STRUTTURE DISCRETE

Appunti del corso a cura della dott.ssa E. Francot

1 Nozioni preliminari

Definizione 1.1 *Una* ***Struttura di Incidenza*** *è una tripla* $(\mathcal{V}, \mathcal{B}, \mathcal{I})$ *con* $\mathcal{V}$, $\mathcal{B}$, $\mathcal{I}$ *insiemi tali che* $\mathcal{V} \cap \mathcal{B} = \emptyset$, $\mathcal{I} \subseteq \mathcal{V} \times \mathcal{B}$. *Gli elementi di* $\mathcal{V}$ *sono detti varietà, quelli di* $\mathcal{B}$ *sono detti blocchi e* $\mathcal{I}$ *è detta una relazione di incidenza. Se* $(V, l) \in \mathcal{I}$ *allora diciamo che* V *è incidente a* l*, se invece* $(V, l) \notin \mathcal{I}$ *allora diciamo che* V *non è incidente a* l*.*

Una classe di Strutture di Incidenza di particolare interesse sono i 2-Disegni.

Definizione 1.2 *Una struttura di incidenza* $(\mathcal{V}, \mathcal{B}, \mathcal{I})$ *è detta un* $2-(v, k, \lambda)$ ***disegno a blocchi bilanciato incompleto*** *(BIBD), con* $v, k, \lambda \in Z^+ \cup \{0\}$ *se valgono le seguenti proprietà:*

1. $|\mathcal{V}| = v$*;*
2. *ad ogni blocco* $l \in \mathcal{B}$ *sono incidenti esattamente* k *varietà;*
3. *ogni coppia di varietà distinte è incidente ad esattamente* λ *blocchi.*

Definizione 1.3 *Un disegno si dice a blocchi ripetuti se esistono blocchi distinti che hanno lo stesso insieme di varietà incidenti.*

Per i disegni non a blocchi ripetuti, ogni blocco è univocamente individuato dall'insieme delle varietà ad esso incidenti. In questo caso conviene allora identificare ogni blocco con l'insieme delle varietà ad esso incidenti ed utilizzare l'appartenenza insiemistica piuttosto che l'incidenza. $\mathcal{B}$ risulta essere un insieme di sottoinsiemi di $\mathcal{V}$ e l'incidenza $\mathcal{I}$ diventa l'appartenenza $\in$.

Sia $(\mathcal{V}, \mathcal{B})$ un 2-(v, k, λ) disegno con $|\mathcal{V}| = v$ e $k = |l|$ con $l \in \mathcal{B}$. Introduciamo altri parametri per tale disegno.

Fissata una varietà A, indichiamo con r il numero $|\{l \in \mathcal{B} : A \in l\}|$ e con $b = |\mathcal{B}|$. Si verifica facilmente che tra i parametri del disegno vale la seguente relazione:

$$bk = vr \tag{1}$$

Nel seguito saremo interessati ad una particolare classe di disegni: i *piani proiettivi.* Per gli evidenti legami con la geometria classica chiameremo in questo caso *punti* gli elementi di $\mathcal{V}$ e *rette* gli elementi di $\mathcal{B}$.

Notazioni
- $P, A, B...$ rappresentano gli elementi di $\mathcal{V}$
- $a, b, l...$ rappresentano gli elementi di $\mathcal{B}$
- AB denota la retta incidente con i punti A e B
- $a \cap b$ denota il punto incidente con le rette a e b
- $[P]$ rappresenta l'insieme di tutte le rette incidenti con P.

Definizione 1.4 *La struttura di incidenza* $\Pi = (\mathcal{V}, \mathcal{B})$ *è un* ***piano proiettivo*** *se soddisfa i seguenti assiomi:*

1. *due punti distinti appartengono ad una ed una sola retta;*
2. *due rette distinte hanno uno ed un solo punto in comune;*
3. *esistono quattro punti a tre a tre non appartenenti ad una stessa retta.*

Nel seguito considereremo, in generale, solo casi in cui $\mathcal{V}$ è un insieme finito da cui segue che anche $\mathcal{B}$ è un insieme finito.

Corollario 1.5 *Se* a *ed* l *sono due rette distinte di un piano proiettivo* Π*, esiste un punto* P *del piano non appartenente nè ad* a *nè ad* l*.*

Dim. Supponiamo per assurdo che tutti i punti di Π appartengano ad a oppure ad l. Consideriamo quattro punti A, B, C, D tali che A,$B \in a$ e C,$D \in l$. Sia $P = AD \cap CB$ allora $P \in a$ oppure $P \in l$. Supponiamo $P \in a$. Poichè A, B, D non appartengono ad una stessa retta, $AB \neq AD$ e poichè $P \in AD$, P deve essere l'unico punto comune alle rette AB e AD. Ma A appartiene ad entrambe queste rette e quindi $A = P$. Ciò è assurdo perchè $P \in CB$ e i punti A, B, C non appartengono ad una stessa retta. Quindi $P \notin a$. Allo stesso modo si prova che $P \notin l$. ■

Teorema 1.6 Π *è un* 2*-*$(n^2 + n + 1, n + 1, 1)$ *disegno con* $n \in Z$*,* $n \geq 2$*.*

Dim. Dal punto 2) della Def. 1.4 segue che $\lambda = 1$. Proviamo che tutte le rette di Π hanno la stessa cardinalità. Consideriamo due rette distinte a, b di Π ed un punto P non appartenente nè ad a nè a b, la cui esistenza è assicurata dal Coroll.1.5. Sia $f : a \to b$ una funzione tale che ad ogni $X \in a$ associa $Y \in b$ con $Y = XP \cap b$. f così definita, è iniettiva infatti: sia $Z \in a$ con $Z \neq X$ e $f(Z) = V$. Se per assurdo fosse $Y = V$ allora da $PY = PV$ segue $X = Z$. f è suriettiva, infatti: sia A' un generico punto di b, esiste $A \in a$ con $A = PA' \cap a$ tale che $f(A) = A'$. Essendo f biunivoca possiamo concludere che $|a| = |b|$ $\forall a, b \in \Pi$. Indicata con $n+1$ la cardinalità di una fissata retta del piano abbiamo $k = n + 1$. Proviamo che Π ha $n^2 + n + 1$ punti. Sia a una retta di Π e P un punto non appartenente ad a. Vi è una corrispondenza biunivoca g tra i punti A_i appartenenti ad a e le rette l_i del fascio $[P]$. Ad ogni $A_i \in a$, g associa la retta $A_iP \in [P]$. Si hanno allora $n + 1$ rette per P e a ciascuna di esse appartengono n punti diversi da P. Le rette di $[P]$, private del punto P, costituiscono una partizione del piano privato del punto P in quanto per la proprietà 2) della Def. 1.4 due generiche rette di $[P]$ si intersecano solo in P e per ogni $X \in \Pi$ esiste $l = XP \in [P]$ tale che $X \in l$. Il numero totale dei punti di Π è pertanto $n(n + 1) + 1 = n^2 + n + 1$. Per l'assioma 3 della Def.1.4 risulta $k \geq 3$ e quindi $n \geq 2$. La tesi è completamente provata. ■

Nel caso di un piano proiettivo Π, r rappresenta la cardinalità di un fascio di rette di centro P fissato, dunque $r = n + 1$ da cui segue che

$$b = \frac{vr}{k} = \frac{(n^2 + n + 1)(n + 1)}{(n + 1)} = n^2 + n + 1$$

è il numero delle rette del piano Π. Ricordiamo che i disegni con $k = r$ (o equivalentemente $b = v$) sono detti *disegni simmetrici.*

Il numero n si dice *ordine* del piano proiettivo.

Sia $\Pi = (\mathcal{V}, \mathcal{B})$ un piano proiettivo, consideriamo la struttura $\Pi^d = (\mathcal{B}, \mathcal{V})$, i cui punti sono le rette di Π e le cui rette sono i punti di Π e definiamo in Π^d una relazione di incidenza "simmetrica" rispetto a quella definita in Π, cioè tale che in Π^d $a \ni A$ se e solo se $A \in a$ in Π. Allora è subito visto che Π^d è ancora un piano proiettivo detto *piano duale* di Π. Ovviamente $(\Pi^d)^d = \Pi$.

Principio di dualità *Sia $\mathcal{A}$ un qualsiasi teorema valido per il piano proiettivo Π. Se $\mathcal{A}^d$ è la proposizione ottenuta da $\mathcal{A}$ scambiando tra loro le parole "punti" e "rette", allora $\mathcal{A}^d$ è un teorema valido per il piano proiettivo Π^d.*

Da ciò segue che se un teorema è valido per tutti i piani proiettivi allora anche il teorema duale lo è.

Definizione 1.7 *La struttura di incidenza $\mathcal{A} = (\mathcal{V}, \mathcal{B})$ è un* ***piano affine*** *se soddisfa i seguenti assiomi:*

1. *due punti distinti appartengono ad una ed una sola retta;*

2. *dato un punto P ed una retta l con $P \notin l$ esiste un'unica retta l' tale che $P \in l'$ e $l \cap l' = \emptyset$;*

3. *esistono tre punti non appartenenti ad una stessa retta.*

In ogni piano affine $\mathcal{A}$ si può definire una relazione di "parallelismo" tra rette in un modo del tutto naturale. Diremo che due rette l, l' sono parallele, e scriveremo $l \| l'$, se e solo se $l = l'$ oppure $l \cap l' = \emptyset$.

Tale relazione risulta essere una relazione di equivalenza, infatti:

1. $l \parallel l$ per definizione, vale cioè la prop. riflessiva;

2. $l \parallel l' \Rightarrow l' \parallel l$ banalmente, prop. simmetrica;

3. siano l, l', l'' tali che $l \parallel l'$ e $l' \parallel l''$.

Se $l = l'$ oppure $l' = l''$ allora segue immediatamente $l \parallel l''$.

Supponiamo allora che $l \neq l'$ e $l' \neq l''$. Si ha $l \cap l' = \emptyset$ e $l' \cap l'' = \emptyset$. Se per assurdo fosse $l \cap l'' \neq \emptyset$ allora esisterebbe $P \in l \cap l''$ con $P \notin l'$. P appartiene ad l con $l \cap l' = \emptyset$ e P appartiene ad l'' con $l' \cap l'' = \emptyset$. Quindi $P \notin l'$ e per esso passano due rette, l ed l'' parallele ad l', contro l'assioma 2) della Def. 1.7. Abbiamo così provato che vale anche la prop. transitiva e dunque il parallelismo è una relazione di equivalenza.

Ripartiamo l'insieme delle rette in classi di equivalenza che indichiamo con $[l]_\parallel$, in questo modo otteniamo una partizione dei punti di Π, infatti: sia $P \notin l$ per l'assioma 3) esiste l' tale che $P \in l'$ e $l' \parallel l$; quindi $P \in l' \in [l]_\parallel$ e le classi sono inoltre a due a due disgiunte.

Partendo da $\mathcal{A} = (\mathcal{V}, \mathcal{B})$ possiamo definire una nuova struttura di incidenza:

poniamo $\mathcal{V}^* = \mathcal{V} \cup \left\{ [l]_\parallel : l \in \mathcal{B} \right\}$ e $\mathcal{B}^* = \mathcal{B} \cup \left\{ \bigcup_{l \in \mathcal{B}} [l]_\parallel \right\}$; per semplicità indichiamo $\left\{ \bigcup_{l \in \mathcal{B}} [l]_\parallel \right\}$ con l_∞ e chiameremo l_∞ *retta impropria*. Diremo *punti impropri* i punti di l_∞ e *punti propri* gli elementi di $\mathcal{V}$. Diremo infine *rette proprie* le rette del tipo $l \cup \left\{ [l]_\parallel \right\}$ con $l \in \mathcal{B}$.

Definiamo la nuova relazione di incidenza $\in^*$nel seguente modo:

Sia P un punto di $\mathcal{V}$ ed l una retta di $\mathcal{B}$, allora $P \in^* l$ se e solo se $P \in l$; sia $[l]_\parallel$ un punto improprio, allora $[l]_\parallel \in^* l_\infty$ mentre $[l]_\parallel \in^* s$ se e solo se $s \in [l]_\parallel$, cioè se s ed l sono parallele.

Teorema 1.8 $(\mathcal{V}^*, \mathcal{B}^*, \in^*)$ *è un piano proiettivo.*

Dim. Siano $A, B \in \mathcal{V}^*$ dobbiamo verificare che esiste un'unica retta di $\mathcal{B}^*$ cui essi appartengono. Se $A, B \in \mathcal{V}$ allora per l'assioma 1) della Def.1.7 esiste esattamente $a \in \mathcal{B} \subset \mathcal{B}^*$ t.c. $A, B \in a$. Se $A \in \mathcal{V}$ e $B = [l]_{\parallel}$ per l'assioma 2) della Def.1.7 esiste esattamente una retta $s \in [l]_{\parallel}$ t.c. $A \in s$. Poichè ovviamente $B \in s \cup \left\{[l]_{\parallel}\right\}$, $s \cup \left\{[l]_{\parallel}\right\}$è l'unica retta passante per A e B. Se infine $A = [s]_{\parallel}$ e $B = [l]_{\parallel}$ allora l_∞ contiene A e B ed è l'unica retta con questa proprietà. Abbiamo così provato che l'assioma 1) della Def. 1.4 è verificato. Siano s ed l due rette distinte di $\mathcal{B}^*$. Se $s \nparallel l$ allora si incontrano in $s \cap l$ che è un punto di $\mathcal{V}$. Se invece $s \parallel l$ allora $l \cap s = [l]_{\parallel} = [s]_{\parallel}$ e quindi le due rette si incontrano in un punto improprio. Infine se $s \in \mathcal{B}^*$ e $l = l_\infty$ allora $s \cap l_\infty = [s]_{\parallel}$. Abbiamo così provato che l'assioma 2) della Def. 1.4 è verificato. Nel piano affine $\mathcal{A} = (\mathcal{V}, \mathcal{B})$ esiste un triangolo ABC. Considerata la retta l_∞ e le classi di equivalenza $[AB]_{\parallel}$ e $[AC]_{\parallel}$ si verifica senza difficoltà che $B, C, [AB]_{\parallel}$ e $[AC]_{\parallel}$ costituiscono un quadrangolo. L'assioma 3) è così verificato. ■

Essendo $(\mathcal{V}^*, \mathcal{B}^*, \in^*)$ un piano proiettivo si ha che $|\mathcal{V}^*| = n^2 + n + 1$. Poichè siamo passati da $\mathcal{V}$ a $\mathcal{V}^*$ aggiungendo gli $n + 1$ punti della retta l_∞, si ha $|\mathcal{V}| = (n^2 + n + 1) - (n + 1) = n^2$. Inoltre per ogni $l \in \mathcal{B}^*$ $|l| = n + 1$. Da ciò segue che l, vista come retta di $\mathcal{B}$, ha $(n + 1) - 1 = n$ punti.

Quindi $\mathcal{A}$ è un 2-$(n^2, n, 1)$ disegno in cui il numero delle rette per un punto è $r = n+1$. Le rette del piano affine sono $b = (n^2 + n + 1) - 1 = n^2 + n$, avendo tolto la retta l_∞. Si noti che un piano affine non è un disegno simmetrico essendo $v \neq b$.

Proposizione 1.9 *Un 2-*$(n^2, n, 1)$ *disegno,* $n \geq 2$ *è un piano affine, .*

Dim. L'assioma 1) della Def.1.7 è banalmente verificato. Si ha $n^2 > n$; quindi tutti i punti della struttura, che sono n^2, non possono appartenere ad una stessa retta che è costituita da n punti. Da ciò segue l'assioma 3). Per provare l'assioma 2) consideriamo una retta l ed un punto $P \notin l$. Siano L_i, $i = 1, ..., n$ i punti incidenti con l. Ci sono n rette per P incidenti ad l, cioè le rette PL_i. Poichè le rette per P sono $n + 1$ esiste una ed una sola retta s per P non incidente con l ossia parallela ad l. ■

Sia $\Pi = (\mathcal{V}, \mathcal{B})$ un piano proiettivo. Fissiamo una retta $l \in \mathcal{B}$ e consideriamo $\mathcal{V}_l = \mathcal{V} - l$; $\mathcal{B}_l = \mathcal{B} - \{l\}$. La relazione di incidenza in $\mathcal{V}_l \times \mathcal{B}_l$ è la naturale restrizione della relazione di incidenza in $\mathcal{V} \times \mathcal{B}$.

Proposizione 1.10 $\mathcal{A} = (\mathcal{V}_l, \mathcal{B}_l)$ *è un piano affine.*

Dim. Siano A, B due punti distinti di $\mathcal{V}_l$, esiste allora un'unica retta s di $\mathcal{B}$ diversa da l che contiene entrambi e l'assioma 1) della Def. 1.7 è verificato. Sia a una retta di $\mathcal{B}_l$ e P un punto non appartenente ad a. Sia $C = a \cap l$, in $\mathcal{A}$ è $PC \cap a = \emptyset$ perchè $C \notin \mathcal{V}_l$. Quindi possiamo dire che esiste un'unica retta PC per P parallela ad a. L'assioma 2) della Def. 1.7 è verificato. La verifica dell'assioma 3) è lasciata per esercizio. ■

Definizione 1.11 *Siano $\mathcal{S} = (\mathcal{V}, \mathcal{B}, \mathcal{I})$ ed $\mathcal{S}' = (\mathcal{V}', \mathcal{B}', \mathcal{I}')$ due strutture di incidenza. Si definisce* isomorfismo *tra $\mathcal{S}$ ed $\mathcal{S}'$ una corrispondenza biunivoca $\varphi : \mathcal{V} \cup \mathcal{B} \to \mathcal{V}' \cup \mathcal{B}'$ tale che:*

1. *$\mathcal{V}^\varphi = \mathcal{V}'$ e $\mathcal{B}^\varphi = \mathcal{B}'$;*
2. *PIl se e solo se $P^\varphi I' l^\varphi$ $\forall P \in \mathcal{V}$ e $\forall l \in \mathcal{B}$*

Se $\mathcal{S} = \mathcal{S}'$ allora φ è detto *automorfismo* di $\mathcal{S}$

Si verifica immediatamente che gli automorfismi di una struttura di incidenza $\mathcal{S}$ formano un gruppo che si indica con $Aut(\mathcal{S})$

2 Collineazioni dei Piani Proiettivi

Nel seguito indichiamo con $(\mathcal{P}, \mathcal{L})$ un piano proiettivo Π in cui $\mathcal{P}$ è l'insieme dei punti ed $\mathcal{L}$ l'insieme delle rette.

Gli automorfismi di Π sono spesso chiamati, per motivi storici, anche *collineazioni*. Nel seguito useremo in generale il termine collineazione. Inoltre useremo il simbolo 1 per indicare la collineazione identica.

Definizione 2.1 *Sia $\mathcal{P}' \subseteq \mathcal{P}$ e $\mathcal{L}' \subseteq \mathcal{L}$. La coppia $(\mathcal{P}', \mathcal{L}')$ è detta* ***sottostruttura*** *di $(\mathcal{P}, \mathcal{L})$ se la relazione di incidenza in essa definita è la restrizione a $\mathcal{P}' \times \mathcal{L}'$ della relazione di incidenza di $(\mathcal{P}, \mathcal{L})$.*

Definizione 2.2 *Sia $\mathcal{P}' \subseteq \mathcal{P}$ e $\mathcal{L}' \subseteq \mathcal{L}$. La coppia $(\mathcal{P}', \mathcal{L}')$ è detta* ***sottostruttura chiusa*** *di $(\mathcal{P}, \mathcal{L})$ se gode delle seguenti proprietà:*

1. *$PQ \in \mathcal{L}'$ per ogni coppia di punti distinti di $\mathcal{P}'$;*
2. *$a \cap b \in \mathcal{P}'$ per ogni coppia di rette distinte di $\mathcal{L}'$.*

Una sottostruttura $(\mathcal{P}', \mathcal{L}')$ di $(\mathcal{P}, \mathcal{L})$ è detta ***sottopiano*** *di $(\mathcal{P}, \mathcal{L})$ se in aggiunta alle proprietà 1 e 2, gode anche della seguente proprietà: esiste un sottoinsieme $\mathcal{K} \subseteq \mathcal{P}'$ tale che $|\mathcal{K}| = 4$ e $|\mathcal{K} \cap l| \leq 2$ per tutte le rette l di $\mathcal{L}$.*

Teorema 2.3 *Una sottostruttura chiusa* $(\mathcal{P}', \mathcal{L}')$ *del piano proiettivo* $(\mathcal{P}, \mathcal{L})$ *è di uno dei seguenti tipi:*

1. *(A)* $(\varnothing, \varnothing)$,
2. *(Br$_i$)* $(\mathcal{P}', \{l\})$ *dove* $l \in \mathcal{L}$, $\mathcal{P}' \subseteq l$ *e* $|\mathcal{P}'| = i$,
3. *(Bp$_i$)* $(\{P\}, \mathcal{L}')$ *dove* $P \in \mathcal{P}$, $\mathcal{L}' \subseteq [P]$ *e* $|\mathcal{L}'| = i$,
4. *(C$_{ij}$)* $(\mathcal{P}', \mathcal{L}')$ *dove* $\mathcal{P}' \subseteq l$ *e* $\mathcal{L}' \subseteq [P]$ *con* $l \in \mathcal{L}'$ *e* $P \in \mathcal{P}' \cap l$*; inoltre* $|\mathcal{P}' - \{P\}| = i$ *e* $|\mathcal{L}' - \{l\}| = j$ *con* $i, j \geq 1$,
5. *(D$_i$)* $(\mathcal{P}', \mathcal{L}')$ *dove* $\mathcal{P}' = \{P\} \cup \mathcal{K}$ *e* $\mathcal{L}' = \{l\} \cup \{XP \,|X \in \mathcal{K}\}$ *con* $l \in \mathcal{L}$, $\mathcal{K} \subseteq l$ *e* $P \notin l$*; inoltre* $|\mathcal{K}| = i$,
6. *(E)* *un sottopiano.*

Dim. Supponiamo che la sottostruttura chiusa $(\mathcal{P}', \mathcal{L}')$ contenga quattro punti a tre a tre non allineati, allora per la Def. 2.2 è un sottopiano, cioè di tipo (E).

Supponiamo ora che $(\mathcal{P}', \mathcal{L}')$ non contenga un quadrangolo ma contenga un triangolo PBC. Se almeno due fra le rette PB, PC e BC contengono punti diversi da P, B e C allora $(\mathcal{P}', \mathcal{L}')$ contiene un quadrangolo, quindi possiamo suppore $\mathcal{P}' \subset BC$ e si vede facilmente che $(\mathcal{P}', \mathcal{L}')$ è di tipo (D$_i$).

Supponiamo ora che $(\mathcal{P}', \mathcal{L}')$ non contenga un triangolo ma contenga almeno 2 punti A, B e quindi la retta $l = AB$. I rimanenti punti di $(\mathcal{P}', \mathcal{L}')$ dovranno appartenere ad AB e le rimanenti rette di $(\mathcal{P}', \mathcal{L}')$ passare tutte per uno stesso punto di AB. La configurazione è di tipo (C$_{ij}$) o (Br$_i$) a seconda che contenga o non contenga rette diverse da l. Se contiene un unico punto è di tipo (Bp$_i$) mentre se non ne contiene è di tipo (A). Utilizzando la dualità si completa la dimostrazione. ■

Sia α una collineazione di Π, denotiamo con $Fix(\alpha) = (\mathcal{P}(\alpha), \mathcal{L}(\alpha))$ l'insieme dei punti e delle rette che sono lasciati fissi da α.

Proposizione 2.4 *$Fix(\alpha)$ è una sottostruttura chiusa di* Π.

Dim. Siano A e B due punti distinti di $Fix(\alpha)$. Poichè α conserva l'incidenza si ha $(AB)^\alpha = A^\alpha B^\alpha = AB$, da cui $AB \in Fix(\alpha)$. In maniera duale si prova che se due rette distinte $l, m \in Fix(\alpha)$ allora $l \cap m \in Fix(\alpha)$. Quindi $Fix(\alpha)$ è una sottostruttura chiusa. ■

E' ragionevole pensare che la conoscenza di $Fix(\alpha)$ possa dare informazioni circa l'azione di α su Π, specialmente quando $Fix(\alpha)$ è, in un certo senso, ampia rispetto a Π. Approfondiremo questi aspetti nel seguito

Definizione 2.5 *Un sottoinsieme $\mathcal{B}$ di punti e rette di un piano proiettivo Π è detto un* ***sottoinsieme di Baer*** *se ogni elemento di Π è incidente con almeno un elemento di $\mathcal{B}$.Un sottoinsieme di Baer che sia anche una sottostruttura chiusa è detto un* ***sottoinsieme di Baer chiuso****.*

Un sottoinsieme di Baer chiuso, che sia anche un sottopiano, è detto **sottopiano di Baer**.

Se α è una collineazione di Π tale che $Fix(\alpha)$ è un sottopiano, diremo che α è una **collineazione planare**. Nel caso in cui $Fix(\alpha)$ sia un sottopiano di Baer, α è detta **collineazione di Baer**.

Osservazione 2.6

Se Π_0 è un sottopiano di Π contenente tutti i punti di una retta l di Π allora $\Pi_0 = \Pi$. Chiaramente $\Pi_0 \subset \Pi$. Proviamo allora il viceversa considerando un punto A di Π e due punti, B e C di Π_0 tali che $AB \neq AC$. Poniamo $X = AB \cap l$ e $Y = AC \cap l$, allora $X, Y \in \Pi_0$ e quindi anche $A \in \Pi_0$ essendo $A = BX \cap CY$.

Proposizione 2.7 *In un piano proiettivo Π, un sottoinsieme di Baer chiuso è un sottopiano di Baer o consiste di una retta l, e di tutti i punti incidenti ad essa e di un punto V e tutte le rette incidenti ad esso. Tali sottostrutture sono massimali in Π.*

Dim. Proviamo inizialmente che se $\mathcal{B}$ è un sottoinsieme di Baer chiuso allora è un sottopiano di Baer o consiste di una retta l, e di tutti i punti incidenti ad essa, insieme con un punto V e tutte le rette incidenti ad esso. Proveremo poi che $\mathcal{B}$ è massimale.

Se $\mathcal{B}$ è chiuso ed è un sottopiano, allora è un sottopiano di Baer.

Supponiamo ora che $\mathcal{B}$ sia un sottoinsieme di Baer chiuso e che non sia un sottopiano, allora $\mathcal{B}$ non può contenere un quadrangolo.

I caso. $\mathcal{B}$ contiene un triangolo ABC.

Poichè $\mathcal{B}$ non contiene un quadrangolo, un punto di $\mathcal{B}$ distinto da A, B, C sarà allineato con due dei tre vertici del triangolo, ad esempio B e C. Sia D un generico punto della retta BC diverso da B e C, m sia una generica retta per D distinta da BC e AD. Poichè $\mathcal{B}$ è un sottoinsieme di Baer m contiene un punto X di $\mathcal{B}$. Se $X \neq D$ allora il quadrangolo $ABXD$ appartiene a $\mathcal{B}$ contro l'ipotesi. Quindi $X = D$ da cui segue che $\mathcal{B}$ consiste di tutti i punti della retta BC insieme con A. Poichè $\mathcal{B}$ è una sottostruttura chiusa, anche il fascio di rette per A deve appartenere a $\mathcal{B}$.

II caso. $\mathcal{B}$ non contiene alcun triangolo.

Per ipotesi quindi, tutti i punti di $\mathcal{B}$ giacciono su una retta l e tutte le rette di $\mathcal{B}$ concorrono in un punto A. Poichè ogni punto di Π è su di una retta di $\mathcal{B}$, $\mathcal{B}$ contiene più di una retta. A è quindi l'intersezione di almeno due rette della sottostruttura chiusa $\mathcal{B}$,

da cui $A \in \mathcal{B}$ è un punto di l. Sia D un qualsiasi punto di l e sia m una generica retta di Π passante per D e distinta da l. Poichè $\mathcal{B}$ è un sottoinsieme di Baer, m deve contenere un punto di $\mathcal{B}$. Questo punto deve essere D perchè tutti i punti di $\mathcal{B}$ giacciono su l. Essendo D un generico punto di l, possiamo concludere che ogni punto di l appartiene a $\mathcal{B}$. In modo duale si prova che ogni retta per A appartiene a $\mathcal{B}$.

Proviamo ora che $\mathcal{B}$ è una sottostruttura di Π massimale. Sia $\mathcal{C}$ una sottostruttura chiusa che contiene $\mathcal{B}$ ed un ulteriore punto X non appartenente a $\mathcal{B}$, allora $\mathcal{C}$ contiene un quadrangolo, infatti:

se $\mathcal{B}$ è un sottopiano esso contiene un quadrangolo e di conseguenza anche $\mathcal{C}$ contiene un quadrangolo. Supponiamo che $\mathcal{B}$ consista di una retta l, e di tutti i punti incidenti ad essa, insieme con un punto V e tutte le rette incidenti ad esso con $V \notin l$. Allora consideriamo la retta VX e sia $Y = VX \cap l$, consideriamo poi due punti $A, B \in l$ con $A \neq Y \neq B$. Si verifica facilmente che $ABXV$ è un quadrangolo di $\mathcal{C}$. Supponiamo infine che $\mathcal{B}$ consista di una retta l, e di tutti i punti incidenti ad essa, insieme con un punto V e tutte le rette incidenti ad esso con $V \in l$. Il punto $X \notin l$ essendo un punto di $\mathcal{C}$ che non sta in $\mathcal{B}$. Le rette per X e per un punto di l stanno in $\mathcal{C}$ essendo $\mathcal{C}$ una configurazione chiusa. Consideriamo due rette m, t per X diverse dalla retta XV ed una retta s per V. Siano A, B due punti tali che $A = m \cap s$ e $B = t \cap l$. Si verifica facilmente che $AXBV$ è un quadrangolo di $\mathcal{C}$.

In definitiva, qualunque sia la scelta di $\mathcal{B}$, abbiamo che $\mathcal{C}$ contiene un quadrangolo e quindi $\mathcal{C}$ è un sottopiano di Π.

Se $\mathcal{B}$ non è un sottopiano allora $\mathcal{C}$ è un sottopiano che contiene tutti i punti di una retta di Π e per l'osservazione precedente si ha che $\mathcal{C} = \Pi$.

Se $\mathcal{B}$ è un sottopiano di Baer, per definizione, ogni retta di Π contiene un punto di $\mathcal{B}$. Quindi, in particolare, ogni retta per X contiene un punto di $\mathcal{B}$. Ogni retta per X, contenendo almeno due punti di $\mathcal{C}$, è una retta di $\mathcal{C}$. Allora $\mathcal{C}$ è un sottopiano contenente tutte le rette per un fissato punto di Π. Per dualità di nuovo $\mathcal{C} = \Pi$. ■

Teorema 2.8 ***(Bruck)*** *Sia Π un piano proiettivo finito di ordine n. Se Π_0 è un sottopiano di Π di ordine m, allora $n = m^2$ oppure $n \geq m^2 + m$.*

Dim. Sia l una retta di Π_0. Allora l contiene $m + 1$ punti di Π_0 e quindi, $n + 1 - (m + 1) = n - m$ sono i punti di l che appartengono a Π ma non a Π_0. Poichè due generiche rette di Π_0 si intersecano sempre in un punto di Π_0 e poichè Π_0 ha $m^2 + m + 1$ rette, esistono $(m^2 + m + 1)(n - m)$ punti di $\Pi - \Pi_0$ che sono incidenti con una retta di Π_0. Quindi in Π ci sono almeno $m^2 + m + 1 + (m^2 + m + 1)(n - m)$ punti. Risulta:
$n^2 + n + 1 \geq m^2 + m + 1 + (m^2 + m + 1)(n - m)$,
$n^2 + n + 1 \geq m^2 n - m^3 + mn + n + 1$,
$0 \geq m^2 n - m^3 + mn - n^2$,
$0 \geq (m^2 - n)(n - m)$.

Ma $n - m > 0$ quindi $n \geq m^2$.

Osserviamo che se $n = m^2$, allora $n^2+n+1 = m^2+m+1+(m^2+m+1)(n-m)$; cioè ogni punto di Π è incidente ad una retta di Π_0 e in modo duale ogni retta di Π incontra Π_0 in un punto. In questo caso Π_0 è un sottopiano di Baer.

Supponiamo allora che $n \neq m^2$. Allora esiste un punto A di Π che non è incidente con alcuna retta di Π_0. Quindi ogni retta per A contiene al più un punto di Π_0. Il numero totale delle rette per A è almeno uguale al numero totale dei punti di Π_0. Da ciò segue che $n + 1 \geq m^2 + m + 1$ ossia $n \geq m^2 + m$. ■

Definizione 2.9 *Una* ***quasiprospettività*** *di un piano proiettivo* Π *è una collinea zione* α *tale che* $Fix(\alpha)$ *è un sottoinsieme di Baer chiuso.*

Se $Fix(\alpha)$ è un sottopiano di Baer la collineazione α è detta *collineazione di Baer.* Se $Fix(\alpha)$ consiste di una retta l e tutti i punti su di essa insieme ad un punto V e tutte le rette per esso, α è detta una (V, l)-*prospettività* o una (V, l)-*collineazione centrale.* V è il *centro* di α ed l è il suo *asse.*

Sia α una (V, l)-prospettività, se $V \in l$, α è detta una **elazione**; se $V \notin l$, α è detta una **omologia**.

