Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Orazio Sorace

Struttura metrica inerente ad una estensione algebrica

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **56** (1974), n.3, p. 280–285.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1974_8_56_3_280_0>

Algebra. — *Struttura metrica inerente ad una estensione algebrica* (*). Nota di ORAZIO SORACE, presentata (**) dal Socio B. SEGRE.

SUMMARY. — A study is performed of a metric structure related to a non purely inseparable extension and of the Galois group isometry.

1. Mostreremo che lo spazio vettoriale V definito da una estensione algebrica finita non puramente inseparabile può venir dotato di una geometria ortogonale ([1], p. 125), cioè di una struttura metrica cui è collegata un'applicazione ψ semilineare mediante la quale si dà una caratterizzazione affinché V risulti non singolare. Una particolarizzazione di tale struttura metrica permette di distinguere le estensioni separabili da quelle non separabili, risultando il discriminante del relativo spazio V rispettivamente diverso da zero ovvero nullo.

Se lo spazio V è inerente ad una estensione inseparabile, si trova per la dimensione del suo radicale una limitazione superiore che, nel caso dell'estensione semplice, è la differenza tra il grado dell'estensione ed il suo grado ridotto. Infine si studiano le rotazioni e le riflessioni cioè le isometrie del gruppo di Galois di una estensione separabile e normale, nel caso dei campi finiti.

2. Riferiamoci ad un campo δ che sia una estensione finita, e quindi algebrica, propria, di *grado* $n \geq 2$, di un fissato campo γ di caratteristica $p \neq 2$. Ricordiamo che, se è $p = 0$, l'estensione δ/γ è certamente separabile. Se invece è $p > 0$ e se γ_0 è la massima estensione separabile di γ in δ, sarà δ puramente inseparabile su γ_0; cioè, per ogni $X \in \delta$, si avrà un minimo esponente intero $e \geq 0$ per cui $X^{p^e} \in \gamma_0$. Il massimo di tali esponenti al variare di X in δ, che designeremo ancora con e, dicesi l'*esponente* dell'estensione δ/γ. Il grado $n_0 = (\gamma_0 : \gamma)$ dicesi il *grado ridotto* dell'estensione δ/γ. L'intero positivo f per cui $n = n_0 p^f$ soddisfa alla $f \geq e$. L'estensione è semplice se, e solo se, $f = e$.

Nel seguito supporremo che l'estensione δ/γ non sia puramente inseparabile cioè che sia $p = 0$, ovvero che, se è $p > 0$, l'estensione γ_0/γ sia propria, onde $n_0 \geq 2$.

Nel caso $p > 0$, chiamiamo φ l'isomorfismo tra δ e δ^{p^e} cioè $\varphi X = X^{p^e}$ per ogni $X \in \delta$. In tal caso, se l'estensione δ/γ è poi separabile, sarà $f = e = 0$ e risulterà essere φ l'automorfismo identico. Se invece è $p = 0$, intenderemo sempre con φ l'automorfismo identico.

(*) Lavoro eseguito nell'ambito del G.N.S.A.G.A. del C.N.R.

(**) Nella seduta del 9 marzo 1974.

Consideriamo tale estensione δ come uno spazio vettoriale V di dimensione finita n sopra il campo γ. Diciamo che una ***struttura metrica simmetrica*** è assegnata ad un tale spazio vettoriale V, quando è definito, per tutti gli $X, Y \in V$, un ***prodotto interno*** $X \cdot Y \in \gamma$, tale che, per ogni $a \in \gamma$, si abbia:

I) $X \cdot Y = Y \cdot X$;

II) $(X_1 + X_2) \cdot Y = X_1 \cdot Y + X_2 \cdot Y$;

III) $(a\, X) \cdot Y = \varphi a\, (X \cdot Y)$.

Quando l'estensione δ/γ è separabile, φ si riduce all'identità e tale struttura metrica risulta una forma bilineare simmetrica.

Se $U_1, U_2, \cdots, U_n$ è una base di δ/γ, due elementi X e Y qualsiasi di V possono rappresentarsi, ed in maniera unica, mediante le

$$X = \sum_{i=1}^{n} x^i\, U_i \quad ; \quad Y = \sum_{i=1}^{n} y^i\, U_i \qquad (x^i, y^i \in \gamma).$$

Posto

$$U_i \cdot U_j = g_{ij} \in \gamma \qquad (i, j = 1, 2, \cdots, n), \tag{1}$$

si avrà

$$X \cdot Y = \sum_{i,j=1}^{n} g_{ij}\, \varphi\, (x^i y^j).$$

Nel seguito chiameremo ***discriminante*** di V, relativamente alla base U_i, il determinante G della matrice (g_{ij}).

