Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Giampaolo Menichetti

Sopra una classe di quasicorpi distributivi di ordine finito

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **59** (1975), n.5, p. 339–348.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1975_8_59_5_339_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1975.

Algebra. — *Sopra una classe di quasicorpi distributivi di ordine finito* (*). Nota di GIAMPAOLO MENICHETTI, presentata (**) dal Corrisp. G. ZAPPA.

SUMMARY. — This paper contains the following results on semifields of order q^{m^2}, $q = p^h$, $m \geq 2$: *a*) it is found a class of semifields which generalizes that of R. Sandler [2]; *b*) it is showed a process which is used for deriving, from any semifield belonging to the class in *a*), a different semifield with the same order.

1. Prefissati un campo di Galois $K = GF(q) = GF(p^h)$ ed un intero $m \geq 2$, siano $K_m = GF(q^m)$ il campo di rango m su K e τ l'automorfismo, di K_m, che porta x in $x\tau = x^q$.

Z_m indica l'anello degli interi modulo m in cui è fissato l'ordinamento $0, 1, 2, \cdots, m-1$. Nel seguito si considerano (m, m)–matrici ad elementi in K_m, le cui righe e colonne si suppongono ordinatamente contrassegnate mediante indici appartenenti a Z_m.

Qualunque siano $i \in Z_m$ e $k \in K_m$, è definita la (m, m)–matrice diagonale

$$D_i(k) = (d_{rs}), \quad d_{rs} = \begin{cases} 0, & s \neq r \\ 1, & s = r \neq i, \\ k, & s = r = i \end{cases}$$

di cui rileviamo le seguenti ovvie proprietà:

$$D_i(k_1) D_i(k_2) = D_i(k_1 k_2), \quad D_i(1) = I_m, \tag{1}$$

essendo I_m la matrice unitaria di ordine m.

In funzione delle $D_i(k)$ si definiscono la matrice scalare

$$S(k) = \prod_0^{m-1} {}_i D_i(k) \tag{2}$$

e la matrice diagonale

$$D(k) = \prod_0^{m-1} {}_i D_i(k \tau^i) \qquad (\tau^0 = Id_{K_m}). \tag{3}$$

(*) Lavoro eseguito nell'ambito dell'attività del «Gruppo nazionale per le strutture algebriche e geometriche e loro applicazioni» del C.N.R. (Sezione n. 4).

(**) Nella seduta del 15 novembre 1975.

Posto

$$T = \begin{bmatrix} 0 & 0 \cdots 0 & 1 \\ 1 & 0 \cdots 0 & 0 \\ 0 & 1 \cdots 0 & 0 \\ \cdots & \cdots & \cdots \\ 0 & 0 \cdots 1 & 0 \end{bmatrix}$$

ovvero, con evidente simbolismo,

$$T = \begin{bmatrix} 0 & I_1 \\ I_{m-1} & 0 \end{bmatrix},$$

si dimostra facilmente che

$$(4) \qquad T^j = \begin{bmatrix} 0 & I_j \\ I_{m-j} & 0 \end{bmatrix}, j \in Z'_m = Z_m - \{0\} \qquad (T^m = T^0 = I_m).$$

È immediata anche la dimostrazione delle seguenti identità

$$(5) \qquad D_i(k)\, T = T D_{i-1}(k), \qquad i \in Z_m.$$

Da (5) segue

$$(6) \qquad D(k)\, T = T D(k\tau).$$

Infatti (cfr. (3))

$$D(k)\, T = \prod_0^{m-1 i} D_i(k\tau^i)\, T = D_0(k)\, D_1(k\tau) \cdots D_{m-2}(k\tau^{m-2})\, T D_{m-2}(k\tau^{m-1}) = \cdots =$$

$$= T D_{m-1}(k)\, D_0(k\tau) \cdots D_{m-3}(k\tau^{m-2})\, D_{m-2}(k\tau^{m-1}) =$$

$$= T D_0(k\tau)\, D_1((k\tau)\,\tau) \cdots D_{m-2}((k\tau)\,\tau^{m-2})\, D_{m-1}((k\tau)\,\tau^{m-1}).$$

Per induzione su j si prova che

$$(7) \qquad [T \prod_0^{m-1 i} D_i(k_i)]^j = T^j \prod_0^{m-1 i} D_i(k_i\, k_{i+1} \cdots k_{i+j-1}), \qquad i \in Z_m, j \in Z'_m$$

qualunque siano $k_i \in K_m$.