Osservazione 2.10

Sia α una omologia di asse l e centro V, X un punto di Π non appartenente ad l con $X \neq V$ osserviamo che:

1. la retta VX è lasciata fissa da α e quindi i punti X ed X^α sono sempre allineati con il centro V;

2. nota la coppia (X, X^α) l'omologia α, se esiste, è univocamente determinata, infatti: sia Y un generico punto di Π non allineato con X e X^α e sia $XY \cap l = A$. Da $Y = VY \cap XA$ segue $Y^\alpha = (VY)^\alpha \cap (XA)^\alpha = VY \cap X^\alpha A$.

Nel caso di una elazione α di asse l e centro V valgono proprietà analoghe a quelle viste nel caso di una omologia.

Nel seguito indicheremo l'ordine di una collineazione α con il simbolo $o(\alpha)$.

Osservazione 2.11 *Sia* G *un sottogruppo di* $Aut(\Pi)$ *che consiste di* (V, l)*-omologie, allora* $|G| \mid (n-1)$.

Infatti: sia X un punto di Π con $X \notin l$ e $X \neq V$ e sia $\alpha \in G_X$. $Fix(\alpha)$ è quindi un sottoinsieme di Baer chiuso unito ad un punto X che non gli appartiene, cioè $Fix(\alpha) = \Pi$

da cui $\alpha = 1$. Sia $A = VX \cap l$, essendo $G_X = \langle 1 \rangle$, G è semiregolare su $AV \setminus \{A, V\}$ con $|AV \setminus \{A, V\}| = n - 1$, cioè $\left|X^G\right| \mid (n-1)$. Da $|G| = |G_X| \left|X^G\right|$ segue che$|G| \mid (n-1)$.

In particolare se α è una (V, l)-omologia allora $o(\alpha) \mid (n-1)$.

Analogamente si prova che se G è un sottogruppo di $Aut(\Pi)$ che consiste di (V, l)-elazioni di $Aut(\Pi)$ allora $|G| \mid n$.

In particolare se α è una (V, l)-elazione allora $o(\alpha) \mid n$.

Infine sia G un sottogruppo delle collineazioni di Baer che fissano lo stesso sottopiano Π_0. Sia s una retta di Π_0 ed X un punto di s non appartenente a Π_0. Anche in questo caso $G_X = \langle 1 \rangle$, G è semiregolare sui punti di s non appartenenti a Π_0 che sono $n - m$ e quindi $|G| \mid n - m$ con $m = \sqrt{n}$.

In particolare se α è una collineazione di Baer allora $o(\alpha) \mid n - \sqrt{n}$.

Sia Π un piano proiettivo. Π è detto (V, l)-**transitivo** se, per ogni scelta di due punti distinti A, B allineati con V, distinti da V e non giacenti sull'asse esiste una (V, l)-prospettività α in $Aut(\Pi)$ con $A^\alpha = B$.

Negli anni '50 è stata proposta una classificazione dei piani proiettivi in base alle coppie punto-retta (V, l) del piano rispetto alle quali il piano sia (V, l)-transitivo. Questa famosa classificazione è dovuta a Lenz e Barlotti. Originariamente Lenz considerò solo le coppie punto-retta incidenti e successivamente Barlotti considerò sia le coppie punto-retta incidenti che quelle non incidenti.

Notazione

Se $G \leq Aut(\mathcal{P}, \mathcal{L})$, $V \in \mathcal{P}$ e $l \in \mathcal{L}$, allora $G(V)$ denota il sottogruppo di G di tutte le prospettività con centro in V, mentre $G(l)$ denota il sottogruppo di G di tutte le prospettività con asse l. Inoltre $G(V, l) = G(V) \cap G(l)$.

Lemma 2.12 *Sia Π un piano proiettivo finito di ordine n. Allora:*

1. *Π è (V, l)-transitivo per $V \in l$ se e solo se $|G(V, l)| = n$;*
2. *Π è (V, l)-transitivo per $V \notin l$ se e solo se $|G(V, l)| = n - 1$.*

Dim. Dire che Π è (V, l)-transitivo per $V \in l$ equivale a dire che $\left|X^{G(V,l)}\right| = n$ e quindi $|G(V, l)| = \left|X^{G(V,l)}\right|$. Analogamente si procede nel caso delle omologie. ■

Teorema 2.13 *Sia Π un piano proiettivo. Se $\alpha \neq 1$ è una collineazione che fissa una retta l punto per punto, allora esiste un punto V tale che α fissa tutte le rette per V. Inoltre α non fissa altri punti o rette di Π.*

Dim. Poichè ogni retta di Π interseca l, possiamo dire che ogni retta di Π è incidente ad un punto di $Fix(\alpha)$. Sia B un punto non appartenente ad l. Se $B^\alpha = B$ allora la retta che congiunge B ad un qualsiasi punto di l è fissata da α. In questo caso B è quindi incidente ad una retta di $Fix(\alpha)$. Se $B^\alpha \neq B$ allora poniamo $P = BB^\alpha \cap l$. Ora $(PB)^\alpha = P^\alpha B^\alpha = PB^\alpha$ (poichè α fissa tutti i punti di l). Quindi da $PB = PB^\alpha$ segue $(PB)^\alpha = PB$ e B risulta appartenere ad una retta di $Fix(\alpha)$. Abbiamo così provato che $Fix(\alpha)$ è un sottoinsieme di Baer ed è una sottostruttura chiusa. Poichè $Fix(\alpha)$ contiene tutti i punti di l allora $Fix(\alpha)$ consiste della retta l, e di tutti i punti incidenti ad essa, insieme con un punto V e tutte le rette incidenti ad esso. ■

Proposizione 2.14 *Sia Π un piano proiettivo ed α una (V,l)-prospettività di Π. Valgono le seguenti proprietà:*

1. *Se β è una collineazione di Π, allora $\beta^{-1}\alpha\beta$ è una (V^β, l^β)-prospettività.*

2. *Se $\alpha \neq 1$ e β è una collineazione che commuta con α, allora $V^\beta = V$ e $l^\beta = l$.*

Dim. *1.* Sia X un generico punto di l^β. Allora $X^{\beta^{-1}}$ appartiene ad l, da cui segue che $X^{\beta^{-1}\alpha} = X^{\beta^{-1}}$. Quindi $X^{\beta^{-1}\alpha\beta} = X$ e $\beta^{-1}\alpha\beta$ fissa l^β punto per punto. In modo analogo si prova che $\beta^{-1}\alpha\beta$ fissa tutte le rette per V^β e quindi $\beta^{-1}\alpha\beta$ è una (V^β, l^β)-prospettività.

2. Se $\alpha\beta = \beta\alpha$ allora $\alpha = \beta^{-1}\alpha\beta$ è una (V,l)-prospettività e contemporaneamente una (V^β, l^β)-prospettività. Da ciò segue che $V^\beta = V$ e $l^\beta = l$. ■

Corollario 2.15 *Se G è un gruppo di collineazioni di un piano proiettivo Π, allora per ogni $\gamma \in G$ e per ogni coppia punto-retta (V,l), si ha $G(V,l)^\gamma = G(V^\gamma, l^\gamma)$.*

Dim. La dimostrazione segue immediatamente dalla Prop.2.14 se si tiene conto del fatto che $\alpha \in G(V,l)^\gamma$ se e solo se $\alpha = \gamma^{-1}\beta\gamma$ con β (V,l)-prospettività di Π. ■

Se $o(\alpha) = 2$ allora diremo che α è una *collineazione involutoria.*

Teorema 2.16 *Ogni collineazione involutoria α è una quasiprospettività.*

Dim. Vogliamo provare che $Fix(\alpha)$ è un sottoinsieme di Baer chiuso. Sia A un punto di Π che non appartiene a $Fix(\alpha)$, ossia tale che $A^\alpha \neq A$. Allora $(AA^\alpha)^\alpha = A^\alpha A^{\alpha^2} = A^\alpha A$ implica che A appartiene ad una retta di $Fix(\alpha)$. In maniera duale ogni retta non fissata da α contiene un punto fisso.

Sia B un punto fissato da α. Se α fissa un altro punto C con $C \neq B$, allora α fissa la retta BC e B appartiene ad una retta di $Fix(\alpha)$. Proviamo allora che α fissa almeno due punti. Sia l una retta non fissa (esiste certamente perchè altrimenti α sarebbe l'identità) che non contiene B. Sia $C = l \cap l^\alpha$, allora $C^\alpha = l^\alpha \cap l^{\alpha^2} = l^\alpha \cap l = C$. Quindi α deve fissare almeno due punti. In maniera duale possiamo dire che α deve fissare almeno due rette e quindi la tesi è provata. ■

Osservazione 2.17 *Sia α una collineazione involutoria e Π un piano proiettivo di ordine n. Se α non è un'involuzione di Baer allora α è una elazione per n pari ed è una omologia per n dispari. Le involuzioni di Baer possono esistere sia per n pari che per n dispari in quanto $2 \mid n - \sqrt{n}$*

Proposizione 2.18 *Se α è una (A,l)-elazione e β è una (B,l)-elazione entrambe non banali e con $A \neq B$, allora $\alpha\beta$ è una (C,l)-elazione non banale con $C \neq A$ e $C \neq B$.*

Dim. Se $\alpha \in G(A,l)$ e $\beta \in G(B,l)$ allora sicuramente $\alpha\beta$ è una prospettività di asse l. Sia C il centro di $\alpha\beta$, ossia $C^{\alpha\beta} = C$. Supponiamo per assurdo che $C \notin l$. Si noti che $C^\alpha C = AC$ e $C^\alpha C^{\alpha\beta} = C^\alpha C = BC^\alpha$, da cui $BC^\alpha = AC$. Quindi A e B apparterrebbero ad una stessa retta distinta da l e ciò non è possibile perchè entrambi i punti appartengono ad l. Il centro C di $\alpha\beta$ appartiene pertanto alla retta AB. Supponiamo per assurdo sia $C = A$. Sia D un punto non appartenente ad l, allora $DD^\alpha \cap l = A$, $DD^{\alpha\beta} \cap l = C$ e $D^\alpha D^{\alpha\beta} \cap l = B$. Se $C = A$ allora $D^{\alpha\beta} = D^\alpha$ ma ciò è assurdo perchè $D^\alpha \notin l$ e quindi non può essere fissato da β. Analogamente si prova che $C \neq B$ e quindi la tesi. ■

Corollario 2.19 *Sia G un gruppo di collineazioni di un piano proiettivo Π. $G(l,l) = \bigcup_{P \in l} G(P,l)$ è un sottogruppo di G.*

Teorema 2.20 *Sia Π un piano proiettivo e G un gruppo di collineazioni di Π. Se $G(l,l)$ contiene due elazioni con centri distinti allora $G(l,l)$ è abeliano. Tutti i suoi elementi non identici hanno lo stesso ordine (infinito o primo). Inoltre, se Π è finito d'ordine n allora tutti gli elementi non identici di $G(l,l)$ hanno ordine lo stesso primo p, con p divisore di n.*

Dim. Proviamo innanzitutto che due elazioni in $G(l,l)$ con centri distinti commutano.

Sia $\alpha \in G(A,l)$ e $\beta \in G(B,l)$ con $A \neq B$, $\alpha \neq 1$ e $\beta \neq 1$. Consideriamo il commutatore di α e β: $[\alpha,\beta] = \alpha^{-1}\beta^{-1}\alpha\beta$. Allora $\alpha^{-1}\beta^{-1}\alpha\beta = \alpha^{-1}(\beta^{-1}\alpha\beta)$ con $\beta^{-1}\alpha\beta \in G(A^\beta, l^\beta) = G(A,l)$ e $\alpha^{-1} \in G(A,l)$, da cui $\alpha^{-1}\beta^{-1}\alpha\beta \in G(A,l)$. D'altra parte $\alpha^{-1}\beta^{-1}\alpha\beta = (\alpha^{-1}\beta^{-1}\alpha)\beta$ con $\alpha^{-1}\beta^{-1}\alpha \in G(B^\alpha, l^\alpha) = G(B,l)$ e $\beta \in G(B,l)$ da cui $\alpha^{-1}\beta^{-1}\alpha\beta \in G(B,l)$. Possiamo allora dire che

$$\alpha^{-1}\beta^{-1}\alpha\beta \in G(A,l) \cap G(B,l) = \langle 1 \rangle$$

da cui $\alpha\beta = \beta\alpha$. Per provare che $G(l,l)$ è abeliano ci resta da provare che due elazioni con lo stesso centro commutano.

Siano α_1, α_2 due (A,l)-elazioni non banali in G. Per ipotesi esiste una (B,l)-elazione $\beta \in G$ con $A \neq B$. Allora per quanto appena provato $\alpha_1\beta = \beta\alpha_1$ e $\alpha_2\beta = \beta\alpha_2$. Il

centro di $\alpha_1\beta$ è diverso da A, da cui $\alpha_1\beta$ commuta con α_2. Quindi $(\alpha_2\alpha_1)\beta = \alpha_2(\alpha_1\beta) = (\alpha_1\beta)\alpha_2 = \alpha_1(\beta\alpha_2) = \alpha_1(\alpha_2\beta) = (\alpha_1\alpha_2)\beta$ da cui $\alpha_1\alpha_2 = \alpha_2\alpha_1$, ossia $G(l,l)$ è abeliano.

Supponiamo che $G(l,l)$ contenga un'elazione di ordine finito (se così non fosse allora tutti gli elementi di $G(l,l)$ avrebbero periodo infinito). Allora $G(l,l)$ contiene una (C,l)-elazione γ di ordine un primo p. Sia $\delta \in G(D,l)$ con $D \in l$ e $D \neq C$. Poichè $\gamma\delta = \delta\gamma$, $(\gamma\delta)^p = \gamma^p\delta^p = \delta^p \in G(D,l)$. $\gamma\delta \in G(E,l)$ per qualche $E \in l$ con $E \neq D$. Quindi $(\gamma\delta)^p \in G(E,l) \cap G(D,l)$, ossia $(\gamma\delta)^p = 1 = \delta^p$. Abbiamo così provato che ogni elazione in G con asse l e centro distinto da C ha ordine p. Sia $\gamma' \in G(C,l)$, $(\gamma'\delta)^p = \gamma'^p\delta^p = \gamma'^p$ e quindi $o(\gamma') = p$. Quindi se α è una generica elazione di $G(l,l)$, allora $o(\alpha) = p$ e $p \mid n$. ■

Lemma 2.21 *Sia* Π *un piano proiettivo e* G *un gruppo di collineazioni di* Π. *Se* $|G(P,l)| > 1$ *e* $|G(A,m)| > 1$ *con* $A, P \in l$ *e* $A \in m$, *allora* $|G(A,l)| > 1$.

Dim. Se $l = m$ o $A = P$ la tesi segue banalmente. Supponiamo allora $l \neq m$ e $A \neq P$. Consideriamo le collineazioni $\alpha \in G(P,l)$ e $\beta \in G(A,m)$, entrambe non identiche, e sia $\gamma = [\alpha,\beta] = \alpha^{-1}\beta^{-1}\alpha\beta$. Vogliamo provare che $\gamma \in G(A,l)$ e $\gamma \neq 1$. Chiaramente essendo $A^\alpha = A = A^\beta$ e $l^\alpha = l = l^\beta$, si ha $A^\gamma = A$ e $l^\gamma = l$. Sia ora X un generico punto di l, allora $X^{\alpha^{-1}} = X$, da cui $X^\gamma = X^{\beta^{-1}\alpha\beta} = (X^{\beta^{-1}\alpha})^\beta$. Ma $X^{\beta^{-1}}$ è sull'asse l di α e quindi da $X^{\beta^{-1}\alpha} = X^{\beta^{-1}}$ segue $X^{\beta^{-1}\alpha\beta} = X$. Abbiamo così provato che γ è una prospettività di asse l. Analogamente si prova che γ fissa tutte le rette per A. Per completare la dimostrazione dobbiamo verificare che γ è non identica. Se $\alpha\beta = \beta\alpha$ allora β fissa il centro P di α, ma questo è assurdo perchè β fissa solo i punti che appartengono al suo asse m. Quindi $\alpha\beta \neq \beta\alpha$ e $\gamma \neq 1$. ■

Proposizione 2.22 *Sia* Π *un piano proiettivo di ordine* n *e* G *un gruppo di collineazioni di* Π.

1. *Se* l, m *sono rette di* Π *con* $m \neq l$ *allora* $(G(l,l))_m = G(A,l)$ *con* $A = l \cap m$.
2. *Se* $|G(l,l)| > n$ *allora* $|G(B,l)| > 1$ *per ogni* $B \in l$.
3. $\left|m^{G(l,l)}\right|$ *divide* n *per ogni retta* m *del piano* Π.

Dim. 1. Banalmente $G(A,l) \leq (G(l,l))_m$. Proviamo il viceversa: sia $\alpha \in (G(l,l))_m$, da $m^\alpha = m$ segue che α fissa $l \cap m = A$. Quindi $\alpha \in G(A,l)$.

2. $|G(l,l)| = \left|m^{G(l,l)}\right| |(G(l,l))_m|$ con m retta di Π distinta da l.

Sia $B = m \cap l$; per quanto appena provato $(G(l,l))_m = G(B,l)$ e quindi $|G(l,l)| = \left|m^{G(l,l)}\right| |G(B,l)|$. Poichè m è una retta passante per B distinta da l, $\left|m^{G(l,l)}\right| \leq n$ e quindi da $|G(l,l)| > n$ segue $|G(B,l)| > 1$.

3. $\frac{|G(l,l)|}{\left|m^{G(l,l)}\right|} = |G(A,l)|$ per ogni retta m passante per A. La cardinalità dell'orbita $m^{G(l,l)}$ è quindi la stessa per ogni retta m per A distinta da l . Poichè le rette per A distinte da l sono n si ha che $\left|m^{G(l,l)}\right|$ divide n. ■

Proposizione 2.23 *Sia G un gruppo di collineazioni del piano proiettivo Π. Sia $\alpha \in G(A,a)$ e $\beta \in G(B,b)$ con $\alpha, \beta \neq 1$; supponiamo inoltre che $a \neq b$ e $A \neq B$. Allora $\alpha\beta$ è una prospettività se e solo se α e β sono omologie tali che $B \in a$, $A \in b$ e $X^\alpha = X^{\beta^{-1}}$ per ogni $X \in AB$. In questo caso $\alpha\beta$ è un'omologia con centro $a \cap b$ ed asse AB.*

Dim. Sia X un punto del piano fissato da $\alpha\beta$, cioè $X^{\alpha\beta} = X$. Se $X^\alpha \neq X$ allora $X, X^\alpha \neq A$. Poichè punti corrispondenti sono allineati con il centro si ha $X^\alpha \in XA$ e $XA = X^\alpha X$, inoltre $(X^\alpha)^\beta = X$. Anche i punti X^α e $(X^\alpha)^\beta$, essendo corrispondenti rispetto a β, sono allineati con il centro, quindi la retta $X^\alpha B = X^\alpha (X^\alpha)^\beta = X^\alpha X = XA$ da cui $X \in AB$. Abbiamo così provato che tutti i punti fissati da $\alpha\beta$ stanno sulla retta AB nell'ipotesi che $X^\alpha \neq X$. Supponiamo allora che $X^\alpha = X$ e $X \notin AB$, ossia $X \neq A$. Se X è fissato da α ed è diverso dal centro di α allora $X \in a$. Da $X^\beta = (X^\alpha)^\beta = X$ segue che X è fissato da β e $X \neq B$ quindi $X \in b$. In conclusione $X \in a \cap b$. I punti fissati da $\alpha\beta$, diversi da $a \cap b$, appartengono allora alla retta AB.

Sia ora $X \in AB$, da $X^{\alpha\beta} = X$ segue $X^\alpha = X^{\beta^{-1}}$ per ogni $X \in AB$. Resta da provare che $A \in b$ e $B \in a$. Sia $X = A$. Si ha $A^\beta = (A^\alpha)^\beta$, essendo A il centro di α e $(A^\alpha)^\beta = (A^{\beta^{-1}})^\beta$ poichè $A \in AB$ quindi $A^\beta = (A^\alpha)^\beta = (A^{\beta^{-1}})^\beta = A$. Il punto A è fissato da β ed è distinto dal suo centro B quindi appartiene all'asse di β, ossia $A \in b$. Analogamente si prova che $B \in a$. Osserviamo che α e β sono necessariamente delle omologie perchè se fossero elazioni allora si avrebbe $B \in b$ e $A \in a$ il che è impossibile. ■

Teorema 2.24 *Siano $\alpha \in G(A,a)$ e $\beta \in G(B,b)$ due omologie non banali con assi differenti (centri differenti). Allora α e β commutano se e solo se $A \in b$ e $B \in a$. In particolare, se α e β commutano, allora esse hanno centri e assi differenti.*

Dim. Supponiamo $\alpha\beta = \beta\alpha$, allora β fissa il centro A di α da cui segue che $A = B$ oppure $A \in b$. Se $A = B$ da $a^\beta = a$ segue $a = b$, contro l'ipotesi, oppure $B \in a$. Se fosse $B \in a$ allora $A = B \in a$ contro l'ipotesi che α sia un'omologia. In conclusione deve essere $A \in b$. Con un procedimento analogo si dimostra che $B \in a$. Viceversa, supponiamo che $A \in b$ e $B \in a$ e consideriamo $\beta^{-1}\alpha\beta$ che è una (A^β, a^β)-omologia. Da $A \in b$ segue $A^\beta = A$ e da $B \in a$ segue $a^\beta = a$. Quindi $\beta^{-1}\alpha\beta$ è una (A,a)-omologia. Allora $[\alpha,\beta] = \alpha^{-1}(\beta^{-1}\alpha\beta)$ è una (A,a)-omologia in quanto prodotto di due (A,a)-omologie. Analogamente si prova che $[\alpha,\beta] = (\alpha^{-1}\beta^{-1}\alpha)\beta$ è una (B,b)-omologia. Quindi

$$[\alpha,\beta] \in G(A,a) \cap G(B,b) = \langle 1 \rangle$$

ossia $\alpha\beta = \beta\alpha$. ■

Proposizione 2.25 *Siano $\alpha \in G(A,a)$ e $\beta \in G(B,b)$ due omologie involutorie con assi differenti (centri differenti). Allora $\alpha\beta$ è un'omologia involutoria se e solo se $A \in b$ e $B \in a$. Se $\alpha\beta$ è un'omologia involutoria, allora valgono le seguenti condizioni:*

1. *$\alpha\beta$ è una $(a \cap b, AB)$- omologia;*

2. *α è l'unica (A, a)-omologia involutoria;*

3. *ogni collineazione che fissa A e a centralizza α.*

Dim. Se $\alpha\beta$ è un'omologia involutoria, allora da $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta = \alpha\beta\alpha\beta = (\alpha\beta)^2 = 1$ segue $\alpha\beta = \beta\alpha$ e, per il Teorema appena dimostrato, si ha $A \in b$ e $B \in a$. Viceversa, se $A \in b$ e $B \in a$, allora $\alpha\beta = \beta\alpha$ e quindi $(\alpha\beta)^2 = \alpha^2\beta^2 = 1$ ossia $\alpha\beta$ è una omologia involutoria.

1. Dal Teorema precedente segue che $\alpha\beta$ è una $(a \cap b, AB)$- omologia.

2. Sia α' una (A, a)-omologia involutoria diversa da α. Allora $\alpha'\beta$ è una $(a \cap b, AB)$-omologia involutoria. $\alpha'\beta$ ha asse AB e quindi $X^{\alpha'\beta} = X$ per ogni $X \in AB$. D'altra parte $X^{\alpha} = X^{\beta}$ per ogni $X \in AB$. Ne segue $X^{\alpha'} = X^{\alpha}$, ossia $X^{\alpha'\alpha} = X$ per ogni $X \in AB$. Allora $\alpha'\alpha$ è una (A, a)-omologia che fissa anche tutti i punti della retta AB, quindi $\alpha'\alpha = 1$ da cui $\alpha' = \alpha$.

3. Sia $\gamma \in G$, allora $\gamma^{-1}\alpha\gamma \in G(A^{\gamma}, a^{\gamma}) = G(A, a)$ poichè per ipotesi γ fissa A e a. Essendo $\gamma^{-1}\alpha\gamma$ una (A, a)-omologia involutoria deve necessariamente coincidere con α. Da $\gamma^{-1}\alpha\gamma = \alpha$ segue $\alpha\gamma = \gamma\alpha$. ■

Corollario 2.26 *Sia $S \leq G$ un 2-gruppo abeliano elementare di ordine strettamente maggiore di 4, i cui elementi non identici siano tutti omologie (involutorie). Allora S è un sottogruppo di omologie di stesso centro e asse.*

Dim. Supponiamo $|S| \gneqq 4$ e $S \not\leq G(D, d)$. Allora esistono in S almeno due omologie, α e β, con assi distinti (centri distinti). Poichè S è abeliano $\alpha\beta = \beta\alpha$ e quindi se $\alpha \in G(A, a)$ e $\beta \in G(B, b)$ si ha che $\alpha\beta$ è una $(a \cap b, AB)$- omologia. Poichè $|S| \gneqq 4$ esiste una (F, f)-omologia $\gamma \in S$, con $o(\gamma) = 2$ e $\gamma \notin \langle \alpha, \beta \rangle$. Poichè γ centralizza α, β e $\alpha\beta$ allora γ fissa A, B e C con $C = a \cap b$. Ne segue che uno fra i punti A, B e C è il suo centro e una fra le rette a, b e AB è il suo asse. Ciò è contro la Prop. 2.25 punto 2. ■

Osserviamo che se $\alpha \in G(l)$ ed è una elazione allora non fissa alcun punto di Π_l mentre se α è una omologia fissa un punto affine che è il centro dell'omologia. Con i risultati che seguono ci proponiamo di analizzare la struttura del gruppo $G(l)$.

Ricordiamo la definizione di *sottogruppo normale*:

$$N \trianglelefteq G \Leftrightarrow g^{-1}Ng = N \quad \forall g \in G$$

Proposizione 2.27 *Sia $G \leq Aut(\Pi)$ ed l una retta di Π. Allora $G(l, l) \trianglelefteq G(l)$.*

Dim. Sia $\gamma \in G(l)$ ed $\alpha \in G(l, l)$. Allora α è una (V, l)-elazione con $V \in l$ e $\gamma^{-1}\alpha\gamma$ è una (V^{γ}, l^{γ})-elazione. Poichè γ fissa l puntualmente possiamo dire che $\gamma^{-1}\alpha\gamma$ è una (V, l)-elazione, cioè $\gamma^{-1}\alpha\gamma \in G(l, l)$. ■

Osserviamo che se $G(l,l) = G(l)$ allora in $G(l)$ ci sono solo elazioni.

Se invece $G(l,l) = \langle 1 \rangle$, ma $G(l) \neq \langle 1 \rangle$ allora in $G(l)$ ci sono solo omologie e vedremo nel seguito che in questo caso tutte le omologie devono avere lo stesso centro.

Se infine $\langle 1 \rangle \neq G(l,l) \neq G(l)$ allora in $G(l)$ esistono omologie di asse l e centri distinti. Infatti:

per ipotesi esiste sicuramente una (V,l)-omologia α ed una elazione τ con $\tau \neq 1$. Allora $\tau^{-1}\alpha\tau$ è una (V^τ, l^τ)-omologia, cioè una (V^τ, l)-omologia. Poichè τ non fissa punti che non appartengono ad l si ha $V \neq V^\tau$. In $G(l)$ esistono quindi omologie di asse l e centri distinti.

Proposizione 2.28 *Siano α e β due omologie involutorie con lo stesso asse l ma differenti centri A e B, rispettivamente.*
Allora $\alpha\beta$ è un'elazione in $G(l \cap AB, l)$.

Dim. Sia C il centro di $\alpha\beta$. Chiaramente i punti C, C^α, A sono allineati come pure $B, C^\alpha, C^{\alpha\beta} = C$. Quindi i punti A, B e C sono allineati. Proviamo ora che $\alpha\beta$ non fissa alcun punto fuori di l su AB.Sia $Q \in AB$, $Q \notin l$ e $Q^{\alpha\beta} = Q$. Se fosse $Q^\alpha = Q$ allora $Q = Q^{\alpha\beta} = Q^\beta$ da cui $Q = A = B$ contro l'ipotesi $A \neq B$. Allora $Q^\alpha \neq Q$ e $(Q^\alpha)^{\alpha\beta} = Q^{\alpha^2\beta} = Q^\beta$. Ora $Q^\beta = (Q^{\alpha\beta})^\beta = Q^{\alpha\beta^2} = Q^\alpha$. Da ciò segue che $\alpha\beta$ fissa anche Q^α oltre a Q e quindi $\alpha\beta = 1$, ma ciò è assurdo perchè si avrebbe $\alpha = \beta^{-1} = \beta$ e quindi $A = B$. Abbiamo così provato che $\alpha\beta$ è una elazione di centro $l \cap AB$. ■

Proposizione 2.29 *Se il gruppo $G(l)$ contiene omologie non banali con centri distinti allora per ogni punto $P \notin l$, il gruppo $G(P,l)$ contiene al più una involuzione.*

Dim. Siano ρ e σ due (P,l)-omologie involutorie distinte. Allora anche $\rho\sigma \in G(P,l)$. D'altra parte esiste in $G(l)$ una omologia $\alpha \neq 1$ con centro Q distinto da P. Sia $\tau = \alpha^{-1}\rho\alpha$, si ha che τ è una (P^α, l)-omologia involutoria con $P^\alpha \neq P$. α infatti non può fissare altri punti fuori di l che siano distinti dal suo centro Q. Ora $\rho\tau$ e $\tau\sigma$, essendo prodotto di omologie involutorie di asse l e centri distinti, sono entrambe elazioni di asse l. Quindi $\rho\sigma = \rho\tau \cdot \tau\sigma$ è anch'essa un'elazione. Ciò è compatibile con $\rho\sigma \in G(P,l)$ se e solo se $\rho\sigma = 1$, ossia $\rho = \sigma$. ■

Teorema 2.30 ***(Andrè)*** *Sia $G \leq Aut(\Pi)$ e sia l una retta fissata di Π. I punti $V \in \Pi - \{l\}$ tali che $G(V,l) \neq 1$ sono in un'unica orbita di punti rispetto a $G(l,l)$.*

Dim. Sia $\mathcal{O}$ l'insieme dei punti $V \in \Pi - \{l\}$ tali che $G(V,l) \neq 1$ e siano $V_1, V_2, ..., V_k$ i punti di $\mathcal{O}$. Se $k = 0, 1$ il risultato è banale, possiamo quindi assumere $k > 1$. Notiamo che i punti $V_1, V_2, ..., V_k$ di Π_l sono centri di omologie non banali di G con asse l. Poniamo $h_i = |G(A_i, l)|$ per $i = 1, 2, ..., k$. Allora il numero delle prospettività non banali con asse l è

(1) $|G(l)| = |G(l,l)| + \sum_{i=1}^{k}(h_i - 1)$.

Poichè $1 \in G(l,l)$, $|G(l,l)| \geq 1$, mentre $h_i \geq 2$ per ogni i perchè, oltre all'identità, in $G(V_i, l)$ c'è almeno una omologia non banale, quindi

(2) $|G(l)| \geq 1 + k > k$.

$G(l)$ permuta gli elementi di $\mathcal{O}$ tra loro e non esiste un elemento $\alpha \neq 1$ di $G(l)$ che fissa tutti i punti di $\mathcal{O}$ (se così fosse da $V_i^\alpha = V_i$ per ogni $i = 1, ..., k$ con $k \geq 2$ seguirebbe $\alpha = 1$). Quindi il gruppo di permutazioni indotto su $\mathcal{O}$ è fedele. Se r denota il numero di orbite di $G(l)$ su $\mathcal{O}$ allora, usando il fatto che l'identità fissa k elementi, le omologie fissano un elemento e le altre collineazioni sono libere da punti fissi (esse fissano solo i punti di l mentre $\mathcal{O} \subset \Pi_l$) , abbiamo

(3) $r\,|G(l)| = k + \sum_{i=1}^{k}(h_i - 1)$.

Sottraendo la (1) dalla (3) otteniamo

(4) $(r-1)\,|G(l)| = k - |G(l,l)|$ con $|G(l)| > k$ e $r \geq 1$.

Chiaramente deve essere $r = 1$ e $|G(l,l)| = k$. Quindi si ha un'unica orbita rispetto a $G(l)$ e $k = |G(l,l)| = |G(l,l)_V| \left|V^{G(l,l)}\right|$ con $|G(l,l)_V| = 1$ perchè le elazioni non fissano alcun punto fuori di l. Allora $k = \left|V^{G(l,l)}\right|$, ossia $V^{G(l,l)}$ è un sottoinsieme di $\mathcal{O}$ con la stessa cardinalità di $\mathcal{O}$, quindi $V^{G(l,l)} = \mathcal{O}$ e $G(l,l)$ è transitivo sui punti di $\mathcal{O}$. ■

Se un piano proiettivo Π è (A,l)-transitivo per tutti i punti A di l allora Π è detto un *piano di traslazione* (rispetto alla retta l). l è detta una *retta di traslazione.* Anche il piano affine Π_l è detto *piano di traslazione*.