Se $V_1, V_2, \cdots, V_n$ è una nuova base di δ/γ e se è $V_j = \sum_{i=1}^{n} a_j^i\, U_i$ con $a_j^i \in \gamma$, posto $\bar{g}_{ij} = V_i \cdot V_j$, si avrà, sotto forma matriciale,

$$(\bar{g}_{ij}) = (\varphi\, a_i^j)\, (g_{ij})\, (\varphi\, a_j^i), \tag{2}$$

dove (φa_i^j) è la trasposta della matrice (φa_j^i).

Quel sottospazio vettoriale di V che contiene tutti i vettori $X \in V$, che siano ortogonali a ciascun vettore di V, tali cioè che sia $X \cdot Y = 0$ per qualsiasi $Y \in V$, è il *radicale* di V e si indica con rad V. Lo spazio V dicesi *non singolare* se rad V contiene soltanto il vettore nullo.

3. Denotiamo con $\mathfrak{L}(V)$ lo spazio delle funzioni semilineari di V cioè delle applicazioni semilineari $V \to \gamma$.

Consideriamo l'applicazione $\psi : V \to \mathfrak{L}(V)$ tale che

$$(\psi X)\, (Y) = X \cdot Y, \tag{3}$$

cioè, per ogni $X \in V$, sia $\psi X \in \mathfrak{L}(V)$ la funzione semilineare che faccia corrispondere ad ogni $Y \in V$ lo scalare $X \cdot Y$.

L'applicazione ψ è semilineare perché, per le II) e III), risulta

$$\psi(X_1 + X_2) = \psi X_1 + \psi X_2 \qquad (X_1, X_2 \in V)$$

$$\psi(aX) = (\varphi a)\,\psi X \qquad (X \in V, a \in \gamma).$$

Analogamente a quanto accade per le forme bilineari, per le quali l'applicazione ψ è lineare ([2], p. 65), si può facilmente verificare che il nucleo di ψ, che indicheremo con Ker ψ, coincide con rad V. E dimostreremo che:

Lo spazio V *è non singolare se e solo se l'applicazione semilineare* ψ *definita dalla* (3) *è iniettiva.*

Infatti se ψ è iniettiva vi è al più un vettore $X \in V$ tale che $\psi X = 0$. Ma $\psi 0 = 0$ e quindi $\mathrm{Ker}\,\psi = \mathrm{rad}\,V = (0)$. Viceversa sia V non singolare. Allora, se $\psi X_1 = \psi X_2$ per due $X_1, X_2 \in V$, si ha $\psi(X_1 - X_2) = \psi X_1 + (-1)^{p^e}\psi X_2 = 0$ essendo $p \neq 2$. Quindi $X_1 - X_2 \in \mathrm{Ker}\,\psi$, è $X_1 = X_2$ e la ψ è iniettiva.

Non possiamo affermare che ψ è suriettiva per uno spazio V non singolare, come nel caso delle forme bilineari, perché in generale l'immagine di ψ non è un sottospazio ma soltanto un sottoinsieme di $\mathfrak{L}(V)$, come si può facilmente verificare.

Se U_i $(i = 1, 2, \cdots, n)$ è una base di V, la base *duale* di $\mathfrak{L}(V)$ è costituita dalle n funzioni f^j $(j = 1, 2, \cdots, n)$ date da $f^j(U_i) = \delta_i^j$ (simbolo di Kronecker). Si ha che

$$\psi X = \sum_{j=1}^{n} X \cdot U_j f^j \qquad (X \in V)$$

$$\psi U_i = \sum_{j=1}^{n} g_{ij} f^j \qquad (i = 1, 2, \cdots, n).$$

Sarà $X \in \ker\psi$ se e solo se $X \cdot U_j = 0$ $(j = 1, 2, \cdots, n)$ cioè se e solo se

$$\sum_{i=1}^{n} (\varphi x^i)\, g_{ij} = 0 \qquad (j = 1, 2, \cdots, n). \tag{4}$$

Avremo quindi che:

Condizione sufficiente affinché V *sia non singolare è che risulti* $G \neq 0$.

Infatti in tal caso il sistema (4) ammette la sola soluzione $\varphi x^j = 0$ e quindi la sola soluzione $x^j = 0$. Si avrà perciò $\mathrm{rad}\,V = \mathrm{Ker}\,\psi = (0)$.

