}_s$ *sono le classi laterali sinistre rispettivamente di* $\mathfrak{C}$ *ed* $\mathfrak{K}$ *in* $\hat{\mathfrak{A}}$;

b) la matrice $(\mathfrak{K}_i^{-1}\mathfrak{C}_j)$ *è a righe e colonne a due a due distinte*;

c) A *è specializzazione banale di* $(\mathfrak{K}_i^{-1}\mathfrak{C}_j)$.

Dim. Essendo A una π-matrice, i gruppi $\hat{\mathfrak{A}}$, $\overline{\mathfrak{A}}$, $\mathfrak{C}$, $\mathfrak{K}$ verificano le condizioni b di cui in 2.8; che, sotto tali condizioni, sussistono gli asserti a, b, c, è provato nel corso della dimostrazione di 2.8, C.V.D..

2.10 Corollario. *Si ha:* $\bigcap_{\sigma\in\hat{\mathfrak{A}}}\sigma\mathfrak{C}\sigma^{-1}=\bigcap_{\sigma\in\hat{\mathfrak{A}}}\sigma\mathfrak{K}\sigma^{-1}=\{\iota\}$. *In particolare:*

a) $\{\iota\}$ *è l'unico sottogruppo di* $\mathfrak{C}$, *normale in* $\hat{\mathfrak{A}}$,

b) $\{\iota\}$ *è l'unico sottogruppo di* $\mathfrak{K}$, *normale in* $\hat{\mathfrak{A}}$.

Dim. Sia $\varphi\in\bigcap\sigma\mathfrak{C}\sigma^{-1}$; per $i=1,\dots,s$, esiste $\eta_i\in\mathfrak{C}$ tale che $\varphi=\sigma_i\eta_i\sigma_i^{-1}$, pertanto $\varphi(i)=\sigma_i\eta_i\sigma_i^{-1}(i)=i$; ne segue $\varphi=\iota$.

Sia $\varphi\in\bigcap\sigma\mathfrak{K}\sigma^{-1}$; per $i=1,\dots,s$, esiste $\eta_i\in\mathfrak{K}$ tale che $\varphi=\xi_i\eta_i\xi_i^{-1}$, pertanto $\varphi^0(i)=(\xi_i\eta_i\xi_i^{-1})^0(i)=(\xi_i^0)^{-1}\eta_i^0\xi_i^0(i)=i$; ne segue $\varphi^0=\iota$, e quindi $\varphi=\iota$.
Gli asserti a e b sono ovvi, C.V.D..

2.11 Corollario. *Se* $\det A\neq 0$, *sussistono gli asserti:*

a) A^{-1} *è una* π-*matrice,*

b) A^{-1} *è specializzazione banale di* ${}^tA$ (nel senso che, posto $A=(a_{ij})$, $A^{-1}=(b_{ij})$, esiste un isomorfismo f di $\boldsymbol{Q}(a_{ij})$ tale che $f(a_{ij})=b_{ji}$).

Dim. Siano: k un corpo infinito e perfetto di caratteristica $p\neq 0$, ed N un prolungamento di Galois di k, tali che $\mathcal{G}(N/k)=\hat{\mathfrak{A}}$ (corpi certamente esistenti); siano inoltre F ed H i corpi di stabilità di $\mathfrak{C}$ ed $\mathfrak{K}$.

Tenuto conto che la trascendenza assoluta di $\boldsymbol{Q}_p$ è infinita, si può supporre A ad elementi in $\boldsymbol{Q}_p$, cosicchè, essendo A specializzazione di $(\mathfrak{K}_i^{-1}\mathfrak{C}_j)$ (cfr. 2.9), esiste un unico π-omomorfismo f: *biv* $F \to$ *biv* H, avente A come matrice rappresentativa rispetto ad N ed a $\mathfrak{C}_1, \ldots, \mathfrak{C}_s, \mathfrak{K}_1, \ldots, \mathfrak{K}_s$ (cfr. 1.12); per 1.13, f è un π-isomorfismo.

Sia B la matrice che rappresenta il π-isomorfismo f^{-1}: *biv* $H \to$ *biv* F, rispetto ad N ed a $\mathfrak{K}_1, \ldots, \mathfrak{K}_s$, $\mathfrak{C}_1, \ldots, \mathfrak{C}_s$. Per ciascun $\nu \in$ *biv* F si ha:

$$BA\begin{pmatrix}\sigma_1\nu\\ \vdots\\ \sigma_s\nu\end{pmatrix} = B\begin{pmatrix}\xi_1 f(\nu)\\ \vdots\\ \xi_s f(\nu)\end{pmatrix} = \begin{pmatrix}\sigma_1 f^{-1}f(\nu)\\ \vdots\\ \sigma_s f^{-1}f(\nu)\end{pmatrix} = \begin{pmatrix}\sigma_1\nu\\ \vdots\\ \sigma_s\nu\end{pmatrix};$$

tenuto conto che esiste $\nu \in$ *biv* F, con s coniugati su *biv* k, linearmente indipendenti su $\boldsymbol{Q}_p$ (cfr. 1.7), si ottiene $BA = I$, e quindi $B = A^{-1}$.

Tenuto conto della definizione di B, e quindi di b di 1.11, ciascuna delle matrici: ${}^tA$, ${}^t(\mathfrak{K}_i^{-1}\mathfrak{C}_j)$, $(\mathfrak{C}_i\mathfrak{K}_j^{-1})$, $(\mathfrak{C}_i^{-1}\mathfrak{K}_j)$, $B = A^{-1}$, si specializza nella successiva, pertanto A^{-1} è specializzazione di ${}^tA$; se tale specializzazione non fosse banale, detti Q_1, Q_2 i corpi ottenuti aggiungendo a $\boldsymbol{Q}$ gli elementi rispettivamente di ${}^tA$ e di A^{-1}, risulterebbe: $\mathrm{trasc}_{\boldsymbol{Q}} Q_2 < \mathrm{trasc}_{\boldsymbol{Q}} Q_1$, mentre risulta $Q_1 = Q_2$.

Che A^{-1} sia una π-matrice, segue dal fatto che ${}^tA$, e quindi anche A^{-1}, è specializzazione banale di $(\mathfrak{C}_i^{-1}\mathfrak{K}_j)$, C.V.D..

Capitolo 3

π-ISOMORFISMO E CONIUGIO

1.

3.1 Teorema. *Siano F, H prolungamenti separabili di k, tali che* $[F:k] = [H:k] \leqslant 6$. *Risultano equivalenti gli asserti*:

a) *F ed H sono π-isomorfi,*

b) *F ed H sono coniugati su k.*

Supponendo k perfetto, risultano inoltre equivalenti gli asserti:

a') *biv F e biv H sono π-isomorfi,*

b') *F ed H sono coniugati su k.*

DIM. Gli asserti: $b) \Rightarrow a)$, $b') \Rightarrow a')$, sono banali. Quanto ai rimanenti asserti, detto N un prolungamento di Galois di k, contenente F ed H, posto $G = \mathcal{G}(N/k)$, $\mathcal{F} = \mathcal{G}(N/F)$, $\mathcal{H} = \mathcal{G}(N/H)$, ed indicate con $\mathcal{F}_1 = \mathcal{F}, \ldots, \mathcal{F}_s$, e con $\mathcal{H}_1 = \mathcal{H}, \ldots, \mathcal{H}_s$, ove $s = [F:k] = [H:k]$, le classi laterali sinistre di $\mathcal{F}$ ed $\mathcal{H}$ in G, si consideri la matrice $B = (\mathcal{H}_i^{-1}\mathcal{F}_j)$. Sia nell'ipotesi a, che a', tenuto conto di 1.14, risulta $\det B \neq 0$; in particolare B è a righe e colonne a due a due diverse, ed è pertanto una π-matrice.

Si consideri la prima riga $(\mathcal{H}_1^{-1}\mathcal{F}_1, \ldots, \mathcal{H}_1^{-1}\mathcal{F}_s)$ di B. Se $s = 1, 2, 3$, tenuto conto di 2.2, in tale riga esiste un elemento privo di ripetizioni (cfr. 2.3); anche nel caso $s = 4, 5, 6$, tenuto conto che $\det B \neq 0$, in tale riga esiste (come verrà provato in successive considerazioni) un elemento privo di ripetizioni. In ciascun caso esiste quindi $\mathcal{F}_j$ tale che, per $h \neq j$, risulti $\mathcal{H}_1^{-1}\mathcal{F}_j \neq \mathcal{H}_1^{-1}\mathcal{F}_h$; conseguentemente esistono λ, μ tali che: $\mathcal{H}_1^{-1}\mathcal{F}_j = \mathcal{F}_\lambda = \mathcal{H}_\mu^{-1}$. Posto allora $\mathcal{F}_\lambda = \sigma\mathcal{F}$, $\mathcal{H}_\mu = \xi\mathcal{H}$, esiste $\varphi \in \mathcal{F}$ tale che: $\xi^{-1} = \sigma\varphi$; pertanto: $\mathcal{H} = \sigma\mathcal{F}\xi = \sigma\mathcal{F}\varphi^{-1}\sigma^{-1} = \sigma\mathcal{F}\sigma^{-1}$. Risultando $\mathcal{H}$ un coniugato di $\mathcal{F}$ rispetto ad un automorfismo interno di G, H ed F risultano allora coniugati su k.