Si noti che ogni elazione con asse l induce nel piano affine Π_l una collineazione che risulta essere f.p.f. (libera da punti fissi) e che trasforma ogni retta in una ad essa parallela. Una tale collineazione è detta *traslazione*.

Il gruppo $G(l,l)$ delle elazioni agisce semiregolarmente su Π_l in quanto le traslazioni non fissano alcun punto di Π_l.

Se vi sono k omologie non banali ripettivamente di centro $V_1, ..., V_k$ allora, per il risultato appena dimostrato, si ha che $G(l,l)$ agisce regolarmente sull'insieme $\{V_1, ..., V_k\}$ e quindi $|G(l,l)| = k$.

Come conseguenza immediata si ha il seguente risultato:

Corollario 2.31 *Sia* Π *un piano proiettivo finito e siano* α *e* β *due omologie non banali con centri distinti* A *e* B *e stesso asse* l*. Allora* $\langle \alpha, \beta \rangle$ *contiene un'elazione che trasforma* A *in* B*.*

Se Π è un piano di traslazione rispetto alla retta l, allora $|G(l,l)| = n^2$. Siano ora A, B due punti distinti di l. Consideriamo i gruppi $G(A,l)$ e $G(B,l)$, abbiamo visto che $|G(A,l)| = |G(B,l)| = n$. Consideriamo il sottogruppo $G(A,l) \cdot G(B,l)$ di $G(l,l)$, poichè

$G(A,l)\cdot G(B,l)$ ha ordine n^2 possiamo concludere che $G(A,l)\cdot G(B,l)=G(l,l)$ e quindi ogni traslazione del piano si ottiene come prodotto di due traslazioni di fissate direzioni.

Vediamo in che modo: siano ad esempio C, C' due punti del piano e sia $\widetilde{C}=AC\cap BC'$. Poichè C e $\widetilde{C}$ sono allineati con A, esiste una traslazione $\alpha\in G(A,l)$ tale che $C^\alpha=\widetilde{C}$ e analogamente, essendo C' e $\widetilde{C}$ allineati con B esiste una traslazione $\beta\in G(B,l)$ tale che $\widetilde{C}^\beta=C'$. In definitiva esiste la traslazione $\alpha\beta$ che muta C in C'.

Teorema 2.32 *(**Hughes**) Sia Π un piano proiettivo finito di ordine n e sia G un gruppo di collineazioni di Π. Supponiamo esista una retta l ed un punto Q su l tale che $|G(A,l)|=h>1$ per tutti gli A in l, $A\neq Q$. Allora $|G(Q,l)|=n$ cioè Π è (Q,l)-transitivo.*

Dim. Sia $|G(Q,l)|=k$ con $k\geq 1$. Ogni punto di l diverso da Q (in tutto sono n) è il centro di $h-1$ elazioni non banali, Q è il centro di $k-1$ elazioni non banali, quindi

(1) $|G(l,l)|=n(h-1)+(k-1)+1=n(h-1)+k$.

Sia A un punto di l diverso da Q. Se m è una retta per A diversa da l allora $|G(l,l)|=|(G(l,l))_m|\,|mG(l,l)|$. Sappiamo che $(G(l,l))_m=G(A,l)$ e $s=\left|m^{G(l,l)}\right|$ divide n. Quindi $|G(l,l)|=hs$ con $s\mid n$. Segue allora $hs=n(h-1)+k$ divide hn o anche $hn-(n-k)\mid hn$. Ciò implica che $hn-(n-k)=hn$ oppure $hn-(n-k)\leq (hn)/2$. Se $hn-(n-k)\leq (hn)/2$ allora $(hn)/2\leq n-k$. Poichè $h\geq 2$ si ha $\frac{hn}{2}\geq n$ da cui $n\leq n-k$ che è assurdo in quanto $k\geq 1$. Allora deve necessariamente essere $hn-(n-k)=hn$ cioè $n=k$ e $|G(Q,l)|=n$. ■

Corollario 2.33 *Sia Π un piano proiettivo e G un gruppo di collineazioni di Π. Supponiamo esista una retta l tale che $|G(A,l)|=h$, per ogni $A\in l$ con $h>1$, allora Π è un piano di traslazione rispetto alla retta l.*

Dim. Basta considerare, nel Teorema di Hughes, come punto Q il generico punto A di l per ottenere $|G(Q,l)|=n$ per ogni $Q\in l$, da cui segue che Π è un piano di traslazione rispetto alla retta l. ■

Corollario 2.34 *Sia Π un piano proiettivo e G un gruppo di collineazioni di Π. Supponiamo esista una retta l tale che G muta in se l ed è transitivo sui suoi punti e $G(A,l)\neq 1$ per un punto $A\in l$. Allora Π è un piano di traslazione rispetto alla retta l.*

Dim. Sia $B\in l$, poichè G è transitivo sui punti di l, esiste $g\in G$ tale che $A^g=B$ e $G(A,l)^g=G(A^g,l^g)=G(B,l)$ da cui segue $G(B,l)\neq 1$ ed inoltre $G(B,l)$ ha lo stesso ordine di $G(A,l)$. Applicando il Corollario precedente si ha la tesi. ■

Lemma 2.35 *Sia Π un piano proiettivo e sia Π_0 un sottopiano di Π. Se α è una (V,l)-prospettività non identica che muta Π_0 in se, allora $V,l\in\Pi_0$, e α induce una prospettività in Π_0.*

Dim. Sicuramente esistono almeno due punti distinti $A, B \in \Pi_0$ che non appartengono alla retta l. Allora $A^\alpha \in \Pi_0$ ed è allineato con A e V così come $B^\alpha \in \Pi_0$ ed è allineato con B e V. Le rette AA^α e BB^α sono rette di Π_0 per cui $AA^\alpha \cap BB^\alpha = V \in \Pi_0$. Dualmente si prova che $l \in \Pi_0$. ■

Sia $\Pi = (\mathcal{P}, \mathcal{L})$ un piano proiettivo finito di ordine n. Allora considerata una numerazione per i punti $P_1, P_2, ..., P_{n^2+n+1}$ e per le rette $l_1, l_2, ..., l_{n^2+n+1}$, possiamo definire una matrice quadrata $A = (a_{ij})$ di ordine $n^2 + n + 1$ tale che

$$a_{i,j} = \begin{cases} 1 \text{ se } P_i \in l_j \\ 0 \text{ se } P_i \notin l_j \end{cases}$$

La matrice A è detta una *matrice di incidenza* di Π.

Osserviamo che la matrice A, che descrive completamente il piano Π, gode delle seguenti proprietà:

1. ogni riga di A contiene esattamente $n+1$ posizioni uguali ad 1 (ogni punto del piano è incidente ad $n + 1$ rette);

2. ogni colonna A contiene esattamente $n+1$ posizioni uguali ad 1 (ogni retta del piano è incidente ad $n + 1$ punti);

3. fissate la i-sima e la k-sima riga di A, esiste esattamente una colonna che ha 1 nella posizione i e k (per due punti passa una ed una sola retta);

4. fissate la i-sima e la k-sima colonna di A, esiste esattamente una riga che ha 1 nella posizione i e k (due rette distinte si incontrano in uno ed un solo punto).

Proposizione 2.36 *Sia $\mathcal{A}$ una matrice di incidenza di un piano proiettivo finito Π di ordine n. Allora $\mathcal{A}\mathcal{A}^t = n\mathcal{I}_\nu + \mathcal{J}_\nu$, dove $\mathcal{I}_\nu$ è la matrice identica d'ordine ν, $\mathcal{J}_\nu$ è la matrice d'ordine ν con 1 in ogni posizione e $\nu = n^2 + n + 1$. Inoltre la matrice A è invertibile.*

Dim. Sia $\mathcal{A}\mathcal{A}^t = (b_{ij})$. Consideriamo innanzi tutto gli elementi b_{ii} della diagonale. Poichè b_{ii} è il prodotto scalare della i-sima riga di $\mathcal{A}$ con se stessa, esso rappresenta la somma degli elementi non nulli della i-sima riga di $\mathcal{A}$ che corrisponde al numero delle rette per P_i. Quindi $b_{ii} = n+1$ per $i = 1, 2, ..., n^2+n+1$. Analogamente b_{ij} è il prodotto scalare della i-sima riga di $\mathcal{A}$ con la j-sima riga di $\mathcal{A}$. Questo è uguale al numero dei valori di k per cui $a_{ik} = a_{jk} = 1$. Ma $a_{ik} = 1$ se e solo se $P_i \in l_k$ e $a_{jk} = 1$ se e solo se

$P_j \in l_k$. Ora poichè P_i e P_j individuano una sola retta, $b_{ij} = 1$ per $i \neq j$. Abbiamo così provato che $\mathcal{A}\mathcal{A}^t = \begin{pmatrix} n+1 & 1 & . & . & . & 1 \\ 1 & n+1 & 1 & . & . & . \\ . & . & . & 1 & 1 & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 1 & 1 & . & 1 & 1 & n+1 \end{pmatrix}$ e quindi vale che $\mathcal{A}\mathcal{A}^t = n\mathcal{I}_\nu + \mathcal{J}$. Proviamo ora che A è invertibile calcolando $\det \mathcal{A}\mathcal{A}^t$.

$$\det \mathcal{A}\mathcal{A}^t = \begin{vmatrix} n+1 & 1 & . & . & . & 1 \\ 1 & n+1 & & & & . \\ . & & . & & & . \\ . & & & . & & . \\ . & & & & . & . \\ 1 & 1 & & & & n+1 \end{vmatrix}$$

sottraendo la prima riga da tutte le altre otteniamo: $\begin{vmatrix} n+1 & 1 & . & . & . & 1 \\ -n & n & 0 & . & . & 0 \\ -n & 0 & n & & & . \\ . & & & . & & . \\ . & & & & . & . \\ -n & 0 & . & . & 0 & n \end{vmatrix}$ Ora, aggiungendo ogni colonna alla prima otteniamo $b_{11} = n + 1 + (n^2 + n)$ essendoci $n^2 + n$ posizioni b_{1j}, con $j > 1$, uguali ad 1 e quindi $b_{11} = n^2 + 2n + 1 = (n+1)^2$ da cui segue

$$\det \mathcal{A}\mathcal{A}^t = \begin{vmatrix} (n+1)^2 & 1 & . & . & . & 1 \\ 0 & n & 0 & . & . & 0 \\ 0 & 0 & n & & & . \\ . & & & . & & . \\ . & & & & . & . \\ 0 & 0 & . & . & 0 & n \end{vmatrix} = (n+1)^2 n^{n^2+n} \neq 0.$$

Abbiamo così provato che A è invertibile. ■

Definizione 2.37 *Una matrice quadrata $\mathcal{A}$ i cui elementi assumono valore solo 1 e 0 è detta* ***matrice di permutazione*** *se ogni riga ed ogni colonna di $\mathcal{A}$ ha esattamente un elemento uguale ad 1 e tutti gli altri uguali a 0.*

Si verifica facilmente che moltiplicando a sinistra una data matrice $\mathcal{A}$ per una matrice di permutazione si ottiene una nuova matrice le cui righe sono una permutazione delle righe di $\mathcal{A}$. Lo stesso accade per le colonne moltiplicando a destra.

Proposizione 2.38 *Sia Π un piano proiettivo di ordine n ed $\alpha \in Aut(\Pi)$. Se $\nu = n^2 + n + 1$, indichiamo con $P_1, P_2, ..., P_\nu$ ed $l_1, l_2, ..., l_\nu$ una numerazione dei punti e delle rette di Π rispettivamente. Siano $\mathcal{P}$ e $\mathcal{Q}$ le $\nu \times \nu$ matrici così definite:*

$\mathcal{P} = (p_{ij})$, *dove* $p_{ij} = 1$ *se e solo se* $P_i^\alpha = P_j$, *altrimenti* $p_{ij} = 0$*;*

$\mathcal{Q} = (q_{ij})$, *dove* $q_{ij} = 1$ *se e solo se* $l_i^\alpha = l_j$, *altrimenti* $q_{ij} = 0$.
Allora $\mathcal{P}$ *e* $\mathcal{Q}$ *sono matrici di permutazione.*

Dim. Supponiamo per assurdo che nella colonna j-sima di $\mathcal{P}$ ci siano $p_{kj} = p_{hj} = 1$ con $k \neq h$. Allora questo vorrebbe dire che $P_k^\alpha = P_j$ e contemporaneamente $P_h^\alpha = P_j$ e ciò è assurdo essendo α una collineazione. Allo stesso modo non è possibile che nella riga i-sima di $\mathcal{P}$ ci sia $p_{ik} = p_{ih} = 1$ con $k \neq h$ perchè questo vorrebbe dire che $P_i^\alpha = P_k$ e contemporaneamente $P_i^\alpha = P_h$. Analogamente si prova che $\mathcal{Q}$ è una matrice di permutazione. ■

Proposizione 2.39 *Sia* $\mathcal{A}$ *una matrice di incidenza per un piano proiettivo finito* Π. *Ogni collineazione di* Π *può essere rappresentata da una coppia di matrici di permutazione* $\mathcal{P}$, $\mathcal{Q}$ *con* $\mathcal{PA} = \mathcal{AQ}$.

Dim. Sia α una collineazione di Π. Se $\nu = n^2 + n + 1$, indichiamo con $P_1, P_2, ..., P_\nu$ ed $l_1, l_2, ..., l_\nu$ una numerazione dei punti e delle rette di Π rispettivamente. Sia $\mathcal{A} = (a_{ij})$ la matrice di incidenza di Π e $\mathcal{P} = (p_{ij}), \mathcal{Q} = (q_{ij})$ le matrici di permutazione associate ad α. Sia $\mathcal{PA} = (u_{ik})$ con $u_{ik} = \sum_{j=1}^{\nu} p_{ij} a_{jk}$. Supponiamo che nella i-sima riga della matrice $\mathcal{P}$ x sia la posizione dell'unico 1, cioè $P_i^\alpha = P_x$. Segue allora che $u_{ik} = a_{xk}$ e $a_{xk} = 1$ se e solo se $P_x \in l_k$. Sia ora $\mathcal{AQ} = (v_{ik})$ con $v_{ik} = \sum_{j=1}^{\nu} a_{ij} q_{jk}$. Allo stesso modo $v_{ik} = a_{iy}$ se y è la posizione dell'unico 1 nella k-sima colonna di $\mathcal{Q}$. In questo caso $l_y^\alpha = l_k$ e $a_{iy} = 1$ se e solo se $P_i \in l_y$. Ora abbiamo che $u_{ik} = a_{xk} = 1 \Leftrightarrow P_x \in l_k \Leftrightarrow P_x^{\alpha^{-1}} \in l_k^{\alpha^{-1}}$ essendo α una collineazione di Π. Ricordando che $P_i^\alpha = P_x$ e $l_y^\alpha = l_k$ si ha $P_x^{\alpha^{-1}} \in l_k^{\alpha^{-1}} \Leftrightarrow P_i \in l_y \Leftrightarrow a_{iy} = v_{ik} = 1$. Quindi $u_{ik} = v_{ik}$ per ogni $i = 1, ..., \nu$ ossia $\mathcal{PA} = \mathcal{AQ}$. ■

Essendo $\mathcal{A}$ una matrice invertibile, dalla Proposizione precedente segue subito il seguente risultato:

Proposizione 2.40 *Due matrici di permutazione* $\mathcal{P}$ *e* $\mathcal{Q}$ *rappresentano una collineazione* α *di un piano proiettivo finito* Π *se e solo se sono coniugate mediante una matrice di incidenza.*

Teorema 2.41 *Sia* α *una collineazione di un piano proiettivo finito* Π. *Allora* α *ha un ugual numero di punti e di rette fissate.*

Dim. Fissiamo una numerazione per i punti e per le rette di Π. Sia α una collineazione di Π e siano $\mathcal{P}$, $\mathcal{Q}$ le matrici di permutazione associate ad α. Un punto P_i di Π è fissato da α se e solo se $P_i^\alpha = P_i$, cioè se e solo se $p_{ii} = 1$. Analogamente una retta l_j è fissata da

α se e solo se $l_j^\alpha = l_j$, cioè se e solo se $q_{jj} = 1$. Il numero dei punti fissati da α è quindi dato dalla traccia della matrice $\mathcal{P}$ così come il numero delle rette fissate da α è dato dalla traccia della matrice $\mathcal{Q}$. Poichè $\mathcal{P}$ e $\mathcal{Q}$ sono coniugate esse hanno la stessa traccia e la tesi è dimostrata. ■

Teorema 2.42 *(Teorema dell'orbita) Sia* Π *un piano proiettivo finito e sia* G *un gruppo di collineazioni di* Π*. Allora* G *ha lo stesso numero di orbite sull'insieme dei punti e sull'insieme delle rette.*

Dim. Per dimostrare il Teorema utilizziamo il seguente risultato di carattere generale sui gruppi di permutazione: $t\,|G| = \sum_{\alpha \in G} f(\alpha)$ dove t è il numero delle orbite di G e $f(\alpha)$ denota il numero dei punti fissati da α. Denotiamo con t_1 e t_2 il numero delle orbite di punti e delle orbite di rette rispettivamente. Inoltre, se $f(\alpha)$ è il numero dei punti fissati da α, allora $f(\alpha)$ è anche il numero delle rette fissate da α per il Teorema precedente. Segue allora che $t_1\,|G| = \sum_{\alpha \in G} f(\alpha) = t_2\,|G|$. Da cui $t_1 = t_2$. ■

Osserviamo che il risultato precedente non può essere esteso anche alla lunghezza delle orbite, infatti: sia G un gruppo transitivo su una retta l di Π e sui punti del corrispondente piano affine Π_l. Le orbite di punti di G sono due, una di lunghezza $n+1$ (che consiste dei punti di l) ed una di lunghezza n^2(che consiste dei punti di Π_l). Le orbite di rette sono sempre due ma una di lunghezza 1 (che consiste della sola retta l) e l'altra di lunghezza $n^2 + n$ (che consiste delle rette di Π_l).

Con i risultati che seguono si presentano alcune caratterizzazioni dei piani desarguesiani, ossia si analizzano quali sono le condizioni del gruppo di collineazioni che inducono il piano ad essere un piano desarguesiano.

Lemma 2.43 ***(Gleason)*** *Sia* G *un gruppo di collineazioni su di un insieme finito* S *e sia* p *un primo. Se* W *è un sottoinsieme di* S *tale che per ogni* $a \in W$*,* G *contiene un elemento di ordine* p *che fissa* a *e nessun altro elemento di* S*, allora* W *è contenuto in un orbita di* G *su* S*.*

Dim. Supponiamo esistano $a, b \in W$ con a e b appartenenti ad orbite distinte di G su S. Per ipotesi esiste un elemento $\alpha \in G$ tale che $a^\alpha = a$ e α è f.p.f. su $S - \{a\}$. Poichè $a \notin b^G$ possiamo dire che α ripartisce l'orbita b^G in un certo numero di orbite ciascuna di lunghezza p, cioè $\left|b^G\right| \equiv 0(p)$. D'altra parte, esiste un elemento $\beta \in G$ tale che $b^\beta = b$ e β è f.p.f. su $S - \{b\}$. L'orbita b^G è suddivisa da β in un orbita di lunghezza 1 ed in un certo numero di orbite di lunghezza p. Da ciò segue che $\left|b^G\right| \equiv 1(p)$ e quindi si ha una contraddizione. ■

Proposizione 2.44 *Sia* Π *un piano proiettivo finito e sia* α *una* (A, a)*-elazione e* β *una* (B, b)*-elazione. Supponiamo che* $A \notin b$ *e* $B \notin a$ *e che inoltre* α *e* β *abbiano lo stesso ordine primo* p*. Allora esiste un elemento* γ *in* $\langle \alpha, \beta \rangle$ *tale che* $A^\gamma = B$ *e* $a^\gamma = b$*.*

Dim. Sia $l = AB$, da $l^\alpha = l$ e $l^\beta = l$ segue che $\langle \alpha, \beta \rangle$ fissa l. Osserviamo che per ipotesi $A \neq B$ e $a \neq l \neq b$. Abbiamo che α fissa A ed agisce semiregolarmente su $l - \{A\}$, mentre β fissa B ed agisce semiregolarmente su $l - \{B\}$. Quindi, per il Lemma di Gleason A e B sono contenuti nella stessa orbita di $\langle \alpha, \beta \rangle$ su l ossia esiste $\gamma \in \langle \alpha, \beta \rangle$ tale che $A^\gamma = B$. Sia ora $L = a \cap b$, si ha che $a^\gamma = (LA)^\gamma = L^\gamma A^\gamma$. Da $L \in a$ segue $L^\alpha = L$ e da $L \in b$ segue $L^\beta = L$, quindi $L^\gamma = L$. In definitiva $a^\gamma = L^\gamma A^\gamma = LB = b$ e la tesi è dimostrata. ■

Sia G un gruppo di collineazioni di Π tale che $G(A, a) \neq \langle 1 \rangle$ e $G(B, b) \neq \langle 1 \rangle$. Supponiamo che Π abbia ordine $n = p^s$ con p primo. Se consideriamo $\alpha \in G(A, a)$ e $\beta \in G(B, b)$ allora $o(\alpha) \mid p^s$ così come $o(\beta) \mid p^s$ e quindi esistono una (A, a) elazione e una (B, b) elazione entrambe di ordine p. Dalla Proposizione precedente segue che esiste un elemento γ in $\langle \alpha, \beta \rangle$ tale che $A^\gamma = B$ e $a^\gamma = b$ ossia $G(A, a)^\gamma = G(A^\gamma, a^\gamma) = G(B, b)$ e quindi $|G(B, b)| = |G(A, a)|$. In un piano di ordine potenza di un primo gli interi gruppi $G(B, b)$ e $G(A, a)$ sono coniugati. Il risultato è quindi interessante se si considera che tutti i piani noti hanno per ordine la potenza di un primo.

Se A è il centro di un'elazione in un dato gruppo di collineazioni G e se l è asse di un'elazione in G con $A \in l$, allora chiameremo la coppia (A, l) una *bandiera di elazione*.

Osservazione 2.45 *La coppia punto-retta incidente (A, l) è una bandiera di elazione se e solo se $G(A, A) \neq \langle 1 \rangle$ e $G(l, l) \neq \langle 1 \rangle$.*

Dim. Se (A, l) è una bandiera di elazione banalmente $G(A, A) \neq \langle 1 \rangle$ e $G(l, l) \neq \langle 1 \rangle$. Proviamo il viceversa: sia $\alpha \in G(A, A)$ e sia m l'asse di α, allora $A \in m$. Se $m = l$ l'asserto è banale. Se $m \neq l$, sia $\beta \in G(l, l)$ e sia P il centro di β, allora $P \in l$. Abbiamo visto che se $|G(P, l)| > 1$ e $|G(A, m)| > 1$ con $A, P \in l$ e $A \in m$, allora $|G(A, l)| > 1$ e quindi la tesi è dimostrata. ■

Due centri di elazioni A e B si dicono *connessi* in G se esiste una sequenza $A_0, l_0, A_1, l_1, ...A_i, l_i, ..., A_n$ di punti e rette di Π tali che $A = A_0$, $A_n = B$, $A_{i-1} \in l_{i-1} \ni A_i$ e (A_{i-1}, l_{i-1}) sono bandiere di elazioni per $i = 1, ..., n$. In modo simile possiamo definire la connessione tra assi di elazioni o tra un centro ed un'asse di elazione. La connessione è una relazione di equivalenza definita sull'insieme dei punti e delle rette di Π. Una classe di equivalenza è detta *insieme connesso* di Π. Un insieme connesso che consiste di una sola bandiera è detto banale.

L'aver introdotto le precedenti definizioni trova giustificazione nella seguente Proposizione che è un'estensione del Teor. 2.20.

Proposizione 2.46 *Sia Π un piano proiettivo finito. Se α e β sono elazioni i cui centri A e B appartengono allo stesso insieme connesso non banale S allora α e β hanno lo stesso ordine primo.*

Dim. Nella sequenza che congiunge A e B, consideriamo $A_{i-1} \in l_{i-1}$ allora $A_i \in l_{i-1}$ e $A_i \in l_i$. Esiste allora una (A_{i-1}, l_{i-1})-elazione α_{i-1} e una (A_i, l_i)-elazione α_i entrambe

non banali. Se $l_i = l_{i-1}$ allora posso supporre $A_i \neq A_{i-1}$ e allora α_{i-1} e α_i avendo lo stesso asse e centri distinti hanno lo stesso ordine primo. Sia allora $l_i \neq l_{i-1}$, in queste ipotesi sappiamo che esiste una (A_i, l_{i-1})-elazione γ non banale e α_{i-1} e γ avendo lo stesso asse, hanno lo stesso ordine primo, cosi come γ e α_i, avendo lo stesso centro, hanno lo stesso ordine primo. Quindi si ha $o(\alpha_{i-1}) = o(\alpha_i)$. Per induzione si dimostra la tesi. ■

Proposizione 2.47 *Sia* Π *un piano proiettivo finito di ordine* n*,* G *un gruppo di collineazioni di* Π *ed* l *una retta di* Π*. Se valgono le seguenti condizioni:*

1. $G(l, l) \neq \langle 1 \rangle$;
2. *per ogni punto* $A_i \in l$, $i = 1, ..., n+1$, *esiste una retta* a_i *tale che* $a_i \neq l$, $A_i \in a_i$ *e* $G(A_i, a_i) \neq \langle 1 \rangle$;

allora $G(l, l)$ *è transitivo sui punti affini di* Π_l*, cioè* l *è una retta di traslazione.*

Dim. Possiamo supporre che $G(P, l) \neq \langle 1 \rangle$ per un dato $P \in l$ perchè per ipotesi $G(l, l) \neq \langle 1 \rangle$. Sia $A_i \in l$ e a_i una retta per A_i distinta da l, dall'esistenza di una (A_i, a_i)-elazione segue l'esistenza di una (A_i, l)-elazione. Se consideriamo ora A_{i+1} e a_{i+1}, ragionando in modo analogo possiamo concludere che esiste una (A_{i+1}, l)-elazione. Abbiamo così costruito un insieme connesso S. Se $\alpha_i \in G(A_i, a_i)$ e $\alpha_j \in G(A_j, a_j)$ con $\alpha_i, \alpha_j \neq 1$ allora α_i e α_j hanno lo stesso ordine primo p per $1 \leq i, j \leq n+1$. Sia $H = \langle G(A_i, a_i) \quad i = 1, ..., n+1 \rangle$. Se consideriamo l'azione di H su l, per ogni punto $A_i \in l$ esiste una elazione $\alpha_i \in H$ che fissa A_i e nessun altro punto di l. Per Il Lemma di Gleason tutti i punti A_i stanno in una stessa orbita rispetto ad H, ossia H è transitivo su l, quindi G_l è transitivo su l. Poichè il gruppo $G(P, l)$ è non identico per il Teorema di Hughes allora Π risulta essere un piano di traslazione. ■

Ricordiamo che un piano proiettivo che sia (l, l)-transitivo per ogni scelta della retta l, è detto *piano di Moufang.* Si può provare che ogni piano di Moufang finito è desarguesiano.

Proposizione 2.48 *Sia* Π *un piano proiettivo finito di ordine* n *e sia* G *un gruppo di collineazioni di* Π*. Se ogni punto di* Π *è centro di un'elazione non banale ed ogni retta è asse di un'elazione non banale in* G*, allora* Π *è desarguesiano d'ordine* $n = p^h = q$ *e* G *contiene* $PSL(3, q)$*.*

Dim. Sia l una retta di Π. Per ipotesi $G(l, l) \neq \langle 1 \rangle$. Sia $A \in l$, allora $G(A, A) \neq \langle 1 \rangle$. Consideriamo $\alpha \in G(A, A)$ con α (A, m)-elazione. Può accadere che $l = m$ oppure $l \neq m$. Nel primo caso sia s una retta per A distinta da l. Allora $G(s, s) \neq \langle 1 \rangle$ ed esiste $P \in s$ centro di una (P, s)-elazione non banale. Allora dall'esistenza di una (A, l)-elazione e di una (P, s)-elazione segue che $G(A, s) \neq \langle 1 \rangle$. Nel caso $l \neq m$, abbiamo direttamente che $G(A, m) \neq \langle 1 \rangle$. Essendo nelle ipotesi della Proposizione precedente, possiamo concludere che l è una retta di traslazione. Poichè la scelta di l è arbitraria, Π è un piano di Moufang finito e quindi è desarguesiano. Poichè G contiene tutte le elazioni di Π, G contiene $PSL(3, q)$. ■

Definizione 2.49 *Sia* $\Pi = (\mathcal{P}, \mathcal{L})$ *un piano proiettivo. Una* correlazione ϑ *di* Π *è un'applicazione biunivoca da* $\mathcal{P} \cup \mathcal{L}$ *in* $\mathcal{P} \cup \mathcal{L}$ *tale che* $\mathcal{P}^\vartheta = \mathcal{L}$, $\mathcal{L}^\vartheta = \mathcal{P}$ *e* $A \in l$ *se e solo se* $l^\vartheta \in A^\vartheta$.

Definizione 2.50 *Una correlazione* ϑ *tale che* $\vartheta^2 = 1$ *è detta* polarità. *Un* punto A *è detto* assoluto *se* $A \in A^\vartheta$. *Analogamente una* retta a *è detta* assoluta *se* $a^\vartheta \in a$.

Lemma 2.51 *Sia* $\mathcal{C} = n\mathcal{I} + \mathcal{J}$, *dove* $\mathcal{I}$ *è la* $\nu \times \nu$ *matrice identica,* $\mathcal{J}$ *è la* $\nu \times \nu$ *matrice con tutti gli elementi uguali ad* 1 *ed* n *è un intero positivo. Allora* $\mathcal{C}$ *ha* $n + \nu$ *come autovalore di molteplicità* 1 *ed* n *come autovalore di molteplicità* $\nu - 1$.