Infatti la (7) vale chiaramente per $j = 1$; inoltre, supponendo che sia vera per l'esponente $j - 1$, si trova (cfr. anche (5))

$$[T \prod_0^{m-1 i} D_i(k_i)]^{j-1}\, T \prod_0^{m-1 i} D_i(k_i) = T^{j-1} \prod_0^{m-1 i} D_i(k_i\, k_{i+1} \cdots k_{i+j-2})\, T \prod_0^{m-1 i} D_i(k_i) =$$

$$= T^j \prod_0^{m-1 i} D_{i-1}(k_i\, k_{i+1} \cdots k_{i+j-2}) \prod_0^{m-1 i} D_i(k_i)$$

da cui, tenendo conto di (1), segue la tesi.

Prefissati $k_i \in K'_m = K_m - \{0\}$, $i = 0, 1, \cdots, m-1$, si definiscono le matrici

$$F_j = [T \prod_0^{m-1}{}_i D_i(k_i)]^j S^{-1}(\prod_0^{j-1}{}_r k_r), \qquad j = 1, 2, \cdots, m-1, \tag{8}$$

le quali, essendo

$$S^{-1}(\prod_0^{j-1}{}_r k_r) = S(\prod_0^{j-1}{}_r k_r^{-1}) = \prod_0^{m-1}{}_i D_i(\prod_0^{j-1}{}_r k_r^{-1})$$

(cfr. (2)), si possono esprimere nella forma (cfr. (1) e (7))

$$F_j = T^j \prod_0^{m-1}{}_i D_i(k_i k_{i+1} \cdots k_{i+j-1}) D_i(k_0^{-1} k_1^{-1} \cdots k_{j-1}^{-1}) =$$

$$= T^j D_0(1) \prod_1^{m-1}{}_i (k_0^{-1} k_1^{-1} \cdots k_{j-1}^{-1} k_i k_{i+1} \cdots k_{i+j-1})$$

ovvero, posto

$$c_{ij} = k_0^{-1} k_1^{-1} \cdots k_{j-1}^{-1} k_i k_{i+1} \cdots k_{i+j-1}, \qquad i, j \in Z'_m, \tag{9}$$

nella seguente

$$F_j = T^j \prod_1^{m-1}{}_i D_i(c_{ji}), \qquad j = 1, 2, \cdots, m-1. \tag{10}$$

In funzione delle m variabili $x_i \in K_m$, $i = 0, 1, \cdots, m-1$, si definisce infine la matrice

$$F(x_0, x_1, \cdots, x_{m-1}) = D(x_0) + \sum_1^{m-1}{}_j F_j D(x_j) \tag{11}$$

la quale evidentemente dipende tramite le F_j, anche dai parametri k_i.

PROPOSIZIONE 1. *Qualunque siano* $x_i \in K_m$, *è* $\det F(x_0, x_1, \cdots, x_{m-1}) = \det F(x_0 \tau, x_1 \tau, \cdots, x_{m-1} \tau)$.

