

---

# BOLLETTINO UNIONE MATEMATICA ITALIANA

---

ALESSANDRO BASILE, PAOLO BRUTTI

## Alcune condizioni per la costruzione di un piano finito di traslazione

*Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. 4-B (2001),  
n.2, p. 429–439.*

Unione Matematica Italiana

[<http://www.bdim.eu/item?id=BUMI\\_2001\\_8\\_4B\\_2\\_429\\_0>](http://www.bdim.eu/item?id=BUMI_2001_8_4B_2_429_0)

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

---

*Articolo digitalizzato nel quadro del programma  
bdim (Biblioteca Digitale Italiana di Matematica)  
SIMAI & UMI*

<http://www.bdim.eu/>



## Alcune condizioni per la costruzione di un piano finito di traslazione (\*)

ALESSANDRO BASILE - PAOLO BRUTTI

**Summary.** – *The construction of any finite translation plane depends on the appropriate determination of a partition  $P(E)$  of a Galois field  $E$ , together with a set  $A$  of automorphisms of  $E$  as a vector space. In this paper we obtain sufficient conditions on  $P(E)$  and  $A$ , so that a translation plane is produced. They are also necessary conditions when  $|A| = 1$ . Particularly, we examine the case where  $E$  is a two-dimensional vector space. We prove that no translation planes are constructible by a single automorphism, other than the André planes. Furthermore, if  $|A| > 1$ , the conditions previously obtained cannot be satisfied.*

1. È noto che se  $E$  è un insieme finito di  $n$  elementi, l'esistenza di un insieme  $G$  di permutazioni su  $E$  strettamente 2-transitivo (scriveremo brevemente S2T) equivale all'esistenza di un piano affine di ordine  $n$  (cfr. [3], [5]). Indicheremo un tale piano con  $\pi(E, G)$ .

Nel seguito  $E$  sarà un campo finito e denoteremo sempre con  $G$  il gruppo delle permutazioni su  $E: x \rightarrow ax + b$ , con  $a \in E^*$  e  $b \in E$ . Il gruppo  $G$  è S2T su  $E$  e il piano  $\pi(E, G)$  è desarguesiano. È noto, ed è esplicitamente osservato in [1], che se sono dati una partizione  $P(G) = \{G_0, G_1, \dots, G_{n-1}\}$  di  $G$  come insieme, con  $\text{id}_E \in G_0$ , e degli automorfismi lineari  $\tau_1, \dots, \tau_{n-1}$  di  $E$  come spazio vettoriale su un suo sottocampo, in modo che l'insieme di permutazioni  $G' = G_0 \cup G_1 \tau_1 \cup \dots \cup G_{n-1} \tau_{n-1}$  sia a sua volta S2T su  $E$ , allora il piano  $\pi(E, G')$  è un piano di traslazione. Viceversa è anche noto che ogni piano di traslazione finito può essere rappresentato in tal modo (cfr. [2]).

Se  $P$  e  $P'$  sono due partizioni di uno stesso insieme, si dice che  $P$  è un «raffinamento» di  $P'$  se ogni elemento di  $P$  è contenuto in un elemento di  $P'$ . Si può ottenere una particolare partizione di  $G$ , che denoteremo con  $G/_\parallel$ , ponendo in ciascuna classe tutte e sole le permutazioni  $x \rightarrow ax + b$  con lo stesso elemento  $a$  di  $E^*$ . Data una partizione  $P(E^*) = \{E_0, E_1, \dots, E_{n-1}\}$  di  $E^*$  e definito

$$G_r = \{x \rightarrow ax + b \mid a \in E_r, b \in E\}$$

(\*) Lavoro eseguito nell'ambito del GNSAGA del CNR.

per ogni  $r = 0, 1, \dots, n-1$ , si ottiene una partizione  $P(G)$  di  $G$  di cui  $G/\parallel$  è un raffinamento. Chiameremo  $P(G)$  la partizione «associata» a  $P(E^*)$ . Viceversa, data una partizione  $P(G) = \{G_0, G_1, \dots, G_{n-1}\}$  di  $G$  tale che  $G/\parallel$  sia un suo raffinamento, denotando con  $E_r$ , per ogni  $r = 0, 1, \dots, n-1$ , l'insieme degli elementi  $a \in E^*$  tali che la permutazione  $x \rightarrow ax$  appartenga a  $G_r$ , si ottiene una partizione  $P(E^*)$  di  $E^*$  la cui partizione associata è  $P(G)$ . Allo stesso modo diremo che  $P(E^*)$  è associata a  $P(G)$ . Si osservi che se la partizione  $P(G)$  e gli automorfismi lineari  $\tau_1, \dots, \tau_{n-1}$  sono dati in modo che l'insieme  $G' = G_0 \cup G_1 \tau_1 \cup \dots \cup G_{n-1} \tau_{n-1}$  sia S2T su  $E$ , allora necessariamente  $G/\parallel$  è un raffinamento di  $P(G)$ .