Dim. Sia $\mathbf{v}_i = (0, 0, ..., 1, -1, ..., 0, 0)$ il vettore riga a ν componenti con 1 nella i-sima poisizione, -1 nella $i+1$-sima poisizione e 0 in tutte le altre. Esistono allora $\nu - 1$ vettori $\mathbf{v}_i$ linearmente indipendenti. Da $\mathbf{v}_i\mathcal{J} = \mathbf{0}$ con $i = 1, ..., \nu - 1$, segue $\mathbf{v}_i\mathcal{C} = \mathbf{v}_i(n\mathcal{I} + \mathcal{J}) = n\mathbf{v}_i\mathcal{I} + \mathbf{v}_i\mathcal{J} = n\mathbf{v}_i$. Allora $\mathbf{v}_i$ è un autovettore relativo all'autovalore n di molteplicità geometrica $\nu - 1$ e quindi di molteplicità algebrica almeno $\nu - 1$. Sia ora $\mathbf{h} = (1, 1, ..., 1)$ il vettore riga a ν componenti con 1 in tutte le posizioni. Allora $\mathbf{h}\mathcal{C} = \mathbf{h}(n\mathcal{I}+\mathcal{J}) = n\mathbf{h}+\nu\mathbf{h} = (n+\nu)\mathbf{h}$, da cui segue che l'autovalore $n+\nu$ ha molteplicità algebrica almeno 1. Poichè la somma delle molteplicità algebriche degli autovalori di $\mathcal{C}$ deve essere uguale a ν, necessariamente $n+\nu$ ha molteplicità 1 ed n ha molteplicità $\nu-1$.
■

Proposizione 2.52 *Ogni polarità di un piano proiettivo finito ha almeno un punto assoluto.*

Dim. Sia Π un piano proiettivo finito di ordine n e sia ϑ una polarità di Π. Poniamo $\nu = n^2 + n + 1$ e fissiamo una numerazione qualsiasi per i punti di Π: $P_1, P_2, ..., P_\nu$. Numeriamo le rette $l_1, l_2, ...l_\nu$ in modo tale che $l_i = P_i^\vartheta$ per $i = 1, 2, ..., \nu$ e sia $\mathcal{A}$ la matrice di incidenza di Π associata a questa numerazione. Abbiamo quindi che $a_{ij} = 1 \Leftrightarrow P_i \in l_j \Leftrightarrow l_j^\vartheta \in P_i^\vartheta$. Per la numerazione scelta si ha che $P_j^\vartheta = l_j \Leftrightarrow (P_j^\vartheta)^\vartheta = l_j^\vartheta \Leftrightarrow P_j = l_j^\vartheta$ da cui $l_j^\vartheta \in P_i^\vartheta \Leftrightarrow P_j \in l_i \Leftrightarrow a_{ji} = 1$. Quindi $\mathcal{A}$ è una matrice simmetrica. Oltre a ciò, $a_{ii} = 1 \Leftrightarrow P_i \in l_i = P_i^\vartheta$ cioè se e solo se P_i è un punto assoluto di ϑ. Allora, il numero dei punti assoluti di ϑ è uguale alla traccia di $\mathcal{A}$. Abbiamo dimostrato che $\mathcal{A}\mathcal{A}^t = n\mathcal{I} + \mathcal{J}$. Poichè $\mathcal{A} = \mathcal{A}^t$ si ha $\mathcal{A}^2 = n\mathcal{I} + \mathcal{J}$ è quindi $\mathcal{A}^2$ ha n come autovalore con molteplicità $\nu - 1 = n^2 + n$ e $n + \nu = n + n^2 + n + 1 = (n + 1)^2$ come autovalore con molteplicità 1. Consideriamo la relazione $|\mathcal{A}^2 - \lambda^2\mathcal{I}| = |\mathcal{A} - \lambda\mathcal{I}|\,|\mathcal{A} + \lambda\mathcal{I}|$. Quindi ogni autovalore di $\mathcal{A}$ è radice quadrata di un autovalore di $\mathcal{A}^2$, ossia i possibili autovalori di $\mathcal{A}$ sono $n + 1$, $-(n + 1)$, $\sqrt{n}$, $-\sqrt{n}$. Supponiamo che $\sqrt{n}$ abbia molteplicità r e $-\sqrt{n}$ molteplicità s. Allora $r + s = n^2 + n$. Se consideriamo il vettore $\mathbf{h}$, il valore di $\sum_{j=1}^{\nu} a_{ij}h_j$ è uguale al numero degli elementi non nulli della riga $(a_{i1}, a_{i2,...,}a_{i\nu})$, che corrisponde al

numero delle rette per un punto, ossia $\sum_{j=1}^{\nu} a_{ij}h_j = n+1$ da cui segue $\mathcal{A}\mathbf{h} = (n+1)\mathbf{h}$. Quindi oltre agli autovalori $\sqrt{n}$ e $-\sqrt{n}$ vi è l'unico autovalore $n+1$. Poichè la traccia di $\mathcal{A}$ corrisponde alla somma dei suoi autovalori, ciascuno contato con la sua molteplicità, $Tr(\mathcal{A}) = (n+1) + r\sqrt{n} + s(-\sqrt{n}) = n+1+(r-s)\sqrt{n}$. Ora, poichè ogni elemento di $\mathcal{A}$ è 0 oppure 1, $n+1+(r-s)\sqrt{n}$ deve essere un intero. Se $r-s=0$ allora ϑ ha $n+1$ punti assoluti. Se $r-s \neq 0$, supponiamo sia $n+1+(r-s)\sqrt{n} = 0$. Osserviamo che $\sqrt{n}$ divide $(r-s)\sqrt{n}$ e quindi $\sqrt{n}$ deve dividere anche $n+1$ ma questo è assurdo perchè $(\sqrt{n}, n+1) = 1$. Quindi necessariamente deve essere $n+1+(r-s)\sqrt{n} \neq 0$ e questo prova che esiste almeno un punto assoluto. ■

Mentre la Prop. 2.48 costituisce una prima caratterizzazione dei piani desarguesiani dovuta a Gleason, quello che segue ne è una generalizzazione dovuta a Wagner.

Teorema 2.53 *Sia $\Pi = (\mathcal{P}, \mathcal{L})$ un piano proiettivo finito di ordine n e sia G un gruppo di collineazioni di Π. Se G è transitivo sui punti di Π e contiene una prospettività non banale allora Π è desarguesiano e G contiene $PSL(3,n)$.*

Dim. Per il Teorerma dell'orbita, dalla transitività di G sui punti segue la transitività di G anche sulle rette di Π. Supponiamo che α sia una (A,a)-elazione non banale di G. Se B è un generico punto di Π, per la transitività di G sui punti, esiste $\beta \in G$ tale che $A^\beta = B$. Allora $\beta^{-1}\alpha\beta$ è una (A^β, l^β)-elazione, ossia una (B, l^β)-elazione. Da ciò segue che ogni punto di Π è il centro di un'elazione non banale in G. Con un ragionamento analogo, sfruttando la transitività di G sulle rette, possiamo provare che ogni retta di Π è asse di un'elazione non banale in G e la tesi segue quindi dalla Prop.2.48. Supponiamo ora, per assurdo, che ogni prospettività α in G sia una omologia. Ripetendo il discorso precedente possiamo affermare che ogni punto di Π è il centro di un'omologia non banale così come ogni retta di Π è asse di un'omologia non banale in G. Se ogni retta è asse di un'omologia per due centri distinti (o in modo duale: ogni punto è centro di un'omologia per due assi distinti) allora G contiene un'elazione. Abbiamo provato infatti che se α e β sono due omologie non banali con centri distinti A e B e stesso asse l, allora $\langle \alpha, \beta \rangle$ contiene un'elazione che trasforma A in B. Si tratta quindi di considerare la situazione in cui: per ogni punto P qualsiasi esiste una ed una sola retta l asse di tutte le omologie di centro P e dualmente, per ogni retta l, esiste uno ed un solo punto P centro di tutte le omologie di asse l . Si può allora considerare un'applicazione biunivoca $\vartheta : \mathcal{P} \cup \mathcal{L} \mapsto \mathcal{P} \cup \mathcal{L}$ che ad ogni punto P fa corrispondere l'asse P^ϑ delle (P, P^ϑ)-omologie non banali e che ad ogni retta l fa corrispondere il centro l^ϑ delle (l^ϑ, l)-omologie non banali. Chiaramente $\vartheta^2 = 1$. Proviamo che ϑ è una polarità, ossia che $A \in l$ se e solo se $l^\vartheta \in A^\vartheta$. Supponiamo, per assurdo, che $A \in l$ e $l^\vartheta \notin A^\vartheta$. Sia α una (l^ϑ, l)-omologia non banale, chiaramente $A^\alpha = A$ perchè $A \in l$, ma $(A^\vartheta)^\alpha \neq A^\vartheta$ poichè la retta A^ϑ non passa per il centro l^ϑ di α e $A^\vartheta \neq l$. Sia δ una (A, A^ϑ)-omologia non banale (esiste sicuramente perchè l'immagine di A tramite ϑ è l'asse A^ϑ di un omologia non banale), allora $\alpha^{-1}\delta\alpha$ è una $(A^\alpha, A^{\vartheta\alpha})$-omologia.

Ora essendo $A^\alpha = A$ si ha che δ e $\alpha^{-1}\delta\alpha$ sono omologie non banali con assi distinti e stesso centro contro quanto abbiamo supposto. Allora $l^\vartheta \in A^\vartheta$ e ϑ è una polarità che non ha punti assoluti, ossia punti P tali che $P \in P^\vartheta$, contro la Prop. precedente, assurdo. Dobbiamo allora concludere che in G le prospettività non banali non possono essere solo omologie, da cui segue che Π è desarguesiano e G contiene $PSL(3,n)$. ■

La Proposizione che segue ci permette di stabilire quando una involuzione non è di Baer, nella dimostrazione faremo uso del seguente risultato sui gruppi di permutazione:

(*) *Sia S un insieme di n elementi con n pari e sia G un gruppo che agisce transitivamente su S. Se Q è un 2-sottogruppo di Sylow di G e $\sigma \in Z(Q)$, allora il numero degli elementi di S fissati da σ è diverso da $\sqrt{n}$ e $\sqrt{n+1}-1$.* (La dimostrazione è riportata nell'Appendice: Gruppi di Permutazioni)

Proposizione 2.54 *Sia Π un piano proiettivo finito. Sia G un gruppo di collineazioni di Π e sia σ un'involuzione in un 2-sottogruppo di Sylow Q di G. Allora vale:*

1. *Se Π ha ordine pari, (P,l) è una coppia punto-retta incidente di Π fissata da G, $\overline{G}$ è il gruppo di permutazioni indotto da G su $l-\{P\}$, $\overline{G}$ agisce transitivamente su $l-\{P\}$ e $\overline{\sigma} \in Z(\overline{Q})$, allora σ è una elazione di Π.*

2. *Se Π ha ordine dispari, G fissa due punti P e R di Π, $\overline{G}$ è il gruppo di permutazioni indotto da G su $PR-\{P,R\}$ e $\overline{G}$ è transitivo su $PR-\{P,R\}$ e $\overline{\sigma} \in Z(\overline{Q})$, allora σ è una omologia di Π.*

Dim. 1. Consideriamo una coppia punto-retta incidente (P,l) e sia $S = l-\{P\}$. $\overline{G}$ è transitivo su $l-\{P\}$ e $|S| = n$ pari. Sia σ un'involuzione in un 2-sottogruppo di Sylow Q di G tale che $\overline{\sigma} \in Z(\overline{Q})$. Se $o(\overline{\sigma}) = 1$, ossia σ appartiene al nucleo della rappresentazione, allora σ fissa puntualmente l e la tesi è vera. Supponiamo allora che $o(\overline{\sigma}) = 2$ e che σ sia una involuzione di Baer. Allora σ fissa $m = \sqrt{n}+1$ punti su l e di conseguenza σ fissa $\sqrt{n}$ punti su S. Ciò contraddice (*) e quindi σ, non potendo essere una involuzione di Baer, è una elazione.

2. Supponiamo che G fissi due punti P e R di Π e sia l la retta PR, allora in questo caso $S = l-\{P,R\}$. Possiamo procedere in modo analogo a quanto fatto nel punto 1 e quindi considerare σ una involuzione in un 2-sottogruppo di Sylow Q di G tale che $\overline{\sigma} \in Z(\overline{Q})$. In questo caso $|l| = n+1$ con n dispari e quindi $|S| = |l|-2 = n-1$ è pari. Se $o(\overline{\sigma}) = 1$ allora σ fissa puntualmente l e σ è una omologia di Π perchè n è dispari. Supponiamo allora che $o(\overline{\sigma}) = 2$ e che σ sia un'involuzione di Baer. Allora σ fissa $m = \sqrt{n}+1$ punti di l, due dei quali sono proprio P e R. Dunque σ fissa $m-1 = \sqrt{n}-1$ punti su S. Poichè $m-1 = \sqrt{(n-1)+1}-1$ nuovamente il risultato (*) è contraddetto. Allora σ è una omologia. ■

Lemma 2.55 *(**Wagner**) Sia Π_l un piano affine finito e sia G un gruppo di collineazioni di Π_l. Allora G agisce transitivamente sui punti di Π_l se e solo se G_P è transitivo sulle rette affini per P, per ogni $P \in l$.*

Dim. Siano $\mathcal{O}_1, \mathcal{O}_2, ..., \mathcal{O}_s$ le orbite di G su l e sia $\mathcal{M}_i$ l'insieme delle rette affini m di Π_l che hanno il loro punto improprio nell'orbita $\mathcal{O}_i$. Chiaramente ogni $\mathcal{M}_i$ è G-invariante. Supponiamo che G sia transitivo sui punti di Π_l. Da ciò segue che G ha esattamente $s+1$ orbite sui punti di Π, perchè s sono le orbite su l e i punti di Π_l costituiscono un'unica orbita. Allora, per il Teorema dell'orbita, G ha esattamente $s+1$ orbite di rette su Π. Una di queste orbite è $\{l\}$ perchè l è una retta fissata. Ora, le altre s orbite sono tali che: ciascuna è contenuta in un insieme $\mathcal{M}_i$ e se esistesse un $\mathcal{M}_i$ con più di un'orbita di rette allora avremmo più di s orbite di rette. Quindi ogni orbita di rette corrisponde esattamente ad un insieme $\mathcal{M}_i$. Sia $P \in l$ con $P \in \mathcal{O}_i$ e siano h e k due rette affini per P distinte. Poichè h e k appartengono allo stesso insieme $\mathcal{M}_i$, ossia alla stessa orbita rispetto a G, possiamo dire che esiste $\alpha \in G$ tale che $h^\alpha = k$. Allora $P^\alpha = (h \cap l)^\alpha = h^\alpha \cap l^\alpha = k \cap l = P$ e quindi $\alpha \in G_P$, abbiamo così provato che G_P è transitivo sulle rette affini per P. Viceversa supponiamo che, per ogni $P \in l$, G_P sia transitivo sulle rette per P. Proviamo che ogni $\mathcal{M}_i$ è un'orbita di rette rispetto a G. Supponiamo siano h,$k \in \mathcal{M}_i$ con $k \cap l = Q$, $h \cap l = P$ e $P \neq Q$. Poichè $P, Q \in \mathcal{O}_i$ esiste $\beta \in G$ tale che $P^\beta = Q$, da cui $Q \in h^\beta$. D'altra parte, poichè $Q \in h^\beta \cap k$, deve esistere $\alpha \in G_Q$ tale che $h^{\beta\alpha} = k$. Ma allora esiste $\beta\alpha \in G$ tale che $h^{\beta\alpha} = k$, ossia $\mathcal{M}_i$ è un'orbita di rette rispetto a G. Agli s insiemi $\mathcal{M}_i$ va aggiunta l'orbita che consiste della sola retta l. Quindi si hanno in tutto $s+1$ orbite di rette. Per il Teorema dell'orbita dunque, G ha esattamente $s+1$ orbite di punti. I punti di l si suddividono nelle s orbite $\mathcal{O}_i$, mentre tutti i punti affini di Π_l devono appartenere ad un'unica orbita rispetto a G. Abbiamo così provato che G è transitivo sui punti di Π_l. ■

Lemma 2.56 *Sia Π_l un piano affine finito di ordine n pari e sia G un gruppo di collineazioni di Π_l. Se G agisce transitivamente sui punti di Π_l, allora G contiene una traslazione non banale di Π_l. Se G agisce primitivamente sui punti di Π_l, allora Π_l è un piano di traslazione e G contiene il gruppo delle traslazioni.*

Dim. Sia l una retta di Π e sia $P \in l$. Allora G_P è transitivo sulle rette affini per P, quindi G_P ha ordine pari. Sia σ una involuzione nel centro di un 2-sottogruppo di Sylow di G_P. Per un risultato precedente sappiamo che: *se Π ha ordine pari, (P, l) è una coppia punto-retta incidente di Π fissata da G, $\overline{G}$ è il gruppo di permutazioni indotto da G su $l - \{P\}$, $\overline{G}$ agisce transitivamente su $l - \{P\}$ e $\overline{\sigma} \in Z(\overline{Q})$ allora σ è una elazione di Π.* Se consideriamo il duale di questo risultato, poichè G_P è transitivo sulle rette affini del fascio per P possiamo concludere che σ è un'elazione del piano duale e quindi anche di Π_l. Se σ ha asse l allora abbiamo una traslazione non banale e quindi la tesi è dimostrata. Supponiamo allora che σ abbia asse m con $m \neq l$. Ricordiamo il Teorema di Hughes: *se esiste una retta l ed un punto Q su l tale che $|G(A, l)| = h > 1$ per tutti gli A in l, $A \neq Q$, allora $|G(Q, l)| = n$ cioè Π è (Q, l)-transitivo.* Se lo consideriamo nella sua forma duale allora Π è (P, l)-transitivo e quindi G, in ogni caso, contiene traslazioni non banali.

Per dimostrare la seconda parte del Lemma supponiamo che G sia primitivo sui punti di Π_l. Consideriamo $T \lhd G$ con T gruppo delle traslazioni in G. Poichè G è primitivo sui punti di Π_l allora T è transitivo sui punti di Π_l (si veda Prop. 15 nell'Appendice sui Gruppi di Permutazioni) e Π_l è un piano di traslazione. ■

Corollario 2.57 *Sia* Π *un piano proiettivo finito e sia* (O, m) *una coppia punto-retta non incidente di* Π. *Se esiste una* (P, OQ)*-omologia involutoria per tutte le coppie di punti distinti* P *e* Q *su* m*, allora l'ordine di* Π *è potenza di un primo.*

Dim. Sia G il gruppo generato dalle (P, OQ)-omologie involutorie per tutte le coppie di punti distinti P e Q su m. Consideriamo il sottogruppo G_Q. Per ogni punto $P \in m$ con $P \neq Q$ esiste in G_Q una omologia involutoria con centro P. Per il Teorema di Andrè, G_Q contiene il gruppo T delle (Q, OQ)-elazioni il quale agisce regolarmente su $m - \{Q\}$. Sia σ una (P, OQ)-omologia involutoria con $P \in m$ e $P \neq Q$. Allora $T \langle\sigma\rangle$ è un gruppo di Frobenius con nucleo di Frobenius T. Proviamo che T è normale in G_Q. Poichè G_Q fissa Q e OQ, il gruppo delle (Q, OQ)-elazioni è G_Q invariante, quindi $T \lhd G_Q$. Ora, applicando un risultato sui gruppi di Frobenius (si vedano le Prop.19 e 20 dell'Appendice: Gruppi di Permutazioni), possiamo dire che T è un p-gruppo abeliano elementare e $|m - \{Q\}|$ è potenza di un numero primo p, ossia $n = p^h$. ■

Proposizione 2.58 *Sia* Π *un piano proiettivo di ordine* n *e sia* G *un 2-gruppo di collineazioni di* Π. *Se* $Fix(G)$ *è un sottopiano di* Π *di ordine* m*, allora* $n = m^{2^t}$ *per un qualche intero* t.

Dim. Dimostriamo la tesi per induzione sull'ordine di G. Se $|G| = 1$ allora la tesi è vera per $n = m$ e $t = 0$. Sia $G \neq \langle 1\rangle$ e sia σ un'involuzione in $Z(G)$. Poichè $Fix(\sigma)$ contiene un sottopiano, allora σ è planare e $Fix(\sigma)$ è un sottopiano di Baer di ordine s con $n = s^2$. Sia $x \in Fix(\sigma)$ e $g \in G$, allora $g^{-1}\sigma g = \sigma$ perchè $\sigma \in Z(G)$ e $x^{g^{-1}\sigma g} = x^{\sigma} = x$, ossia G muta in sè $Fix(\sigma)$. Quindi $Fix(G)$ è un sottopiano di $Fix(\sigma)$. Se $\overline{G}$ è il gruppo di collineazioni indotto da G su $Fix(\sigma)$, allora $\left|\overline{G}\right| < |G|$ perchè $\overline{\sigma} = 1$. Per l'ipotesi induttiva si ha che $s = m^{2^h}$ per un qualche intero h. Quindi $n = s^2 = (m^{2^h})^2 = m^{2^{h+1}}$ e la tesi è provata. ■

Teorema 2.59 *Sia* Π_l *un piano affine finito e sia* G *un gruppo di collineazioni di* Π_l. *Allora le seguenti condizioni sono equivalenti:*

1. G *è transitivo sulle rette di* Π_l*;*
2. G *è transitivo sia sui punti affini di* Π_l *che sui punti di* l*;*
3. G *è transitivo sulle bandiere di* Π_l.

Dim. Supponiamo sia vera la condizione 1. Allora G, considerato come gruppo di collineazioni di Π, ha due orbite di rette, una costituita dalla sola retta l e l'altra che contiene tutte le rette affini. Per il Teorema dell'orbita, G ha due orbite di punti: una costituita dai punti di l e l'altra che contiene tutti i punti di Π_l. Abbiamo così provato che da 1 segue 2. In modo analogo si prova che da 2 segue 1. Si dimostra facilmente che 1 segue da 3 in quanto la transitività sulle bandiere implica ovviamente la transitività sulle rette. Supponiamo ora che G sia transitivo sulle rette di Π_l e sia (M, m) una bandiera. Si ha

$|G| = \left|G_{(M,m)}\right| \left|(M,m)^G\right|$ e $|G| = |G_m| \left|m^G\right|$.

Se guardiamo G_m agire sui punti di m allora $|G_m| = \left|G_{(M,m)}\right| \left|M^{G_m}\right|$ da cui

$|G| = \left|G_{(M,m)}\right| \left|(M,m)^G\right| = |G_m| \left|m^G\right| = \left|G_{(M,m)}\right| \left|M^{G_m}\right| \left|m^G\right|$ ossia

$\left|(M,m)^G\right| = \left|M^{G_m}\right| \left|m^G\right|$.

Allora la lunghezza di un'orbita di bandiere è divisibile per $\left|m^G\right| = n^2 + n$ essendo G transitivo sulle rette di Π_l.

Analogamente $|G| = |G_M| \left|M^G\right|$. Se guardiamo G_M agire sulle rette per M allora $|G_M| = \left|G_{(M,m)}\right| \left|m^{G_M}\right|$ da cui

$|G| = \left|G_{(M,m)}\right| \left|(M,m)^G\right| = |G_M| \left|M^G\right| = \left|G_{(M,m)}\right| \left|m^{G_M}\right| \left|M^G\right|$ ossia

$\left|(M,m)^G\right| = \left|m^{G_M}\right| \left|M^G\right|$.

Ma G è anche transitivo sui punti di Π_l e quindi la lunghezza di un'orbita di bandiere è divisibile per $n^2 = \left|M^G\right|$. Quindi la lunghezza di un'orbita di bandiere è divisibile per $n^2(n+1)$. Contiamo ora le possibili bandiere: se facciamo variare M su m, otteniamo n bandiere; se facciamo variare m in Π_l allora otteniamo $n^2 + n$ bandiere. In tutto avremo $n(n^2+n) = n^2(n+1)$ bandiere. Poichè la lunghezza di un'orbita di bandiere è esattamente $n^2(n+1)$, cioè G è transitivo sulle bandiere di Π_l. ■

L'obiettivo dei risultati che seguono è provare che un piano affine finito che ammette un gruppo di collineazioni transitivo sulle sue rette affini è un piano di traslazione. Come conseguenza immediata si può provare che un piano proiettivo finito con un gruppo di collineazioni 2-transitivo sui suoi punti è Desarguesiano. La dimostrazione del teorema, dovuto a Wagner, fa largo uso di risultati riguardanti i gruppi di permutazioni.

Teorema 2.60 *(**Wagner**) Sia Π_l un piano affine finito e sia G un gruppo di collineazioni di Π_l. Se G è transitivo sulle rette di Π_l, allora Π_l è un piano di traslazione e G contiene il gruppo delle traslazioni di Π_l.*

Dim. Abbiamo precedentemente provato che: "se $G \leq Aut(\Pi)$ ed esiste una retta l tale che G muta in sè l ed è transitivo sui suoi punti e $G(A, l) \neq 1$ per un punto $A \in l$, allora Π è un piano di traslazione rispetto alla retta l". Chiaramente nel nostro caso G è transitivo su l. Se $G(l, l) \neq \langle 1 \rangle$ allora, applicando il risultato su citato, possiamo concludere che Π_l è di traslazione. Quindi tutta la dimostrazione del teorema mira a provare che G possiede almeno una traslazione non banale. Se Π ha ordine pari abbiamo

provato che dalla transitività di G sui punti di Π_l segue l'esistenza di una traslazione non banale. Poichè la transitività di G sulle rette di Π_l è equivalente alla transitività di G sui punti di Π_l, possiamo concludere che se Π ha ordine pari allora G possiede almeno una traslazione non banale e la tesi è provata. Nel seguito supponiamo quindi che Π abbia ordine dispari n. Facciamo delle osservazioni preliminari che risulteranno utili per la dimostrazione successiva del teorema.

(a) Se (P,m) è una bandiera di Π_l e $\left|G_{(P,m)}\right| = k$ allora $|G| = kn^2(n+1)$.

Poichè G è transitivo sulle bandiere $\left|(P,m)^G\right| = n^2(n+1)$ e da $|G| = \left|G_{(P,m)}\right| \left|(P,m)^G\right|$ segue $|G| = kn^2(n+1)$.

(b) Se m è una retta di Π_l allora $|G_m| = kn$.

Se consideriamo l'azione di G_m sui punti di m si ha $|G_m| = \left|G_{(P,m)}\right| \left|P^{G_m}\right| = kn$ essendo G_m transitivo sui punti affini di m.

(c) Se P è un punto di Π_l allora $|G_P| = k(n+1)$.

Sia P un punto di Π_l, allora $|G| = |G_P| \left|P^G\right|$. Essendo G transitivo sui punti affini di Π_l si ha $\left|P^G\right| = n^2$ e poichè $|G| = kn^2(n+1)$ segue $kn^2(n+1) = |G_P|\, n^2$ e quindi $|G_P| = k(n+1)$.

(d) Se A è un punto di l allora $|G_A| = kn^2$.

Poichè G è transitivo sui punti di l che sono $n+1$, da $|G| = |G_A| \left|A^G\right|$ segue $kn^2(n+1) = |G_A|\,(n+1)$ e quindi $|G_A| = kn^2$.

(e) Se $A, B \in l$ ed r,s sono due rette affini per B, allora $|G_{A,B,r}| = |G_{A,B,s}|$.

Se $A = B$ la tesi è immediata. Supponiamo allora $A \neq B$ e siano P, Q punti di Π_l. Per la transitività di G sulle bandiere, esiste $\alpha \in G$ tale che $(P, AP)^\alpha = (Q, AQ)$. Poichè α fissa A, $\alpha \in G_A$. Quindi G_A è transitivo sui punti di Π_l, in quanto i punti P e Q sono stati scelti arbitrariamente in Π_l. Se $B \in l$, per il Lemma di Wagner allora $G_{A,B}$ è transitivo sul fascio di rette di centro B, ossia $\left|r^{G_{A,B}}\right| = \left|s^{G_{A,B}}\right|$ e quindi da

$|G_{A,B}| = |G_{A,B,r}| \left|r^{G_{A,B}}\right| = |G_{A,B,s}| \left|s^{G_{A,B}}\right|$ segue $|G_{A,B,r}| = |G_{A,B,s}|$.

Proviamo ora che n è potenza di un numero primo.

Sia Φ un sottopiano di Π con le seguenti proprietà:

(1) esiste un 2-sottogruppo M di G (anche banale) tale che $Fix(M) = \Phi$,

(2) non esiste un sottopiano proprio di Φ con la proprietà (1).

Se $M = \langle 1 \rangle$ allora $\Phi = \Pi$ e quindi un tale sottopiano Φ esiste.

Osserviamo che $l^G = l$, quindi l è una retta di Φ. Sia M un 2-sottogruppo di G e supponiamo che M sia massimale rispetto alla proprietà $Fix(M) = \Phi$. Denotiamo con F il sottogruppo di G che muta in sè Φ_l globalmente. Inoltre, sia 2^a la massima potenza di 2 che divide $n+1$, in simboli $2^a \parallel n+1$, e $2^b \parallel k$. Poniamo $|M| = 2^c$.

(f) Ogni bandiera di Φ_l è fissata da un elemento di F che induce una omologia involutoria in Φ_l.

Osserviamo che le omologie involutorie in Φ_l sono di due tipi distinti o hanno centro in un punto affine e asse improprio l, oppure hanno asse affine e centro in un punto improprio. Sia (P,m) una bandiera di Φ_l. Chiaramente poichè M fissa tutto Φ_l, si ha

$M \subset G_{(P,m)}$. Per ipotesi $\left|G_{(P,m)}\right| = k$ e $2^b \parallel k$, quindi un 2-sottogruppo di Sylow di $G_{(P,m)}$ ha ordine 2^b. Poichè $M \subset G_{(P,m)}$ ed M è un 2-sottogruppo di G allora $2^c \mid 2^b$. Poichè n è dispari e $2^a \parallel n+1$ segue che $a \geq 1$. Allora $a+b \geq 1+b$. Ricordiamo che $|G| = kn^2(n+1)$ con n dispari, quindi da $2^a \parallel n+1$ e $2^b \parallel k$ segue che $2^{a+b} \parallel |G|$. Quindi 2^{a+b} è l'ordine di un 2-sottogruppo di Sylow Q di G. Poichè $c \leq b$ si ha che $a+b > b \geq c$, da cui $a+b > c$ e $M < Q$. Costruiamo ora una catena di 2-sottogruppi $M < M_1 < M_2 < ... < Q$ in modo tale che $[M_{i+1} : M_i] = 2$ e quindi $M_i \lhd M_{i+1}$. Sia allora M_1 tale che $[M_1 : M] = 2$. Poichè $M \lhd M_1$ si ha che M_1 muta in sè Φ_l e quindi $M_1 \leq F$. Sia $\overline{M} = \frac{M_1}{M} = \langle \sigma \rangle$ il sottogruppo indotto su Φ_l. Se σ fosse una involuzione di Baer allora esisterebbe un sottopiano Φ_0 di Φ con la proprietà di essere fissato da M_1 che è un 2-sottogruppo di G. Quindi σ non è una involuzione di Baer. Se Π ha ordine $n = m^{2^t}$ dispari allora Φ ha ordine m anch'esso dispari. Quindi σ è una omologia involutoria in Φ_l che fissa sicuramente una bandiera (R, s) di Φ_l. Chiaramente $M < M_1 \leq G_{(R,s)}$ e $\left|G_{(R,s)}\right| = k$. Abbiamo posto $|M| = 2^c$ da cui $|M_1| = 2^{c+1} \leq 2^b$ essendo 2^b l'ordine di un 2-sottogruppo di Sylow di $G_{(R,s)}$. Quindi $c < b$ ed M non è un 2-sottogruppo di Sylow di $G_{(P,m)}$. Allora esiste un 2-sottogruppo M_2 tale che $M < M_2 \leq G_{(P,m)}$ e $[M_2 : M] = 2$. Analogamente M_2 induce una omologia involutoria in Φ_l che fissa la bandiera (P, m).

(g) Siano $A, B \in l$ e $A, B \in \Phi$. Inoltre, siano h e k due rette di Φ_l per B. Se F contiene una collineazione che fissa A, B ed h e induce un'omologia involutoria in Φ_l, allora F contiene anche una collineazione che fissa A, B e k e induce un'omologia involutoria in Φ_l.

Sia F_0 il sottogruppo di F che fissa puntualmente Φ, cioè il nucleo della rappresentazione di F su Φ. Allora F_0 è normale in F e $M \leq F_0$. In particolare F_0 è normale in $F_{A,B,h}$. Per le nostre ipotesi $F_{A,B,h}/F_0$ contiene una involuzione perchè abbiamo supposto che in F esiste un elemento che fissa A, B e h che induce una involuzione su Φ che ritroviamo nel quoziente $F_{A,B,h}/F_0$. Ne segue che M non è un 2-sottogruppo di Sylow in $G_{A,B,h}$ perchè $M < F_0$ e il quoziente $F_{A,B,h}/F_0$ non può avere ordine dispari. In *(e)* abbiamo dimostrato che $|G_{A,B,h}| = |G_{A,B,k}|$, cioè M non è neanche un 2-sottogruppo di Sylow in $G_{A,B,k}$. Allora esiste un 2-sottogruppo M_1 di $G_{A,B,k}$, contenente M e tale che $[M_1 : M] = 2$. Poichè M è normale in M_1 ed M_1 muta in sè gli elementi fissati da un suo sottogruppo normale, si ha che M_1 muta in sè Φ_l e induce una involuzione. Se M_1 inducesse in Φ_l una involuzione di Baer, allora Φ_l conterrebbe un sottopiano proprio fissato da M_1 contro l'ipotesi. Dunque M_1 induce in Φ_l una omologia involutoria che fissa A, B e k.

(h) L'ordine di Π_l è potenza di un primo.

Abbiamo dimostrato che :"Se Π è un piano proiettivo di ordine n e G è un 2-gruppo di collineazioni di Π tale che $Fix(G)$ è un sottopiano di ordine m, allora $n = m^{2^t}$ per qualche intero t". Per dimostrare la tesi è quindi sufficente provare che l'ordine di Φ_l è potenza di un primo. Sia $\overline{F} = F/F_0$ il gruppo delle collineazioni indotte da F in Φ_l. Esaminiamo diversi casi:

I Caso. $\overline{F}$ *non contiene un'omologia involutoria con centro un punto di* Φ_l.

Per *(f)*, ogni bandiera è mutata in sè da una omologia involutoria $\sigma \in \overline{F}$ che ricordiamo può essere di uno dei due seguenti tipi:

$\left\langle \begin{array}{l} (O,l)\text{-omologia con centro proprio e asse improprio} \\ (A,a)\text{-omologia con centro improprio e asse proprio} \end{array} \right.$

Allora sicuramente esiste una (A,a)-omologia involutoria $\sigma \in \overline{F}$ con $A \in l$ e a retta di Π_l. Poniamo $B = l \cap a$ e sia c una retta di Φ_l per B. Osserviamo che σ fissa A, B e a. Per *(g)*, $\overline{F}$ contiene una omologia involutoria γ che fissa A, B e c. Supponiamo che c non sia l'asse di γ. Allora B è il centro di γ e l'asse b di γ passa per A. Si hanno allora due omologie involutorie tali che il centro dell'una, ossia il punto B centro di γ, giace sull'asse dell'altra, ossia la retta a asse di σ. Per la Prop. 2.25, $\sigma\gamma$ è una $(a \cap b, AB)$-omologia involutoria. Poichè $AB = l$ e $a \cap b \in l$ si ha che $\sigma\gamma$ è una omologia involutoria con asse e centro impropri, contro l'ipotesi. Quindi, ogni retta di Φ_l per B è asse di un'omologia involutoria in $\overline{F}$ con centro A. Per il duale del Teorema di Andrè le rette di Φ_l per B sono tutte nella stessa orbita rispetto a $\overline{F}(A,A)$. Un'elazione di centro A che trasforma una retta per B in una retta per B deve avere asse $AB = l$. Quindi, Φ è (A,l)-transitivo. Se esiste una omologia involutoria in $\overline{F}$ con centro C distinto da A, allora possiamo ripetere un ragionamento analogo a quanto fatto per A e concludere che Φ è anche (C,l)-transitivo e quindi l è una retta di traslazione. In questo caso, per il Cor. 2.57, Φ_l ha ordine una potenza di un primo. L'ultimo caso da esaminare è che tutte le omologie involutorie in $\overline{F}$ abbiano centro A. Per *(f)* ogni bandiera (P,p) è fissata da una omologia involutoria, quindi ogni retta p di Φ_l che non passa per A è asse di una omologia involutoria in $\overline{F}$. Se l'ordine di Φ_l è m, allora le rette di Φ_l sono $m^2 + m$ di cui m sono le rette per A. Le rimanenti m^2 rette, ciascuna asse di una omologia involutoria di centro A, per il duale del Teorema di Andrè, stanno tutte in una stessa orbita. Il piano Φ allora è il duale di un piano di traslazione e nuovamente il suo ordine è potenza di un numero primo.