Dimostrazione. Posto $T \prod_0^{m-1}{}_i D_i(k_i) = \overline{F}$ ed osservando che le matrici scalari S commutano nel prodotto con qualunque matrice, si trova (cfr. anche (8)).

$$(*) \quad F_1^{-1} F_j F_1 = S(k_0) \overline{F}^{-1} \overline{F}^j S^{-1}(\prod_0^{j-1}{}_r k_r) \overline{F} S^{-1}(k_0) = \overline{F}^j S^{-1}(\prod_0^{j-1}{}_r k_r) = F_j.$$

In virtù della (6) e della commutatività del prodotto di matrici diagonali (cfr. ancora (8))

$$(**) \quad F_1^{-1} D(x_i) F_1 = S(k_0) [\prod_0^{m-1}{}_i D_i(k_i)]^{-1} T^{-1} D(x_i) T \prod_0^{m-1}{}_i D_i(k_i) S^{-1}(k_0) =$$

$$= S(k_0) [\prod_0^{m-1}{}_i D_i(k_i)]^{-1} D(x_i \tau) \prod_0^{m-1}{}_i D_i(k_i) S^{-1}(k_0) = D(x_i \tau).$$

Da (*) e (**) segue

$$F_1^{-1} F(x_0, x_1, \cdots, x_{m-1}) F_1 = F_1^{-1} D(x_0) F_1 +$$
$$+ \sum_1^{m-1}{}_j F_1^{-1} F_j F_1 F_1^{-1} D(x_j) F_1 = D(x_0 \tau) +$$
$$+ \sum_1^{m-1}{}_j F_j D(x_j \tau) = F(x_0 \tau, x_1 \tau, \cdots, x_{m-1} \tau)$$

e, quindi, la tesi.

Tenendo conto di (4) e (10), si trova

$$F_j = \begin{bmatrix} 0 & F'_j \\ F'_{m-j} & 0 \end{bmatrix}, \qquad j \in Z'_m,$$

dove con zero sono indicati due blocchi di elementi tutti nulli e

$$F'_{m-j} = \begin{bmatrix} x_j & 0 & \cdots & 0 \\ 0 & c_{j1}(x_j \tau) & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & c_{j,m-j-1}(x_j \tau^{m-j-1}) \end{bmatrix}$$

$$F'_j = \begin{bmatrix} c_{j,m-j}(x_j \tau^{m-j}) & 0 & \cdots & 0 \\ 0 & c_{j,m-j+1}(x_j \tau^{m-j+1}) & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & c_{j,m-1}(x_j \tau^{m-1}) \end{bmatrix}.$$

Di qui si determina l'espressione esplicita della matrice (11)

$$(11)' \qquad F = \begin{bmatrix} x_0 & c_{m-1,1}(x_{m-1} \tau) & \cdots & c_{1,m-1}(x_1 \tau^{m-1}) \\ x_1 & x_0 \tau & \cdots & c_{2,m-1}(x_2 \tau^{m-1}) \\ x_2 & c_{1,1}(x_1 \tau) & \cdots & c_{3,m-1}(x_3 \tau^{m-1}) \\ \cdots & \cdots & \cdots & \cdots \\ x_{m-2} & c_{m-3,1}(x_{m-3} \tau) & \cdots & c_{m-1,m-1}(x_{m-1} \tau^{m-1}) \\ x_{m-1} & c_{m-2,1}(x_{m-2} \tau) & \cdots & x_0 \tau^{m-1} \end{bmatrix}.$$

Lo sviluppo del det F è pertanto (cfr. anche (9)) la somma di termini della forma

$$k_0^{n_0} k_1^{n_1} \cdots k_{m-1}^{n_{m-1}} x_0^{\sigma_0} x_1^{\sigma_1} \cdots x_{m-1}^{\sigma_{m-1}}$$

dove n_i sono degli interi e σ_i o è zero oppure indica una somma $q^{r_1} + q^{r_2} + \cdots + q^{r_s}$ di potenze (distinte) di q ad esponente r_j in Z_m.