Nel seguito, per ciascun automorfismo  $\tau_r$ ,  $r = 1, \dots, n-1$ , considereremo l'insieme

$$M_r = \{x^{-1} \tau_r(x) \mid x \in E^*\}$$

e denoteremo con  $T(\tau_1, \dots, \tau_{n-1})$  il sottogruppo di  $E^*$  generato dagli insiemi  $M_r$ . La proposizione che segue fornisce un criterio di scelta della partizione  $P(G)$  affinché l'insieme  $G'$  sia S2T su  $E$ , e quindi  $\pi(E, G')$  sia un piano di traslazione. Essa è la generalizzazione della proposizione 2 di [1], che riguarda il caso in cui gli automorfismi  $\tau_1, \dots, \tau_{n-1}$  siano automorfismi del campo  $E$  e il piano  $\pi(E, G')$  un piano finito generalizzato di André.

**PROPOSIZIONE 1.** – Siano  $E$  un campo finito,  $\tau_1, \dots, \tau_{n-1}$  automorfismi lineari di  $E$  come spazio vettoriale su un suo sottocampo,  $P(E^*) = \{E_0, E_1, \dots, E_{n-1}\}$  una partizione di  $E^*$  con  $1 \in E_0$  e con partizione associata  $P(G) = \{G_0, G_1, \dots, G_{n-1}\}$ ,  $T = T(\tau_1, \dots, \tau_{n-1})$ . Se la partizione  $E^*/T$  è un raffinamento di  $P(E^*)$  allora l'insieme di permutazioni  $G' = G_0 \cup G_1 \tau_1 \cup \dots \cup G_{n-1} \tau_{n-1}$  è S2T su  $E$ .

**DIM.** – Detto  $t$  l'indice di  $T$  in  $E^*$ , esiste un generatore  $\omega$  di  $E^*$  tale che  $\omega^t$  sia un generatore di  $T$ . I laterali distinti di  $T$  sono allora  $T, \omega T, \dots, \omega^{t-1} T$ . Per ogni  $r = 0, 1, \dots, t-1$  poniamo

$$\overline{G}_r = \{x \rightarrow ax + b \mid a \in \omega^r T, b \in E\}.$$

Inoltre, per ogni  $r = 1, \dots, t-1$ , se  $E_s$  è l'elemento di  $P(E^*)$  tale che risulti  $\omega^r T \subseteq E_s$ , poniamo  $\bar{\tau}_r = \text{id}_E$  nel caso  $s = 0$ ,  $\bar{\tau}_r = \tau_s$  nel caso  $s \neq 0$ . L'insieme  $\overline{G} = \{\overline{G}_0, \overline{G}_1, \dots, \overline{G}_{t-1}\}$  è una partizione di  $G$  con  $\text{id}_E \in \overline{G}_0$ . Ma si ha ovviamente

$$G' = \overline{G}_0 \cup \overline{G}_1 \bar{\tau}_1 \cup \dots \cup \overline{G}_{t-1} \bar{\tau}_{t-1}.$$

Si potrà allora concludere che l'insieme  $G'$  è S2T su  $E$  mostrando che  $G$ , la sua partizione  $\overline{G}$  e gli automorfismi  $\bar{\tau}_1, \dots, \bar{\tau}_{t-1}$  soddisfano le ipotesi della proposizione 1 di [1].

Siano infatti  $g \in \overline{G}_r$ ,  $1 \leq r \leq t-1$ , e  $g' \in \overline{G}_0$  due arbitrarie permutazioni definite da

$$g(x) = ax + b \quad \text{con} \quad a \in \omega^r T,$$

$$g'(x) = a'x + b' \quad \text{con} \quad a' \in T.$$

Si ha allora  $g^{-1}g'(x) = a^{-1}a'x + a^{-1}(b' - b)$ . Posto quindi  $a = \omega^{r+at}$  e  $a' = \omega^{\beta t}$ , con  $\alpha$  e  $\beta$  interi, si ottiene

$$a^{-1}a' = \omega^{(t-r)+t(\beta-a-1)} \in \omega^{t-r} T,$$

pertanto  $g^{-1}g' \in \overline{G}_{t-r}$ .