Resta da provare che, se nella prima riga di una π-matrice A di tipo $s \times s$, con $s = 4, 5, 6$, ciascun elemento è ripetuto almeno due volte, allora $\det A = 0$; questo è il caso, infatti:

Oss. 1 – Per $s = 4$, eventualmente permutando righe e colonne (cfr. **1** del cap. 2), possiamo supporre che la 1-a riga di A sia (a, a, b, b), e la 1-a colonna sia ${}^t(a, a, b, b)$, con a, b indeterminate su $\boldsymbol{Q}$. Qualora risultasse $\det A \neq 0$, esisterebbe A^{-1}; per 2.11, A^{-1} sarebbe specializzazione banale di ${}^tA$. Dette quindi x, y indeterminate su $\boldsymbol{Q}$, ed X la matrice ottenuta da ${}^tA$ specializzando a in x, e b in y, sarebbe risolubile il sistema. $XA = I$. In particolare sarebbe risolubile il sistema:

$$(x, x, y, y)A = (1, 0, 0, 0)\,;$$

osservando però che le possibili 2-e colonne di A sono: ${}^t(a, b, a, b)$ e ${}^t(a, b, b, a)$, e che l'insieme della 3-a e 4-a colonna, nel primo caso è $\{{}^t(b, a, b, a), {}^t(b, b, a\; a)\}$, e nel secondo è $\{{}^t(b, a, a, b), {}^t(b, b, a, a)\}$, tale sistema si riduce a:

$$\begin{cases} 2ax + 2by = 1 \\ (a+b)x + (a+b)y = 0\,, \\ 2bx + 2ay = 0 \end{cases}$$

che è ovviamente non risolubile.

Oss. 2. – Per $s = 5$, eventualmente permutando righe e colonne, possiamo supporre che la 1-a riga di A sia (a, a, b, b, b), e la 1-a colonna sia ${}^t(a, a, b, b, b)$, con a, b indeterminate su $\boldsymbol{Q}$. Qualora risultasse $\det A \neq 0$, dette x, y indeterminate su $\boldsymbol{Q}$, ed X la matrice ottenuta da ${}^tA$, specializzando a in x, e b in y, analogamente alla osservazione precedente, sarebbe risolubile il sistema: $XA = I$. In particolare sarebbe risolubile il sistema:

$$(x, x, y, y, y)A = (1, 0, 0, 0, 0)\,;$$

osservando però che la 2-a colonna di A è del tipo ${}^t(a, b, ., ., .)$, e che le rimanenti colonne sono: una del tipo ${}^t(b, b, ., ., .)$, e due del tipo ${}^t(b, a, ., ., .)$, tale sistema si riduce a:

$$\begin{cases} 2ax + 3by = 1 \\ (a + b)x + (2a + b)y = 0\,, \\ 2bx + 3ay = 0 \end{cases}$$

che è ovviamente non risolubile.

Oss. 3. – Per $s = 6$, supponiamo in primo luogo che, previa permutazione sulle righe e sulle colonne, la 1-a riga di A sia (a, a, b, b, b, b) e la 1-a colonna sia ${}^t(a, a, b, b, b, b)$, con a, b indeterminate su $\boldsymbol{Q}$. Qualora risultasse $\det A \neq 0$, dette x, y indeterminate su $\boldsymbol{Q}$, analogamente alle osservazioni precedenti, sarebbe risolubile il sistema:

$$(x, x, y, y, y, y)A = (1, 0, 0, 0, 0, 0)\,;$$

osservando però che la 2-a colonna di A è del tipo ${}^t(a, b, ., ., ., .)$, e che le rimanenti colonne sono: una del tipo ${}^t(b, a, ., ., ., .)$, e tre del tipo ${}^t(b, b, ., ., ., .)$, tale sistema si riduce a:

$$\begin{cases} 2ax + 4by = 1 \\ (a + b)x + (a + 3b)y = 0\,, \\ 2bx + (2a + 2b)y = 0 \end{cases}$$

che è ovviamente non risolubile.

Oss. 4 – Per $s = 6$, supponiamo in secondo luogo che, previa permutazione sulle righe e sulle colonne, la 1-a riga di A sia (a, a, a, b, b, b), e la 1-a colonna sia ${}^t(a, a, a, b, b, b)$, con a, b indeterminate su $\boldsymbol{Q}$. Qualora risultasse $\det A \neq 0$, dette x, y indeterminate su $\boldsymbol{Q}$, analogamente alle osservazioni precedenti, sarebbe risolubile il sistema:

$$(x, x, x, y, y, y)A = (1, 0, 0, 0, 0, 0) .$$

Il prodotto della riga (x, x, x, y, y, y) per la 1-a colonna di A, è: $3ax + 3by$. Se i prodotti di tale riga, per le rimanenti colonne di A, avessero un unico risultato, tale risultato sarebbe: o $(a + 2b)x + (2a + b)y$, o $(2a + b)x + (a + 2b)y$ (non potrebbe infatti essere: nè $3ax + 3by$, perchè le colonne di A sono a due a due diverse, nè $3bx + 3ay$, perchè il primo elemento della 2-a e 3-a colonna è a); nel primo caso la somma degli elementi delle prime tre righe di A, che è $9a + 9b$, risulterebbe essere $3a + 5(a + 2b)$, nel secondo risulterebbe essere $3a + 5(2a + b)$.

Tenuto conto di quanto precede, e del fatto che i prodotti di (x, x, x, y, y, y) per le colonne di A di indice $\geqslant 2$, possono essere solo: $(a+2b)x + (2a+b)y$, $(2a + b)x + (a + 2b)y$, $3bx + 3by$, si conclude che nel sistema detto compaiono, oltre l'equazione:

$$3ax + 3by = 1 ,$$

almeno due delle equazioni:

$$(a + 2b)x + (2a + b)y = 0$$

$$(2a + b)x + (a + 2b)y = 0$$

$$3bx + 3ay = 0 ,$$

e che pertanto tale sistema è non risolubile.

Oss. 5. – Per $s = 6$, supponiamo infine che, previa permutazione sulle righe e sulle colonne, la 1-a riga di A sia (a, a, b, b, c, c), e la 1-a colonna sia ${}^t(a, a, b, b, c, c)$, con a, b, c indeterminate su $\boldsymbol{Q}$. Qualora risultasse $\det A \neq 0$, dette x, y, z indeterminate su $\boldsymbol{Q}$, analogamente alle osservazioni precedenti, sarebbe risolubile il sistema S, di 6 equazioni in 3 incognite:

$$(x, x, y, y, z, z)A = (1, 0, 0, 0, 0, 0) .$$

Le note che seguono provano invece che il sistema S è non risolubile.

Nota 1. – Se i coefficienti con i quali figura x nelle 6 equazioni di S sono in numero $\leqslant 3$, si verifica direttamente che la matrice costituita dalla 1-a e dalla 2-a riga di A è:

$$\begin{pmatrix} a & a & b & b & c & c \\ a & a & c & c & b & b \end{pmatrix};$$

se sono in numero $\leqslant 3$ i coefficienti con i quali figura y (risp.: z) nelle 6 equazioni di S, si verifica direttamente che la matrice costituita dalla 3-a e 4-a (risp.: 5-a e 6-a) riga di A, si ottiene da:

$$\begin{pmatrix} b & b & a & a & c & c \\ b & b & c & c & a & a \end{pmatrix} \quad \left(\text{risp.:} \begin{pmatrix} c & c & a & a & b & b \\ c & c & b & b & a & a \end{pmatrix}\right),$$

tramite permutazioni sulle colonne.

Nota 2. – In S esistono almeno 4 equazioni a due a due diverse.

Infatti: Qualora in S esistessero al più 3 equazioni a due a due diverse, le righe di A avrebbero la struttura di cui alla nota 1; conseguentemente, ed in contrasto con 2.2, la 2-a colonna di A verrebbe ad essere: ${}^{t}(a, a, b, b, c, c)$.

Nota 3. – Nel sistema S esistono 3 equazioni omogenee, a due a due diverse, tali che la matrice N, di tipo 3×3, dei loro coefficienti, abbia le colonne a due a due diverse.