In virtù della Proposizione 1 lo sviluppo di det F torna in sè mutando x_i in $x_i\tau$, $i = 0, 1, \cdots, m-1$ (e quindi, in generale, mutando x_i in $x_i\tau^j$, $j \in Z_m$), onde se

$$k_0^{n_0} k_1^{n_1} \cdots k_{m-1}^{n_{m-1}} x_0^{\sigma_0} x_1^{\sigma_1} \cdots x_{m-1}^{\sigma_{m-1}} = k_0^{n_0} k_1^{n_1} \cdots k_{m-1}^{n_{m-1}} x$$

è un elemento di tale sviluppo, allora lo sono anche

$$k_0^{n} k_1^{n} \cdots k_{m-1}^{n} (x\tau^j), \qquad j \in Z_m.$$

Poiché, qualunque sia $x \in K_m$, la somma degli elementi distinti dell'insieme $\{x, x\tau, \cdots, x\tau^{m-1}\}$ appartiene a K, dalle osservazioni precedenti segue il

COROLLARIO 1. *Qualunque siano* $k_i \in K_m' = K_m - \{0\}$, $i = 0, 1, \cdots, m-1$, *lo sviluppo di* det F $(x_0, x_1, \cdots, x_{m-1})$ *è la somma di elementi della forma*

$$k_0^{n_0} k_1^{n_1} \cdots k_{m-1}^{n_{m-1}} f_{n_0 n_1, \cdots, n_{m-1}} (x_0, x_1, \cdots, x_{m-1})$$

dove n_i *sono degli interi ed* $f_{n_0 n_1, \cdots, n_{m-1}}$ *è una funzione polinomiale a valori in* K.

Una matrice $F(x_0, x_1, \cdots, x_{m-1})$ si dirà *non singolare* se det F $=$ $= 0 \Longleftrightarrow x_0 = x_1 = \cdots = x_{m-1} = 0$. Nel § successivo dimostreremo che ad ogni matrice F che soddisfa tale condizione, è associato un quasicorpo distributivo; per questa ragione andremo ora ad esaminare due casi in cui appunto F è non singolare.

Se fissiamo $k_0 = 1$, $k_1 = k_2 = \cdots = k_{m-2} = k$, $k_{m-1} = kk'$ $(k, k' \in K_m' =$ $= K_m - \{0\})$, allora (cfr. (9))

$$c_{ji} = \begin{cases} k & , i + j < m \\ kk' & , i + j = m \\ k' & , i + j > m \end{cases} \tag{12}$$

e quindi (cfr. (11)')

$$F = \begin{bmatrix} x_0 & kk'(x_{m-1}\tau) & kk'(x_{m-2}\tau^2) & \cdots & kk'(x_1\tau^{m-1}) \\ x_1 & x_0\tau & k'(x_{m-1}\tau^2) & \cdots & k'(x_2\tau^{m-1}) \\ x_2 & k(x_1\tau) & x_0\tau^2 & \cdots & k'(x_3\tau^{m-1}) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x_{m-1} & k(x_{m-2}\tau) & k(x_{m-3}\tau^2) & \cdots & x_0\tau^{m-1} \end{bmatrix}. \tag{13}$$

Supposto $k = \varepsilon_1 + \varepsilon_2 k'$, $\varepsilon_1, \varepsilon_2 \in K$, si trova che il determinante di (13) è un polinomio del tipo

$$\text{(')} \qquad \det F = f_0(x_0, \cdots, x_{m-1}) + kk' f_1(x_0, \cdots, x_{m-1}) + \\ + \cdots + kk'^{m-1} f_{m-1}(x_0, \cdots, x_{m-1}),$$

dove, qualunque siano $x_i \in K_m$, è $f_j(x_0, \cdots, x_{m-1}) \in K$, $j = 0, 1, \cdots, m-1$ (cfr. Corollario 1).