Consideriamo ora un qualsiasi automorfismo  $\bar{\tau}_r$ ,  $1 \leq r \leq t-1$ , e due arbitrari elementi  $x_1, x_2$  di  $E$ ,  $x_1 \neq x_2$ . Se  $\bar{\tau}_r = \text{id}_E$  allora si ha ovviamente  $\bar{\tau}_r(x_i) = \text{id}_E(x_i)$ ,  $i = 1, 2$ , con  $\text{id}_E \in \overline{G}_0$ . Se invece  $\bar{\tau}_r = \tau_s$  con  $1 \leq s \leq n-1$ , poiché il gruppo  $G$  è S2T su  $E$ , esiste ed è unica la permutazione  $g \in G$ ,  $g: x \rightarrow ax + b$ , tale che  $g(x_i) = \tau_s(x_i)$ ,  $i = 1, 2$ . Da queste segue

$$a = (x_1 - x_2)^{-1} \tau_s(x_1 - x_2) \in T$$

e quindi  $g \in \overline{G}_0$ .

Il teorema precedente non è invertibile. Il prossimo esempio mostra infatti come si possa costruire un piano di traslazione  $\pi(E, G')$ , senza che il gruppo  $T(\tau_1, \dots, \tau_{n-1})$  e la partizione  $P(E^*)$  rispondano ai requisiti della proposizione 1.

ESEMPIO. — Siano  $E = GF(q^2)$  e  $K = GF(q)$ . Denotiamo con  $\eta: E^* \rightarrow K^*$  l'omomorfismo suriettivo «norma» definito da  $\eta(x) = x\sigma(x)$  per ogni  $x \in E^*$ , dove  $\sigma$  è l'automorfismo  $x \rightarrow x^q$  del campo  $E$ . Il nucleo di  $\eta$  è il sottogruppo  $H = \{x^{-1}\sigma(x) \mid x \in E^*\}$  di  $E^*$ . Dato un generatore  $\omega$  di  $E^*$ , l'elemento  $u = \omega^{q-1}$  è un generatore di  $H$ . Si ha pertanto

$$H = \{u, u^2, \dots, u^{q+1} = 1\}.$$

Consideriamo un elemento  $\alpha$  di  $E^*$  tale che risulti

$$1 - \alpha - \alpha^q \neq 0.$$

Da questa segue  $\alpha u^r + 1 - \alpha \neq 0$  per ogni  $r = 1, \dots, q+1$ . Poniamo quindi

$$\beta_r = \alpha u^r (\alpha u^r + 1 - \alpha)^{-1}$$

e

$$\tau_r = \beta_r \sigma + (1 - \beta_r) \text{id}_E.$$

Da  $\tau_r(x) = 0$  con  $x \neq 0$  segue  $1 - \alpha - \alpha^q = 0$ . Pertanto  $\tau_1, \dots, \tau_{q+1}$  sono automorfismi lineari dello spazio vettoriale  $E$  su  $K$ .

Consideriamo ora l'insieme

$$M = M_{q+1} = \{x^{-1}\tau_{q+1}(x) \mid x \in E^*\} = \{\alpha x + 1 - \alpha \mid x \in H\}.$$

Fissato un qualsiasi elemento  $\xi$  di  $E^*$  tale che  $\xi^{-1} \notin M$ , poniamo

$$G_0 = \{x \rightarrow ax + b \mid a \in E^* - \xi M, b \in E\}$$

e

$$G_r = \{x \rightarrow ax + b \mid a = \xi(\alpha u^r + 1 - \alpha), b \in E\},$$

per  $r = 1, \dots, q+1$ . L'insieme di permutazioni  $G' = G_0 \cup G_1 \tau_1 \cup \dots \cup G_{q+1} \tau_{q+1}$  è S2T su  $E$ .