II Caso. Esiste esattamente un punto O *in* Φ_l *che è il centro di un'omologia involutoria di* $\overline{F}$.

Siano $P, Q \in l$ e sia B un punto di OQ, distinto da O e da Q. Per *(f)* esiste una omologia involutoria $\sigma \in \overline{F}$ che fissa la bandiera (B, BP). Poichè O è il centro di tutte le omologie involutorie, $O^\sigma = O$, inoltre σ fissando O e Q, fissa la retta OQ che non passando per il punto P deve essere l'asse di σ. Dunque σ deve essere una (P, OQ)-omologia. Allora Φ_l ha ordine la potenza di un primo per il Cor. 2.57.

III Caso. Esistono due punti distinti di Φ_l *che sono centri di omologie involutorie in* $\overline{F}$.

I Sottocaso. Supponiamo che ogni retta di Φ_l contenga il centro di un'omologia involutoria in $\overline{F}$.

Sia $A \in l$ e sia m una retta di Φ_l per A. Allora m contiene il centro B di una (B,l)-omologia involutoria σ. Poichè m passa per B, si ha che σ fissa m e nessun altra retta per A. Il gruppo delle omologie involutorie che fissano A, quindi, fissa una retta per

A e nessun altra. Per il Lemma di Gleason, $\overline{F}_A$ è transitivo sulle rette affini di Φ_l per A. Poichè il punto A è stato scelto in modo arbitrario, possiamo applicare il Lemma di Wagner secondo cui: "un gruppo di collineazioni G agisce transitivamente sui punti di Π_l se e solo se G_P è transitivo sulle rette affini per P, per ogni $P \in l$" e concludere che $\overline{F}$ è transitivo sui punti di Φ_l. Allora ogni punto di Φ_l è centro di una omologia di asse l e per il Teorema di Andrè $\overline{F}(l,l)$ è transitivo sui punti di Φ_l che risulta essere un piano di traslazione.

II Sottocaso. Supponiamo che esista una retta m di Φ_l che non contenga alcun centro di omologie involutorie in $\overline{F}$.

Poniamo $B = m \cap l$ e sia $A \in l$, $A \neq B$. Sia inoltre P un punto affine, centro di una omologia. Esiste, allora, una omologia involutoria in $\overline{F}$ che fissa i punti A e B, perchè appartengono all'asse l, e la retta BP, perchè passa per il centro P. Per *(g)* esiste una omologia involutoria ρ in $\overline{F}$ che fissa A, B ed m. Se m è l'asse di ρ, allora A è il suo centro, mentre se m non è l'asse di ρ allora B è il centro di ρ poichè m non contiene alcun centro affine. In entrambi i casi, A è l'unico punto fisso di ρ su $l - \{B\}$. Per l'arbitrarietà della scelta di A possiamo applicare il Lemma di Gleason e concludere che $\overline{F}_{(B,m)}$ è transitivo su $l - \{B\}$. Poichè ci sono almeno due centri P e Q di omologie di asse l che stanno nella stessa orbita di punti, $\overline{F}$ contiene una traslazione non banale.

Se $\overline{F}$ non fissa B si ha un altro punto B', che è il trasformato di B, che gode delle stesse proprietà di B, cioè B' è tale che $\overline{F}_{(B',m)}$ è transitivo su $l - \{B'\}$. Da ciò segue la transitività di $\overline{F}$ su l. Infatti, siano $A, A' \in l$. Se sono entrambi distinti sia da B che da B' allora esiste ad esempio $\alpha \in \overline{F}_{(B',m)}$ tale che $A^\alpha = A'$. Se $A' \neq B, B'$ e $A = B$ (o $A = B'$) allora esiste $\beta \in \overline{F}_{(B',m)}$ (o $\beta \in \overline{F}_{(B,m)}$) tale che $A^\beta = A'$. Se $A = B$ e $A' = B'$ allora consideriamo un punto $C \neq B, B'$. Esiste $\beta \in \overline{F}_{(B',m)}$ tale che $A^\beta = C$ ed esiste $\gamma \in \overline{F}_{(B,m)}$ tale che $C^\gamma = A'$. Quindi $A^{\beta\gamma} = C^\gamma = A'$. Per il Teorema di Hughes quindi Φ_l è un piano di traslazione.

Supponiamo che $\overline{F}$ fissi B. Sia C un punto di Φ_l su m e sia $A \in l$, $A \neq B$. Per *(f)* esiste una omologia involutoria ρ in $\overline{F}$ che fissa la bandiera (C, CA). Ci sono due possibilità: ρ è una (A, CB)-omologia oppure è una (B, CA)-omologia. Supponiamo che ρ sia una (A, CB)-omologia. Usando le stesse argomentazioni precedenti, possiamo provare che $\overline{F}_{B,C}$ è transitivo su $l - \{B\}$ e quindi una coniugata di ρ è una omologia con lo stesso asse CB ma centro X distinto da A. Ogni punto X su $l - \{B\}$ è quindi il centro di una (X, CB)-omologia involutoria. Per il Teorema di Andrè allora, Φ è (B, CB)-transitivo. Sia ora ρ una (B, CA)-omologia, allora ogni retta x per C distinta da CB, è l'asse di una (B, x)-omologia e nuovamente Φ è (B, CB)-transitivo per il duale del Teorema di Andrè.

Possiamo allora assumere che Φ è (B, CB)-transitivo. Sappiamo che esistono almeno due punti distinti di Φ_l che sono centri di omologie di asse l. Sia $\alpha \in \overline{F}$ una di queste omologie. Chiaramente, $(CB)^\alpha = C^\alpha B^\alpha = C^\alpha B \neq CB$ e quindi Φ è anche $(B, (CB)^\alpha)$-transitivo. Per il duale del Cor. 2.33 quindi, possiamo affermare che Φ è il duale di un piano di traslazione il cui ordine è, per il punto *(h)*, uguale a p^r per qualche primo p.

Allora anche l'ordine di Φ è p^r.

Sia P un p-sottogruppo di Sylow di G e sia $p^t \parallel k$. Allora $|P| = p^{2r+t}$ perchè da $n^2 = p^{2r}$ e $|G| = kn^2(n+1)$ segue che $p^{2r+t} \parallel |G|$. Se C è un punto di Π_l, allora $|P_C| = p^t$ essendo $|G_C| = k(n+1)$ per *(c)* e $p^t \parallel k(n+1)$. Se consideriamo $|P| = |P_C| \left|C^P\right|$, da $|P| = p^{2r+t}$ e $|P_C| = p^t$ segue che $\left|C^P\right| = p^{2r} = n^2$. Quindi P è transitivo sui punti di Π_l. Ogni orbita di P su l ha una lunghezza che è divisibile per p e la somma delle lunghezze delle orbite è $n+1$. Poichè p non divide $n+1$ allora esiste un punto $A \in l$ tale che $A^P = A$. Sia $B \in l$, $B \neq A$. Allora $|P| = \left|B^P\right| |P_B|$ e $\left|B^P\right| \leq n = p^r$ perchè i punti di l distinti da A sono n. Ora $|P_B| \geq p^r$ essendo $|P| = p^{2r+t}$ ossia $p^r \mid |P_B|$. Scegliamo $B \in l$, $B \neq A$, tale che P_B abbia ordine massimo. Sia F un punto fisso di P_B su $l - \{A\}$. Allora $P_B = P_{B,F} \leq P_F$, ma P_B ha ordine massimo quindi $P_B = P_F$. Poichè P è transitivo sui punti di Π_l, P_B agisce transitivamente sull'insieme delle rette affini per F per ogni punto $F \in l$ che sia fissato da P con $F \neq A$. Sia S un p-sottogruppo di Sylow di G_B contenente P_B. Per *(d)*, $|G_B| = kn^2$ quindi se $p^u \parallel kn^2$ allora $p^u \parallel kn^2(n+1)$. Quindi S è un p-sottogruppo di Sylow di G essendo $|G| = kn^2(n+1)$. Inoltre, da $P_B \leq S$ segue che $P_{B,A} \leq S_A$. Quindi $P_B \leq S_A$ poichè P_B fissa A. Ciò implica $P_B = S_A$, essendo P ed S coniugati pochè entrambi sottogruppi di Sylow. Allora P_B è transitivo sull'insieme delle rette affini per A.

Ora, sia $\tau \in Z(P_B)$, $\tau \neq 1$ essendo il centro di un p-gruppo non identico. Allora τ fissa i punti A e B in l. Per il Teor. 2.41 τ fissa almeno una retta affine m di Π_l. Se il punto $m \cap l$ non è fissato da P_B, allora esiste $\alpha \in P_B$ tale che $m^\alpha \cap m$ è un punto affine. Abbiamo allora che $(m^\alpha \cap m)^\tau = m^{\alpha\tau} \cap m^\tau = m^{\tau\alpha} \cap m^\tau = m^\alpha \cap m$. quindi $(m^\alpha \cap m)A$ è una retta fissata da τ. Poichè $((m^\alpha \cap m)A) \cap l = A$, abbiamo che esiste sempre una retta affine fissata da τ, passante per un punto di l fissato da P_B. Poichè P_B è transitivo sulle rette per A diverse da l si ha $\left|m^{P_B}\right| = n$ ed inoltre ogni retta per A diversa da l è della forma m^α con $\alpha \in P_B$. Ora $m^{\alpha\tau} = m^{\tau\alpha}$, essendo τ centrale, e $m^{\tau\alpha} = m^\alpha$ implica che τ fissa ogni retta per A. Allora τ, fissando tutte le rette per A ed il punto B, è una elazione di asse AB. Ossia τ è una traslazione di Π_l di centro A. G è transitivo su l e quindi per il Teorema di Hughes possiamo concludere che Π_l è un piano di traslazione. ■

Teorema 2.61 *(Ostrom-Wagner) Sia* Π *un piano proiettivo finito con un gruppo* G *di collineazioni che agisce 2-transitivamente sull'insieme dei punti di* Π. *Allora* Π *è desarguesiano di ordine* q *e* G *contiene* $PSL(3,q)$.

Dim. Sia Q un punto di Π e siano P,P' due punti distinti da Q. Per la 2-transitività di G sui punti possiamo affermare che esiste una collineazione α di G che porta la coppia (Q,P) nella coppia (Q,P'), ossia $(Q,P)^\alpha = (Q^\alpha, P^\alpha) = (Q,P')$. Questo ci dice che G_Q è transitivo sui punti di Π distinti da Q e quindi, G_Q ha due orbite di punti: $\{Q\}$ e l'insieme dei punti $\Pi - \{Q\}$. Per il Teorema dell'orbita, G_Q ha due orbite di rette. Una consiste delle rette per Q e l'altra delle rette che non passano per Q. Sia l una retta di Π. Chiaramente G_l è transitivo sui punti di l. Siano A, B due punti di Π non appartenenti ad

l. Allora esiste $\beta \in G$ tale che $A^\beta = B$. Da $A \notin l$ segue che $A^\beta \notin l^\beta$ ossia $B \notin l^\beta$. Poichè l ed l^β sono rette di Π che non passano per B, esse sono nella stessa orbita di rette rispetto a G_B, quindi esiste $\alpha \in G_B$ tale che $(l^\beta)^\alpha = l$. Allora $l^{\beta\alpha} = l$ e $A^{\beta\alpha} = B^\alpha = B$. Quindi G_l è transitivo sui punti di Π che non appartengono ad l. Avendo già osservato che G_l transitivo sui punti di l, possiamo concludere che G_l ha due orbite di punti: l'insieme dei punti di l e l'insieme dei punti di Π_l. Allora G_l ha due orbite di rette: $\{l\}$ e l'insieme di tutte le rette di Π_l. In conclusione G_l è transitivo sulle rette affini di Π_l. Per il Teorema di Wagner l è una retta di traslazione per Π. Poichè ogni retta di Π è una retta di traslazione, Π è un piano di Moufang, ma ogni piano di Moufang finito è desarguesiano. Inoltre G contiene tutte le elazioni di Π e quindi contiene $PSL(3, q)$. ■

3 Elementi di Teoria dei Piani di Traslazione.

Sia $(\mathcal{P}, \mathcal{L}, \in)$ una struttura d'incidenza.

Definizione 3.1 $(\mathcal{P}, \mathcal{L})$ *è detta* Struttura di Andrè *se soddisfa i seguenti assiomi:*

1. *due punti distinti appartengono ad una ed una sola retta;*
2. *esiste una relazione di equivalenza su $\mathcal{L}$ tale che ogni classe di equivalenza è una partizione di $\mathcal{P}$;*
3. *esistono* 3 *punti distinti non appartenenti tutti ad una stessa retta.*

La relazione di equivalenza definita su $\mathcal{L}$ è detta *parallelismo* ed è indicata con il simbolo $\|$. Due rette che appartengono alla stessa classe di equivalenza si dicono *parallele* e le classi di equivalenza sono dette *classi di parallelismo*.

Osserviamo che dall'assioma 2 segue che, considerata una retta l ed un punto P non appartenente ad essa, esiste ed è unica la retta s della classe $[l]_{\|}$ che passa per P, ossia esiste una unica retta per P parallela ad l.

Una Struttura di Andrè per cui tutte le rette hanno la stessa cardinalità è detta uno *Spazio di Sperner*.

Definizione 3.2 *Siano $(\mathcal{P}, \mathcal{L})$ ed $(\mathcal{P}', \mathcal{L}')$ due strutture di Andrè. Si definisce* isomorfismo *tra $(\mathcal{P}, \mathcal{L})$ ed $(\mathcal{P}', \mathcal{L}')$ una corrispondenza biunivoca*

$$\alpha : \mathcal{P} \cup \mathcal{L} \to \mathcal{P}' \cup \mathcal{L}'$$

tale che:

1. *$\mathcal{P}^\alpha = \mathcal{P}'$ e $\mathcal{L}^\alpha = \mathcal{L}'$;*
2. *α conserva l'appartenenza ed il parallelismo.*

Se $(\mathcal{P}, \mathcal{L}) = (\mathcal{P}', \mathcal{L}')$ allora α è detto *automorfismo* di $(\mathcal{P}, \mathcal{L})$, o più comunemente *collineazione*

Si verifica immediatamente che gli automorfismi di una struttura di Andrè $(\mathcal{P}, \mathcal{L})$ formano un gruppo che si indica con $Aut((\mathcal{P}, \mathcal{L}))$.

Proposizione 3.3 *Sia α un collineazione di una struttura di André $(\mathcal{P}, \mathcal{L})$ con la seguente proprietà: $l^\alpha \| l$ per ogni $l \in \mathcal{L}$; allora α fissa al più un punto di $(\mathcal{P}, \mathcal{L})$.*

Dim. Sia P un punto di $\mathcal{P}$ tale che $P^\alpha = P$ e sia l una retta per P. Da $P \in l$ segue che $P = P^\alpha \in l^\alpha$ ossia $l \cap l^\alpha \neq \varnothing$. Allora da $l^\alpha \parallel l$ segue $l = l^\alpha$. Se per assurdo α fissasse due punti P, Q, allora, detto R un punto non appartenente alla retta PQ si avrebbe $(PR)^\alpha = PR$ e $(QR)^\alpha = QR$ da cui $R^\alpha = R$. Allora α fisserebbe tutti punti non appartenenti alla retta PQ. Se consideriamo i punti fissati P ed R e ripetiamo un ragionamento analogo al precedente otteniamo che α fissa tutti i punti non appartenenti alla retta PR. In definitiva α è l'identità. ■

In generale questo tipo di collineazioni si dicono *dilatazioni*.

- Se α fissa un punto, allora α è detta *dilatazione propria* (o più semplicemente *dilatazione*);

- Se α è priva di punti fissi è detta *traslazione*.

Definizione 3.4 *Una struttura di André* $(\mathcal{P}, \mathcal{L})$ *è detta* struttura (di André) di traslazione*, se esiste un gruppo* T *di traslazioni di* $(\mathcal{P}, \mathcal{L})$ *trasitivo su* $\mathcal{P}$*.*

Osserviamo che, in generale, le traslazioni di una struttura di Andrè non costituiscono un gruppo.

Nel caso finito, invece, le traslazioni costituiscono un gruppo per il teorema di Frobenius in quanto il gruppo D, costituito dalle collineazioni α tali che $l^\alpha \parallel l$ per ogni $l \in \mathcal{L}$, è un gruppo di Frobenius nella sua azione sui punti della struttura e le traslazioni sono quindi tutte e sole le collineazioni appartenenti al nucleo T di D.

Sia $(\mathcal{P}, \mathcal{L})$ una struttura di Andrè di traslazione, sia O un punto di $\mathcal{P}$ ed $\mathcal{S} = \{T_r : r \in \mathcal{L} \text{ e } O \in r\}$. Valgono le seguenti proprietà:

1. $\langle 1 \rangle \neq T_r \neq T$ per ogni $T_r \in \mathcal{S}$;
2. $T_r \cap T_s = \langle 1 \rangle$ per ogni $T_r, T_s \in \mathcal{S}$ con $T_r \neq T_s$:
3. $\bigcup_{O \in r} T_r = T$.

Verifichiamole:

1. Sia $P \in r$ e sia τ la traslazione che porta O in P. Allora $\tau \neq 1$ e $\tau \in T_r$ ossia $\langle 1 \rangle \neq T_r$. Banalmente si ha $T_r \neq T$.
2. Supponiamo per assurdo che esista $\sigma \in T_r \cap T_s$ allora da $r \cap s = O$ segue $O^\sigma = O$ e quindi $\sigma = 1$.
3. Sia $\tau \in T$ allora l'immagine di O tramite τ sarà un qualche punto Q e da $(OQ)^\tau = OQ$ segue $\tau \in T_{OQ}$.

Il sistema $\mathcal{S}$ di sottogruppi propri associato alla struttura di Andrè $(\mathcal{P}, \mathcal{L})$ così definito, è detto *partizione del gruppo* T e si indica con $(T, \mathcal{S})$. Gli elementi di $\mathcal{S}$ sono detti *componenti*. La partizione $\mathcal{S}$ è detta *non banale* se contiene almeno tre componenti.

Sia $(T, \mathcal{S})$ un gruppo con partizione (da questo momento in poi useremo per i gruppi la notazione additiva).

Definiamo una struttura di incidenza $\mathcal{A}(T, \mathcal{S})$ nel seguente modo:

1. i punti di $\mathcal{A}$ sono gli elementi di T;
2. le rette di $\mathcal{A}$ sono i laterali destri dei sottogruppi T_i in $\mathcal{S}$. Cioè sono tutti e soli gli elementi della forma $T_i + a$ con $T_i \in \mathcal{S}$ e $a \in T$;
3. l'incidenza è l'appartenenza.

Proposizione 3.5 *La struttura $\mathcal{A}(T, \mathcal{S})$ è una struttura di Andrè di traslazione.*

Dim. Siano u e v due punti distinti di $\mathcal{A}$. Allora $u - v \neq 0$ ed esiste uno ed un solo T_i tale che $u - v \in T_i$. Da $u - v \in T_i$ segue che $u, v \in T_i + v$, quindi due punti distinti appartengono ad una ed una sola retta.

Definiamo in $\mathcal{A}(T, \mathcal{S})$ una relazione che indichiamo con $\|$:

$$T_i + a \parallel T_j + b \Leftrightarrow T_i = T_j$$

Si verifica facilmente che $\|$ è una relazione di equivalenza e che ogni classe di equivalenza $[T_i + a]_{\|} = \{T_i + a \mid a \in T\}$ è una partizione di T. Poichè esistono 3 punti distinti di T che non appartengono tutti ad una stessa retta (la verifica è lasciata per esercizio) si può concludere che $\mathcal{A}(T, \mathcal{S})$ è una struttura di Andrè.

Proviamo ora che $\mathcal{A}(T, \mathcal{S})$ è una struttura di traslazione. Fissiamo $g \in T$ e consideriamo l'applicazione

$$\tau_g : x \mapsto x + g \quad \text{per ogni } x \in T.$$

Vogliamo provare che τ_g è una traslazione.

Si ha $(T_i + a)^{\tau_g} = (T_i + a) + g = T_i + (a + g)$ e quindi τ_g manda ogni retta in una ad essa parallela. Poichè τ_g non fissa alcun punto, essa è una traslazione.

Consideriamo infine due punti $a, b \in T$, allora esiste la traslazione τ_{-a+b} che porta a in b, infatti $a^{\tau_{-a+b}} = a + (-a + b) = b$. Il gruppo delle traslazioni è dunque transitivo sui punti di $\mathcal{A}(T, \mathcal{S})$ che risulta essere una struttura di Andrè di traslazione. ■

Se $\mathcal{A}$ è una struttura di Andrè di traslazione è possibile costruire un gruppo con partizione $(T(\mathcal{A}), \mathcal{S}(\mathcal{A}))$. Partendo da questo gruppo possiamo considerare la struttura di Andrè associata che indichiamo con $\mathcal{A}(T(\mathcal{A}), \mathcal{S}(\mathcal{A}))$. Si prova che $\mathcal{A} \cong \mathcal{A}(T(\mathcal{A}), \mathcal{S}(\mathcal{A}))$.

Quindi ogni struttura di Andrè di traslazione si può rappresentare come un gruppo con partizione.

Nel caso finito i gruppi con partizione sono stati ampiamente studiati e classificati sopratutto ad opera di Suzuki verso la fine degli anni '50.

Definizione 3.6 *Una partizione non banale $(T, \mathcal{S})$ è detta uno* spread *(o* partizione di congruenza*), se per ogni $T_i, T_j \in \mathcal{S}$ con $T_i \neq T_j$ risulta $T = T_i + T_j$.*

Proposizione 3.7 *Sia $\mathcal{S}$ uno spread di un gruppo T. Allora vale:*

1. *$T_i \lhd T$ per ogni $T_i \in \mathcal{S}$;*
2. *$T_i \cong T_j$ per ogni $T_i, T_j \in \mathcal{S}$.*

Dim. Siano $T_1 \in \mathcal{S}$, $x \in T$ e $h \in T_1$ con $h \neq 0$. Allora il coniugato di h tramite x sarà non nullo, ossia $x + h - x \neq 0$ ed esiste un unico $T_2 \in \mathcal{S}$ tale che $x + h - x \in T_2$. Cioè, $x + h \in T_2 + x$ e quindi vale che

$$T_2 + x + h = T_2 + x \tag{2}$$

in quanto i laterali non dipendono dalla scelta del rappresentante. Supponiamo sia $T_1 \neq T_2$. Poichè $\mathcal{S}$ è uno spread, si ha $T = T_2 + T_1$ e quindi esistono $h_i \in T_i$, con $i = 1, 2$, tali che $x = h_2 + h_1$. Quindi

$$T_2 + x + h = T_2 + (h_2 + h_1) + h = (T_2 + h_2) + h_1 + h = T_2 + h_1 + h$$

d'altra parte

$$T_2 + x = T_2 + (h_2 + h_1) = T_2 + h_1$$

per la (1)

$$T_2 + h_1 + h = T_2 + h_1$$

ossia $T_2 + (h_1 + h - h_1) = T_2$ da cui $h_1 + h - h_1 \in T_2$. Poichè $h, h_1 \in T_1$ allora $h_1 + h - h_1 \in T_1$ e quindi $h_1 + h - h_1 \in T_1 \cap T_2 = \langle 0 \rangle$ da cui $h_1 + h - h_1 = 0$ contro l'ipotesi $h \neq 0$. Allora deve essere $T_1 = T_2$ e quindi $x + h - x \in T_1$ cioè $T_1 \lhd T$. Ciò prova l'asserto 1.

Consideriamo una componente T_h e siano T_i e T_j due componenti di $\mathcal{S}$ distinte da T_h. Allora $T = T_h + T_i = T_h + T_j$. Dalla proprietà 1 segue che $(T_h + T_i)/T_h \cong T_i$ e analogamente $(T_h + T_j)/T_h \cong T_j$ da cui segue $T_i \cong T_j$. Se consideriamo $(T_i + T_h)/T_i \cong T_h$ e $(T_i + T_j)/T_i \cong T_j$ otteniamo $T_h \cong T_j$, possiamo allora concludere che $T_i \cong T_j$ per ogni $T_i, T_j \in \mathcal{S}$. ■

Corollario 3.8 *Se il gruppo T è finito, le componenti T_i di uno spread hanno tutte lo stesso ordine.*

Teorema 3.9 *(**Andrè 1954**)Sia $\mathcal{S}$ uno spread di un gruppo T. Allora vale:*

1. *$\mathcal{A}(T,\mathcal{S})$ è un piano affine di traslazione;*
2. *Se $g \in T$, l'applicazione $\tau_g : x \to x+g$ è una traslazione di $\mathcal{A}(T,\mathcal{S})$;*
3. *$\tau : T \to T(\mathcal{A}(T,\mathcal{S}))$, dove $T(\mathcal{A}(T,\mathcal{S}))$ è il gruppo delle traslazioni di $\mathcal{A}(T,\mathcal{S})$, è un isomorfismo di gruppi;*
4. *Il gruppo T è abeliano.*

Dim. 1. Proviamo che $\mathcal{A}(T,\mathcal{S})$ è un piano di traslazione. Poichè $\mathcal{A}(T,\mathcal{S})$ è una struttura di Andrè, per due punti distinti passa una ed una sola retta. Siano ora $T_i \in \mathcal{S}$ e $a, b \in T$ tali che $a \notin T_i + b$. Allora $T_i + a \cap T_i + b = \varnothing$, cioè esiste una retta per a che non interseca la retta $T_i + b$. Sia $T_j + c$ una retta per a distinta da $T_i + a$, allora $T_j + c = T_j + a$ con $T_j \neq T_i$. Poichè $b - a \in T$ e $T = T_i + T_j$ allora esistono $v \in T_i$ ed $x \in T_j$ tali che $b - a = v + x$. Se poniamo $y = -v$ allora $b - a = -y + x$ ossia $y + b = x + a$. da $y + b \in T_i + b$ e $x + a \in T_j + a$ segue $T_i + b \cap T_j + a \neq \varnothing$, quindi abbiamo provato che per a passa una ed una sola retta che non interseca $T_i + b$.

Resta da provare che esistono tre punti non allineati. Siano T_i e T_j due componenti distinte di $\mathcal{S}$, la loro esistenza è assicurata dalla non banalità di $\mathcal{S}$. Consideriamo i punti $a \in T_i$, $b \in T_j$ e 0. La retta T_i contiene a e 0, ma non contiene b, quindi i tre punti a, b e 0 non sono allineati. Abbiamo così provato che $\mathcal{A}(T,\mathcal{S})$ è un piano di traslazione.

2. Sia $g \in T$, e si consideri l'applicazione $\tau_g : x \to x + g$ per ogni punto x di $\mathcal{A}(T,\mathcal{S})$. Abbiamo già provato nella Prop. 3.5 che τ_g è una traslazione di $\mathcal{A}(T,\mathcal{S})$.

3. Sia $\tau : T \to T(\mathcal{A}(T,\mathcal{S}))$ tale che $\tau : g \to \tau_g$ per ogni $g \in T$. Siano $g, h \in T$, vogliamo provare che $\tau_{g+h} = \tau_g \tau_h$. Sia $x \in T$ allora

$$x^{\tau_{g+h}} = x + (g+h) = (x+g) + h = x^{\tau_g} + h = (x^{\tau_g})^{\tau_h} = x^{\tau_g \tau_h}$$

chiaramente τ è suriettiva ed è quindi un isomorfismo da T su $T(\mathcal{A}(T,\mathcal{S}))$.

4. L'asserto segue immediatamente dall'asserto 3. ■

Teorema 3.10 *Sia Π_l un piano di traslazione rispetto alla retta l e sia $G(l,l)$ il gruppo delle traslazioni. allora $\mathcal{S} := \{G(P,l) \mid P \in l\}$ è una partizione di $G(l,l)$ e $\mathcal{A}(G(l,l),\mathcal{S}) \simeq \Pi_l$.*

Dim. Per esercizio. ■

In virtù dei teoremi precedenti possiamo assumere che un piano di traslazione sia della forma $\mathcal{A}(V,\mathcal{S})$, cioè si ottenga a partire da uno spread $\mathcal{S}(V)$ di un gruppo abeliano $(V,+)$.

Si consideri l'insieme

$$K(V,\mathcal{S}) = \{\varphi \in End(V) : X^\varphi = X \text{ per ogni } X \in \mathcal{S}\}.$$

Come è noto in $End(V)$ si può definire una operazione di *somma* nel seguente modo:
$\forall \varphi, \omega \in End(V)$, $\forall v \in V$ la somma $\varphi + \omega$ è tale che

$$\varphi + \omega : v \to v^{\varphi+\omega} = v^\varphi + v^\omega$$

e una operazione di *prodotto* nel seguente modo:
$\forall \varphi, \omega \in End(V)$, $\forall v \in V$ il prodotto $\varphi \circ \omega$ è tale che

$$\varphi \circ \omega : v \to v^{\varphi\circ\omega} = (v^\varphi)^\omega$$

E' altresì noto che $(End(V), +, \circ)$ è un anello dotato di unità.

Si prova facilmente che $K(V,\mathcal{S})$ è un sottoanello di $End(V)$. Infatti se consideriamo $\varphi, \omega \in K(V,\mathcal{S})$ e $v \in X$, vale:

1. $v^{\varphi+\omega} = v^\varphi + v^\omega \in X$ essendo $v^\varphi, v^\omega \in X$
2. $v^{-\varphi} = (-v)^\varphi \in X$ essendo $-v \in X$
3. $v^{\varphi\omega} = (v^\varphi)^\omega \in X$ essendo $v^\varphi \in X$.

Teorema 3.11 *Sia $(V,\mathcal{S})$ una partizione non banale di un gruppo V abeliano.*

1. *Se $\varphi \in K(V,\mathcal{S})$, $\varphi \neq 0$, allora φ è iniettivo e $K(V,\mathcal{S})$ è un dominio di integrità*[1]*;*
2. *Se $\mathcal{A}(V,\mathcal{S})$ è un piano (di traslazione), allora $K(V,\mathcal{S})$ è un corpo*[2]*.*

Dim. 1. Sia $\varphi \in K(V,\mathcal{S})$, $\varphi \neq 0$ e supponiamo che esista $u \in Ker(\varphi)$ con $u \neq 0$. Allora esiste un unico $X \in \mathcal{S}$ tale che $u \in X$. Sia $v \in V - X$, $v \neq 0$. Allora esiste $Y \in \mathcal{S}$ tale che $v \in Y$, $Y \neq X$. Vale $u + v \in Z$ con $X \neq Z \neq Y$, $Z \in \mathcal{S}$. Inoltre $v^\varphi \in Y$ e

$$(u+v)^\varphi = u^\varphi + v^\varphi \text{ e } u \in Ker(\varphi) \Rightarrow\ u^\varphi + v^\varphi = 0 + v^\varphi = v^\varphi. \tag{3}$$

Poichè $u+v \in Z$ e $\varphi \in K(V,\mathcal{S})$ allora $(u+v)^\varphi \in Z$ e da (3) segue $(u+v)^\varphi \in Y \cap Z = \langle 0 \rangle$. Si ottiene quindi $v^\varphi = 0$. Pertanto $V - X \subseteq Ker(\varphi)$. Con un ragionamento analogo si ottiene che $u^\varphi = 0$ per ogni $u \in X$, cioè φ è l'endomorfismo nullo, contro le ipotesi fatte. L'assurdo deriva dall'aver supposto che esiste $u \in Ker(\varphi)$ con $u \neq 0$, pertanto φ è iniettivo e l'asserto 1 è provato.

[1] Un dominio di integrità è una anello privo di divisori dello zero non banali.
[2] Nel caso finito $K(V,\mathcal{S})$ è un campo per il Teorema di Weddeburn.