Sviluppando infatti i determinanti per gli elementi della prima riga,

$$\det F = x_0 \det \begin{bmatrix} x_0\tau & kk'(x_{m-1}\tau^2) & \cdots & kk'(x_2\tau^{m-1}) \\ x_1\tau & x_0\tau^2 & \cdots & k'(x_3\tau^{m-1}) \\ \cdots & \cdots & \cdots & \cdots \\ x_{m-2}\tau & k(x_{m-3}\tau^2) & \cdots & x_0\tau^{m-1} \end{bmatrix} +$$

$$+ kk' [\text{polinomio in } k' \text{ di grado} \leq m-2] =$$

$$= x_0(x_0\tau) \det \begin{bmatrix} x_0\tau^2 & \cdots & k'(x_3\tau^{m-1}) \\ \cdots & \cdots & \cdots \\ k(x_{m-3}\tau^2) & \cdots & x_0\tau^{m-1} \end{bmatrix} + kk'[\cdots] = \cdots =$$

$$= x_0^{1+q+\cdots+q^{m-1}} + kk' f_1(x_0, \cdots, x_{m-1}) + \cdots + kk'^{m-1} f_{m-1}(x_0, \cdots, x_{m-1}).$$

Di qui, in particolare, $f_0(x_0, \cdots, x_{m-1}) = x_0^{1+q+\cdots+q^{m-1}}$.
Qualunque sia i, inoltre

$$('') \qquad f_1(0, \cdots, 0, x_i, x_{i+1}, \cdots, x_{m-1}) = (-1)^{(i+2)(m-i)} \varepsilon_1^{m-i-1} x_i^{\sum_r^{m-1} q^r}.$$

In effetti si trova che

$$\det F(0, \cdots, 0, x_i, x_{i+1}, \cdots, x_{m-1}) =$$

$$= kk'^i \{(-1)^{(m-i)(i+2)} \varepsilon_1^{m-i-1} x_i^{\sum_r^{m-1} q^r} + k'[\cdots]\}^{(1)}.$$

Supponendo k e k' fissati in modo che $1, kk', kk'^2, \cdots, kk'^{1-m}$ siano linearmente indipendenti rispetto a K ed $\varepsilon_1 \neq 0$, in virtù di (') e ('') è $\det F = 0 \Longleftrightarrow f_0 = f_1 = \cdots = f_{m-1} = 0 \Longleftrightarrow x_0 = x_1 = \cdots = x_{m-1} = 0$.

Riassumendo:

La matrice $F(x_0, x_1, \cdots, x_{m-1})$ *è non singolare quando* $k_0 = 1$, $k_1 = k_2 = \cdots = k_{m-2} = k$, $k_{m-1} = kk'$ *ed inoltre* $k' \in K_m$ *e* $k = \varepsilon_1 + \varepsilon_2 k'$, $\varepsilon_1, \varepsilon_2 \in K$, $\varepsilon_1 \neq 0$, *sono fissati in modo che* $1, kk', kk'^2, \cdots, kk'^{m-1}$ *risultino linearmente indipendenti rispetto a* K.

Per completezza vediamo come sia possibile trovare delle coppie k, k' che soddisfano le condizioni suddette.

Si fissa k' in modo che $1, k', \cdots, k'^{m-1}$ siano una base di K_m (per esempio scegliendo un elemento primitivo di K_m). Gli elementi $1, kk' = \varepsilon_1 k' +$

(1) Conviene sviluppare il determinante per gli elementi della $(i+1)$-sima riga.

$+ \varepsilon_2 k'^2, \cdots, kk'^{m-2} = \varepsilon_1 k'^{m-2} + \varepsilon_2 k'^{m-1}, kk'^{m-1} = \varepsilon_2 \lambda_0 + \varepsilon_2 \lambda_1 k' + \cdots + (\varepsilon_1 + \varepsilon_2 \lambda_{m-1}) k'^{m-1}$ (dove i $\lambda_i \in K$ sono determinati dalla condizione $k'^m = \sum_0^{m-1}{}_i \lambda_i k'^i$) risultano indipendenti rispetto a K se e solo se

$$\det \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \varepsilon_1 & \varepsilon_2 & \cdots & 0 & 0 \\ 0 & 0 & \varepsilon_1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \varepsilon_1 & \varepsilon_2 \\ \varepsilon_2 \lambda_0 & \varepsilon_2 \lambda_1 & \varepsilon_2 \lambda_2 & \cdots & \varepsilon_2 \lambda_{m-2} & \varepsilon_1 + \lambda_{m-1} \varepsilon_2 \end{bmatrix} \neq 0.$$