Infatti: Si scelgano 3 equazioni omogenee diverse di S (cfr. nota 2). Se la matrice dei loro coefficienti ha due colonne uguali (ad es.: la 1-a e la 2-a), si constata che ciascuno degli elementi della rimanente colonna (nell'es.: la 3-a) è diverso dal corrispondente elemento delle altre due (altrimenti una delle equazioni scelte avrebbe come somma dei coefficienti un multiplo di 3 in $\boldsymbol{Z}[a, b, c]$, mentre tale somma è $2(a + b + c)$). Tenuto conto che la somma dei coefficienti con i quali figura ciascuna incognita nelle 6 equazioni di S, è $4(a + b + c)$, e che nella equazione non omogenea, x, y, z compaiono con coefficienti $2a, 2b, 2c$, in S esistono equazioni omogenee con il coefficiente di x (risp.: x, y) diverso da quello di y (risp.: z, z). Una opportuna di tali equazioni (nell'es.: una con il coefficiente di x diverso da quello di y), e due qualsiansi delle 3 equazioni inizialmente scelte, danno allora 3 equazioni del tipo richiesto.

Nota 4. – Sia $\mathcal{T}$ il sistema costituito da 3 equazioni del tipo descritto nella nota 3, e ne sia

$$N = \begin{pmatrix} \alpha & \lambda & \varphi \\ \beta & \mu & \psi \\ \gamma & \nu & \xi \end{pmatrix}$$

la matrice.

Se $\det N \neq 0$, il sistema S è ovviamente non risolubile.

Da qui innanzi supponiamo invece che $\det N = 0$.

Nota 5 – In N esistono almeno 2 colonne, ciascuna delle quali con gli elementi a due a due diversi.

Infatti: Si noti in primo luogo che la somma dei coefficienti di ciascuna equazione di S, e quindi degli elementi di ciascun riga di N, è $2(a+b+c)$. Qualora, ad es., $\alpha=\beta$, tenuto conto che:

$$\det\begin{pmatrix}\alpha & \lambda & 1\\ \beta & \mu & 1\\ \gamma & \nu & 1\end{pmatrix}=0,$$

e quindi che esistono u, v tali che:

$$\begin{pmatrix}1\\1\\1\end{pmatrix}=u\begin{pmatrix}\alpha\\ \beta\\ \gamma\end{pmatrix}+v\begin{pmatrix}\lambda\\ \mu\\ \nu\end{pmatrix},$$

e tenuto conto che $\lambda\neq\mu$ (altrimenti N avrebbe due righe uguali), e quindi che $v=0$, si ha: $\alpha=\beta=\gamma$. Per l'osservazione iniziale, si conclude che:

$$\begin{pmatrix}\lambda\\ \mu\\ \nu\end{pmatrix},\quad\begin{pmatrix}\varphi\\ \psi\\ \xi\end{pmatrix}$$

hanno ciascuna gli elementi a due a due diversi.

Nota 6. – Eventualmente permutando le righe di A, possiamo supporre che in N, le colonne di cui alla nota 5, siano la 1-a e la 2-a. Tenuto conto che:

$$0=\det N=\det\begin{pmatrix}\alpha & \lambda & 1\\ \beta & \mu & 1\\ \gamma & \nu & 1\end{pmatrix}=\det\begin{pmatrix}\alpha & \lambda & 1\\ \beta-\alpha & \mu-\lambda & 0\\ \gamma-\alpha & \nu-\lambda & 0\end{pmatrix}=$$

$$=\det\begin{pmatrix}\beta-\alpha & \mu-\lambda\\ \gamma-\alpha & \nu-\lambda\end{pmatrix},$$

si ha: $(\beta-\alpha)(\nu-\lambda)=(\gamma-\alpha)(\mu-\lambda)$.

Tenuto conto che: $\beta-\alpha$, $\nu-\lambda$, $\gamma-\alpha$, $\mu-\lambda$ sono elementi non nulli di $\boldsymbol{Q}[a, b, c]$ e che essendo di 1° grado sono primi, possono darsi due casi:

i) esiste $q\in\boldsymbol{Q}$ tale che: $\beta-\alpha=q(\gamma-\alpha)$, $\mu-\lambda=q(\nu-\lambda)$,

ii) esiste $q\in\boldsymbol{Q}$ tale che: $\beta-\alpha=q(\mu-\lambda)$, $\gamma-\alpha=q(\nu-\lambda)$;

in entrambi i casi, tenuto conto che $\beta-\alpha$, $\gamma-\alpha$, $\mu-\lambda$, $\nu-\lambda$ sono particolari tra i seguenti polinomi: $\pm(2a-2b)$ $\pm(2a-2c)$, $\pm(2b-2c)$, $\pm(a-b)$, $\pm(a-c)$, $\pm(b-c)$, $\pm(2a-b-c)$, $\pm(2b-a-c)$, $\pm(2c-a-b)$, si ha che $q \in \{\pm 2, \pm 1, \pm 1/2\}$.

Le considerazioni che seguono, esaminano i risultanti 12 casi a priori possibili:

1° *caso* $(i, q=2)$. – In tale caso si ha: $\alpha+\beta=2\gamma$, $\lambda+\mu=2\nu$. Tenuto conto che α, β, γ (risp.: λ, μ, ν) sono a due a due distinti; che $\alpha, \beta, \gamma, \lambda, \mu, \nu \in \{2a, 2b, 2c, a+b, a+c, b+c\}$; che la somma degli elementi in ciascuna riga di N è $2a+2b+2c$; che la somma degli elementi nella 1-a (risp.: 2-a, 3-a) colonna di N, è $ra+sb+tc$ con $r \leqslant 2$ (risp.: $s \leqslant 2$, $t \leqslant 2$), si ha che la 1-a colonna di N, è una delle seguenti:

$$\begin{pmatrix} 2b \\ 2c \\ b+c \end{pmatrix}, \quad \begin{pmatrix} 2c \\ 2b \\ b+c \end{pmatrix},$$

e che la 2-a colonna di N, è una delle seguenti:

$$\begin{pmatrix} 2a \\ 2c \\ a+c \end{pmatrix}, \quad \begin{pmatrix} 2c \\ 2a \\ a+c \end{pmatrix};$$

pertanto:

$$\text{o } N = \begin{pmatrix} 2b & 2c & 2a \\ 2c & 2a & 2b \\ b+c & a+c & a+b \end{pmatrix}, \quad \text{o } N = \begin{pmatrix} 2c & 2a & 2b \\ 2b & 2c & 2a \\ a+c & b+c & a+b \end{pmatrix}.$$

2° *caso* $(i, q=-2)$. – In tale caso risulterebbe: $3\alpha=\lambda+2\gamma$, $3\lambda=\mu+2\nu$. Essendo tali relazioni incompatibili con l'essere α, β, γ (risp.: λ, μ, ν) a due a due diversi, e con l'essere $\alpha, \beta, \gamma, \lambda, \mu, \nu \in \{2a, 2b, 2c, a+b, a+c, b+c\}$, tale caso non può verificarsi.

3° *caso* $(i, q=1)$. – In tale caso risulterebbe: $\beta=\gamma$, $\mu=\nu$. Essendo tali relazioni incompatibili con l'essere: $\beta \neq \gamma$, $\mu \neq \nu$, tale caso non può verificarsi.

4° *caso* $(i, q=-1)$. – In tale caso si ha: $\beta+\gamma=2\alpha$, $\mu+\nu=2\lambda$. Considerazioni analoghe a quelle del 1° caso, provano che:

$$\text{o } N = \begin{pmatrix} b+c & a+c & a+b \\ 2b & 2c & 2a \\ 2c & 2a & 2b \end{pmatrix}, \quad \text{o } N = \begin{pmatrix} b+c & a+c & a+b \\ 2c & 2a & 2b \\ 2b & 2c & 2a \end{pmatrix}.$$

5° *caso* $(i, q = 1/2)$. – In tale caso si ha: $\alpha + \gamma = 2\beta$, $\lambda + \nu = 2\mu$. Considerazioni analoghe a quelle del 1° caso, provano che:

$$\text{o } N = \begin{pmatrix} 2b & 2c & 2a \\ b+c & a+c & a+b \\ 2c & 2a & 2b \end{pmatrix}, \qquad \text{o } N = \begin{pmatrix} 2c & 2a & 2b \\ b+c & a+c & a+b \\ 2b & 2c & 2a \end{pmatrix}.$$

6° *caso* $(i, q = -1/2)$. – In tale caso risulterebbe: $3\alpha = 2\beta + \gamma$, $3\lambda = 2\mu + \nu$. Come il 2°, questo caso non può verificarsi.