Siano infatti  $x_1 \neq x_2$ ,  $y_1 \neq y_2$  arbitrari elementi di  $E$  e  $g$  la permutazione del gruppo  $G$  tale che  $g(x_i) = y_i$ ,  $i = 1, 2$ . Se  $g \in G_0$  allora ovviamente  $g \in G'$ , supponiamo quindi  $g \in G_r$ ,  $1 \leq r \leq q+1$ . Posto  $g(x) = \xi(\alpha u^r + 1 - \alpha)x + b$ , si consideri l'elemento di  $H$

$$u^s = \frac{u^r}{(x_1 - x_2)^{q-1}}$$

e la permutazione  $h \in G_s$  definita da

$$h(x) = \xi(\alpha u^s + 1 - \alpha)x + b',$$

con

$$b' = \xi\alpha(u^r x_1 - u^s x_1^q) + b.$$

La permutazione  $h\tau_s$  appartiene a  $G_s\tau_s$  e, poichè si ha anche  $b' = \xi\alpha(u^r x_2 - u^s x_2^q) + b$ , si ottiene  $h\tau_s(x_i) = y_i$ ,  $i = 1, 2$ .

Siano ora  $f$  ed  $f'$  due permutazioni di  $G'$  tali che  $x_i \rightarrow y_i$ ,  $i = 1, 2$ . Se  $f$  ed  $f'$  appartengono entrambe a  $G_0$  si ha un assurdo, in quanto il gruppo  $G$  è S2T su  $E$ . Supponiamo  $f \in G_r\tau_r$  e  $f' \in G_s\tau_s$  con  $1 \leq r \leq q+1$ ,  $1 \leq s \leq q+1$ . Posto

$$f(x) = \xi[\alpha u^r x^q + (1 - \alpha)x] + b,$$

$$f'(x) = \xi[\alpha u^s x^q + (1 - \alpha)x] + b',$$

da  $f(x_i) = f'(x_i)$ ,  $i = 1, 2$ , si ottiene  $u^r = u^s$ . Quindi da  $f(x_1) = f'(x_1)$  segue  $b = b'$  cioè  $f = f'$ . Se ora si suppone  $f \in G_0$  e  $f' \in G_s\tau_s$ ,  $1 \leq s \leq q+1$ , posto  $f(x) = ax + b$ , con  $a \in E^* - \xi M$ , e  $f'$  come in precedenza, da  $f(x_i) = f'(x_i)$ ,  $i = 1, 2$  segue

$$a = \xi[\alpha u^s(x_1 - x_2)^{q-1} + 1 - \alpha] \in \xi M$$

che è assurdo.

La partizione  $\{E_0, E_1, \dots, E_{q+1}\}$  di  $E^*$  associata alla partizione  $\{G_0, G_1, \dots, G_{q+1}\}$  di  $G$  è in questo caso la seguente:

$$E_0 = E^* - \xi M, \quad E_r = \{\xi(\alpha u^r + 1 - \alpha)\},$$

$r = 1, \dots, q+1$ . Pertanto, posto  $T = T(\tau_1, \dots, \tau_{q+1})$ ,  $E^*/T$  non soddisfa la condizione della proposizione 1. Si può mostrare che il piano di traslazione  $\pi(E, G')$  può essere riguardato come il piano derivato del piano desarguesiano  $\pi(E, G)$ , rispetto all'insieme di derivazione individuato da  $\xi M$ . Pertanto  $\pi(E, G')$  è un piano finito di Hall e poichè gli elementi di  $\xi M$  non hanno norma costante, esso non è un piano di André (cfr. [4]).

La non invertibilità della proposizione 1 dipende essenzialmente dal fatto che gli automorfismi che vi compaiono, distinti fra loro e diversi da  $\text{id}_E$ , siano almeno due. Vale infatti la seguente

**PROPOSIZIONE 2.** – Siano  $E$  un campo finito,  $\tau$  un automorfismo lineare di  $E$  come spazio vettoriale su un suo sottocampo,  $P(E^*) = \{E_0, E_1\}$  una partizione di  $E^*$  con  $1 \in E_0$  e partizione associata  $P(G) = \{G_0, G_1\}$ ,  $T = T(\tau)$ . L'insieme di permutazioni  $G' = G_0 \cup G_1 \tau$  è  $S_2 T$  su  $E$  se e solo se la partizione  $E^*/T$  è un raffinamento di  $P(E^*)$ .