A conti fatti si trova che, fissato k' come si è detto, basta scegliere $\varepsilon_1 \neq 0$, ε_2 in modo che

$$\varepsilon_1^{m-1} + \sum_1^{m-1}{}_i (-1)^{i+1} \lambda_{m-i} \varepsilon_1^{m-i-1} \varepsilon_2^i \neq 0.$$

Si può dimostrare che

Per $k_0 = 1$, $k_1 = k_2 = \cdots = k_{m-2} = k$, $k_{m-1} = kk'$, *essendo* $k \in K_m$, $k' = \varepsilon_1 + \varepsilon_2 k$, $\varepsilon_1, \varepsilon_2 \in K$, $\varepsilon_1 \neq 0$, *elementi fissati in modo che* $1, k'k, k'k^2, \cdots, k' k^{m-1}$ *siano linearmente indipendenti rispetto a* K, *la matrice* $F(x_0, x_1, \cdots, x_{m-1})$ *è non singolare.*

Per verificarlo si segue un procedimento del tutto simile a quello del caso precedente. Basta infatti osservare che ora il determinante di $F(x_0, x_1, \cdots, x_{m-1})$ è un polinomio del tipo

$$\det F = f_0(x_0, \cdots, x_{m-1}) + k' \sum_1^{m-1}{}_j k^j f_j(x_0, \cdots, x_{m-1}), f_j \in K, \forall x_i \in K_m,$$

e che

$$f_0(x_0, \cdots, x_{m-1}) = x_0^{\sum_r^{m-1} q^r} q^r, f_j(0, x_1, \cdots, x_{m-j}, 0, \cdots, 0) =$$

$$= (-1)^{(j+2)(m-j)} \varepsilon_1^{m-j-1} x_{m-j}^{\sum_r^{m-1} q^r}, \qquad j = 1, 2, \cdots, m-1.$$

2. Sia $V = V(m, q^m)$ lo spazio vettoriale di dimensione m su K_m. Si osservi che scelta una base $\{u_0, u_1, \cdots, u_{m-1}\}$ di V e posto $u = (u_0 u_1 \cdots u_{m-1})$, qualunque elemento $\sum_0^{m-1}{}_i a_i u_i \in V$ si può scrivere nella forma ua, essendo $a = {}^t(a_0 a_1 \cdots a_{m-1})$.

Fissati $k_i \in K_m'$, $i = 0, 1, \cdots, m-1$, in modo che la matrice $F(x_0, x_1, \cdots, x_{m-1})$ risulti non singolare, si definisce in V una moltiplicazione, « $\circ$ », ponendo

$$ua \circ ua' = uF(a)\, a', \quad \forall ua, ua' \in V,$$

dove $F(a) = F(a_0, a_1, \cdots, a_{m-1})$.

PROPOSIZIONE 2. *La struttura algebrica* $(V^+, \circ)$ *è un quasicorpo distributivo (semifield),* $Q(k_0, k_1, \cdots, k_{m-1})$, *di ordine* q^{m^2}

Dimostrazione. È evidente che (cfr. (11)')

i) $|\{F(a) : ua \in V\}| = q^{m^2}$,

ii) $F(0, 0, \cdots, 0) = O_m$, $F(1, 0, \cdots, 0) = I_m$,

iii) $F(a) + F(a') = F(a + a')$.

Inoltre, essendo F non singolare

iv) se $a \neq a'$ allora $\det(F(a) - F(a')) = \det F(a - a') \neq 0$.

La tesi è quindi dimostrata (cfr. [1], p. 220).