Verifichiamo ora che $K(V,\mathcal{S})$ è un dominio di integrità: siano $\varphi,\omega \in K(V,\mathcal{S})$ tali che $\varphi\omega = 0$. Allora per ogni $u \in V$ si ha $u^{\varphi\omega} = 0$ cioè $(u^{\varphi})^{\omega} = 0$. Se $\varphi \neq 0$ esiste $u^{\varphi} \neq 0$ con $u^{\varphi} \in Ker(\omega)$ e, quindi, $\omega = 0$.

2. Verifichiamo che $\varphi \in K(V,\mathcal{S})$, $\varphi \neq 0$, è suriettivo e quindi è invertibile. Poichè abbiamo già provato in 1 che $K(V,\mathcal{S})^*$ è chiuso rispetto al prodotto, ne segue che $K(V,\mathcal{S})$ è un corpo. Sia $\varphi \in K(V,\mathcal{S})$ e sia $v \in V$, $v \neq 0$, e sia X l'unica componente di $\mathcal{S}$ che contiene v. Poichè $\mathcal{S}$ è non banale, esiste $Y \in \mathcal{S}$ con $Y \neq X$. Sia $u \in Y$, $u \neq 0$. Da 1 segue che $u^{\varphi} \neq 0$. Se fosse $u^{\varphi} = v$ si avrebbe $v \in Y$ e quindi $v \in X \cap Y = \langle 0 \rangle$ contro l'ipotesi $v \neq 0$. Quindi $u^{\varphi} \neq v$ da cui $u^{\varphi} - v \neq 0$. Allora esiste $Z \in \mathcal{S}$ tale che $u^{\varphi} - v \in Z$. Poichè $v \in X$ e $u^{\varphi} \notin X$, allora $u^{\varphi} - v \notin X$ cioè $Z \neq X$. Osserviamo che $Z + u$ e X sono rette di $\mathcal{A}(V,\mathcal{S})$ non parallele. Pertanto esiste $w \neq 0$ tale che $w \in (Z+u) \cap X$. Poichè $w \in Z + u$ allora $w - u \in Z$ e quindi $(w-u)^{\varphi} \in Z$, ossia $w^{\varphi} - u^{\varphi} \in Z$. Poichè $u^{\varphi} - v \in Z$, allora $w^{\varphi} - v = (w^{\varphi} - u^{\varphi}) + (u^{\varphi} - v) \in Z$. D'altra parte $w \in X$ e quindi $w^{\varphi} \in X$. Poichè $v \in X$, $w^{\varphi} - v \in X$. Pertanto, $w^{\varphi} - v \in X \cap Z = \langle 0 \rangle$ e quindi $v = w^{\varphi}$. Questo prova che φ è suriettivo. ■

Osservazione 3.12 *Come conseguenza del teorema precedente si ha che V può essere considerato come uno spazio vettoriale su $K := K(V,\mathcal{S})$. Le componenti X di $\mathcal{S}(V)$ sono sottospazi di V.*

Consideriamo il caso in cui $\mathcal{A}(V,\mathcal{S})$ sia un piano affine. Per ogni coppia di componenti X,Y di $\mathcal{S}$ si ha $V = X \oplus Y$ con X, Y spazi vettoriali isomorfi.

Sia K il *nucleo* di $\mathcal{A}(V,\mathcal{S})$. Se $X \in \mathcal{S}$, la dimensione di X come sottospazio vettoriale su K, non dipende quindi dalla scelta di X. Tale dimensione, indicata con $\dim_K X$ è detta *dimensione sul nucleo del piano* $\mathcal{A}(V,\mathcal{S})$.

Se $\dim_K X$ è finita ed uguale ad n allora $\dim_K V = 2n$, essendo V somma diretta di due sottospazi aventi entrambi dimensione n.

I piani di traslazione di dimensione 1 sul nucleo sono quelli associati alla partizione costituita dai sottospazi 1-dimensionali di uno spazio vettoriale 2-dimensionale e quindi sono i piani desarguesiani. Se consideriamo i piani di traslazione di dimensione maggiore di 1 sul nucleo, otteniamo piani non desarguesiani.

Corollario 3.13 *Sia $\mathcal{A}(V,\mathcal{S})$ un piano di traslazione di finito, allora l'ordine di $\mathcal{A}(V,\mathcal{S})$ è la potenza di un numero primo.*

Dim. Se V è uno spazio vettoriale di dimensione k su un campo finito F, si ha $|F| = p^h$ con p primo e $|V| = |F|^k$ poichè $V \simeq F^k$. Quindi l'ordine di $\mathcal{A}(V,\mathcal{S})$, essendo uguale a $|F|^{\frac{k}{2}} = (p^h)^{\frac{k}{2}}$, è la potenza di un numero primo. ■

Sia $\mathcal{A}(V,\mathcal{S})$ un piano di traslazione, G il gruppo di tutte le collineazioni di $\mathcal{A}(V,\mathcal{S})$ e T il gruppo delle traslazioni del piano.

Sia $\alpha \in G$ e supponiamo che $0^\alpha = a$. Se consideriamo la traslazione $\tau_{-a} \in T$ allora $0^{\alpha\tau_{-a}} = a^{\tau_{-a}} = 0$ ossia $\alpha\tau_{-a} \in G_0$, pertanto G è il prodotto semidiretto di T con G_0 e la determinazione del gruppo delle collineazioni coincide, nella sostanza, con la determinazione del gruppo G_0, che è detto *complemento delle traslazioni*.

Teorema 3.14 *Siano $(V,\mathcal{S})$ e $(V',\mathcal{S}')$ due spazi vettoriali con spread. Se σ è un isomorfismo di $\mathcal{A}(V,\mathcal{S})$ in $\mathcal{A}(V',\mathcal{S}')$ con $0^\sigma = 0'$, allora σ è una trasformazione semilineare invertibile di V, come spazio vettoriale su $K(V,\mathcal{S})$, in V' come spazio vettoriale su $K(V',\mathcal{S}')$.*

Dim. Poichè σ è un isomorfismo di $\mathcal{A}(V,\mathcal{S})$ in $\mathcal{A}(V',\mathcal{S}')$, segue dalla definizione di $\mathcal{A}(V,\mathcal{S})$ e $\mathcal{A}(V',\mathcal{S}')$ che σ è una applicazione biiettiva di V in V'.

Proviamo che σ è additiva. Consideriamo la traslazione $\tau_v : x \to x+v$ in $\mathcal{A}(V,\mathcal{S})$ e $\tau'_{v'} : x \to x+v'$ in $\mathcal{A}(V',\mathcal{S}')$. Ricordiamo che l'applicazione $v \to \tau_v$ è un isomorfismo da V sul gruppo delle traslazioni T di $\mathcal{A}(V,\mathcal{S})$ e analogamente l'applicazione $v' \to \tau'_{v'}$ è un isomorfismo da V' sul gruppo delle traslazioni T' di $\mathcal{A}(V',\mathcal{S}')$. Consideriamo $\sigma^{-1}\tau_v\sigma$, allora

$$\mathcal{A}' \to_{\sigma^{-1}} \mathcal{A} \to_{\tau_v} \mathcal{A} \to_\sigma \mathcal{A}'$$

ossia $\sigma^{-1}\tau_v\sigma$ è una collineazione di $\mathcal{A}'$ in quanto conserva sia l'appartenenza che il parallelismo. Sia l una retta di $\mathcal{A}'$, proviamo che $l^{\sigma^{-1}\tau_v\sigma} \parallel l$. Sia $l^{\sigma^{-1}} = m \in \mathcal{A}$. Si ha $l^{\sigma^{-1}\tau_v} = m^{\tau_v}$ e $m^{\tau_v} \parallel m$ in quanto τ_v è una traslazione. Ne segue $m^{\tau_v\sigma} \parallel m^\sigma$ ossia $l^{\sigma^{-1}\tau_v\sigma} \parallel l$ essendo $m^\sigma = (l^{\sigma^{-1}})^\sigma = l$. Inoltre, essendo τ_v priva di punti fissi, lo è anche $\sigma^{-1}\tau_v\sigma$ che risulta pertanto essere una traslazione di $\mathcal{A}'$. Vediamo ora di quale traslazione si tratta. Si ha

$$0'^{\sigma^{-1}\tau_v\sigma} = 0^{\tau_v\sigma} = v^\sigma \tag{4}$$

quindi $\sigma^{-1}\tau_v\sigma$ è la traslazione che porta $0'$ in v^σ. Consideriamo ora

$$\tau'_{(v+w)^\sigma} = \sigma^{-1}\tau_{(v+w)}\sigma = \sigma^{-1}\tau_v\tau_w\sigma = (\sigma^{-1}\tau_v\sigma)(\sigma^{-1}\tau_w\sigma) = \tau'_{v^\sigma}\tau'_{w^\sigma} = \tau'_{v^\sigma+w^\sigma},$$

poichè le traslazioni sono univocamente determinate dal vettore che le definisce, allora $(v+w)^\sigma = v^\sigma + w^\sigma$. Pertanto, σ è additiva.

Proviamo ora che σ è semilineare.

Sia $k \in K(V,\mathcal{S})$. Si verifica facilmente che $\sigma^{-1}k\sigma \in K(V',\mathcal{S}')$. Poniamo $\sigma^{-1}k\sigma = k^\alpha$. Allora risulta che (per maggior chiarezza useremo la notazione $v\phi$ invece di v^ϕ)

$$(vk)\sigma = v(k\sigma) = v\sigma\sigma^{-1}(k\sigma) = (v\sigma)(\sigma^{-1}k\sigma) = v\sigma k^\alpha.$$

Inoltre, per ogni $h,k \in K(V,\mathcal{S})$ vale che

$$\begin{aligned} v\sigma(k+h)^\alpha &= (v(k+h))\sigma = (vk+vh)\sigma = \\ &= (vk)\sigma + (vh)\sigma = v\sigma k^\alpha + v\sigma h^\alpha = v\sigma(k^\alpha + h^\alpha) \end{aligned}$$

ed anche

$$v\sigma(kh)^\alpha = (v(kh))\sigma = ((vk)h)\sigma = (vk)\sigma h^\alpha = v\sigma(k^\alpha h^\alpha).$$

Essendo σ biiettiva, da $v\sigma(k+h)^\alpha = v\sigma(k^\alpha + h^\alpha)$ per ogni v, segue $(k+h)^\alpha = k^\alpha + h^\alpha$ e da $v\sigma(kh)^\alpha = v\sigma(k^\alpha h^\alpha)$ per ogni v, segue $(kh)^\alpha = k^\alpha h^\alpha$. Infine, ripetendo un ragionamento analogo al precedente con σ^{-1} al posto di σ, si prova che α è biiettiva e quindi α è un automorfismo del campo. Pertanto, per quanto visto, σ è una trasformazione semilineare. ■

Se consideriamo una (O, l_∞)-omologia σ di $\mathcal{A}(V, \mathcal{S})$, abbiamo appena provato che questa opera come un endomorfismo del gruppo abeliano V . Tale endomorfismo muta in sé ogni componente di $\mathcal{S}$ in quanto σ muta in sé ogni retta per O, quindi l'endomorfismo appartiene a $K(V, \mathcal{S})^*$. Ovviamente vale anche il viceversa e quindi si ha $G(O, l_\infty) \simeq K(V, \mathcal{S})^*$.

Corollario 3.15 *Se $\mathcal{A}(V, \mathcal{S})$ è un piano di traslazione finito, il gruppo $G(O, l_\infty)$ è ciclico.*

Se ora consideriamo una generica traslazione τ, si ha $\tau^{-1}G(O, l_\infty)\tau = G(O^\tau, l_\infty)$ da cui segue che $G(P, l_\infty)$ è ciclico per ogni punto P del piano. Nei piani desarguesiani quindi, i gruppi di omologie sono tutti ciclici poichè ogni retta è di traslazione.

Corollario 3.16 *Le collineazioni del piano di traslazione $\mathcal{A}(V, \mathcal{S})$ che fissano lo zero sono tutte e sole le trasformazioni semilineari invertibili di V che mutano $\mathcal{S}$ in sé.*

Dim. Che le collineazioni del piano che fissano lo zero siano trasformazioni semilineari

invertibili di V che mutano $\mathcal{S}$ in sé è stato provato nel Teorema precedente. Consideriamo allora una trasformazione semilineare invertibile σ di V tale che $\mathcal{S}^\sigma = \mathcal{S}$. Sia $X \in \mathcal{S}$ allora $(X + a)^\sigma = X^\sigma + a^\sigma$ con $X^\sigma \in \mathcal{S}$ e quindi $X^\sigma + a^\sigma$ è una retta del piano. Poichè σ è biiettiva e conserva l'appartenenza ed il parallelismo, possiamo concludere che σ è una collineazione. ■

Teorema 3.17 *Siano $(V, \mathcal{S})$ e $(V', \mathcal{S}')$ due spazi vettoriali con spread. Le seguenti affermazioni sono equivalenti:*

1. *$\mathcal{A}(V, \mathcal{S}) \simeq \mathcal{A}(V', \mathcal{S}')$;*
2. *esiste una applicazione biiettiva semilineare tra spazi vettoriali che trasforma V in V' ed $\mathcal{S}$ in $\mathcal{S}'$;*
3. *esiste un isomorfismo di gruppi da $(V, +)$ su $(V', +)$ che trasforma $\mathcal{S}$ in $\mathcal{S}'$.*

Dim. Dimostriamo che 1 implica 2.

Sia $\rho : \mathcal{A}(V,\mathcal{S}) \to \mathcal{A}(V',\mathcal{S}')$ un isomorfismo. Allora esiste la traslazione τ' di $\mathcal{A}(V',\mathcal{S}')$ tale che $0^{\rho\tau'} = 0'$. Quindi $\rho\tau' : \mathcal{A}(V,\mathcal{S}) \to \mathcal{A}(V',\mathcal{S}')$ è un isomorfismo che muta 0 in $0'$. Applicando il Teorema precedente segue la tesi.

Che 2 implica 3 è banale.

Proviamo infine che 3 implica 1.

Sia ω un isomorfismo di gruppi da $(V,+)$ su $(V',+)$ che trasforma $\mathcal{S}$ in $\mathcal{S}'$. Se consideriamo una retta $X+a$ di $\mathcal{A}(V,\mathcal{S})$, $\omega : X+a \to X^\omega + a^\omega$, ossia ω trasforma rette in rette. Siano ora $X+a$ e $X+b$ due rette di $\mathcal{A}(V,\mathcal{S})$, $X+a \parallel X+b \Rightarrow X^\omega + a^\omega \parallel X^\omega + b^\omega$, ossia ω conserva il parallelismo. L'asserto 1 è così provato. ■

Sia $(V,\mathcal{S})$ uno spazio vettoriale con spread. Abbiamo osservato che tutte le componenti in $\mathcal{S}$, come spazi vettoriali sul nucleo K, sono tra loro isomorfe. Sia $X \in \mathcal{S}$ allora $V = X \oplus X$ ed un qualsiasi elemento di V sarà del tipo $\underline{x}+\underline{y}$ con $\underline{x},\underline{y} \in X$. Rappresentiamo un tale elemento di V con la coppia $(\underline{x},\underline{y})$. Consideriamo due particolari sottospazi di V:

- lo spazio vettoriale $V(0)$ che è costituito da tutti e soli i vettori della forma $(\underline{x},\underline{0})$ con $\underline{x} \in X$

- lo spazio vettoriale $V(\infty)$ che è costituito da tutti e soli i vettori della forma $(\underline{0},\underline{y})$ con $\underline{y} \in X$.

Vogliamo analizzare il gruppo delle omologie di centro improprio (0) ed asse proprio $V(\infty)$ che indichiamo con $G((0),V(\infty))$.

Proposizione 3.18 *$G((0),V(\infty)) \leq GL(V,K(V,\mathcal{S}))$*

Dim. Sia $\delta \in G((0),V(\infty))$, allora $(\underline{0},\underline{y})^\delta = (\underline{0},\underline{y})$ poichè $(\underline{0},\underline{y})$ appartiene all'asse di δ. Inoltre $(\underline{x},\underline{0})^\delta = (\underline{x}^{\alpha_\delta},\underline{0})$ in quanto δ induce una trasformazione semilineare su $V(0)$ che indichiamo con α_δ e $(\underline{x}^{\alpha_\delta},\underline{0}) \in V(0)$ poichè $V(0)$, essendo una retta per il centro, è lasciata fissa da δ. Sia $k \in K$, allora

$$\begin{aligned}((\underline{x},\underline{y})k)^\delta &= (\underline{x}k,\underline{y}k)^\delta = ((\underline{x}k,\underline{0}) + (\underline{0},\underline{y}k))^\delta = (\underline{x}k,\underline{0})^\delta + (\underline{0},\underline{y}k)^\delta = \\ &= ((\underline{x}k)^{\alpha_\delta},\underline{0}) + (\underline{0},\underline{y}k) = ((\underline{x}k)^{\alpha_\delta},\underline{y}k) \\ ((\underline{x},\underline{y})k)^\delta &= (\underline{x},\underline{y})^\delta k^\theta = ((\underline{x},\underline{0}) + (\underline{0},\underline{y}))^\delta k^\theta = (\underline{x},\underline{0})^\delta k^\theta + (\underline{0},\underline{y})^\delta k^\theta = (\underline{x}^{\alpha_\delta}k^\theta, \underline{y}k^\theta),\end{aligned}$$

dove $\theta \in Aut(K)$. Da cui si ricava che $x^{\alpha_\delta}k^\theta = (xk)^{\alpha_\delta}$ e $yk^\theta = yk$. La seconda uguaglianza, valendo per ogni y, implica $k^\theta = k$ per ogni $k \in K$. Quindi $\theta = 1$ e l'applicazione δ è lineare cioè $G((0),V(\infty)) \leq GL(V,K(V,\mathcal{S}))$. ■

Corollario 3.19 *Sia $G(P,m) \leq Aut(\Pi_l)$ con $P \in l$ e $m \in \Pi_l$. Allora:*

1. *$G(P,m)$ contiene un'unica involuzione;*

2. *se $G(P,m)$ contiene una involuzione, il nucleo di Π_l ha caratteristica diversa da 2;*

3. se Π_l è finito, la struttura di $G(P,m)$ è quella di un complemento di Frobenius.

Dim. Sia m una retta affine e sia $m \cap l \neq P$. Sia $Q \in m$, allora esiste una traslazione τ tale che $Q^\tau = O$, da cui segue che $m^\tau = m'$ con m' retta passante per 0. Ora

$$G(P,m)^\tau = G(P^\tau, m^\tau) = G(P,m')$$

e quindi studiare $G(P,m)$ equivale a studiare $G(P,m')$, essendo i due sottogruppi coniugati. Per il risultato precedente, $G(P,m') \leq GL(V,K(V,\mathcal{S}))$. Sia U il sottospazio vettoriale di $\mathcal{S}$ cui appartiene P. Osserviamo che $G(P,m')$ fissa O in quanto è un punto appartenente all'asse m' ed inoltre $G(P,m')$ fissa OP poichè è una retta per il centro P. Allora possiamo concludere che $U^{G(P,m')} = U$. Le trasformazioni indotte da $G(P,m')$ in U sono ancora trasformazioni lineari. Consideriamo il gruppo delle traslazioni di direzione P che indichiamo con T_P. Si ha $U^{T_P} = U$. Consideriamo ora il prodotto semidiretto di $G(P,m')$ con T_P. Osserviamo che $T_P \lhd G(P,m') \cdot T_P$. Inoltre, sia $\sigma \in G(P,m')$ e $\tau_{\underline{b}} \in T_P$, allora la trasformazione $\sigma\tau_{\underline{b}}$ agisce su U nel seguente modo

$$\sigma\tau_{\underline{b}} : \underline{x} \to \underline{x}^\sigma + \underline{b} \qquad \text{per ogni } \underline{x} \in U.$$

Supponiamo per assurdo che ci siano due punti fissi $\underline{x}, \underline{y} \in U$, allora $\underline{x} = \underline{x}^\sigma + \underline{b}$ e $\underline{y} = \underline{y}^\sigma + \underline{b}$ $\Rightarrow \underline{x} - \underline{y} = \underline{x}^\sigma - \underline{y}^\sigma = (\underline{x} - \underline{y})^\sigma$ per la linearità di σ. Ma allora σ fissa $\underline{x} - \underline{y}$. Poichè σ è una omologia, in U essa fissa solo lo zero e quindi $\underline{x} - \underline{y} = \underline{0}$ da cui $\underline{x} = \underline{y}$ e quindi σ fissa al più un punto di U.

Abbiamo quindi provato che il gruppo $G(P,m') \cdot T_P$ è transitivo su U e ogni suo elemento fissa al più un punto, ossia $G(P,m') \cdot T_P$ è un gruppo di Frobenius con nucleo di Frobenius T_P e complemento di Frobenius $G(P,m')$.

Se Π_l è finito, per quanto appena dimostrato, possiamo allora concludere che l'asserto 3 è vero.

1. Sia $\sigma \in G(P,m')$ con $\sigma^2 = 1$ e $\sigma \neq 1$. Poichè σ è involutoria si ha $\underline{x}^\sigma = \underline{y}$ e $\underline{y}^\sigma = \underline{x}$. Ne segue $(\underline{x} + \underline{y})^\sigma = \underline{x}^\sigma + \underline{y}^\sigma = \underline{y} + \underline{x} = \underline{x} + \underline{y}$. Ma σ fissa solo lo zero quindi $\underline{x} + \underline{y} = \underline{0}$ da cui segue $\underline{x} = -\underline{y}$. Abbiamo così provato che se esiste una involuzione in $G(P,m')$ allora questa è unica e si tratta della trasformazione che porta $\underline{x}$ in $-\underline{x}$.

2. Se per assurdo il nucleo avesse caratteristica uguale a 2, allora da $-\underline{x} = \underline{x}$ seguirebbe $\sigma : \underline{x} \to \underline{x}$ ossia $\sigma = 1$ contro l'ipotesi. ■

3.1 Quasicorpi

Nel seguito intendiamo descrivere un tipo di struttura algebrica in grado di coordinatizzare i Piani di Traslazione, "meno ricca" di proprietà rispetto ai campi.

Definizione 3.20 *Una struttura algebrica $(Q,+,\circ)$ si dice* Quasicorpo *se soddisfa le seguenti proprietà:*

1. $(Q,+)$ *è un gruppo abeliano;*
2. *per ogni* $a,b,c \in Q$ *vale che* $(a+b)\circ c = a\circ c + b\circ c$*;*
3. *per ogni* $a \in Q$ *risulta* $a\circ 0 = 0$*;*
4. *per ogni* $a,c \in Q$*, con* $a \neq 0$*, esiste un unico* $x \in Q$ *tale che* $a\circ x = c$*;*
5. *per ogni* $a,b,c \in Q$*, con* $a \neq b$*, esiste un unico* $y \in Q$ *tale che* $y\circ a - y\circ b = c$*.*
6. *esiste un elemento* $1 \in Q - \{0\}$ *tale che* $1\circ a = a\circ 1 = a$ *per ogni* $a \in Q$*.*

Osserviamo che

(i) per la proprietà 2, si ha

$$0\circ a = (0+0)\circ a = 0\circ a + 0\circ a$$

da cui segue $0\circ a = 0$ per ogni $a \in Q$.

(ii) per la proprietà (i), si ha

$$0 = (a-a)\circ b = a\circ b + (-a)\circ b$$

da cui segue $(-a)\circ b = -(a\circ b)$.

Definizione 3.21 *L'insieme*

$$\mathcal{N}(Q) = \left\{ c \in Q : \left\{ \begin{array}{c} c\circ(x+y) = c\circ x + c\circ y \\ c\circ(x\circ y) = (c\circ x)\circ y \end{array} \right. \text{ per ogni } x,y \in Q \right\}.$$

si dice nucleo *di* Q*.*

Teorema 3.22 $\mathcal{N}(Q)$ *è un corpo, e* Q *è uno spazio vettoriale su* $\mathcal{N}(Q)$*.*

Dim. a) Proviamo che $\mathcal{N}(Q)$ è chiuso rispetto alla somma, ossia che $h,k \in \mathcal{N}(Q) \Rightarrow h-k \in \mathcal{N}(Q)$.

Siano $a,b \in Q$ e $h,k \in \mathcal{N}(Q)$. Dalla distributività in Q e da (ii) segue che

$$(h-k)\circ(a+b) = h\circ(a+b) - k\circ(a+b).$$

Poichè $h, k \in \mathcal{N}(Q)$ risulta

$$(h-k)\circ(a+b) = h\circ a + h\circ b - k\circ a - k\circ b = h\circ a - k\circ a + h\circ b - k\circ b.$$

Infine, ancora dalla distributività in Q vale che

$$(h-k)\circ(a+b) = (h-k)\circ a + (h-k)\circ b \tag{5}$$

ossia $h-k$ distribuisce a destra.

Consideriamo ora $(h-k)\circ(a\circ b)$. Per la distributività di Q segue che

$$(h-k)\circ(a\circ b) = h\circ(a\circ b) - k\circ(a\circ b)$$

poichè $h, k \in \mathcal{N}(Q)$ possiamo sfruttare la proprietà associativa e quindi

$$(h-k)\circ(a\circ b) = (h\circ a)\circ b - (k\circ a)\circ b$$

e per la distributività in Q si ricava che

$$(h-k)\circ(a\circ b) = (h\circ a - k\circ a)\circ b$$

e di nuovo per la distributività in Q

$$(h-k)\circ(a\circ b) = ((h-k)\circ a)\circ b$$

ossia $h-k$ associa. Possiamo allora concludere che $h-k \in \mathcal{N}(Q)$.

b) Proviamo che $\mathcal{N}(Q)$ non è un insieme vuoto. Poichè vale

$$0\circ(a+b) = 0 = 0+0 = 0\circ a + 0\circ b$$

e

$$0\circ(a\circ b) = 0 = 0\circ a = (0\circ a)\circ b$$

allora $0 \in \mathcal{N}(Q)$.

Da a) e b) segue $(\mathcal{N}(Q), +) \leq (Q, +)$.

c) Proviamo che $\mathcal{N}(Q)$ è chiuso rispetto al prodotto, ossia che $h, k \in \mathcal{N}(Q) \Rightarrow h\circ k \in \mathcal{N}(Q)$.

Siano $h, k \in \mathcal{N}(Q)$, da

$$\begin{aligned}(k\circ h)\circ(a+b) &= k\circ(h\circ(a+b)) = k\circ(h\circ a + h\circ b) = \\ &= k\circ(h\circ a) + k\circ(h\circ b) = (k\circ h)\circ a + (k\circ h)\circ b\end{aligned}$$

e

$$(k\circ h)\circ(a\circ b) = k\circ(h\circ(a\circ b)) = k\circ((h\circ a)\circ b) = (k\circ(h\circ a))\circ b = ((k\circ h)\circ a)\circ b$$

segue $h \circ k \in \mathcal{N}(Q)$.

d) Proviamo ora che per ogni $k \in \mathcal{N}(Q)^*$ esiste $k' \in \mathcal{N}(Q)^*$ tale che $k \circ k' = 1 = k' \circ k$.

Sia $k \in \mathcal{N}(Q)^*$. Per la proprietà 4 della Definizione 3.20 esiste un unico $k' \in Q$ tale che $k \circ k' = 1$. Se poniamo $a = k$, $b = 0$ e $c = 1$, per la proprietà 5 della Definizione 3.20 possiamo affermare che esiste un unico $k'' \in Q$ tale che $k'' \circ k = 1$. Si tratta allora di provare che $k', k'' \in \mathcal{N}(Q)^*$ e che $k' = k''$.

Proviamo che $k' \in \mathcal{N}(Q)$. Infatti, valgono:

$$\begin{aligned} k \circ (k' \circ (a+b)) &= (k \circ k') \circ (a+b) = 1 \circ (a+b) = a+b = 1 \circ a + 1 \circ b \\ &= (k \circ k') \circ a + (k \circ k') \circ b = k \circ (k' \circ a) + k \circ (k' \circ b) = \\ &= k \circ (k' \circ a + k' \circ b). \end{aligned}$$

Allora per la proprietà 4 della Definizione 3.20, segue che $k' \circ (a+b) = k' \circ a + k' \circ b$. In modo analogo si prova che $k' \circ (a \circ b) = (k' \circ a) \circ b$. Pertanto, $k' \in \mathcal{N}(Q)$. Allo stesso modo si prova che $k'' \in \mathcal{N}(Q)^*$.

Ora da

$$(k'' \circ k) \circ k' = 1 \circ k' = k'$$

e

$$k'' \circ (k \circ k') = k'' \circ 1 = k''$$

segue $k' = k''$.

Si noti che se $h, k \in \mathcal{N}(Q)^*$ e $h \circ k = 0$, essendo anche $h \circ 0 = 0$ risulta contraddetta la proprietà 4 della Definizione 3.20. Pertanto $\mathcal{N}(Q)^*$ è chiuso rispetto al prodotto e quindi $(\mathcal{N}(Q), +, \circ)$ è un corpo. Poichè gli elementi di $\mathcal{N}(Q)$ soddisfano entrambe le proprietà distributive, si prova facilmente che Q è uno spazio vettoriale su $\mathcal{N}(Q)$. ■

Osservazione: se Q è finito allora la proprietà 5 della Definizione 3.20 segue dalle altre. Proviamolo:

siano $a, b \in Q$ con $a \neq b$, consideriamo l'applicazione

$$\alpha : x \to x \circ a - x \circ b.$$

Vale

$$\begin{aligned} (x+y)^\alpha &= (x+y) \circ a - (x+y) \circ b = x \circ a + y \circ a - x \circ b - y \circ b = \\ &= (x \circ a - x \circ b) + (y \circ a - y \circ b) = x^\alpha + y^\alpha \end{aligned}$$

da cui segue che α è lineare rispetto alla somma in Q. Sia $k \in \mathcal{N}(Q)$ allora vale

$$(k \circ x)^\alpha = (k \circ x) \circ a - (k \circ x) \circ b = k \circ (x \circ a) - k \circ (x \circ b) = k \circ (x \circ a - x \circ b) = k \circ x^\alpha$$

da cui segue che α è lineare anche rispetto al prodotto per uno scalare, ossia α è una trasformazione lineare dello spazio vettoriale sinistro Q su $\mathcal{N}(Q)$ in sé.

Sia $x \in Q$ tale che $x^\alpha = 0$, allora $0 = x \circ a - x \circ b$, ossia $x \circ a = x \circ b$. Poniamo $x \circ a = x \circ b = c$. Dalla proprietà 4 della Definizione 3.20 segue che se $x \neq 0$ allora esiste un unico elemento $a \in Q$ tale che $x \circ a = c$. Poichè $x \circ a = c = x \circ b$ con $a \neq b$, necessariamente deve essere $x = 0$. Allora $Ker(\alpha) = \{0\}$ e poichè α è un endomorfismo, α è suriettiva. Quindi, considerato un elemento $c \in Q$, esiste $y \in Q$ tale che $y^\alpha = c$, cioè tale che $y \circ a - y \circ b = c$.

Consideriamo un quasicorpo Q e sia $V = Q \oplus Q$. Definiamo i seguenti sottoinsiemi di V:

$$\begin{aligned} V(0) &= \{(x,0) \mid x \in Q\} \\ V(\infty) &= \{(0,y) \mid y \in Q\} \\ V(m) &= \{(x, x \circ m) \mid x \in Q\}, \quad m \neq 0. \end{aligned}$$

Ciascuno di essi risulta essere un sottospazio di $(V,+)$ su $\mathcal{N}(Q)$. La verifica nei primi due casi è banale, limitiamoci allora a considerare l'insieme $V(m)$.

Siano $(x, x \circ m), (x', x' \circ m) \in V(m)$, allora vale

$$(x, x \circ m) - (x', x' \circ m) = (x - x', x \circ m - x' \circ m) = (x - x', (x - x') \circ m)$$

per la prop. distributiva del prodotto in Q. Inoltre ponendo

$$k\,(x, x \circ m) = (k \circ x, k \circ (x \circ m)) = (k \circ x, (k \circ x) \circ m)$$

si ha che $V(m)$ è un sottospazio di V su $\mathcal{N}(Q)$.