**DIM.** – Se  $E^*/T$  è un raffinamento di  $P(E^*)$ , si ha un caso particolare della proposizione 1. Supponiamo viceversa che l'insieme  $G'$  sia  $S_2 T$  su  $E$ . Il gruppo  $T$  è generato dall'insieme  $M = \{x^{-1} \tau(x) \mid x \in E^*\}$ . Scelti comunque un elemento  $z \in E_0$  ed un elemento  $y \in M$ , si ha  $zy \in E_0$ . Se infatti  $y = t^{-1} \tau(t)$  con  $t \in E^*$ , posto  $t = t_1 - t_2$ , da  $t_1 \neq t_2$  segue che esiste una permutazione  $g \in G'$  tale che  $g(t_i) = z\tau(t_i)$ ,  $i = 1, 2$ . Se  $g$  appartiene a  $G_1 \tau$ , posto  $g(x) = \alpha \tau(x) + b$  con  $\alpha \in E_1$ , si ha  $\alpha \tau(t_i) + b = z\tau(t_i)$ ,  $i = 1, 2$ , quindi  $\alpha \tau(t) = z\tau(t)$  cioè  $\alpha = z$  che è assurdo. Ne segue  $g \in G_0$ . Posto allora  $g(x) = a'x + b'$  con  $a' \in E_0$ , si ottiene  $g(t_i) = a't_i + b' = z\tau(t_i)$ ,  $i = 1, 2$ , e da queste  $a't = z\tau(t)$ . Pertanto  $a' = zy$ , cioè  $zy \in E_0$ . Sia ora  $v$  un qualsiasi elemento di  $zT$ . Si ha allora  $v = zu_1 \dots u_h$  con  $h$  intero positivo e  $u_1, \dots, u_h$  elementi di  $M$ . Ma per quanto dimostrato prima,  $zu_1$  è un elemento di  $E_0$ , e quindi si ha subito per induzione che  $v$  appartiene a  $E_0$ . Ne segue che  $zT$  è contenuto in  $E_0$  e quindi che  $E^*/T$  è un raffinamento di  $P(E^*)$ .

**2.** In questo paragrafo considereremo il caso in cui  $E$  sia uno spazio vettoriale di dimensione due su un suo sottocampo  $K$ , per mostrare come non sia possibile costruire un piano di traslazione  $\pi(E, G')$ , quando si voglia comunque utilizzare un unico automorfismo lineare, oppure se ne vogliano utilizzare più d'uno ma rispettando le condizioni della proposizione 1. Restano naturalmente aperti due problemi. Il primo consiste nello stabilire se le conclusioni precedenti sussistano anche quando la dimensione di  $E$  su  $K$  sia maggiore di

due. Il secondo, nel caso invece di dimensione due, riguarda la possibilità di ottenere un piano di traslazione  $\pi(E, G')$ , con un metodo diverso da quello usato nel paragrafo precedente per la costruzione di un piano finito di Hall.

Siano  $E = GF(q^2)$ ,  $K = GF(q)$ ,  $\sigma$  l'automorfismo  $x \rightarrow x^q$  del campo  $E$ ,  $H$  il nucleo dell'omomorfismo «norma»,  $\tau$  un qualsiasi automorfismo dello spazio vettoriale  $E$  su  $K$ . Il caso  $\tau = \sigma$  è stato trattato in [1], supporremo quindi  $\tau \neq \sigma$  e ovviamente  $\tau \neq \text{id}_E$ . Inoltre, poichè ciò non costituisce una limitazione sulla scelta di  $\tau$ , supporremo anche  $\tau(1) = 1$ . Esiste allora (cfr. [6]) un elemento  $a \in E$ ,  $a \neq 0$ ,  $a \neq 1$ , tale che

$$\tau = \alpha\sigma + (1 - \alpha) \text{id}_E.$$

L'elemento

$$\xi = 1 - \alpha - \alpha^q$$

appartiene a  $K$  e l'invertibilità di  $\tau$  è equivalente alla condizione  $\xi \neq 0$ .

Consideriamo ora l'insieme

$$M = \{x^{-1} \tau(x) \mid x \in E^*\} = \{\alpha u + 1 - \alpha \mid u \in H\}$$

e definiamo la seguente applicazione di  $H$  in sè:

$$u \rightarrow \bar{u} = -u \frac{(1 - \alpha)}{(1 - \alpha)^q} \frac{(\alpha u + 1 - \alpha)^q}{(\alpha u + 1 - \alpha)}.$$

Da  $\xi \neq 0$  segue che essa è biiettiva. Si ottiene subito che è anche involutoria e che si ha

$$\bar{\bar{1}} = - \frac{(1 - \alpha)}{(1 - \alpha)^q}.$$

Vale inoltre la seguente proprietà.