7° *caso* $(ii, q = 2)$ – In tale caso risulterebbe: $\beta - \alpha = 2(\mu - \lambda)$, $\gamma - \alpha = 2(\nu - \lambda)$, e quindi anche: $\beta - \gamma = 2(\mu - \nu)$. Essendo $\beta - \alpha$, $\gamma - \alpha$, $\beta - \gamma$ multipli di 2 in $\boldsymbol{Z}[a, b, c]$, tenuto conto delle possibilità allora risultanti per: $\beta - \alpha$, $\gamma - \alpha$, $\beta - \gamma$ (cfr. nota 6), e quindi delle conseguenti possibilità per: α, β, γ, si avrebbe: $\{\alpha, \beta, \gamma\} = \{2a, 2b, 2c\}$. Tenuto allora conto che: $\mu - \lambda$, $\nu - \lambda$, $\mu - \nu \in \{\pm(a-b), \pm(a-c), \pm(b-c)\}$ si otterrebbe allora la uguaglianza di $\{\lambda, \mu, \nu\}$ con uno dei seguenti insiemi: $\{2a, a+b, a+c\}$, $\{2b, a+b, b+c\}$, $\{2c, a+c, b+c\}$, $\{a+b, a+c, b+c\}$. L'uguaglianza con uno dei primi tre insiemi non è compatibile con l'essere $2a + 2b + 2c$ la somma degli elementi di ciascuna riga di N; qualora sussistesse l'uguaglianza con il quarto, si avrebbe (a meno di permutazioni sulle righe):

$$N = \begin{pmatrix} 2a & b+c & b+c \\ 2b & a+c & a+c \\ 2c & a+b & a+b \end{pmatrix},$$

contro l'ipotesi che le colonne di N siano a due a due diverse. Questo caso non può pertanto verificarsi.

8° *caso* $(ii, q = -2)$. – In tale caso risulterebbe: $\beta - \alpha = -2(\mu - \lambda)$, $\gamma - \alpha = -2(\nu - \lambda)$, e quindi anche: $\beta - \gamma = -2(\mu - \nu)$. Con argomentazioni pressochè identiche a quelle del 7°, si prova che questo caso non può verificarsi.

9° *caso* $(ii, q = 1)$. – In tale caso risulterebbe $\alpha - \lambda = \beta - \mu = \gamma - \nu \neq 0$ (si ricordi che le colonne di N sono a due a due diverse). Tenuto conto che, dato $\eta \in \{\pm 2(a-b), \pm 2(a-c), \pm 2(b-c), \pm(2a-b-c), \pm(2b-a-c), \pm(2c-a-b)\}$, risultano univocamente determinati $\sigma, \varrho \in \{2a, 2b, 2c, a+b, a+c, b+c\}$ tali che $\sigma - \varrho = \eta$; e che, se $\sigma - \varrho = a - b$ allora, o: $\sigma = 2a$, $\varrho = a + b$, o: $\sigma = a + c$, $\varrho = b + c$; e che relazioni analoghe sussistono per $\sigma - \varrho$ coincidente con $-(a-b)$, $\pm(a-c)$, $\pm(b-c)$; e che la somma degli elementi di ciascuna riga di N, è $2a+2b+2c$; risulterebbe $\alpha=\beta=\gamma$, $\lambda=\mu=\nu$, contro l'ipotesi che, sia gli elementi della 1-a che della 2-a colonna di N siano a due a due diversi. Tale caso non può pertanto verificarsi.

10° *caso* (ii, $q=-1$). – In tale caso si ha $\alpha+\lambda=\beta+\mu=\gamma+\nu$. Per la solita condizione sulla somma degli elementi di ciascuna riga di N, si ottiene allora che gli elementi della 3-a colonna di N sono a due a due uguali. Tenuto conto che la somma dei coefficienti con i quali compare z nelle 6 equazioni di S, è $4(a+b+c)$, e che il coefficiente di z nell'equazione non omogenea, è $2c$, si deduce che la 3-a colonna di N è

$$\begin{pmatrix} a+b \\ a+b \\ a+b \end{pmatrix}.$$

11°, 12° *caso* (ii, $q=\pm 1/2$). – In tali casi risulterebbe: $\mu-\lambda=\pm(\beta-\alpha)$, $\nu-\lambda=\pm 2(\gamma-\alpha)$, $\mu-\nu=\pm 2(\beta-\gamma)$. Con argomentazioni pressochè identiche a quelle del 7°, si prova che questi casi non possono verificarsi.

Osserviamo quindi, a conclusione della nota 6, che i soli casi possibili risultano: il 1°, il 4°, il 5°, ed il 10°.

Nota 7. – Nelle ipotesi del 10° caso, nel sistema S esiste certamente una equazione omogenea: $nx+my+lz=0$, con $l\neq a+b$. Si consideri il sistema:

$$\begin{cases} \alpha x+\lambda y+(a+b)z=0 \\ \beta x+\mu y+(a+b)z=0\,, \\ nx+my+lz=0 \end{cases}$$

costituito da equazioni omogenee di S. Detta M la matrice di tale sistema, tenuto conto che: $\alpha+\lambda+(a+b)=\beta+\mu+(a+b)=2a+2b+2c$, e quindi che: $\alpha+\lambda=\beta+\mu=a+b+2c$, si ha:

$$\det M=\det\begin{pmatrix} a+b+2c & \lambda & a+b \\ a+b+2c & \mu & a+b \\ n+m & m & l \end{pmatrix}=\det\begin{pmatrix} a+b+2c & \lambda & a+b \\ 0 & \mu-\lambda & 0 \\ n+m & m & l \end{pmatrix}=$$

$$=(\mu-\lambda)[(a+b+2c)l-(a+b)(n+m)]\,.$$

Essendo $\mu \neq \lambda$ (cfr. nota 6), si ha: $\mu - \lambda \neq 0$; essendo $l \in \{2a, 2b, 2c, a + c, b + c\}$ (si ricordi che $l \neq a + b$), il polinomio $(a + b + 2c)l$ non è divisibile per $a + b$ in $Q[a, b, c]$, onde: $(a + b + 2c)l - (a + b)(n + m) \neq 0$; ne segue: $\det M \neq 0$, e conseguentemente il sistema $\mathcal{S}$ è, in questo caso, non risolubile.

Nota 8. – Nelle ipotesi di uno qualsiasi dei rimanenti 1°, 4°, 5° caso, nel sistema $\mathcal{S}$ figurano le equazioni:

$$\begin{cases} 2ax + 2by + 2cz = 1 \\ 2bx + 2cy + 2az = 0 \\ 2cx + 2ay + 2bz = 0 \\ (b + c)x + (a + c)y + (a + b)z = 0 \end{cases}$$

tenuto conto che: la somma dei coefficienti con i quali ciascuna incognita compare nelle 6 equazioni di $\mathcal{S}$, è $4(a + b + c)$, e che l'equazione omogenea: $2ax + 2by + 2cz = 0$ non figura in $\mathcal{S}$, si conclude che in $\mathcal{S}$, oltre alle equazioni dette, figurano anche, o le equazioni:

$$\begin{cases} 2ax + (b + c)y + (b + c)z = 0 \\ (b + c)x + (a + b)y + (a + c)z = 0 \end{cases},$$

o le equazioni:

$$\begin{cases} (a + b)x + (a + c)y + (b + c)z = 0 \\ (a + c)x + 2by + (a + c)z = 0 \end{cases};$$

anche in entrambi tali residui casi, il sistema $\mathcal{S}$ risulta non risolubile, C.V.D..

L'equivalenza degli asserti a, b di 3.1, sussiste per prolungamenti anche non separabili di k, di ordine $\leqslant 6$ (vedi l'appendice). Per prolungamenti di k di ordine $\geqslant 7$:

i) il π-isomorfismo non comporta necessariamente il coniugio; in particolare, mentre per prolungamenti di ordine $\leqslant 6$, l'isomorfismo delle iperalgebre locali R_F, R_H comporta l'isomorfismo di F ed H come prolungamenti di k, per prolungamenti di ordine $\geqslant 7$, tale implicazione può non sussistere;

ii) supponendo k perfetto, il π-isomorfismo dei bivettori non comporta necessariamente il π-isomorfismo tra i prolungamenti, e quindi (cfr. 3.3 di [2]) neppure il π-isomorfismo tra i vettori; in particolare, mentre per prolungamen i di ordine $\leqslant 6$, due iperalgebre locali R_F, R_H isogene, sono anche isomorfe, per prolungamenti di ordine $\geqslant 7$, tale implicazione può non sussistere.

I paragrafi seguenti provano l'esistenza di prolungamenti di ordine $\geqslant 7$, non coniugati ma π-isomorfi, e, nel caso di un corpo perfetto, di prolungamenti di ordine $\geqslant 7$, non π-isomorfi ma con i bivettori π-isomorfi.