Teorema 3.23 *Sia $(Q,+,\circ)$ un quasicorpo e si consideri lo spazio vettoriale $V = Q \oplus Q$ su $\mathcal{N}(Q)$. Allora $\mathcal{S} = \{V(m) \mid m \in Q - \{0\}\} \cup \{V(0), V(\infty)\}$ è una partizione di congruenza di $(V,+)$ e $\mathcal{A}(Q \oplus Q, \mathcal{S})$ è un piano di traslazione.*

Dim. Sia $(x,y) \in V$. Se $x, y \neq 0$, per la prop. 4 della Definizione 3.20 esiste $m \in Q$ tale che $x \circ m = y$ ossia $(x,y) \in V(m)$. Mentre se $x = 0$, allora $(0,y) \in V(\infty)$ e se $y = 0$ allora $(x,0) \in V(0)$. Abbiamo quindi verificato che $V = V(m) \cup V(0) \cup V(\infty)$. Dobbiamo ora provare che le componenti di $\mathcal{S}$ sono a due a due disgiunte. Si verifica facilmente che

$$V(0) \cap V(\infty) = V(0) \cap V(m) = V(m) \cap V(\infty) = \{(0,0)\}$$

Proviamo ora che $V(m_1) \cap V(m_2) = \{(0,0)\}$. Sia $(x,y) \in V(m_1) \cap V(m_2)$ con $m_1 \neq m_2$. Allora da $y = x \circ m_1 = x \circ m_2$ segue $x \circ m_1 - x \circ m_2 = 0$. Per la prop. 5 della Definizione 3.20 esiste un unico $x \in Q$ tale che $x \circ m_1 - x \circ m_2 = 0$, quindi $x = 0$ e di conseguenza $y = 0$. Abbiamo così provato che $\mathcal{S}$ è una partizione. Per dimostrare che si tratta di una partizione di congruenza dobbiamo verificare che la somma di due qualsiasi componenti è

tutto V. Si verifica facilmente che $V(0)+V(\infty)=V$. Proviamo ora che $V(0)+V(m)=V$. Un generico elemento di $V(0)+V(m)$ è del tipo

$$(x,0)+(z,z\circ m)=(x+z,z\circ m).$$

Sia $(u,v)\in V$. Consideriamo le equazioni $\begin{cases} x+z=u \\ z\circ m=v \end{cases}$. Allora per la proprietà 5 con $a=m$ e $b=0$ esiste $\overline{z}\in Q$ tale che $\overline{z}\circ m=v$. Sia $\overline{x}\in Q$ tale che $\overline{x}=u-\overline{z}$. Allora

$$(u,v)=(\overline{x},0)+(\overline{z},\overline{z}\circ m) \quad \text{con } (\overline{x},0)\in V(0) \text{ e } (\overline{z},\overline{z}\circ m)\in V(m).$$

Proviamo ora che $V(\infty)+V(m)=V$. Un generico elemento di $V(\infty)+V(m)$ è del tipo

$$(0,y)+(z,z\circ m)=(z,y+z\circ m).$$

Sia $(u,v)\in V$. Consideriamo le equazioni $\begin{cases} z=u \\ y+z\circ m=v \end{cases}$. Allora esiste $\overline{z}\in Q$ tale che $\overline{z}=u$ ed esiste $\overline{y}\in Q$ tale che $\overline{y}=v-\overline{z}\circ m$. Quindi

$$(u,v)=(0,\overline{y})+(\overline{z},\overline{z}\circ m) \quad \text{con } (0,\overline{y})\in V(\infty) \text{ e } (\overline{z},\overline{z}\circ m)\in V(m).$$

Proviamo infine che $V(n)+V(m)=V$ con $n\neq m$. Sia $(x,y)\in V$. Applichiamo la proprietà 5 della Definizione 3.20 ponendo $c=y$, $a=m$ e $b=n$; vale

$$z\circ m-z\circ n=y \;\Rightarrow \exists \overline{z}\in Q \;\text{ t.c. } \overline{z}\circ m-\overline{z}\circ n=y.$$

Se invece poniamo $c=x\circ m$. Si ha

$$w\circ n-w\circ m=x\circ m \;\Rightarrow \exists \overline{w}\in Q \;\text{ t.c. } \overline{w}\circ n-\overline{w}\circ m=x\circ m.$$

Si ha $(\overline{z}+\overline{w}+x)-(\overline{z}+\overline{w})=x$ ed inoltre

$$\begin{aligned}(\overline{z}+\overline{w}+x)\circ m-(\overline{z}+\overline{w})\circ n &= (\overline{z}\circ m-\overline{z}\circ n)-(\overline{w}\circ n-\overline{w}\circ m)+x\circ m= \\ &= y-x\circ m+x\circ m=y.\end{aligned}$$

Ora $(\overline{z}+\overline{w}+x,(\overline{z}+\overline{w}+x)\circ m)\in V(m)$ e $(-(\overline{z}+\overline{w}),-(\overline{z}+\overline{w})\circ n)\in V(n)$ e si ha

$$(\overline{z}+\overline{w}+x,(\overline{z}+\overline{w}+x)\circ m)+(-(\overline{z}+\overline{w}),-(\overline{z}+\overline{w})\circ n)=(x,y).$$

Quindi $\mathcal{S}$ è uno spread e di conseguenza $\mathcal{A}(Q\oplus Q,\mathcal{S})$ è un piano affine.

Sia $V_i\in\mathcal{S}$, allora una generica retta di $\mathcal{A}$ è del tipo $V_i+(a,b)$. Se consideriamo un'applicazione

$$\tau_{(c,d)}:(x,y)\to(x+c,y+d) \text{ con } c,d\in Q$$

questa opera sulle rette di $\mathcal{A}$ nel seguente modo:

$$\tau_{(c,d)} : V_i + (a,b) \to V_i + (a,b) + (c,d)$$

cioè trasforma rette in rette. Si verifica facilmente che l'applicazione $\tau_{(c,d)}$ è una traslazione e che $T = \left\{\tau_{(c,d)} \mid (c,d) \in V\right\}$ è un gruppo transitivo sui punti di $\mathcal{A}$. Possiamo quindi concludere che $\mathcal{A}(Q \oplus Q, \mathcal{S})$ è un piano di traslazione. ■

Osserviamo che è possibile rappresentare le rette di $\mathcal{A}$, in termini di equazioni, in uno dei seguenti modi:

1. $y = x \circ m + b$ con $m \in Q^*$ e $b \in Q$;
2. $x = c$ con $c \in Q$;
3. $y = d$ con $d \in Q$.

Nel primo caso l'equazione $y = x \circ m + b$ corrisponde all'insieme di punti

$$\{(x, x \circ m + b) \mid m \in Q^* \text{ e } b \in Q\} = \{(x, x \circ m) \mid m \in Q^*\} + (0, b)$$

che è il traslato della componente $V(m)$ mediante $(0,b)$ e quindi si tratta effettivamente di una retta.

Nel secondo caso l'equazione $x = c$ corrisponde all'insieme di punti

$$\{(c, y) \mid c \in Q\} = \{(0, y) \mid y \in Q\} + (c, 0)$$

che è il traslato della componente $V(\infty)$ mediante $(c,0)$ e quindi è una retta.

Nell'ultimo caso l'equazione $y = d$ corrisponde all'insieme di punti

$$\{(x, d) \mid c \in Q\} = \{(x, 0) \mid x \in Q\} + (0, d)$$

che è il traslato della componente $V(0)$ mediante $(0,d)$ e quindi è una retta.

E' vero anche il viceversa, cioè ogni retta di $\mathcal{A}$ si può rappresentare con una delle equazioni precedenti. Consideriamo, ad esempio, l'insieme di punti $\{(x, x \circ m) \mid m \in Q^*\}+ (a,b)$ il cui generico elemento è $(x + a, x \circ m + b)$. Tale retta si può rappresentare con un'equazione del tipo $y = x \circ m - a \circ m + b$, infatti

$$(x+a) \circ m - a \circ m + b = (x \circ m + a \circ m) - a \circ m + b = x \circ m + a \circ m - a \circ m + b = x \circ m + b.$$

Vale anche il seguente teorema, del quale omettiamo la dimostrazione, il quale afferma che un qualsiasi piano di traslazione $\mathcal{A}$ è isomorfo ad $\mathcal{A}(Q \oplus Q, \mathcal{S})$ per un opportuno quasicorpo Q.

Teorema 3.24 (M. Hall Jr. 1943) *Sia $\mathcal{A}$ un piano di traslazione, e siano P e R due punti distinti su l_∞ e O un punto affine. Allora esiste un quasicorpo Q ed un isomorfismo $\psi : \mathcal{A} \longrightarrow \mathcal{A}(Q \oplus Q, \mathcal{S})$ tale che $(OP)^\psi = V(0)$ e $(OR)^\psi = V(\infty)$.*

Osserviamo che ad ogni scelta della terna O, P, R corrisponde un diverso quasicorpo Q e che esistono quasicorpi non isomorfi che coordinatizzano piani isomorfi.

Nel seguito ci limiteremo a considerare il caso di Q finito ed indicheremo $\mathcal{A}(Q \oplus Q, \mathcal{S})$ semplicemente con $\mathcal{A}(Q)$.

Definizione 3.25 *Un quasicorpo $(Q, +, \circ)$ per il quale vale*

$$a \circ (b \circ c) = (a \circ b) \circ c \quad \text{per ogni } a, b, c \in Q$$

si dice Quasicorpo Associativo *o* Nearfield.

Definizione 3.26 *Un quasicorpo $(Q, +, \circ)$ per il quale vale*

$$a \circ (b + c) = a \circ b + a \circ c \quad \text{per ogni } a, b, c \in Q$$

si dice Semicorpo *o* Semifield.

I teoremi che seguono mostrano come proprietà algebriche del quasicorpo che coordinatizza un piano di traslazione siano equivalenti all'esistenza di opportune collineazioni dello stesso piano.

Teorema 3.27 *Sia $(Q, +, \circ)$ un quasicorpo. Allora Q è un semifield se e solo se $\mathcal{A}(Q)$ è $((\infty), (\infty))$-transitivo.*

Di tale teorema si omette la dimostrazione.

Se consideriamo una generica retta l per (∞), l risulta parallela alla retta $V(\infty)$. Esiste quindi τ tale che $l^\tau = V(\infty)$. Da cui segue $G((\infty)^{\tau^{-1}}, V(\infty)^{\tau^{-1}}) = G((\infty), l)$. Possiamo quindi affermare che Q è un semifield se e solo se $\mathcal{A}(Q)$ è $((\infty), V(\infty))$-transitivo.

Se passiamo al piano duale $\mathcal{A}(Q)^d$, questo è ancora $((\infty), (\infty))$-transitivo. Quindi il piano contiene tutte le elazioni di asse (∞) e centro un punto di (∞) ed è pertanto ancora un piano di traslazione.

Teorema 3.28 *Sia $(Q, +, \circ)$ un quasicorpo. Allora Q è un nearfield se e solo se $\mathcal{A}(Q)$ è $((0), V(\infty))$-transitivo.*

Dim. Diamo un cenno della dimostrazione provando solo che se Q è un nearfield allora $\mathcal{A}(Q)$ è $((0), V(\infty))$-transitivo.

Sia $a \in Q^*$, consideriamo l'applicazione ϕ_a che opera sui punti nel seguente modo:

$$\phi_a : (x, y) \to (x \circ a, y)$$

e trasforma la retta $y = x \circ m + k$ nella retta $y = x \circ (a^{-1} \circ m) + k$ e la retta $x = k$ nella retta $x = k \circ a$. Vogliamo dimostrare che ϕ_a è una omologia di centro (0) e asse $V(\infty)$ tale che $\phi_a : (1, 0) \to (a, 0)$.

Proviamo che ϕ_a conserva l'appartenenza. Consideriamo un punto $P = (x_0, y_0)$ appartenente alla retta r di equazione $y = x \circ m + k$.

$$\begin{aligned} y_0 &= x_0 \circ m + k \Leftrightarrow y_0 = (x_0 \circ 1) \circ m + k \Leftrightarrow \\ &\Leftrightarrow y_0 = (x_0 \circ (a \circ a^{-1})) \circ m + k \Leftrightarrow y_0 = (x_0 \circ a) \circ (a^{-1} \circ m) + k. \end{aligned}$$

$y_0 = (x_0 \circ a) \circ (a^{-1} \circ m) + k$ equivale a dire che $(x_0 \circ a, y_0)$ appartiene alla retta di equazione $y = x \circ (a^{-1} \circ m) + k$ che è l'immagine di r tramite ϕ_a. Se r è una retta di equazione $x = k$ allora $P = (x_0, y_0)$ appartiene ad r se e solo se $x_0 = k$. Ora $(x_0, y_0)^{\phi_a} = (x_0 \circ a, y_0)$ e $(x_0 \circ a, y_0)$ appartiene alla retta di equazione $x = k \circ a$ perchè $x_0 \circ a = k \circ a$. Abbiamo così provato che $P \in r \Rightarrow P^{\phi_a} \in r^{\phi_a}$.

Da quanto appena dimostrato segue che ϕ_a conserva il parallelismo.

Vale $\phi_a : (0, y) \to (0, y)$ quindi ϕ_a fissa puntualmente la retta $V(\infty)$ e $\phi_a : (x, 0) \to (x \circ a, 0)$, ossia ϕ_a muta in sé le rette per (0). Inoltre $\phi_a : (1, 0) \to (1 \circ a, 0) = (a, 0)$.

Abbiamo così provato che ϕ_a è una omologia di centro (0) e asse $V(\infty)$ tale che $\phi_a : (1, 0) \to (a, 0)$. Da quest'ultima proprietà segue che tutti i punti della retta $V(0)$ stanno in una stessa orbita, al variare di $a \in Q^*$. Possiamo quindi concludere che $\mathcal{A}(Q)$ è $((0), V(\infty))$-transitivo. ■

3.2 Esempi di Quasicorpi

Vogliamo ora descrivere la costruzione di due particolari famiglie di quasicorpi.

3.2.1 Semicorpi di Dickson

Sia $F \cong GF(p^n)$, con p primo dispari e $n > 1$, a un non quadrato in F e sia $K = GF(p^{2n})$ sovracampo di F. Allora K può essere riguardato come uno spazio vettoriale di dimensione 2 su F con base $\{1, \lambda\}$ per $\lambda \in K - F$. In K conserviamo la somma di F e definiamo un nuovo prodotto nel seguente modo.

Sia $\theta \in Aut(F)$ con $\theta \neq 1$ fissato e tale che $x \to x^\theta = x^{p^r}$ per ogni $x \in F$. Sia $\lambda \in K - F$, si definisce

$$(x + \lambda y) \circ (z + \lambda t) = (xz + ay^\theta t^\theta) + \lambda(yz + xt). \tag{6}$$

Inoltre se $x = 1$ e $y = 0$ si ha $(x + \lambda y) \circ (z + \lambda t) = (z + \lambda t)$, ossia $(K, \circ)$ possiede un'unità. Poichè stiamo considerando il caso finito, per provare che $(K, +, \circ)$ è un semicorpo, è sufficiente provare che è privo di divisori dello zero. Ossia che

$$(x + \lambda y) \circ (z + \lambda t) = 0 \ \Rightarrow x + \lambda y = 0 \text{ oppure } z + \lambda t = 0.$$

Quindi supponiamo che $(x + \lambda y) \circ (z + \lambda t) = 0$. Allora da (6) segue che

$$\begin{aligned} xz + ay^\theta t^\theta &= 0 \quad (7) \\ yz + xt &= 0. \quad (8) \end{aligned}$$

Sia $z = 0$, allora $\begin{cases} ay^\theta t^\theta = 0 \\ xt = 0 \end{cases}$. Se $t = 0$ segue $z + \lambda t = 0$. Se $t \neq 0$ allora $\begin{cases} ay^\theta = 0 \\ x = 0 \end{cases}$. Ma $ay^\theta = 0 \Leftrightarrow y^\theta = 0 \Leftrightarrow y = 0$ essendo θ un automorfismo. Quindi se $t \neq 0$ si ha $x + \lambda y = 0$.

Sia $z \neq 0$. Se $t \neq 0$, da $yz + xt = 0$ segue $x = -yz/t$ e da $xz + ay^\theta t^\theta = 0$ segue $-\frac{yz}{t} z + ay^\theta t^\theta = 0$, ossia $-yz^2 + ay^\theta t^{\theta+1} = 0$. Ora se $y = 0$ si ha

$$yz + xt = 0 \Rightarrow xt = 0 \Rightarrow x = 0 \Rightarrow x + \lambda y = 0.$$

Se $y \neq 0$ allora $z^2 = ay^{\theta-1} t^{\theta+1} = ay^{p^r-1} t^{p^r+1}$. Ora y^{p^r-1} e t^{p^r+1} sono due quadrati essendo p dispari e $ay^{p^r-1} t^{p^r+1}$ è un non quadrato in quanto abbiamo supposto che a sia un non quadrato. Allora $z^2 = ay^{p^r-1} t^{p^r+1}$ con $z \neq 0$, $t \neq 0$ e $y \neq 0$ non è mai verificata. Possiamo quindi allora concludere che K è privo di divisori dello zero.

Osserviamo che se K fosse anche associativo sarebbe un campo e quindi non avremmo costruito una nuova famiglia di semicorpi propri. Verifichiamo quindi che K non è associativo.

Siano $e, f, g \in K$. Si definisce *associatore* di e, f e g, l'elemento di K così definito:

$$[e, f, g] = (e \circ f) \circ g - e \circ (f \circ g).$$

Quindi $(K, +, \circ)$ è associativo $\Leftrightarrow [e, f, g] = 0 \ \forall e, f, g \in K$. Siano $x + \lambda y$, $z + \lambda t$, $h + \lambda k \in K$, si ha

$$[x + \lambda y, z + \lambda t, h + \lambda k] = at^\theta (y^\theta (h^\theta - h) + k^\theta (x^\theta - x)) + \lambda at^\theta (y^\theta k - y k^\theta).$$

Se poniamo $h = x = 0$, si ha

$$[x + \lambda y, z + \lambda t, h + \lambda k] = \lambda at^\theta (y^\theta k - y k^\theta).$$

Sia $t \neq 0$, y appartenente al sottocampo fissato da θ e k non appartenente a tale sottocampo. Allora $y^\theta k - y k^\theta = yk - yk^\theta$ e

$$[x + \lambda y, z + \lambda t, h + \lambda k] = 0 \Leftrightarrow yk - yk^\theta = 0 \Leftrightarrow k = k^\theta.$$

Poichè k non appartiene al sottocampo fissato da θ, si ha $k \neq k^\theta$.

$(K, +, \circ)$ è un semicorpo proprio detto *Semicorpo di Dickson*.

3.2.2 Quasicorpi associativi (Nearfields)

Sia q la potenza di un primo ed n un intero positivo tale che tutti i divisori primi di n dividono $q-1$. Supponiamo inoltre che 4 non divida n se $q \equiv 3$ (4). Sia ω un elemento primitivo del campo $F \cong GF(q^n)$ (ossia ω è un generatore di F^*). Si considera $G = \langle \omega^n \rangle$ un sottogruppo di F^*. Si dimostra che G ha indice n in F^* e che $\left\{ \omega_i = \omega^{\frac{q^i-1}{q-1}} \right\}_{i=0}^{n-1}$ è un sistema di rappresentanti per i laterali di G in F^*.

Se $f \in G\omega_i$ associamo ad f l'automorfismo $\alpha(f) \in Aut(F)$ tale che $\alpha(f) : x \to x^{q^i}$. Possiamo allora definire in $GF(q^n)$ una nuova operazione di prodotto tale che per ogni $x, y \in GF(q^n)$ vale:

$$\begin{aligned} x \circ 0 &= 0 \\ x \circ y &= x^{\alpha(y)} y \end{aligned}$$

Ossia se $y \in G\omega_j$ allora $x \circ y = x^{q^j} y$. Si prova che $(F, +, \circ)$ è un nearfield.

Osserviamo che $(x+y) \circ z = (x+y)^{\alpha(z)} z = (x^{\alpha(z)} + y^{\alpha(z)}) z$ essendo $\alpha(z)$ un automorfismo, e $(x^{\alpha(z)} + y^{\alpha(z)}) z = x^{\alpha(z)} z + y^{\alpha(z)} z$ poichè nel campo $GF(q^n)$ vale la proprietà distributiva. Quindi

$$(x+y) \circ z = x^{\alpha(z)} z + y^{\alpha(z)} z = x \circ z + y \circ z$$

cioè vale la proprietà distributiva a sinistra. Si ha invece

$$\begin{aligned} z \circ (x+y) &= z^{\alpha(x+y)}(x+y) = z^{\alpha(x+y)} x + z^{\alpha(x+y)} y \\ z \circ x + z \circ y &= z^{\alpha(x)} x + z^{\alpha(y)} y \end{aligned}$$

Poichè in generale $\alpha(x+y) \neq \alpha(x)$, $\alpha(y)$ la proprietà distributiva a destra non vale e quindi $(F, +, \circ)$ non è un campo.

I nearfield finiti sono stati classificati da Zassenhaus nel 1935.

4 APPENDICE I: Gruppi di Permutazione.

Sia $\Omega = \{\alpha, \beta, ...\}$ un insieme non vuoto.

Definizione 4.1 *Una funzione biunivoca di Ω in sè prende il nome di permutazione su Ω. Se τ e σ sono permutazioni su Ω, la funzione*

$$\tau\sigma : \alpha \to \alpha^{\tau\sigma} = (\alpha^{\tau})^{\sigma} \qquad \alpha \in \Omega$$

è ancora una permutazione e l'operazione appena definita induce una struttura di gruppo sull'insieme di tutte le permutazioni su Ω. Tale gruppo prende il nome di gruppo simmetrico *su Ω e si denota con $Sym(\Omega)$.*

Ovviamente, l'unità di $Sym(\Omega)$ è la permutazione identica, cioè la funzione identità su Ω, che denoteremo col simbolo 1.

Definizione 4.2 *Definiamo gruppo di permutazioni su un insieme Ω un qualsiasi sottogruppo di $Sym(\Omega)$.*

Sia G un gruppo. Un omomorfismo $j : G \to Sym(\Omega)$ prende il nome di *azione* di G su Ω. Quando è assegnata un'azione j di G su Ω, diciamo che G *opera*, o *agisce*, sull'insieme Ω. In tali ipotesi la terna (G, Ω, j) prende il nome di *rappresentazione di G come gruppo di permutazioni su Ω* e il nucleo dell'omomorfismo j è detto *nucleo della rappresentazione.*

Quando l'omomorfismo j è iniettivo, l'azione j e la rappresentazione (G, Ω, j) si dicono *fedeli.*

Se Ω è finito d'ordine n, l'intero n si chiama *grado della rappresentazione.*

Se la rappresentazione (G, Ω, j) è fedele, identifichiamo G con la sua immagine e riguardiamo G come gruppo di permutazioni su Ω.

Richiamiamo alcune definizioni che saranno utili nel seguito:

1. Un elemento α di Ω è detto *unito* o *fisso* per una permutazione $g \in G$ se risulta $\alpha^g = \alpha$. Denotiamo con $Fix(g)$ l'insieme degli elementi uniti di g, cioè $Fix(g) = \{\alpha \in \Omega : \alpha^g = \alpha\}$.

2. Si definisce *orbita* di α in G, e si indica con α^G, l'insieme $\{\alpha^g / g \in G\}$.

3. Si definisce *stabilizzatore* di α in G, e si indica con G_α, l'insieme di tutti e soli gli elementi di G che fissano α, ossia $G_\alpha = \{g \in G / \alpha^g = \alpha\}$.

Supponiamo che G sia un gruppo finito ed Ω sia un insieme finito.

Proposizione 4.3 *Siano $\alpha, \beta \in \Omega$, se esiste $g \in G$ tale che $\alpha^g = \beta$ allora G_α e G_β sono coniugati in G.*

Dim. Proviamo che $G_\beta = G_\alpha^g$. Sia $y \in G_\beta$ allora $\beta^y = \beta$, da $\beta = \alpha^g$ segue $(\alpha^g)^y = \alpha^g$ e quindi $\alpha^{gyg^{-1}} = \alpha^{gg^{-1}} = \alpha$. Quindi $gyg^{-1} \in G_\alpha$ e $y = g^{-1}(gyg^{-1})g \in G_\alpha^g$. Sia ora $x \in G_\alpha^g$, allora esiste $y \in G_\alpha$ tale che $x = g^{-1}yg$ da cui $y = gxg^{-1}$. Poichè $y \in G_\alpha$ si ha $\alpha^{gxg^{-1}} = \alpha$ e quindi $\alpha^{gx} = \alpha^g$, ora poichè $\alpha^g = \beta$ si ha $\beta^x = \beta$ da cui $x \in G_\beta$. ■

Se G possiede una sola orbita su Ω; cioè se per ogni $\alpha, \beta \in \Omega$ esiste $g \in G$ tale che $\alpha^g = \beta$ diciamo che G è *transitivo*, o che ha un'azione transitiva, su Ω. Se nell'ultima uguaglianza l'elemento g è univocamente determinato dalla coppia (α, β), diciamo che G è strettamente transitivo o *regolare*. In tal caso $G_\alpha = \langle 1 \rangle$. In generale, se per ogni $\alpha \in \Omega$ si ha che G_α è banale allora diciamo che G è *semiregolare*.

Se per ogni 2 k-ple $(y_1, y_2, ..., y_k)$, $(z_1, z_2, ..., z_k)$ di elementi distinti di Ω, esiste un elemento $g \in G$ tale che $(y_1^g, y_2^g, ..., y_k^g) = (z_1, z_2, ..., z_k)$ diciamo che G è k-transitivo su Ω. Un gruppo 1-transitivo altro non è che un gruppo transitivo.

Sia G un gruppo di permutazioni su un insieme finito Ω, valgono i seguenti risultati:

Proposizione 4.4 *Se G è regolare su Ω, allora G ed Ω sono equipotenti.*

Dim. Nell'ipotesi che G sia regolare, fissiamo un elemento $\alpha \in \Omega$ e, per ogni $\beta \in \Omega$, sia g_β l'unico elemento di G tale che $\alpha^{g_\beta} = \beta$. Allora l'applicazione $\phi : \Omega \to G$ definita da $\beta \to g_\beta$ è biunivoca e quindi si ha la tesi. ■

Proposizione 4.5 *Sia G transitivo su Ω e supponiamo che esista un elemento $\alpha \in \Omega$ per cui G_α è $(k-1)$-transitivo su $\Omega \setminus \{\alpha\}$ con $k > 1$. Allora G è k-transitivo.*

Quando $\Omega = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ è finito poniamo $G_{\alpha_1,\alpha_2} = (G_{\alpha_1})_{\alpha_2}$ e per induzione $G_\Omega = G_{\alpha_1 ... \alpha_n} = \left(G_{\alpha_1 ... \alpha_{n-1}}\right)_{\alpha_n}$

Proposizione 4.6 *Per ogni elemento $\alpha \in \Omega$, la cardinalità dell'orbita α^G è uguale all'indice in G dello stabilizzatore G_α di α, cioè $|G| = \left|\alpha^G\right| |G_\alpha|$.*

Dim. Poichè G_α è un sottogruppo di G, possiamo considerare l'insieme dei laterali destri di G_α che indichiamo con $\mathcal{L} = \{G_\alpha g \mid g \in G\}$. Definiamo ora l'applicazione $\varphi : \mathcal{L} \to \alpha^G$ con $\varphi(G_\alpha g) = \alpha^g$. Poichè $|\mathcal{L}| = |G : G_\alpha|$, per provare la tesi è sufficiente dimostrare che φ è biettiva. Proviamo innanzitutto che φ è ben posta. Infatti, se si ha $G_\alpha g = G_\alpha h$, allora esiste un $x \in G_\alpha$ tale che $h = xg$. Ne segue $\varphi(G_\alpha h) = \alpha^h = \alpha^{xg} = \alpha^g = \varphi(G_\alpha g)$. Proviamo ora che φ è iniettiva. Siano $g, h \in G$ tali che $\alpha^g = \alpha^h$. Ma $\alpha^g = \alpha^h \Rightarrow \alpha^{gh^{-1}} = \alpha \Rightarrow gh^{-1} \in G_\alpha \Rightarrow G_\alpha g = G_\alpha h$. Ovviamente φ è anche suriettiva. ■

Proposizione 4.7 *Se t è il numero delle orbite di G su Ω e $f(g)$ denota il numero dei punti di Ω fissati da g allora*

$$t\,|G| = \sum_{g\in G} f(g).$$

Dim. Chiamiamo **bandiera** una coppia (α, g) con $\alpha \in \Omega$ e $g \in G$, tale che $\alpha^g = \alpha$. Ora contiamo le bandiere in due differenti modi. Per ogni $\alpha \in \Omega$ esistono esattamente $|G_\alpha|$ elementi g tali che (α, g) è una bandiera. Quindi il numero totale delle bandiere è $\sum_{\alpha\in\Omega} |G_\alpha|$. D'altra parte, per ogni $g \in G$, esistono esattamente $f(g)$ elementi α di Ω tali che (α, g) è una bandiera, quindi il numero totale delle bandiere è $\sum_{g\in G} f(g)$. Consideriamo $\alpha_1, \alpha_2, ..., \alpha_t$ elementi di Ω, uno per ogni orbita di G. Per ogni $\alpha_i \in \Omega$ si ha $\left|\alpha_i^G\right| |G_{\alpha_i}| = |G|$. Indichiamo con $\mathcal{O}_i$ l'orbita di α_i rispetto a G. Naturalmente $|\mathcal{O}_i| = \left|\alpha_i^G\right|$ per $i = 1, ..., t$.

Se α_i e α_j appartengono alla stessa orbita rispetto a G allora $|G_{\alpha_i}| = \left|G_{\alpha_j}\right|$ da cui segue $\sum_{\alpha\in\mathcal{O}_h} |G_\alpha| = |\mathcal{O}_h|\,|G_\alpha| = \left|\alpha_h^G\right| |G_{\alpha_h}| = |G|$ quindi

$$\sum_{g\in G} f(g) = \sum_{\alpha\in\Omega} |G_\alpha| = \sum_{\alpha\in\mathcal{O}_1} |G_\alpha| + \sum_{\alpha\in\mathcal{O}_2} |G_\alpha| + ... + \sum_{\alpha\in\mathcal{O}_t} |G_\alpha| = \sum_{i=1}^{t} |G| = t\,|G|$$

Abbiamo così provato la tesi. ■

Richiamiamo la definizione di p-sottogruppo di Sylow di un gruppo G: se p è un primo tale che $p \mid |G|$ e p^h è la massima potenza di p che divide $|G|$ allora G ammette sottogruppi di ordine p^h. Tali sottogruppi sono detti *p-sottogruppi di Sylow di G*.

Proposizione 4.8 *Sia p un numero primo, supponiamo che p^m sia un divisore di $\left|\alpha^G\right|$ e che P sia un p-sottogruppo di Sylow di G. Allora p^m è anche un divisore di $\left|\alpha^P\right|$.*

Dim. Se applichiamo più volte la Prop. 4.6 otteniamo che $\left|\alpha^G\right| |G_\alpha : P_\alpha| = |G : G_\alpha|\,|G_\alpha : P_\alpha| = |G : P_\alpha| = |G : P|\,|P : P_\alpha| = |G : P| \left|\alpha^P\right|$. Per ipotesi $p^m \mid \left|\alpha^G\right|$ ed essendo P un p-sottogruppo di Sylow di G si ha $(|G : P|, p) = 1$ da cui $p^m \mid \left|\alpha^P\right|$. ■

Proposizione 4.9 *Sia S un insieme di n elementi con n pari e sia G un gruppo che agisce transitivamente su S. Se Q è un 2-sottogruppo di Sylow di G e $\sigma \in Z(Q)$, allora il numero degli elementi di S fissati da σ è diverso da $\sqrt{n}$ e $\sqrt{n+1} - 1$.*

Dim. Ricordiamo che $Z(Q)$, il centro di Q, è l'insieme degli elementi di Q che permutano con ogni altro elemento di Q. Sia $F = Fix(\sigma)$, allora F è un sottoinsieme proprio di S. Consideriamo $q \in Q$ e $\alpha \in F$, poichè $\sigma \in Z(Q)$ si ha $q\sigma = \sigma q$ da cui $(\alpha^q)^\sigma = (\alpha^\sigma)^q = \alpha^q$, cioè $\alpha^q \in F$. Abbiamo così verificato che per ogni $\alpha \in F$ e per ogni $q \in Q$, $\alpha^q \in F$ ossia F è Q-invariante. Ne segue che F è unione di orbite di Q. Sia 2^h la massima potenza di 2 che divide n con $h \geq 1$, essendo n pari. Per la Proposizione

precedente si ha che $2^h \mid \left|\alpha^Q\right|$ per ogni $\alpha \in F$, da cui $2^h \mid |F|$. Se fosse $|F| = \sqrt{n}$ allora da $2^h \mid \sqrt{n}$ seguirebbe $2^{2h} \mid n$, ma questo contraddice l'ipotesi: 2^h è la massima potenza di 2 che divide n. Supponiamo allora che sia $|F| = \sqrt{n+1} - 1$ da cui $2^h \mid \sqrt{n+1} - 1$. Poichè n è pari allora $n+1$ è dispari e $\sqrt{n+1}+1$ è pari da cui segue che $2 \mid \sqrt{n+1}+1$ e quindi 2^{h+1} divide $(\sqrt{n+1}-1)(\sqrt{n+1}+1)$ ossia $2^{h+1} \mid n$ e di nuovo si ha un assurdo. ■

Definizione 4.10 *Un sottoinsieme Δ di Ω prende il nome di* blocco *per G se per ogni $g \in G$ verifica la seguente proprietà: $\Delta \cap \Delta^g \neq \emptyset \Rightarrow \Delta = \Delta^g$. Cioè, se Δ e Δ^g non coincidono, allora sono disgiunti. Ovviamente l'insieme vuoto, i singoletti di Ω e Ω stesso sono blocchi di G che si dicono* blocchi banali.