( $p_1$ ) Gli elementi  $u$  di  $H$  tali che  $u = \bar{u}$  sono due distinti o nessuno, se  $q$  è dispari, uno ed uno solo, se  $q$  è pari.

DIM. — Si ha infatti  $u = \bar{u}$  se e solo se  $u$  è una soluzione dell'equazione

$$\alpha(1 - \alpha)^q x^2 + 2(1 - \alpha)^{q+1} x + \alpha^q(1 - \alpha) = 0.$$

Se  $q$  è dispari, essa ha per discriminante l'elemento non nullo di  $K$ :  $\Delta = (1 - \alpha)^{q+1} \xi$ . Ne segue che  $\Delta$  è un quadrato di  $E^*$  e che pertanto si hanno due soluzioni distinte. Ma il loro prodotto è un elemento di  $H$ , quindi esse sono entrambe in  $H$  o entrambe in  $E^* - H$ .

Se invece  $q$  è pari, l'equazione precedente ha una ed una sola soluzione  $u$ , la controimmagine dell'elemento di  $H$

$$\frac{\alpha^q(1-\alpha)}{\alpha(1-\alpha)^q}$$

nell'automorfismo  $x \rightarrow x^2$ . Ma tale automorfismo muta  $H$  in sè, dunque  $u$  è un elemento di  $H$ .

La permutazione su  $H$   $u \rightarrow \bar{u}$  induce la seguente permutazione su  $M$ :

$$z = \alpha u + 1 - \alpha \rightarrow \tilde{z} = \alpha \bar{u} + 1 - \alpha.$$

Essa è a sua volta involutoria. Si ha subito

$$\tilde{\tilde{1}} = \frac{(1-\alpha)}{(1-\alpha)^q} \xi,$$

e inoltre

$$z\tilde{z} = \tilde{1}$$

per ogni  $z \in M$ . Da ciò la proprietà che segue.

( $p_2$ ) Per ogni  $z, t \in M$ ,  $z \neq t$ , si ha

$$zM \cap tM = \{\tilde{1}, zt\}$$

e risulta  $\tilde{1} = zt$  se e solo se  $t = \tilde{z}$ .

DIM. — Per quanto osservato prima, è infatti ovvio che  $\tilde{1}$  e  $zt$  siano elementi di  $zM \cap tM$ . D'altra parte, posto  $z = \alpha u + 1 - \alpha$ ,  $t = \alpha v + 1 - \alpha$ ,  $u$  e  $v$  in  $H$ , se  $\omega$  è un qualsiasi elemento di  $zM \cap tM$ , esistono  $x, y \in H$  tali che

$$\omega = z(\alpha x + 1 - \alpha) = t(\alpha y + 1 - \alpha).$$

Si ha allora  $\alpha xz = t(\alpha y + 1 - \alpha) - z(1 - \alpha)$  e da questa, poichè  $x^{q+1} = 1$ , si ottiene che  $y$  è una soluzione dell'equazione  $ay^2 + by + c = 0$ , dove

$$a = t(1 - \alpha)^{q-1}(v - u)^{q-1},$$

$$b = (1 - \alpha)^q(v - u)^q + \alpha(1 - \alpha)^{q-1} + \alpha^q(v - u)^{q-1},$$

$$c = t^q.$$

L'insieme  $zM \cap tM$  è pertanto costituito da due elementi al più, quindi  $zM \cap tM = \{\tilde{1}, zt\}$ . Gli elementi  $\tilde{1}$  e  $zt$  coincidono nel caso  $t = \tilde{z}$ , e solo in questo, in quanto da  $zt = \tilde{1}$  segue subito  $v = \tilde{u}$  cioè  $t = \tilde{z}$ .

Consideriamo ora il sottogruppo  $T(\tau)$  di  $E^*$  generato da  $M$  ed il seguente sottoinsieme di  $T(\tau)$ :

$$F = \bigcup_{z \in M} zM.$$

La proprietà  $(p_2)$  permette di calcolare l'ordine di  $F$ . Se  $q$  è dispari, dalla  $(p_1)$  segue che gli elementi  $z$  di  $M$  tali che  $z = \tilde{z}$  sono due distinti o nessuno. In quest'ultimo caso, posto

$$M = \{1, \tilde{1}, z_1, \tilde{z}_1, \dots, z_{(q-1)/2}, \tilde{z}_{(q-1)/2}\},$$

si ha

$$|M \cup \tilde{1}M| = 2q + 1,$$

$$|M \cup \tilde{1}M \cup z_1M \cup \tilde{z}_1M| = (2q + 1) + 2(q - 2),$$

$$|M \cup \tilde{1}M \cup z_1M \cup \tilde{z}_1M \cup z_2M \cup \tilde{z}_2M| = (2q + 1) + 2(q - 2) + 2(q - 4),$$