È facile verificare che il prodotto « O » in V^+ può essere definito anche dalle seguenti condizioni:

j) « O » è distributivo rispetto all'addizione;

jj) $(a_1 u_i) \circ (a_2 u_j) = (a_1 \tau^j)\, a_2 (u_i \circ u_j)$, $\forall a_1, a_2 \in K_m$;

jjj) $u_i \circ u_0 = u_0 \circ u_i = u_i$, $\forall i \in Z_m$; $u_i \circ u_j = c_{ij}\, u_{i+j}$, $\forall i, j \in Z_m' = Z_m - \{0\}$.

Tenuto conto di quanto è dimostrato nell'ultima parte del §1, possiamo affermare che

$Q(1, k, \cdots, k, kk')$ *è un quasicorpo distributivo in ciascuno dei seguenti casi*

a) $k' \in K_m$, $k = \varepsilon_1 + \varepsilon_2 k'$, $\varepsilon_1, \varepsilon_2 \in K$, $\varepsilon_1 \neq 0$ *e* $1, kk', kk'^2, \cdots, kk'^{m-1}$ *lin. ind. rispetto a* K;

b) $k \in K_m$, $k' = \varepsilon_1 + \varepsilon_2 k$, $\varepsilon_1, \varepsilon_2 \in K$, $\varepsilon_1 \neq 0$ *e* $1, k'k, k'k^2, \cdots, k'k^{m-1}$ *lin. ind. rispetto a* K.

La condizione jjj) diviene allora (cfr. 12))

$$u_i \circ u_0 = u_0 \circ u_i = u_i \quad , \quad u_i \circ u_j = \begin{cases} ku_{i+j} & , i + j < m \\ kk'u_0 & , i + j = m, i, j \neq 0 \\ k'u_{i+j-m} & , i + j > m. \end{cases}$$

Si osservi che la condizione *a)* è soddisfatta in particolare se $k' \in K_m$, $\varepsilon_1 = 1$, $\varepsilon_2 = 0$ $(k = 1)$ e $1, k', k'^2, \cdots, k'^{m-1}$ sono lin. ind. rispetto a K.

I corrispondenti quasicorpi $Q(1, \cdots, 1, k')$ coincidono con quelli determinati da Sandler in [2] in quanto in tal caso

$$u_i \circ u_j = \begin{cases} u_{i+j} & , i+j < m \\ k' u_{i+j-m} & , i+j \geq m . \end{cases}$$

3. In questo § si definisce un procedimento, formalmente analogo a quello dato da Knuth in [3], il quale consente di derivare da un quasicorpo $Q(k_0, k_1, \cdots, k_{m-1})$ un altro quasicorpo distributivo dello stesso ordine.

Sia $F(x_0, x_1, \cdots, x_{m-1})$ una matrice non singolare, data esplicitamente da (11)'. Poichè le righe di F sono linearmente indipendenti rispetto a K_m, il sistema lineare

$$\mu_0 x_0 + \mu_1 x_1 + \cdots + \mu_{m-1} x_{m-1} = 0$$
$$\mu_0 c_{m-1,1}(x_{m-1}\tau) + \mu_1 x_0 \tau + \cdots + \mu_{m-1} c_{m-2,1}(x_{m-2}\tau) = 0$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\mu_0 c_{1,m-1}(x_1 \tau^{m-1}) + \mu_1 c_{2,m-1}(x_2 \tau^{m-1}) + \cdots + \mu_{m-1} x_0 \tau^{m-1} = 0$$

nelle variabili μ_i ha solo la soluzione banale, qualunque siano $x_i \in K_m$ non non tutti nulli. In altri termini le equazioni precedenti sono incompatibili qualunque siano le m-ple $x_0, x_1, \cdots, x_{m-1}$ e $\mu_0, \mu_1, \cdots, \mu_{m-1}$ distinte dalla m-pla di elementi tutti nulli. Tale circostanza sussiste evidentemente per il sistema equivalente