2. Siano a, b indeterminate su $\boldsymbol{Q}$, e sia A la matrice 7×7, a elementi in $\boldsymbol{Q}(a, b)$, definita da:

$$A = \begin{pmatrix} a & a & a & a & b & b & b \\ a & a & b & b & b & a & a \\ a & b & b & a & a & a & b \\ a & b & a & b & a & b & a \\ b & b & a & a & b & a & a \\ b & a & b & a & a & b & a \\ b & a & a & b & a & a & b \end{pmatrix}.$$

Ovviamente A verifica le condizioni 2.2, 2.3; quanto ai gruppi $\mathfrak{A}, \overline{\mathfrak{A}}$, $\mathfrak{C}, \mathfrak{K}$ (cfr. **2** del cap. 2), indicando con $h_1 \ldots h_7$ la permutazione $\begin{pmatrix} 1 & \ldots & 7 \\ h_1 & \ldots & h_7 \end{pmatrix}$, riferendo quindi gli elementi di $\mathfrak{A}, \mathfrak{C}, \mathfrak{K}$ in ordine lessicografico, e gli elementi di $\overline{\mathfrak{A}}$ nell'ordine dei trasformati degli elementi di $\mathfrak{A}$ tramite ^{0}: $\mathfrak{A} \to \overline{\mathfrak{A}}$ (cfr. 2.4), si ha:

$\mathfrak{A} = \{$ 1234567 , 1243576 , 1267534 , 1276543 , 1324657 , 1342675 ,
1357624 , 1375642 , 1423756 , 1432765 , 1456723 , 1465732 ,
1537264 , 1546273 , 1564237 , 1573246 , 1627354 , 1645372 ,
1654327 , 1672345 , 1726453 , 1735462 , 1753426 , 1762435 ,
2134576 , 2143567 , 2167543 , 2176534 , 2314756 , 2341765 ,
2356714 , 2365741 , 2413657 , 2431675 , 2457613 , 2475631 ,
2536174 , 2547163 , 2563147 , 2574136 , 2617453 , 2635471 ,
2653417 , 2671435 , 2716354 , 2745361 , 2754316 , 2761345 ,
3124675 , 3142657 , 3157642 , 3175624 , 3214765 , 3241756 ,
3256741 , 3265714 , 3412567 , 3421576 , 3467512 , 3476521 ,
3517462 , 3526471 , 3562417 , 3571426 , 3625174 , 3647152 ,
3652147 , 3674125 , 3715264 , 3746251 , 3751246 , 3764215 ,
4123765 , 4132756 , 4156732 , 4165723 , 4213675 , 4231657 ,
4257631 , 4275613 , 4312576 , 4321567 , 4367521 , 4376512 ,
4516372 , 4527361 , 4561327 , 4572316 , 4615273 , 4637251 ,
4651237 , 4673215 , 4725163 , 4736152 , 4752136 , 4763125 ,

5137246 , 5146237 , 5164273 , 5173264 , 5236147 , 5247136 ,
5263174 , 5274163 , 5317426 , 5326417 , 5362471 , 5371462 ,
5416327 , 5427316 , 5461372 , 5472361 , 5614723 , 5623714 ,
5632741 , 5641732 , 5713624 , 5724613 , 5731642 , 5742631 ,
6127345 , 6145327 , 6154372 , 6172354 , 6217435 , 6235417 ,
6253471 , 6271453 , 6325147 , 6347125 , 6352174 , 6374152 ,
6415237 , 6437215 , 6451273 , 6473251 , 6514732 , 6523741 ,
6532714 , 6541723 , 6712534 , 6721543 , 6734512 , 6743521 ,
7126435 , 7135426 , 7153462 , 7162453 , 7216345 , 7245316 ,
7254361 , 7261354 , 7315246 , 7346215 , 7351264 , 7364251 ,
7425136 , 7436125 , 7452163 , 7463152 , 7513642 , 7524631 ,
7531624 , 7542613 , 7612543 , 7621534 , 7634521 , 7643512 },

$\overline{\mathcal{A}}$ = {1234567 , 1243576 , 2143567 , 2134576 , 1432657 , 1342756 ,
2341657 , 2431756 , 1423675 , 1324765 , 2314675 , 2413765 ,
4321567 , 4312576 , 3412567 , 3421576 , 4123657 , 4213756 ,
3214657 , 3124756 , 4132675 , 4231765 , 3241675 , 3142765 ,
1267534 , 1276543 , 2176534 , 2167543 , 1457632 , 1356742 ,
2357641 , 2456731 , 1475623 , 1365724 , 2375614 , 2465713 ,
4367521 , 4376512 , 3476521 , 3467512 , 4175632 , 4265731 ,
3275641 , 3165742 , 4157623 , 4256713 , 3257614 , 3156724 ,
1762354 , 1672453 , 2671354 , 2761453 , 1754362 , 1653472 ,
2654371 , 2753461 , 1574263 , 1563274 , 2573164 , 2564173 ,
4571362 , 4562371 , 3572461 , 3561472 , 4763251 , 4673152 ,
3674251 , 3764152 , 4751263 , 4652173 , 3651274 , 3752164 ,
1726345 , 1627435 , 2617345 , 2716435 , 1745326 , 1635427 ,
2645317 , 2735416 , 1547236 , 1536247 , 2546137 , 2537146 ,
4517326 , 4526317 , 3516427 , 3527416 , 4715236 , 4625137 ,
3615247 , 3725146 , 4736215 , 4637125 , 3647215 , 3746125 ,
7621534 , 7612543 , 6712534 , 6721543 , 7634521 , 7643512 ,
6743521 , 6734512 , 7541632 , 7532641 , 6542731 , 6531742 ,
7514623 , 7523614 , 6513724 , 6524713 , 5714632 , 5723641 ,
5624731 , 5613742 , 5741623 , 5732614 , 5631724 , 5642713 ,
7126354 , 7216453 , 6217354 , 6127453 , 7145362 , 7235461 ,
6245371 , 6135472 , 7436251 , 7346152 , 6347251 , 6437152 ,
7415263 , 7325164 , 6315274 , 6425173 , 5417362 , 5426371 ,
5327461 , 5316472 , 5147263 , 5136274 , 5237164 , 5246173 ,
7162345 , 7261435 , 6271345 , 6172435 , 7154326 , 7253416 ,
6254317 , 6153427 , 7451236 , 7352146 , 6351247 , 6452137 ,
7463215 , 7364125 , 6374215 , 6473125 , 5471326 , 5462317 ,
5361427 , 5372416 , 5174236 , 5163247 , 5264137 , 5273146 },

$$\mathcal{C} = \{1234567\,,\ 1243576\,,\ 1267534\,,\ 1276543\,,\ 1324657\,,\ 1342675\,,\\ 1357624\,,\ 1375642\,,\ 1423756\,,\ 1432765\,,\ 1456723\,,\ 1465732\,,\\ 1537264\,,\ 1546273\,,\ 1564237\,,\ 1573246\,,\ 1627354\,,\ 1645372\,,\\ 1654327\,,\ 1672345\,,\ 1726453\,,\ 1735462\,,\ 1753426\,,\ 1762435\}\,,$$

$$\mathfrak{K} = \{1234567\,,\ 1243576\,,\ 1324657\,,\ 1342675\,,\ 1423756\,,\ 1432765\,,\\ 2134576\,,\ 2143567\,,\ 2314756\,,\ 2341765\,,\ 2413657\,,\ 2431675\,,\\ 3124675\,,\ 3142657\,,\ 3214765\,,\ 3241756\,,\ 3412567\,,\ 3421576\,,\\ 4123765\,,\ 4132756\,,\ 4213675\,,\ 4231657\,,\ 4312576\,,\ 4321567\}\,.$$

Verificando $\mathcal{A}, \overline{\mathcal{A}}, \mathfrak{K}$ la condizione b di 2.8, A risulta una π-matrice; indicando con $\mathcal{C}_1 = \mathcal{C}, \mathcal{C}_2, \ldots, \mathcal{C}_7$, e con $\mathfrak{K}_1 = \mathfrak{K}, \mathfrak{K}_2, \ldots, \mathfrak{K}_7$ le classi laterali sinistre rispettivamente di $\mathcal{C}$ ed $\mathfrak{K}$ in $\mathcal{A}$, scelte con il criterio descritto in **5.** del cap. 2, per 2.9 la matrice A risulta specializzazione banale di $(\mathfrak{K}_i^{-1}\mathcal{C}_j)$.