Ricordiamo che, nel caso delle forme bilineari, dalla condizione $G = 0$ si deduce che $\mathrm{rad}\,V \neq (0)$. Per approfondire, nel nostro caso, lo studio delle metriche degli spazi vettoriali a discriminante nullo, associamo ad ogni applicazione semilineare ψ, l'applicazione lineare $\bar{\psi} : V \to \mathfrak{L}(V)$ definita per mezzo delle:

$$\bar{\psi} U_i = \sum_{j=1}^{n} g_{ij} f^j \qquad (i = 1, 2, \cdots, n).$$

Sarà $X \in \operatorname{Ker} \bar{\psi}$ se e solo se

$$\sum_{i=1}^{n} x^i g_{ij} = 0 \qquad (j = 1, 2, \cdots, n).$$

Se indichiamo con β l'isomorfismo lineare $V \to \gamma^n$ definito da $\beta : X \to \to (x^1, x^2, \cdots, x^n)$, essendo $X = \sum_{i=1}^{n} x^i U_i$, si deduce che:

Il nucleo dell'applicazione semilineare ψ *è in corrispondenza biiettiva con* $\operatorname{Ker} \bar{\psi} \cap \beta^{-1} \varphi\beta V$.

Ricordando che il *rango* r della matrice (g_{ij}) dell'applicazione lineare $\bar{\psi}$ è eguale alla dimensione di $\bar{\psi}V$ ([2], p. 78) e che $\dim V = \dim \operatorname{Ker} \bar{\psi} + r$, possiamo concludere per il teorema precedente che

$$\dim \operatorname{rad} V = \dim \operatorname{Ker} \psi \leq \dim \operatorname{Ker} \bar{\psi} = n - r. \tag{5}$$

4. Consideriamo ora il prodotto interno così definito

$$X \cdot Y = T_{\gamma_0/\gamma} [\varphi (XY)] \tag{6}$$

il secondo membro essendo la traccia di $\varphi(XY)$ nell'estensione separabile γ_0/γ.

È facile verificare che sono soddisfatte le condizioni I), II), III) perché tale prodotto interno definisca una struttura metrica.

Nel caso che l'estensione data δ/γ sia separabile onde è $\gamma_0 = \delta$ e φ è l'identità, la struttura metrica sopra introdotta equivale a quella definita in [2] (p. 124) nello spazio vettoriale delle trasformazioni lineari ottenuto associando ad ogni fissato $X \in \delta$ l'applicazione $Z \to ZX$ per ogni $Z \in \delta$.

Se l'estensione data è separabile il discriminante risulta diverso da zero, perché allora esso coincide con il discriminante–campo dell'estensione δ/γ ([3], p. 93) e quindi in tal caso è noto che risulta $G \neq 0$.

Dimostreremo ora che:

Se l'estensione δ/γ *è inseparabile il discriminante risulta nullo.*

Infatti, ricordiamo che, se γ^* è la minima estensione normale di γ contenente γ_0, vi sono n_0 γ–isomorfismi di γ_0 in γ^*; li denoteremo con $\psi_1, \psi_2, \cdots, \psi_{n_0}$ (ψ_1 sia l'identità). La traccia di un elemento $X \in \gamma_0$ nell'estensione separabile γ_0/γ vien data da ([3], p. 94)

$$T_{\gamma_0/\gamma} (X) = \sum_{l=1}^{n_0} \psi_l X. \tag{7}$$

Per le (1) e (6) abbiamo

$$g_{ij} = T_{\gamma_0/\gamma} [\varphi (U_i U_j)]$$

e per la (7)

$$g_{ij} = \sum_{l=1}^{n_0} \psi_l \varphi (U_i U_j).$$

Il discriminante $G = \det(g_{ij})$ sarà quindi il determinante del quadrato, per righe, della matrice ad n righe ed n_0 colonne, avente per righe $\psi_1 \varphi U_i, \psi_2 \varphi U_i, \cdots, \psi_{n_0} \varphi U_i$ $(i = 1, 2, \cdots, n)$.

Essendo l'estensione δ/γ inseparabile, ma non puramente inseparabile, è $n_0 < n$ e quindi è nullo il determinante della matrice di cui sopra.

5. Se supponiamo che l'estensione δ/γ sia inseparabile ($n > n_0 \geq 2$, $G=0$) e semplice ($f = e$) i calcoli verranno agevolati dalla seguente rappresentazione degli elementi dell'estensione. Il campo δ sarà attualmente isomorfo al campo $\gamma(\theta)$ ottenuto da γ con l'aggiunzione simbolica di una indeterminata θ, soggetta ad una equazione algebrica inseparabile:

$$f(x) = x^{n_0 p^e} + a_1 x^{(n_0-1)p^e} + a_2 x^{(n_0-2)p^e} + \cdots + a_{n_0} = 0$$

a coefficienti in γ ed ivi irriducibile. Posto per abbreviare $\alpha = \theta^{p^e}$, la massima estensione separabile γ_0 di γ in δ sarà isomorfa al campo $\gamma(\alpha)$ ottenuto da γ con l'aggiunzione simbolica della indeterminata α, soggetta all'equazione separabile

$$g(y) = y^{n_0} + a_1 y^{n_0-1} + \cdots + a_{n_0} = 0$$

a radici distinte $\alpha_1, \alpha_2, \cdots, \alpha_{n_0}$.