.....

$$|F| = (2q + 1) + 2(q - 2) + 2(q - 4) + \dots + 2 =$$

$$2(1 + 3 + \dots + q) + 1 = \frac{(q + 1)^2}{2} + 1.$$

Supponiamo ora che esistano due elementi distinti  $x$  e  $y$  di  $M$  tali che  $x = \tilde{x}$ ,  $y = \tilde{y}$ . Se nessuno di essi è 1, posto

$$M = \{1, \tilde{1}, x, y, z_1, \tilde{z}_1, \dots, z_{(q-3)/2}, \tilde{z}_{(q-3)/2}\},$$

si ottiene

$$|M \cup \tilde{1}M| = 2q + 1,$$

$$|M \cup \tilde{1}M \cup xM \cup yM| = (2q + 1) + (q - 2) + (q - 3),$$

$$|M \cup \tilde{1}M \cup xM \cup yM \cup z_1M \cup \tilde{z}_1M| = (2q + 1) + (q - 2) + (q - 3) + 2(q - 4),$$

.....

$$|F| = (2q + 1) + (q - 2) + (q - 3) + 2(q - 4) + 2(q - 6) + \dots + 2 =$$

$$2(1 + 3 + \dots + q) = \frac{(q + 1)^2}{2}.$$

Se invece uno di essi è 1, posto

$$M = \{1, x, z_1, \tilde{z}_1, \dots, z_{(q-1)/2}, \tilde{z}_{(q-1)/2}\},$$

si ha

$$|M \cup xM| = 2q,$$

$$|M \cup xM \cup z_1 M \cup \tilde{z}_1 M| = 2q + 2(q-2),$$

.....

$$|F| = 2q + 2(q-2) + 2(q-4) + \dots + 2 = 2(1 + 3 + \dots + q) = \frac{(q+1)^2}{2}.$$

Si ottiene quindi in ogni caso  $|F| \geq (q+1)^2/2$ . Ne segue  $|T(\tau)| > (q^2-1)/2$  e quindi  $T(\tau) = E^*$ . Se invece  $q$  è pari, esiste uno ed un solo elemento  $x$  di  $M$  tale che  $x = \tilde{x}$ . Supponiamo dapprima  $x \neq 1$ . Posto allora

$$M = \{1, \tilde{1}, x, z_1, \tilde{z}_1, \dots, z_{(q-2)/2}, \tilde{z}_{(q-2)/2}\},$$

si ottiene

$$|M \cup \tilde{1}M| = 2q + 1,$$

$$|M \cup \tilde{1}M \cup xM| = (2q + 1) + (q-2),$$

$$|M \cup \tilde{1}M \cup xM \cup z_1 M \cup \tilde{z}_1 M| = (2q + 1) + (q-2) + 2(q-3),$$

.....

$$|F| = (2q + 1) + (q-2) + 2(q-3) + 2(q-5) + \dots + 2 =$$

$$2[1 + 3 + \dots + (q-1)] + (q+1) = \frac{(q+1)^2 + 1}{2}.$$

Se invece  $1 = \tilde{1}$ , posto

$$M = \{1, z_1, \tilde{z}_1, \dots, z_{q/2}, \tilde{z}_{q/2}\},$$

si ha

$$|M \cup z_1 M \cup \tilde{z}_1 M| = (q+1) + 2(q-1),$$

$$|M \cup z_1 M \cup \tilde{z}_1 M \cup z_2 M \cup \tilde{z}_2 M| = (q+1) + 2(q-1) + 2(q-3),$$

.....

$$|F| = (q+1) + 2(q-1) + 2(q-3) + \dots + 2 = \frac{(q+1)^2 + 1}{2}.$$

Pertanto, nel caso  $q$  pari, si ha sempre  $|T(\tau)| \geq |F| > (q^2 - 1)/3$ , e quindi anche ora  $T(\tau) = E^*$ .

Possiamo allora riassumere gli ultimi risultati nella seguente proposizione 3. Essa permette di dimostrare le proposizioni 4 e 5, nelle quali vengono formalizzate le due affermazioni fatte all'inizio del paragrafo.