Scelti allora un corpo infinito k di caratteristica p (che possiamo supporre perfetto), ed un prolungamento di Galois N di k, tali che $\mathcal{G}(N/k) = \hat{\mathcal{A}}$; detti F, H i corpi di stabilità rispettivamente di $\mathcal{C}$ e di $\mathfrak{K}$, si ha:

$[N:k] = 168$ ($\mathcal{A}$ è di ordine 168),

$[F:k] = [H:k] = 7$ ($\mathcal{C}$ ed $\mathfrak{K}$ hanno indice 7),

N è la chiusura normale su k sia di F che di H (cfr. 2.10),

F ed H non sono coniugati su k (qualora risultasse $\mathfrak{K} = \sigma\mathcal{C}\sigma^{-1}$, posto $\mathcal{C}_\mu = \sigma\mathcal{C}$, per $j \neq \mu$ si avrebbe $\mathfrak{K}_1^{-1}\mathcal{C}_j \neq \mathfrak{K}_1^{-1}\mathcal{C}_\mu$, mentre sulla prima riga di A ciascun elemento è ripetuto almeno due volte).

3.2 OSSERVAZIONE. *Se $p \neq 2$, allora F ed H sono π-isomorfi.*

DIM. Essendo: $\det A = 8(a-b)^6(4a+3b)$, sulla specializzazione di a, b in $\boldsymbol{F}_p$, definita da: $a \to 1$, $b \to 0$, $\det A$ non si annulla; l'asserto segue allora da 1.14, C.V.D..

3.3 OSSERVAZIONE. *Se $p = 2$, sussistono gli asserti*:

a) F ed H non sono π-isomorfi,

b) $\operatorname{biv} F$ e $\operatorname{biv} H$ sono π-isomorfi.

DIM. Tenuto conto che $\det A = 8(a-b)^6(4a+3b) \neq 0$, e che su qualsiani specializzazione di a, b in $\boldsymbol{F}_2$ $\det A$ è nullo, gli asserti seguono da 1.14, C.V.D..

3. L'osservazione 3.2 fornisce esempi di prolungamenti di ordine 7, non coniugati ma π-isomorfi; tali esempi sussistono per $p \neq 2$. Per $p = 2$, esempi analoghi si trovano per prolungamenti di ordine 8, come provato dalle considerazioni seguenti.

Siano a, b, c indeterminate su $\boldsymbol{Q}$, e sia A la matrice 8×8, a elementi in $\boldsymbol{Q}(a, b, c)$, definita da:

$$A = \begin{pmatrix} a & a & a & b & b & b & c & c \\ a & b & c & b & a & c & a & b \\ a & c & b & b & c & a & b & a \\ b & a & c & a & b & c & b & a \\ b & c & a & a & c & b & a & b \\ b & b & b & a & a & a & c & c \\ c & a & b & c & b & a & a & b \\ c & b & a & c & a & b & b & a \end{pmatrix}.$$

Ovviamente A verifica le condizioni 2.2, 2.3; quanto ai gruppi $\mathfrak{A}$, $\overline{\mathfrak{A}}$, $\mathfrak{C}$, $\mathfrak{K}$ (cfr. **2.** del cap. 2), riferendone gli elementi nel modo precisato per i gruppi analoghi di cui in **2.**, si ha:

$$\begin{aligned} \mathfrak{A} = \{ & 12345678, 13246587, 15742836, 16843725, 17548263, 18647352, \\ & 21354687, 23156478, 24851736, 26753814, 27658341, 28457163, \\ & 31264578, 32165487, 34761825, 35862714, 37468152, 38567241, \\ & 42815763, 43716852, 45612387, 46513278, 47318625, 48217536, \\ & 51724863, 53826741, 54621378, 56423187, 57128436, 58327614, \\ & 61834752, 62735841, 64531287, 65432178, 67238514, 68137425, \\ & 71584236, 72685314, 73486125, 74381652, 75182463, 76283541, \\ & 81674325, 82475136, 83576214, 84271563, 85372641, 86173452 \}, \end{aligned}$$

$$\begin{aligned} \overline{\mathfrak{A}} = \{ & 12345678, 13254687, 21365487, 23156478, 31264578, 32146587, \\ & 14728635, 15837624, 26817435, 25738416, 34827516, 36718524, \\ & 17482653, 18573642, 28671453, 27583461, 37681542, 38472561, \\ & 46513278, 45631287, 64523187, 65432178, 54621378, 56412387, \\ & 41768253, 43857261, 62847153, 63758142, 51867342, 52748361, \\ & 47186235, 48375216, 68274135, 67385124, 57284316, 58176324, \\ & 71462835, 72543816, 73651824, 82641735, 81563724, 83452716, \\ & 74126853, 76315842, 75234861, 86214753, 84325761, 85136742 \}, \end{aligned}$$

$$\mathfrak{C} = \{ 12345678, 13246587, 15742836, 16843725, 17548263, 18647352 \},$$

$$\mathfrak{K} = \{ 12345678, 13246587, 21354687, 23156478, 31264578, 32165487 \}.$$

Verificando $\hat{\mathfrak{A}}, \overline{\mathfrak{A}}, \mathfrak{K}$ la condizione b di 2.8, A risulta una π-matrice; indicando con $\mathfrak{C}_1 = \mathfrak{C}, \mathfrak{C}_2, \ldots, \mathfrak{C}_8$, e con $\mathfrak{K}_1 = \mathfrak{K}, \mathfrak{K}_2, \ldots, \mathfrak{K}_8$ le classi laterali sinistre rispettivamente di $\mathfrak{C}$ ed $\mathfrak{K}$ in $\hat{\mathfrak{A}}$, scelte con il criterio descritto in **5.** del cap. 2, per 2.9 la matrice A risulta specializzazione banale di $(\mathfrak{K}_i^{-1}\mathfrak{C}_j)$.

Scelti allora un corpo infinito k di caratteristica p (che possiamo supporre perfetto), ed un prolungamento di Galois N di k, tali che $\mathfrak{G}(N/k) = \hat{\mathfrak{A}}$; detti F, H i corpi di stabilità rispettivamente di $\mathfrak{C}$ e di $\mathfrak{K}$, si ha:

$[N:k] = 48$ ($\hat{\mathfrak{A}}$ è di ordine 48),

$[F:k] = [H:k] = 8$ ($\mathfrak{C}$ ed $\mathfrak{K}$ hanno indice 8),

N è la chiusura normale su k sia di F che di H (cfr. 2.10),

F ed H non sono coniugati su k (vedi l'asserto analogo in **2.**).

3.4 Osservazione. *Se $p \neq 3$ (in particolare se $p = 2$), allora F ed H sono π-isomorfi.*

Dim. Essendo: $\det A = -9(3a+3b+2c)(a-b)^4(a+b-2c)^3$, sulla specializzazione di a, b, c in $\boldsymbol{F}_p$, definita da: $a \to 1$, $b \to 0$, $c \to 0$, $\det A$ non si annulla; l'asserto segue allora da 1.14, C.V.D..

3.5 Osservazione. *Se $p = 3$, sussistono gli asserti:*

a) F ed H non sono π-isomorfi,

b) $\operatorname{biv} F$ e $\operatorname{biv} H$ sono π-isomorfi.

Dim. Gli asserti seguono da considerazioni analoghe a quelle relative a 3.3, C.V.D..

4. Le osservazioni 3.3, 3.5 provano che, nell'ambito dei prolungamenti di ordine 7, in caratteristica 2, e nell'ambito dei prolungamenti di ordine 8, in caratteristica 3, ne esistono di non π-isomorfi ma con i moduli dei bivettori π-isomorfi.

3.6 Osservazione. *Sia s un intero positivo; per quasi tutti i primi positivi p, sussiste l'asserto:*

Dati comunque un corpo perfetto k di caratteristica p, e suoi prolungamenti F, H di ordine s, allora: $\operatorname{biv} F$ e $\operatorname{biv} H$ sono π-isomorfi, se e solo se F ed H sono π-isomorfi;

in particolare (cfr. 3.3 di [2]): *$\operatorname{biv} F$ e $\operatorname{biv} H$ sono π-isomorfi se e solo se $\operatorname{vect} F$ e $\operatorname{vect} H$ sono π-isomorfi.*

DIM. Dette $a_1, \ldots, a_s$ indeterminate su $\boldsymbol{Q}$, le π-matrici di tipo $s \times s$, ad elementi appartenenti ad $\{a_1, \ldots, a_s\}$, sono ovviamente in numero finito. Siano $A_1, \ldots, A_\lambda$ quelle tra esse con determinante non nullo.