Scegliendo come base di $V: 1, \theta, \theta^2, \cdots, \theta^{n-1}$ sarà

$$\varphi U_i = \alpha^{i-1} \qquad (i = 1, 2, \cdots, n).$$

Pertanto si ha che

$$g_{ij} = T_{\gamma_0/\gamma}(\alpha^{i+j-2}) = S_{i+j-2} \qquad (i, j = 1, 2, \cdots, n)$$

avendo posto $S_m = \alpha_1^m + \alpha_2^m + \cdots + \alpha_{n_0}^m$.

La matrice discriminante (g_{ij}) sarà allora il quadrato, per righe, della matrice avente per colonne

$$1, \alpha_i, \alpha_i^2, \cdots, \alpha_i^{n-1} \qquad (i = 1, 2, \cdots, n_0).$$

Il rango di (g_{ij}) è pertanto n_0 e per la (5) abbiamo

$$\dim \operatorname{rad} V \leq n - n_0.$$

6. Supporremo ora che l'estensione δ/γ sia separabile e quindi semplice e che sia ottenuta mediante l'aggiunzione di una delle radici dell'equazione irriducibile

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0 \qquad (a_i \in \gamma) \tag{8}$$

che supporremo normale in γ. Ricordiamo che il *gruppo di Galois di δ rispetto a γ* è il gruppo Γ degli automorfismi di δ che lasciano fissi i singoli elementi di γ. Tale gruppo risulta di ordine n ed induce tra le n radici della (8) un gruppo transitivo di sostituzioni a quello isomorfo. Ricordiamo anche ([1], p. 119) che un automorfismo lineare σ in V viene denominato una *isometria*, rispetto ad una assegnata struttura metrica, se, qualunque siano $X, Y \in V$, risulta

$$\sigma X \cdot \sigma Y = X \cdot Y .$$

Dimostreremo che:

Ogni automorfismo del gruppo Γ *di Galois di* δ *rispetto a* γ *risulta una isometria rispetto alla struttura metrica* (6).

Poniamo infatti $Z = XY$. Per la (6) risulta

$$X \cdot Y = T_{\delta/\gamma}(Z)$$
$$\sigma X \cdot \sigma Y = T_{\delta/\gamma}(\sigma Z).$$

Ricordando che la traccia di un elemento di δ in una estensione δ/γ è la somma dei suoi coniugati rispetto a γ, i secondi membri delle due eguaglianze di sopra risultano eguali, perché due elementi sono coniugati se e solo se possono essere portati l'uno nell'altro da una sostituzione del gruppo di Galois.

Poiché in una isometria è $\det(g_{ij}) = \det(\bar{g}_{ij})$, dalla (2) si ha, essendo $G \neq 0$,

$$\det \sigma = \det (a_j^i) = \pm 1 .$$

Quando $\det \sigma = 1$ l'isometria chiamasi una *rotazione* e quando $\det \sigma = -1$ essa chiamasi una *riflessione*.

Nel caso in cui δ sia finito, il gruppo di Galois risulta ciclico ([4], p. 21). In tal caso dimostreremo che:

Le isometrie del gruppo di Galois di ordine n su di un campo finito sono tutte rotazioni se n è dispari, e sono per metà rotazioni e per metà riflessioni se n è pari.

Consideriamo infatti un arbitrario e non banale determinante–funzione ([2], p. 98) $\Delta(X_1, X_2, \cdots, X_n)$, essendo X_i le radici della (8), e ricordiamo che se σ è una qualsiasi trasformazione lineare risulta

$$\Delta(\sigma X_1, \sigma X_2, \cdots, \sigma X_n) = \det \sigma \, \Delta(X_1, X_2, \cdots, X_n).$$

Se σ è un automorfismo del gruppo ciclico di Galois, esso opera una sostituzione circolare sulle X_i. Quindi, per delle note proprietà dei determinanti–funzioni, se n è dispari, sarà $\det \sigma = 1$, poiché le n sostituzioni del gruppo Γ sono tutte pari, e, se n è pari, sarà $\det \sigma = 1$ in corrispondenza alle $n/2$ sostituzioni pari e $\det \sigma = -1$ in corrispondenza alle $n/2$ sostituzioni dispari.

BIBLIOGRAFIA

[1] E. ARTIN, *Algebra geometrica*, Feltrinelli, Milano (1968).
[2] W. H. GREUB, *Linear Algebra*, Springer–Verlag, Berlin (1967).
[3] O. ZARISKI e P. SAMUEL, *Commutative Algebra*, vol. I, New–Jersey (1958).
[4] B. SEGRE, *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane*, « Annali di Mat. », IV, *64*, 1–76 (1964).