PROPOSIZIONE 3. – Siano  $E = GF(q^2)$ ,  $K = GF(q)$ . Per ogni automorfismo  $\tau$  dello spazio vettoriale  $E$  su  $K$ ,  $\tau \neq \text{id}_E$ ,  $\tau \neq \sigma$ , il gruppo  $T(\tau)$  coincide con  $E^*$ .

PROPOSIZIONE 4. – Siano  $E = GF(q^2)$ ,  $K = GF(q)$ ,  $\tau$  un automorfismo dello spazio vettoriale  $E$  su  $K$ ,  $\tau \neq \text{id}_E$ ,  $\tau \neq \sigma$ . Non esiste una partizione  $\{G_0, G_1\}$  di  $G$ , con  $\text{id}_E \in G_0$  e  $G_0 \neq G$ , tale che l'insieme  $G_0 \cup G_1 \tau$  sia  $S2T$  su  $E$ .

DIM. – Sia  $P(G) = \{G_0, G_1\}$  una partizione di  $G$ , con  $\text{id}_E \in G_0$  e  $G_0 \neq G$ , tale che l'insieme  $G_0 \cup G_1 \tau$  risulti  $S2T$  su  $E$ . In questo caso la partizione  $G/_\tau$  è un raffinamento di  $P(G)$ , si può quindi considerare la partizione  $P(E^*) = \{E_0, E_1\}$  di  $E^*$  associata a  $P(G)$ . Da  $\text{id}_E \in G_0$  segue  $1 \in E_0$  e da  $G_0 \neq G$  segue  $E_0 \neq E^*$ . Ma, per la proposizione 2, la partizione  $E^*/T(\tau)$  è un raffinamento di  $P(E^*)$ . Ne segue  $T(\tau) \subseteq E_0$ . E questo è assurdo in quanto, per la proposizione 3, si ha  $T(\tau) = E^*$  quindi  $E_0 = E^*$ .

La proposizione 4 implica, nel caso  $E = GF(q^2)$ , che gli unici piani di traslazione ottenibili con un unico automorfismo non identico, si hanno per  $\tau = \sigma$  e pertanto sono piani finiti di André (cfr. [1]).

PROPOSIZIONE 5. – Siano  $E = GF(q^2)$ ,  $K = GF(q)$ ,  $\tau_1, \dots, \tau_{n-1}$  automorfismi dello spazio vettoriale  $E$  su  $K$ , almeno uno diverso da  $\text{id}_E$  e da  $\sigma$ ,  $T = T(\tau_1, \dots, \tau_{n-1})$ . Non esiste una partizione  $\{E_0, E_1, \dots, E_{n-1}\}$  di  $E^*$ , con  $1 \in E_0$  e  $E_0 \neq E^*$ , tale che  $E^*/T$  sia un suo raffinamento.

DIM. – Esiste un automorfismo  $\tau_r$ ,  $1 \leq r \leq n-1$ , tale che  $\tau_r \neq \text{id}_E$  e  $\tau_r \neq \sigma$ . Allora la dimostrazione segue subito dalla proposizione 3 e dall'osservazione che si ha  $T(\tau_r) \subseteq T(\tau_1, \dots, \tau_{n-1})$ .

## REFERENCES

- [1] A. BASILE - P. BRUTTI, *Insiemi di permutazioni strettamente 2-transitivi e costruzione di alcune classi di piani di traslazione*, Atti Sem. Mat. Fis. Univ. Modena, **255** (1995).
- [2] P. DEMBOWSKI, *Finite Geometries*, Springer Verlag, 1968.

- [3] W. HEISE - P. QUATTROCCHI, *Survey on sharply  $k$ -transitive sets of permutations and Minkowski  $m$ -structures*, Atti Sem. Mat. Fis. Univ. Modena, **27** (1978).
- [4] H. LUNEBURG, *Translation Planes*, Springer-Verlag, 1980.
- [5] P. QUATTROCCHI - C. FIORI - G. RINALDI, *Permutazioni e geometrie*, Accad. Naz. Sc. Lett. Arti. Modena, **69** (1994).
- [6] B. SEGRE - U. BARTOCCI, *Ovali e altre curve nei piani di Galois di caratteristica due*, Acta Arithmetica, **423** (1971).

Alessandro Basile - Paolo Brutti: Dipartimento di Matematica  
Via Pascoli - 06100 Perugia

---

*Pervenuta in Redazione*  
*il 6 maggio 1999*