Sia $A_i \in \{A_1, \ldots, A_\lambda\}$, e siano $\boldsymbol{F}_{p_{i1}}, \boldsymbol{F}_{p_{i2}}, \ldots$ i corpi fondamentali per i quali, su ciascuna specializzazione di $a_1, \ldots, a_s$, $\det A_i$ è nullo. Tali corpi sono in numero finito; altrimenti, tenuto conto che l'applicazione

$$f\colon \boldsymbol{Z} \to \boldsymbol{F}_{p_{i1}} \dotplus \boldsymbol{F}_{p_{i2}} \dotplus \ldots,$$

definita da $f(n) = n1_{p_{i1}} \dotplus n1_{p_{i2}} \dotplus \ldots$, sarebbe un omomorfismo iniettivo di anelli, qualsiasi specializzazione di $a_1, \ldots, a_s$ in $\boldsymbol{Z}$ annullerebbe $\det A_i$, e pertanto risulterebbe $\det A_i = 0$.

Posto $\{\boldsymbol{F}_{p_1}, \ldots, \boldsymbol{F}_{p_r}\} = \{\boldsymbol{F}_{p_{11}}, \ldots; \boldsymbol{F}_{p_{21}}, \ldots; \ldots; \boldsymbol{F}_{p_{\lambda 1}}, \ldots\}$, sia $p \neq p_1, \ldots, p_r$, e siano: k un corpo perfetto di caratteristica p ed F, H suoi prolungamenti di ordine s.

Tenuto conto di 3.3 di [2], se F ed H sono π-isomorfi, anche $biv\, F$ e $biv\, H$ lo sono. Viceversa, se $biv\, F$ e $biv\, H$ sono π-isomorfi, detto N un prolungamento di Galois di k contenente F ed H, posto $G = \mathcal{G}(N/k)$, dette $\mathcal{F}_1 = \mathcal{F}, \ldots, \mathcal{F}_s$ ed $\mathcal{H}_1 = \mathcal{H}, \ldots, \mathcal{H}_s$ le classi laterali sinistre di $\mathcal{F} = \mathcal{G}(N/F)$ ed $\mathcal{H} = \mathcal{G}(N/H)$ in G, per 1.14 si ha: $\det(\mathcal{H}_i^{-1}\mathcal{F}_j) \neq 0$; in particolare $(\mathcal{H}_i^{-1}\mathcal{F}_j)$ è una π-matrice di tipo $s \times s$ a determinante non nullo, ed è pertanto specializzazione banale di una delle $A_1, \ldots, A_\lambda$. Essendo $p \neq p_1, \ldots, p_r$, esiste allora una specializzazione delle $\mathcal{H}_i^{-1}\mathcal{F}_j$ in $\boldsymbol{F}_p$ che non annulla $\det(\mathcal{H}_i^{-1}\mathcal{F}_j)$; tenuto conto di 1.14, H ed F risultano allora π-isomorfi, C.V.D..

APPENDICE

TEOREMA. *Siano F, H prolungamenti qualsiansi di k, tali che $[F:k] = [H:k] \leqslant 6$. Risultano equivalenti gli asserti:*

a) F ed H sono π-isomorfi,

b) F ed H sono coniugati su k.

DIM. Ovviamente l'asserto b implica a. Supponiamo viceversa che F ed H siano π-isomorfi, e sia $f\colon F \to H$ un π-isomorfismo. Dette $\tilde{F}, \tilde{H}$ le chiusure separabili di k rispettivamente in F ed H, da 1.1 di [2] segue facilmente $f\tilde{F} = \tilde{H}$, cosicchè, detta $\tilde{f}$ la restrizione di f a $\tilde{F}$, $\tilde{f}\colon \tilde{F} \to \tilde{H}$ è un π-isomorfismo. Per 3.1, $\tilde{F}$ ed $\tilde{H}$ sono coniugati su k.

Se $\tilde{F} = F$, l'asserto risulta dimostrato. Se $\tilde{F} = k$, ossia se F è puramente inseparabile su k, l'asserto, di per sè banale, è comunque conseguenza di 2.1 di [1]. Da qui innanzi supponiamo $\tilde{F} \neq k, F$; ciò comporta $[F:k] = 4$ o $[F:k] = 6$.

Per $[F:k] = 4$, si ha $[F:\tilde{F}] = 2$, $[\tilde{F}:k] = 2$; ne segue che $p = 2$, e che $\tilde{F}$ è di Galois su k. Posto $\mathcal{G}(\tilde{F}/k) = \{\iota, \sigma\}$, per 1.1 di [2] esistono $a, b \in \boldsymbol{F}_2$ tali che $\tilde{f} = a\iota + b\sigma$. Se fosse $a = b = 0$, risulterebbe $\tilde{f} = 0$; se fosse $a = b = 1$, risulterebbe $\tilde{f} = T_{\tilde{F}/k}$. Essendo invece $\tilde{f}$ bigettiva, si conclude che $\tilde{f} = \iota$, o che $\tilde{f} = \sigma$. Dati allora $x, y \in F$, si ha: $[f(x+y)]^2 = \tilde{f}((x+y)^2) = \tilde{f}(x^2 + y^2) = \tilde{f}(x^2) + \tilde{f}(y^2) = f(x)^2 + f(y)^2 = [f(x) + f(y)]^2$, da cui segue $f(x+y) = f(x) + f(y)$; analogamente $f(xy) = f(x)\,f(y)$; ovviamente se $x \in k$, $f(x) = x$. Si conclude che $f\colon F \to H$ è un isomorfismo di prolungamenti di k.

Per $[F:k] = 6$, possono darsi due casi: $[F:\tilde{F}] = 3$, $[\tilde{F}:k] = 2$, oppure $[F:\tilde{F}] = 2$, $[\tilde{F}:k] = 3$.

Supponiamo in primo luogo $[F:\tilde{F}] = 3$, $[\tilde{F}:k] = 2$, cosicchè $p = 3$, ed $\tilde{F}$ è di Galois su k. Posto $\mathcal{G}(\tilde{F}/k) = \{\iota, \sigma\}$, per 1.1 di [2] esistono $a, b \in \boldsymbol{F}_3$ tali che $\tilde{f} = a\iota + b\sigma$. Per ciascun $\theta \in \tilde{F}$ risulta:

$$\begin{pmatrix} \iota f(\theta) \\ \sigma f(\theta) \end{pmatrix} = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} \iota\theta \\ \sigma\theta \end{pmatrix} \quad \text{(cfr. 1.8);}$$

essendo $\tilde{f}$ un π-isomorfismo, per 1.10 si ha:

$$\det \begin{pmatrix} a & b \\ b & a \end{pmatrix} \neq 0\,,$$

ossia $a^2 - b^2 \neq 0$; ne segue che sussiste uno dei seguenti casi: $\tilde{f} = \iota$, $\tilde{f} = \sigma$, $\tilde{f} = -\iota$, $\tilde{f} = -\sigma$. Come per $[F:k] = 4$, nei primi due casi si prova che $f\colon F \to H$ è un isomorfismo di prolungamanti di k; nei secondi due casi si prova che $-f\colon F \to H$ lo è.

Supponiamo quindi che $[F:\tilde{F}] = 2$, $[\tilde{F}:k] = 3$, nel qual caso $p = 2$, e supponiamo inoltre che $\tilde{F}$ sia di Galois su k. Posto $\mathcal{G}(\tilde{F}/k) = \{\iota, \sigma, \sigma^2\}$, per 1.1 di [2] esistono $a, b, c \in \boldsymbol{F}_2$ tali che $\tilde{f} = a\iota + b\sigma + c\sigma^2$. Per ciascun $\theta \in \tilde{F}$ risulta:

$$\begin{pmatrix} \iota\tilde{f}(\theta) \\ \sigma\tilde{f}(\theta) \\ \sigma^2\tilde{f}(\theta) \end{pmatrix} = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \begin{pmatrix} \iota\theta \\ \sigma\theta \\ \sigma^2\theta \end{pmatrix} \quad \text{(cfr. 1.8);}$$

essendo $\tilde{f}$ un π-isomorfismo, per 1.10 si ha:

$$\det \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \neq 0\,,$$

ossia $a^3 + b^3 + c^3 - 3abc \neq 0$, e quindi $a + b + c + abc \neq 0$; ne segue che sussiste uno dei seguenti casi: $\tilde{f} = \iota$, $\tilde{f} = \sigma$, $\tilde{f} = \sigma^2$. Analogamente ai casi precedenti si conclude che $f: F \to H$ è un isomorfismo di prolungamenti di k.

Supponiamo infine che $[F:\tilde{F}] = 2$, $[\tilde{F}:k] = 3$, nel qual caso $p = 2$, e che $\tilde{F}$ non sia normale su k. Sia quindi N un prolungamento di Galois di k, contenente $\tilde{F}$ e $\tilde{H}$, e siano $\mathcal{F} = \mathcal{G}(N/\tilde{F})$, $\mathcal{H} = \mathcal{G}(N/\tilde{H})$. Dette $\mathcal{F}, \sigma\mathcal{F}, \eta\mathcal{F}$ le classi laterali sinistre di $\mathcal{F}$ in $\mathcal{G}(N/k)$, per 1.1 di [2] esistono $a, b, c \in \boldsymbol{F}_2$ tali che $\tilde{f} = a\iota + b\sigma + c\eta$.