$$\mu_0 x_0 + \mu_1 x_1 + \cdots + \mu_{m-1} x_{m-1} = 0$$
$$((\mu_0 c_{m-1,1})\tau^{m-1}) x_{m-1} + (\mu_1 \tau^{m-1}) x_0 + \cdots + ((\mu_{m-1} c_{m-2,1})\tau^{m-1}) x_{m-2} = 0$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$((\mu_0 c_{1,m-1})\tau) x_1 + ((\mu_1 c_{2,m-1})\tau) x_2 + \cdots + (\mu_{m-1}\tau) x_0 = 0$$

ottenuto elevando primo e secondo membro di ciascuna delle equazioni precedenti ordinatamente alla potenza $q^0, q^{m-1}, \cdots, q$.

Riguardando l'ultimo come un sistema lineare nelle variabili x_i, da quanto precede si deduce che esso, per $\mu_0, \mu_1, \cdots, \mu_{m-1}$ non tutti nulli, ha solamente la soluzione banale: onde la matrice dei coefficienti

$$(14) \qquad \begin{bmatrix} \mu_0 & \mu_1 & \cdots & \mu_{m-1} \\ \mu_1 \tau^{m-1} & (c_{11}\mu_2)\tau^{m-1} & \cdots & (c_{m-1,1}\mu_0)\tau^{m-1} \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots \\ \mu_{m-1}\tau & (\mu_0 c_{1,m-1})\tau & \cdots & (c_{m-1,m-1}\mu_{m-2})\tau \end{bmatrix}$$

ha determinante nullo solo per $\mu_0 = \mu_1 = \cdots = \mu_{m-1} = 0$. La (14) è pertanto

non singolare e tale è quindi

$$\overline{F}' = \begin{bmatrix} \mu_0 & \mu_{m-1}\,\tau & \mu_{m-2}\,\tau^2 & \cdots & \mu_1\,\tau^{m-1} \\ \mu_1 & c^{q}_{1,m-1}(\mu_0\,\tau) & c^{q^2}_{1,m-2}(\mu_{m-1}\,\tau^2) & \cdots & c^{q^{m-1}}_{11}(\mu_2\,\tau^{m-1}) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \mu_{m-1} & c^{q}_{m-1,m-1}(\mu_{m-2}\,\tau) & c^{q^2}_{m-1,m-2}(\mu_{m-3}\,\tau^2) & \cdots & c^{q^{m-1}}_{m-1,1}(\mu_0\,\tau^{m-1}) \end{bmatrix}$$

ottenuta trasponendo la (14) dopo aver eseguito una evidente permutazione sulle righe.

Se, come avviene in generale, non esiste una m-pla di elementi μ_i in corrispondenza dei quali la $\overline{F}'$ coincida con I_m, si fissino in K_m m elementi μ'_0, $\mu'_1, \cdots, \mu'_{m-1}$ non tutti nulli e si consideri la matrice

$$F'(\mu_0, \mu_1, \cdots, \mu_{m-1}) = \overline{F}'^{-1}(\mu'_0, \mu'_1, \cdots, \mu'_{m-1})\,\overline{F}'(\mu_0, \cdots, \mu_{m-1}).$$

È facile dimostrare che la $F'(\mu_0, \mu_1, \cdots, \mu_{m-1})$ soddisfa le condizioni i), ii), iii) e iv) del § 2 e quindi, come la F, consente di definire un quasicorpo distributivo di ordine q^{m^2}.

Bibliografia

[1] Dembowski (1968) – *Finite geometries*, « Ergebn. der Mathem. und ihrer Grenzg », Band *44*, Springer.

[2] R. Sandler (1961) – *Autotopism groups of some finite non-associative algebras*, « Amer. J. Math. », *84*, 239–264.

[3] D. E. Knuth (1965) – *Finite semifields and projective planes*, « J. Algebra », *2*, 182–217.