Essendo $\tilde{H}$ un coniugato di $\tilde{F}$ su k, sussiste uno dei seguenti casi: $\tilde{H} = \tilde{F}$, $\tilde{H} = \sigma\tilde{F}$, $\tilde{H} = \eta\tilde{F}$; tenuto conto (come si verifica facilmente) che i corpi $\tilde{F}$, $\sigma\tilde{F}$, $\eta\tilde{F}$ sono a due a due diversi:

i) se $\tilde{H} = \tilde{F}$, allora $\mathcal{H} = \mathcal{F}$, e $\iota\mathcal{F}, \sigma\mathcal{F}, \eta\mathcal{F}$ sono le classi laterali sinistre di $\mathcal{H}$ in $\mathcal{G}(N/k)$,

ii) se $\tilde{H} = \sigma\tilde{F}$, allora $\mathcal{H} = \sigma\mathcal{F}\sigma^{-1}$, e $\iota\mathcal{H}, \sigma^{-1}\mathcal{H}, \eta\sigma^{-1}\mathcal{H}$ sono le classi laterali sinistre di $\mathcal{H}$ in $\mathcal{G}(N/k)$,

iii) se $\tilde{H} = \eta\tilde{F}$, allora $\mathcal{H} = \eta\mathcal{F}\eta^{-1}$, e $\iota\mathcal{H}, \eta^{-1}\mathcal{H}, \sigma\eta^{-1}\mathcal{H}$ sono le classi laterali sinistre di $\mathcal{H}$ in $\mathcal{G}(N/k)$.

Posto $\mathcal{F}_1 = \mathcal{F}$, $\mathcal{F}_2 = \sigma\mathcal{F}$, $\mathcal{F}_3 = \eta\mathcal{F}$, dette $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$ le classi laterali sinistre di $\mathcal{H}$ indicate separatamente nei casi i), ii), iii), e detti ξ_1, ξ_2, ξ_3 i rappresentanti ivi indicati, si consideri la matrice A che rappresenta $\tilde{f}$ rispetto ad N, e ad $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$, ossia la matrice tale che per ciascun $\theta \in \tilde{F}$ risulti:

$$\begin{pmatrix} \xi_1\tilde{f}(\theta) \\ \xi_2\tilde{f}(\theta) \\ \xi_3\tilde{f}(\theta) \end{pmatrix} = A \begin{pmatrix} \iota\theta \\ \sigma\theta \\ \eta\theta \end{pmatrix} \qquad \text{(cfr. 1.8);}$$

$\det A \neq 0$ (cfr. 1.10); la prima riga di A è (a, b, c); A è specializzazione della π-matrice $(\mathcal{H}_i^{-1}\mathcal{F}_j)$ (cfr. 1.8).

Nel caso i), si ha

$$(\mathcal{H}_i^{-1}\mathcal{F}_j) = \begin{pmatrix} \mathcal{F} & \mathcal{F}\sigma\mathcal{F} & \mathcal{F}\eta\mathcal{F} \\ \mathcal{F}\sigma^{-1}\mathcal{F} & \mathcal{F} & \mathcal{F}\sigma^{-1}\eta\mathcal{F} \\ \mathcal{F}\eta^{-1}\mathcal{F} & \mathcal{F}\eta^{-1}\sigma\mathcal{F} & \mathcal{F} \end{pmatrix}.$$

Gli insiemi $\mathcal{F}$, $\mathcal{F}\sigma\mathcal{F}$, $\mathcal{F}\eta\mathcal{F}$ sono a due a due disgiunti o coincidenti. Ovviamente $\mathcal{F} \neq \mathcal{F}\sigma\mathcal{F}$, $\mathcal{F}\eta\mathcal{F}$ (essendo $\sigma, \eta \notin \mathcal{F}$). Inoltre $\mathcal{F}\sigma\mathcal{F} \supset \sigma\mathcal{F}$, $\mathcal{F}\eta\mathcal{F} \supset \eta\mathcal{F}$;

allora se fosse $\mathcal{F}\sigma\mathcal{F} \neq \mathcal{F}\eta\mathcal{F}$, essendo $\mathcal{F}, \sigma\mathcal{F}, \eta\mathcal{F}$ una partizione di $\mathcal{G}(N/k)$, risulterebbe $\mathcal{F}\sigma\mathcal{F} = \sigma\mathcal{F}$, $\mathcal{F}\eta\mathcal{F} = \eta\mathcal{F}$, e ne seguirebbe $\mathcal{F}\sigma = \sigma\mathcal{F}$, $\mathcal{F}\eta = \eta\mathcal{F}$ contro l'ipotesi che $\mathcal{F}$ non sia normale in $\mathcal{G}(N/k)$. Si ha allora $\mathcal{F}\sigma\mathcal{F} = \mathcal{F}\eta\mathcal{F}$. Dette quindi b_1, b_2 indeterminate su $\boldsymbol{Q}$, $(\mathcal{K}_i^{-1}\mathcal{F}_j)$ risulta specializzazione banale di

$$\begin{pmatrix} b_1 & b_2 & b_2 \\ b_2 & b_1 & b_2 \\ b_2 & b_2 & b_1 \end{pmatrix} \quad \text{(cfr. } \mathbf{1.} \text{ del cap. 2, e 2.1)}\,.$$

Quanto alla matrice A, si ha allora $b = c$, e inoltre:

$$A = \begin{pmatrix} a & b & b \\ b & a & b \\ b & b & a \end{pmatrix}.$$

Essendo $\det A \neq 0$, risulta $a^3 + 2b^3 + 3ab^2 = a + ab = a(b+1) \neq 0$, e quindi $a = 1$, $b = c = 0$; conseguentemente $\tilde{f} = \iota$. Come nei casi precedenti si conclude allora che $f\colon F \to H$ è un isomorfismo di prolungamenti di k (in questo caso è $f = \iota$).

Nel caso ii), si ha

$$(\mathcal{K}_i^{-1}\mathcal{F}_j) = \begin{pmatrix} \sigma\mathcal{F}\sigma^{-1}\mathcal{F} & \sigma\mathcal{F} & \sigma\mathcal{F}\sigma^{-1}\eta\mathcal{F} \\ \sigma\mathcal{F} & \sigma\mathcal{F}\sigma\mathcal{F} & \sigma\mathcal{F}\eta\mathcal{F} \\ \sigma\mathcal{F}\eta^{-1}\mathcal{F} & \sigma\mathcal{F}\eta^{-1}\sigma\mathcal{F} & \sigma\mathcal{F} \end{pmatrix}.$$

Tenuto conto che $\mathcal{F} \neq \mathcal{F}\sigma\mathcal{F}, \mathcal{F}\eta\mathcal{F}$, e che $\mathcal{F}\sigma\mathcal{F} = \mathcal{F}\eta\mathcal{F}$ (cfr. le considerazioni del caso i)), dette b_1, b_2 indeterminate su $\boldsymbol{Q}$, $(\mathcal{K}_i^{-1}\mathcal{F}_j)$ risulta specializzazione banale di

$$\begin{pmatrix} b_1 & b_2 & b_1 \\ b_2 & b_1 & b_1 \\ b_1 & b_1 & b_2 \end{pmatrix} \quad \text{(cfr. } \mathbf{1.} \text{ del cap. 2, e 2.1)}\,.$$

Quanto alla matrice A, si ha allora $a = c$, e inoltre

$$A = \begin{pmatrix} a & b & a \\ b & a & a \\ a & a & b \end{pmatrix}.$$

Essendo $\det A \neq 0$, risulta $3a^2b + 2a^3 + b^3 = ab + b = b(a+1) \neq 0$, e quindi $a = c = 0$, $b = 1$; conseguentemente $\tilde{f} = \sigma$. Come nei casi precedenti si conclude che $f\colon F \to H$ è un isomorfismo di prolungamenti di k.

Nel caso iii), procedendo con criterio analogo al caso ii), si prova che $\tilde{f} = \eta$, e si conclude nuovamente che $f\colon F \to H$ è un isomorfismo di prolungamenti di k, C.V.D..

BIBLIOGRAFIA

[MC] I. Barsotti, *Moduli canonici e gruppi analitici commutativi*, Ann. Scuola Norm. Sup. Pisa, **13** (1959), pg. 303.

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

[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 appl., (IV), **115** (1977), pg. 381.

[3] S. Lang, *Algebra*, Addison-Wesley, 1965.

Istituto di Matematiche Applicate
Facoltà di Ingegneria dell'Università
via Diotisalvi, 6
56100 Pisa

Accademia Navale
viale Italia, 72
57100 Livorno