Valgono le seguenti proprietà:

Proposizione 4.11 *Se Δ è un blocco per G allora anche Δ^g, con $g \in G$, è un blocco per G.*

Dim. Supponiamo che esista $f \in G$ con $\Delta^g \cap (\Delta^g)^f \neq \varnothing$. Allora si ha che anche $\Delta^{gg^{-1}} \cap (\Delta^g)^{fg^{-1}} \neq \varnothing$ ossia $\Delta \cap \Delta^{gfg^{-1}} \neq \varnothing$. Ma Δ è un blocco per ipotesi, quindi $\Delta = \Delta^{gfg^{-1}}$ da cui $\Delta^g = \Delta^{gf}$, ossia Δ^g è un blocco. ■

Definizione 4.12 *Il gruppo G si dice* primitivo *su Ω se è transitivo su Ω e non ammette blocchi diversi da quelli banali. Se G è transitivo e non è primitivo si dice* imprimitivo.

Sia G transitivo su Ω. Se esiste un blocco Δ non banale per G allora Δ^G è una partizione di Ω in blocchi non banali per G. Infatti sia $\alpha \in \Omega$ e $\beta \in \Delta$, allora per la transitività di G esiste $g \in G$ tale che $\beta^g = \alpha$, quindi $\alpha \in \Delta^g$ cioè Δ^G ricopre Ω. Inoltre i blocchi in Δ^G sono a due a due disgiunti.

Δ^G prende il nome di *sistema di imprimitività* per G e spesso Δ è chiamato *blocco di imprimitività* per G.

Proposizione 4.13 *Se G è 2-transitivo allora G è primitivo.*

Dim. Sia G 2-transitivo e sia Δ un blocco non banale. Consideriamo due coppie di elementi di Ω, (α_1, α_2) e (α_1', α_2') con $\alpha_1, \alpha_2, \alpha_1' \in \Delta$ e $\alpha_2' \in \Omega - \Delta$. Per la 2-transitività di G esiste $g \in G$ tale che $\alpha_1^g = \alpha_1'$ e $\alpha_2^g = \alpha_2'$. Se $\alpha_1^g = \alpha_1'$ allora $\Delta \cap \Delta^g \neq \varnothing$ e quindi $\Delta = \Delta^g$. Ma allora α_2' appartiene a Δ essendo $\alpha_2^g = \alpha_2'$ e ciò è assurdo perchè per ipotesi $\alpha_2' \in \Omega - \Delta$. ■

Osserviamo che dalla transitività di G non segue la primitività di G. Se ad esempio consideriamo il gruppo $G(l, l)$ delle traslazioni del piano affine Π_l, questo è transitivo sull'insieme dei punti di Π_l ma non è primitivo. Infatti: se L è un punto della retta l,

allora l'insieme delle rette del fascio di centro L rappresenta un sistema di imprimitività per $G(l,l)$. In effetti $G(l,l)$ ha più sistemi di imprimitività, uno per ogni punto P su l.

Il risultato che segue caratterizza i gruppi primitivi.

Proposizione 4.14 *Sia G transitivo su Ω e $\alpha \in \Omega$. Allora G è primitivo se e soltanto se lo stabilizzatore G_α di α in G è un sottogruppo proprio massimale in G.*

Dim. Supponiamo che G sia primitivo e denotiamo con H un sottogruppo di G tale che $G_\alpha < H < G$. Considerati un elemento $g \in G - H$ e l'orbita α^H di α in H, supponiamo che esista un elemento $\beta \in \Omega$ comune a α^H e $(\alpha^H)^g$. In queste ipotesi, esistono due elementi f ,h di H tali che $\beta = \alpha^f = (\alpha^h)^g = \alpha^{hg}$ e abbiamo così che hgf^{-1} appartiene a G_α. Dal fatto che $G_\alpha < H$ segue che hgf^{-1} appartiene ad H e, poichè f e h sono in H, anche g deve essere un elemento di H, contro quanto supposto. Ne segue che G_α è massimale. Ora, per dimostrare il viceversa, sia G_α un sottogruppo proprio massimale in G. Supponiamo per assurdo che G sia imprimitivo. Chiamiamo Δ un suo blocco non banale contenente α e osserviamo che lo stabilizzatore G_Δ di Δ è un sottogruppo proprio di G, altrimenti, essendo G transitivo, avremmo $\Delta = \Omega$. Detto g un elemento di G_α, abbiamo che $\alpha^g = \alpha \in \Delta$, e quindi, $\Delta \cap \Delta^g$ è non vuoto, cioè $\Delta = \Delta^g$ e $G_\alpha \leq G_\Delta$. A questo punto, essendo Δ non banale, possiamo considerare un elemento $\beta \in \Delta$ diverso da α e, essendo G transitivo, esiste un elemento $f \in G - G_\alpha$ tale che $\alpha^f = \beta$. Allora, anche in questo caso, da $\beta = \alpha^f \in \Delta$, segue $\Delta = \Delta^f$ e cioè f appartiene a G_Δ. Allora G_Δ è un sottogruppo proprio di G contenente propriamente G_α contro l'ipotesi G_α massimale. ■

Proposizione 4.15 *Sia G primitivo su Ω e sia $N \lhd G$ con $N \neq \langle 1 \rangle$. Allora N è transitivo su Ω.*

Dim. Sia $\alpha \in \Omega$, consideriamo un'orbita α^N e sia $g \in G$. Allora $\left(\alpha^N\right)^g = \left(\alpha^{gg^{-1}N}\right)^g = (\alpha^g)^{g^{-1}Ng}$, ma $N \lhd G$ e quindi $g^{-1}Ng = N$ da cui $\left(\alpha^N\right)^g = (\alpha^g)^N$, cioè G permuta le orbite di N e quindi α^N è un blocco per G. Poichè G è primitivo su Ω, G ammette solo blocchi banali, ossia $\alpha^N = \Omega$ oppure $\left|\alpha^N\right| = 1$. Nel secondo caso N fisserebbe puntualmente Ω contro l'ipotesi $N \neq \langle 1 \rangle$. Quindi deve essere $\alpha^N = \Omega$ e la tesi è provata. ■

Definizione 4.16 *Un gruppo di permutazioni G su Ω si dice di* Frobenius *se è transitivo su Ω e $G_{\alpha,\beta} = \langle 1 \rangle$ per ogni $\alpha, \beta \in \Omega$ con $\alpha \neq \beta$.*

Osserviamo che se G, oltre ad essere transitivo è anche regolare, cioè $G_\alpha = \langle 1 \rangle$, allora G risulterebbe un gruppo di Frobenius. In effetti si considerano gruppi di Frobenius per i quali $G_\alpha \neq \langle 1 \rangle$.

Dalla definizione segue subito che in un gruppo di Frobenius ogni elemento non identico fissa al più un punto.

Teorema 4.17 *(esistenza del nucleo di Frobenius) In un gruppo di Frobenius finito gli elementi f.p.f. insieme all'identità costituiscono un sottogruppo detto* nucleo di Frobenius*.*

Si verifica che il nucleo di Frobenius è regolare su Ω.

Sia G un gruppo di Frobenius su Ω, allora G_α, con $\alpha \in \Omega$, è detto *complemento di Frobenius*.

Per la transitività di G su Ω si ha che tutti i complementi di Frobenius sono tra loro coniugati.

Tra le proprietà dei gruppi di Frobenius ricordiamo:

1. Se un complemento di Frobenius ha ordine pari allora il nucleo è abeliano.

2. Un complemento di Frobenius contiene al più una involuzione. Da cui segue che se un gruppo di Frobenius ha ordine pari e il nucleo ha ordine dispari allora un complemento di Frobenius contiene esattamente una involuzione.

3. Se G è un gruppo di Frobenius allora $G = KF$, con $K \lhd G$ e $K \cap F = \langle 1 \rangle$. K è il nucleo di G ed F un complemento. Il prodotto $G = KF$ con le ipotesi introdotte, è detto *prodotto semidiretto* di K con F.

4. Il nucleo di Frobenius K è risolubile. (Ricordiamo: si dice *derivato* di K, e si indica con K', il sottogruppo generato da tutti i commutatori di elementi di K, ossia $K' = \langle xyx^{-1}y^{-1} \mid x, y \in K \rangle$. Un gruppo K si dice *risolubile* se la sequenza $K \supseteq K' \supseteq K'' \supseteq ... \supseteq K^{(h)} \supseteq ...$in cui ogni gruppo $K^{(h)}$ è il derivato del precedente, termina nell'elemento neutro in un numero finito di passi, cioè esiste un intero non negativo t tale che $K^{(t)} = \{1\}$) .

5. L'involuzione di F agisce sul nucleo K come l'inversione. Infatti: consideriamo $i \in F$ tale che $i \neq 1$ e $i^2 = 1$ e sia $a \in K$. Supponiamo sia $a^i = b$ con $b \in K$. allora $b^i = a$ essendo $i^2 = 1$. Ora $(ab)^i = a^i b^i = ba = ab$ essendo K abeliano. Quindi l'elemento ab, essendo fissato dall'involuzione i, deve necessariamente essere uguale ad 1, ossia $b = a^{-1}$. Allora $a^i = a^{-1}$.

Lemma 4.18 *Sia S un insieme di n elementi con n dispari e sia G un gruppo di ordine $2n$ che agisce transitivamente su S. Se $G_{a,b} = \langle 1 \rangle$ per tutti gli a,b $\in S$ con $a \neq b$, allora per ogni a,b $\in S$ con $a \neq b$ esiste un'involuzione $\alpha \in G$ tale che $a^\alpha = b$.*

Dim. Poichè n è dispari e $G_{a,b} = \langle 1 \rangle$, ogni involuzione in G fissa un punto di S. Inoltre, essendo G transitivo su S, G contiene esattamente n involuzioni. Siano $1 \neq \gamma \in G_a$ e $1 \neq \delta \in G_b$ con $a \neq b$, supponiamo per assurdo che $\{\{x, x^\gamma\} : x \in S - \{a\}\} \cap \left\{\left\{x, x^\delta\right\} : x \in S - \{b\}\right\} \neq \emptyset$. Allora esiste $x \in S - \{a, b\}$ tale che $x^\gamma = x^\delta$. Da ciò segue che $x^{\gamma\delta} = x$ e quindi $(\gamma\delta)^2 = 1$ poichè un elemento non banale di ordine dispari è

f.p.f. su S. Allora $\gamma\delta = \delta\gamma$. Ora $a^{\gamma\delta} = a^{\delta}$ poichè γ fissa a e quindi $a^{\delta} = a^{\gamma\delta} = a^{\delta\gamma}$ da cui segue che γ fissa a^{δ}, mentre un'involuzione può fissare un solo elemento, quindi deve essere $a^{\delta} = a$. Ma ciò implicherebbe che $a = b$ contro quanto supposto. Quindi $\{\{x, x^{\gamma}\} : x \in S - \{a\}\} \cap \{\{x, x^{\delta}\} : x \in S - \{b\}\} = \emptyset$ per $a \neq b$. Per ogni $a \in S$ sia γ_a un'involuzione in G_a. Abbiamo allora che $|\{\{x, x^{\gamma_a}\} : x \in S - \{a\}\}| = \frac{n-1}{2}$ essendo $n-1$ il numero dei punti non fissati e $\frac{n-1}{2}$ il numero delle possibili coppie del tipo $\{x, x^{\gamma_a}\}$. Quindi $\left|\bigcup_{a \in S} \{\{x, x^{\gamma_a}\} : x \in S - \{a\}\}\right| = \sum_{a \in S} |\{\{x, x^{\gamma_a}\} : x \in S - \{a\}\}| = \frac{n(n-1)}{2}$. Poichè il numero delle coppie di elementi distinti di S è esattamente $\frac{n(n-1)}{2}$, la tesi è provata. ■

Proposizione 4.19 *Sia S un insieme, $|S| = n+1$ con n dispari. Sia $G \leq Sym(S)$ con le seguenti proprietà:*

1. *per ogni $a \in S$ lo stabilizzatore G_a contiene un sottogruppo F_a di ordine pari che agisce transitivamente su $S - \{a\}$,*

2. *$F_{a,b,c} = \langle 1 \rangle$ per ogni coppia $b, c \in S - \{a\}$ con $b \neq c$.*

Allora G_a è primitivo su $S - \{a\}$.

Dim. Poichè F_a agisce transitivamente su $S - \{a\}$ e $F_{a,b,c} = \langle 1 \rangle$, possiamo dire che F_a è un gruppo di Frobenius su $S - \{a\}$. Il nucleo di Frobenius K_a di F_a ha ordine dispari perchè è regolare su $S - \{a\}$ e quindi il suo ordine coincide con il suo grado $|S - \{a\}|$ che è dispari. Sia $F_{a,b}$ un complemento di Frobenius di F_a. Ora $F_a = K_a F_{a,b}$ con F_a di ordine pari e K_a di ordine dispari, quindi $F_{a,b}$ è di ordine pari, cioè contiene un'involuzione σ. Possiamo assumere, senza perdità di generalità, che $F_a = K_a \langle \sigma \rangle$ perchè anche questo gruppo, pur essendo d'ordine potenzialmente inferiore, soddisfa le ipotesi richieste nell'enunciato della Proposiozione. Supponiamo per assurdo che G_a non sia primitivo su $S - \{a\}$ e sia $I = \{a_1, ..., a_t\}$ un blocco di imprimitività per G_a nella sua azione su $S - \{a\}$, vale $1 < t < n$ per escludere il caso di blocchi banali. Inoltre $t \mid n$ perchè i blocchi costituiscono una partizione dell'insieme $S - \{a\}$ la cui cardinalità è n. Quindi t è dispari. Poniamo $T = I \cup \{a\}$. Poichè $t < n$, esiste $b \in S - \{a\}$ tale che $b \notin T$. Per l'ipotesi 1. lo stabilizzatore G_b contiene un sottogruppo F_b di ordine pari che agisce transitivamente su $S - \{b\}$ e per la Prop. precedente esiste una involuzione $\gamma_i \in F_b$ tale che $a^{\gamma_i} = a_i$. Proviamo che T è invariante rispetto all'azione di γ_i. Chiaramente $a^{\gamma_i} = a_i$ per $a_i \in T$. Consideriamo un elemento a_j e supponiamo che $a_j^{\gamma_i} = c \notin T$. Poichè $c \notin T$ e $a_i, a \in T$, esiste un'involuzione $\delta \in F_c$ tale che $a_i^{\delta} = a$. Quindi $a^{\gamma_i \delta} = a_i^{\delta} = a$ cioè $\gamma_i \delta \in G_a$. Inoltre γ_i è una involuzione che trasforma a_i in a e viceversa a in a_i, quindi $a_i^{\gamma_i \delta} = a^{\delta} = a_i$, da cui $a_i \in I \cap I^{\gamma_i \delta}$, infatti $a_i \in I$ per costruzione e $I^{\gamma_i \delta}$ contiene $a_i^{\gamma_i \delta}$ che coincide con a_i, quindi $I \cap I^{\gamma_i \delta} \neq \varnothing$ da cui $I = I^{\gamma_i \delta}$ essendo I un blocco di imprimitività. Ora $c = c^{\delta} = a_j^{\gamma_i \delta} \in I^{\gamma_i \delta}$ e $c \in S - T$ quindi $c \in I \cap (S - T) = \emptyset$ che è un assurdo essendo $I \subset T$. L'assurdo deriva dall'aver supposto che esiste $a_j^{\gamma_i} = c \notin T$. Allora T è

γ_i-invariante per ogni i. Sia $D = \langle \gamma_1, ..., \gamma_t \rangle$, ovviamente T è D-invariante perchè abbiamo appena provato che T è γ_i-invariante per ogni i. Se consideriamo $a, a_i \in T$ esiste $\gamma_i \in D$ tale che $a^{\gamma_i} = a_i$ cioè D è transitivo su T. Quindi, $|D| = \left|a^D\right| |D_a| = (t+1)|D_a|$. Poichè D è un sottogruppo di F_b, $|D|$ non è divisibile per 4 essendo $|F_b| = 2n$ con n dispari. Inoltre $|D_a| \leq |F_{b,a}| \leq 2$ e $t+1$ è pari perchè $t \mid n$. Se fosse $|D_a| = 2$ da $|D| = (t+1)|D_a|$ seguirebbe che $4 \mid |D|$, assurdo. Quindi deve essere $|D_a| = 1$ e $|D| = t+1$ da cui segue che D è costituito dall'unità e dalle t involuzioni $\gamma_1, ..., \gamma_t$. Se consideriamo $a, b \in D$ si ha $(ab)^2 = 1$ da cui $ab = ba$ cioè D è abeliano elementare. Ma un gruppo di Frobenius non può contenere involuzioni che commutano, quindi $|D| = 2$ e $t = 1$ contro l'ipotesi $1 < t < n$. ■

Richiamiamo la definizione di *sottogruppo caratteristico* che ci sarà utile per la dimostrazione del Corollario che segue:

Definizione 4.20 *Sia G un gruppo ed H un suo sottogruppo. Si dice che H è un* sottogruppo caratteristico *di G se per ogni automorfismo $\phi \in Aut(G)$ si ha $H^\phi = H$.*

Proprietà:

- l'essere un sottogruppo caratteristico è una condizione più forte dell'essere un sottogruppo normale. Infatti se tutti gli automorfismi di G mutano H in sé, in particolare questo sarà vero per gli automorfismi interni, e quindi H sarà normale.

- siano $K \leq H \leq G$. Se K è caratteristico in H e H è caratteristico in G, K lo è anche in G.

- siano $K \leq H \lhd G$. Se K è caratteristico in H e H è normale in G allora $K \lhd G$. Infatti se guardiamo all'azione per coniugio di G su H, G muta in sè H. Quindi G induce un automorfismo su H e di conseguenza muta in sè K perchè K è caratteristico in H.

Corollario 4.21 *Con le stesse ipotesi della Prop. 4.19, supponiamo che il nucleo di Frobenius K_a di F_a sia un sottogruppo normale di G_a. Allora K_a è un p-gruppo abeliano elementare ed n è una potenza di un primo p.*

Dim. Poichè F_a contiene involuzioni, K_a è abeliano. Supponiamo che K_a abbia un sottogruppo caratteristico H. Allora da $H \leq K_a \lhd G_a$ segue che H è normale in G_a. Per la Prop. 4.19, G_a è primitivo su $S - \{a\}$ da cui segue che H è transitivo. Ora, essendo H sottogruppo di K_a si ha necessariamente $H = K_a$. Poichè K_a non può contenere alcun sottogruppo caratteristico non banale allora, per un risultato di carattere generale, K_a deve essere un p-gruppo abeliano elementare. Essendo K_a regolare su $S - \{a\}$, si ha che $n = |K_a| = p^h$ e quindi la tesi. ■

5 APPENDICE II: Il Piano Desarguesiano.

Definizione 5.1 *Un piano proiettivo* Π *è un insieme di punti e rette, detti elementi di* Π*, in cui è definita una relazione di incidenza tale che:*

1. *due punti distinti sono incidenti ad una ed una sola retta;*
2. *due rette distinte hanno uno ed un solo punto incidente in comune;*
3. *esistono quattro punti a tre a tre non incidenti ad una stessa retta.*

Sia $\mathcal{K}$ un campo, un esempio ben noto di piano proiettivo si ha considerando nello spazio vettoriale $\mathcal{K}^3$ di dimensione 3 sul campo $\mathcal{K}$ come:

1. **punti**: le rette vettoriali, ossia i sottospazi 1-dimensionali di $\mathcal{K}^3$;
2. **rette**: i piani vettoriali, ossia i sottospazi 2-dimensionali di $\mathcal{K}^3$;
3. **relazione di incidenza**: l'inclusione.

E' noto che ogni retta per l'origine può essere individuata mediante un vettore $\mathbf{v}(x_0, y_0, z_0)$, non nullo, detto vettore direttore; tale vettore è determinato a meno di un fattore di proporzionalità. Possiamo allora rappresentare un punto proiettivo P con la scrittura (x_0, y_0, z_0). Ogni altra terna non nulla e proporzionale a (x_0, y_0, z_0), individuando la stessa retta vettoriale, rappresenterà lo stesso punto P.

Ogni piano per l'origine ha equazione $ax + by + cz = 0$, dove a, b, c sono tre coefficienti non tutti nulli e, chiaramente, individuati a meno di un fattore di proporzionalità. Possiamo allora rappresentare la retta proiettiva r con la scrittura $[a, b, c]$, ogni altra terna non nulla e proporzionale ad $[a, b, c]$ rappresenterà la stessa retta r.

L'incidenza del punto proiettivo $P = (x_0, y_0, z_0)$ con la retta proiettiva $r = [a, b, c]$ è semplicemente data da $ax_0 + by_0 + cz_0 = 0$, poiché se un punto della retta vettoriale diverso dall'origine appartiene al piano vettoriale, tutti gli altri punti della retta vettoriale gli appartengono.

Verifichiamo ora gli assiomi che definiscono un piano proiettivo:

1. Indichiamo con $\mathbf{v}_P(x, y, z)$ e $\mathbf{v}_Q(x', y', z')$ i vettori non nulli corrispondenti ai punti distinti P e Q. Da $P \neq Q$ segue che $\mathbf{v}_P$ e $\mathbf{v}_Q$ sono linearmente indipendenti, quindi generano uno ed un solo sottospazio 2-dimensionale che corrisponde ad una ed una sola retta proiettiva $r = \left[\begin{vmatrix} y & z \\ y' & z' \end{vmatrix}, - \begin{vmatrix} x & z \\ x' & z' \end{vmatrix}, \begin{vmatrix} x & y \\ x' & y' \end{vmatrix} \right]$. Pertanto, due punti distinti sono incidenti ad una ed una sola retta;

2. Indichiamo con $ax + by + cz = 0$ e $a'x + b'y + c'z = 0$, rispettivamente, le equazioni dei piani vettoriali corrispondenti alle rette distinte r ed l. I due piani si intersecano necessariamente lungo una ed una sola retta vettoriale, data dal sistema delle loro equazioni, che rappresenta uno ed solo punto proiettivo $P = \left(\begin{vmatrix} b & c \\ b' & c' \end{vmatrix}, - \begin{vmatrix} a & c \\ a' & c' \end{vmatrix}, \begin{vmatrix} a & b \\ a' & b' \end{vmatrix} \right)$. Dunque due rette distinte hanno uno ed un solo punto incidente in comune;

3. I vettori $\mathbf{v}_P\,(1,0,0)$, $\mathbf{v}_Q\,(0,1,0)$, $\mathbf{v}_R\,(0,0,1)$, $\mathbf{v}_S\,(1,1,1)$ essendo a tre a tre non complanari, rappresentano quattro punti proiettivi a tre a tre non allineati, cioè non incidenti ad una stessa retta proiettiva.

Il piano proiettivo Π appena costruito si denota con $PG(2,\mathcal{K})$ e, se $\mathcal{K} = GF(q)$, dove $q = p^h$, p primo, allora Π si denota spesso con $PG(2,q)$, poichè esiste a meno di isomorfismi un solo campo finito di ordine q.

5.1 Automorfismi Lineari di $\mathcal{K}^3$

Consideriamo il gruppo degli automorfismi lineari di $\mathcal{K}^3$ che indichiamo con $GL(\mathcal{K}^3)$. Sia $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ la base canonica di $\mathcal{K}^3$, allora ad ogni automorfismo $f \in GL(\mathcal{K}^3)$ resta associata una matrice A appartenente al *Gruppo Generale Lineare* di dimensione 3 su $\mathcal{K}$, che si denota con $GL(3,\mathcal{K})$ e, viceversa, ad ogni matrice di $GL(3,\mathcal{K})$ resta associato uno ed un solo automorfismo lineare di $\mathcal{K}^3$.

Ogni automorfismo f, trasformando sottospazi vettoriali di $\mathcal{K}^3$ in sottospazi della stessa dimensione, di fatto trasforma punti proiettivi in punti proiettivi e rette proiettive in rette proiettive conservando l'inclusione. Pertanto ogni $f \in GL(3,\mathcal{K})$ induce una collineazione α su $PG(2,\mathcal{K})$. Se indichiamo con G il gruppo delle collineazioni di $PG(2,\mathcal{K})$, si ha allora un'applicazione $\Phi : GL(3,\mathcal{K}) \to G$ ed è immediato verificare che si tratta di un omomorfismo il cui nucleo è costituito dagli automorfismi f che trasformano in sè ogni sottospazio di dimensione 1. Un tale automorfismo f agisce quindi su $\mathcal{K}^3$ come l'applicazione lineare di matrice $\lambda I_3 = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$. Il nucleo di Φ è quindi $\{\lambda I_3 \mid \lambda \in \mathcal{K}^*\}$. Questo sottogruppo costituisce il centro $Z(GL(3,\mathcal{K}))$ di $GL(3,\mathcal{K})$. Il quoziente si denota con $PGL(3,\mathcal{K}) = GL(3,\mathcal{K})/Z(GL(3,\mathcal{K}))$ ed è isomorfo quindi ad un sottogruppo del gruppo delle collineazioni di $PG(2,\mathcal{K})$.

Il *Gruppo Speciale Lineare* $SL(3,\mathcal{K})$ è il sottogruppo normale di $GL(3,\mathcal{K})$ che consiste delle matrici a determinante 1. Non è difficile provare che il centro $Z = \mathbf{Z}(SL(3,\mathcal{K}))$ consiste esattamente nell'insieme delle matrici scalari a determinante 1, cioè matrici della forma λI con $\lambda^3 = 1$. Quindi $|Z|$ è uguale al numero d degli elementi $\lambda \in \mathcal{K}^*$ tali che $\lambda^3 = 1$. Poichè $\mathcal{K}^*$ è ciclico di ordine $q-1$, segue che $d = (3, q-1)$. Il gruppo quoziente $SL(3,\mathcal{K})/\mathbf{Z}(SL(3,\mathcal{K}))$ è detto *Gruppo Speciale Proiettivo* ed è denotato con $PSL(3,\mathcal{K})$.

Vediamo ora come si può rileggere, in termini algebrici, l'esistenza di punti uniti e di rette unite per una collineazione α indotta da una matrice A di $GL(3,\mathcal{K})$.

Sia $P=(x,y,z)$ un punto di $PG(2,\mathcal{K})$ e sia $\mathbf{v}_P$ il vettore associato a P. Dire che P è un punto unito per α equivale a dire che $P^\alpha = P$ ossia $A\mathbf{v}_P = \rho\mathbf{v}_P$, per qualche autovalore ρ non nullo. Cercare i punti uniti di α, quindi, equivale a cercare gli autovettori della matrice A.

Sia ρ_i, per $i=1,2,3$, la generica radice dell'equazione caratteristica di A. Con $Mult(\rho_i)$ indichiamo la molteplicità algebrica di ρ_i e con $Null(\rho_i)$ la sua molteplicità geometrica. Supponiamo inoltre che per ogni $i=1,2,3$ la radice ρ_i appartenga al campo $\mathcal{K}$. Consideriamo alcuni casi significativi.

I) Gli autovalori ρ_1,ρ_2,ρ_3 di A sono distinti. In questo caso la matrice A è simile ad una matrice della forma $\begin{pmatrix}\rho_1&0&0\\0&\rho_2&0\\0&0&\rho_3\end{pmatrix}$. A ciascun autovalore ρ_i, corrisponde un autospazio di dimensione 1 e quindi un punto unito R_i e, dualmente, una retta unita r_i. In particolare $R_1=(1,0,0)$, $R_2=(0,1,0)$, $R_3=(0,0,1)$, e dualmente, $r_1=[1,0,0]\,, r_2=[0,1,0]\,, r_3=[0,0,1]$. I punti e le rette sono vertici e lati di uno stesso triangolo; la retta r_i contiene i due punti diversi da R_i.

Consideriamo ad esempio la retta $r_3=[0,0,1]$ ed un punto $P=(x,y,0)$ appartenente a tale retta. L'immagine di P tramite α è data da:

$$\begin{pmatrix}\rho_1&0&0\\0&\rho_2&0\\0&0&\rho_3\end{pmatrix}\begin{pmatrix}x\\y\\0\end{pmatrix}=\begin{pmatrix}\rho_1 x\\\rho_2 y\\0\end{pmatrix}$$

si ha allora che P^α appartiene ancora alla retta r_3 e quindi effettivamente r_3 è mutata in sè da α.

II) Gli autovalori distinti sono due: ρ_1 e ρ_2 con $Mult(\rho_1)=1$ e $Mult(\rho_2)=2=Null(\rho_2)$. La matrice A è simile ad una matrice della forma $\begin{pmatrix}\rho_1&0&0\\0&\rho_2&0\\0&0&\rho_2\end{pmatrix}$. A ρ_1 corrisponde un autospazio di dimenzione 1 e quindi un solo punto unito $R=(1,0,0)$ e, dualmente, una sola retta unita $l=[a,0,0]$. Invece a ρ_2 corrisponde un autospazio di dimenzione 2, ossia i punti uniti di una retta (che sarà necessariamente l) e le rette unite di un fascio (che avrà necessariamente centro in R). Osserviamo che $R\notin l$.

Verifichiamo, ad esempio, che l è fissata punto per punto da α: sia $P\in l$ con $P=(0,y,z)$. L'immagine di P tramite α è data da

$$\begin{pmatrix} \rho_1 & 0 & 0 \\ 0 & \rho_2 & 0 \\ 0 & 0 & \rho_2 \end{pmatrix} \begin{pmatrix} 0 \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ \rho_2 y \\ \rho_2 z \end{pmatrix}$$

quindi per ogni punto $P \in l$ si ha $P^\alpha = P$ in quanto la terna $(0, \rho_2 y, \rho_2 z)$ rappresenta sempre il punto P.

In modo duale le rette per R sono lasciate fisse da A, infatti: sia r una retta per R con $r = [0, b, c]$

$$\begin{pmatrix} \rho_1 & 0 & 0 \\ 0 & \rho_2 & 0 \\ 0 & 0 & \rho_2 \end{pmatrix} \begin{bmatrix} 0 \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 \\ \rho_2 b \\ \rho_2 c \end{bmatrix}$$

e la terna $[0, \rho_2 b, \rho_2 c]$ rappresenta proprio la retta r.

Le collineazioni di questo tipo si dicono **omologie** di **centro** R ed **asse** l.

Le equazioni di α sono: $\begin{cases} x' = \rho_1 x \\ y' = \rho_2 y \\ z' = \rho_2 z \end{cases}$ e in coordinate non omogenee $\begin{cases} x' = ax \\ y' = y \end{cases}$

III) La matrice A ha un solo autovalore ρ con $Mult(\rho) = 3$ e $Null(\rho) = 2$ La matrice A è simile ad una matrice della forma $\begin{pmatrix} \rho & 0 & 0 \\ 0 & \rho & 1 \\ 0 & 0 & \rho \end{pmatrix}$. A ρ corrispondono i punti uniti di una retta l e le rette unite di un fascio il cui centro R appartiene ad l. Procedendo come sopra, si può verificare facilmente che A fissa puntualmente la retta $l = [0, 0, c]$ e, dualmente, fissa tutte le rette per il punto $R = (0, 1, 0)$.

Le collineazioni di questo tipo si dicono **elazioni** di **centro** R ed **asse** l.

Le equazioni di α sono: $\begin{cases} x' = \rho x \\ y' = \rho y + z \\ z' = \rho z \end{cases}$ e in coordinate non omogenee $\begin{cases} x' = x \\ y' = y + 1/\rho \end{cases}$

Consideriamo ora una generica retta s del piano distinta da l e sia $S = s \cap l$. Se ad esempio $s = [0, b, c]$ allora $S = (1, 0, 0)$. L'immagine di s tramite α è data da $s^\alpha = [0, \rho b + c, \rho c]$ e $s^\alpha \cap l = S$.

Nel piano affine Π_l allora, $s^\alpha \cap s = \varnothing$ e quindi le rette s^α e s sono parallele. Possiamo allora affermare che ogni elazione di Π di asse l induce nel piano affine Π_l una traslazione.

IV) La matrice A ha un solo autovalore ρ con $Mult(\rho) = 3 = Null(\rho)$. In questo caso la matrice A è simile ad una matrice della forma $\begin{pmatrix} \rho & 0 & 0 \\ 0 & \rho & 0 \\ 0 & 0 & \rho \end{pmatrix}$, cioè è simile

ad una matrice scalare. A ρ corrisponde un autospazio di dimensione 3 e quindi tutti i punti del piano proiettivo sono lasciati fissi da α che rappresenta la collineazione identica.

Nel seguito vogliamo mettere in evidenza alcune proprietà delle collineazioni del piano desarguesiano. Useremo il simbolo Π per indicare il piano desarguesiano.

Proposizione 5.2 *Date due quaterne di punti a tre a tre non allineati P, Q, R, S e P', Q', R', S' esiste, ed è unica, la collineazione α tale che $P^\alpha = P', Q^\alpha = Q', R^\alpha = R', S^\alpha = S'$.*

Dim. Siano $\mathbf{u}_P$, $\mathbf{u}_Q$, $\mathbf{u}_R$ tre vettori non nulli corrispondenti, rispettivamente, ai punti proiettivi P, Q ed R. Poiché questi non sono allineati, i tre vettori non sono complanari e costituiscono quindi una base di $\mathcal{K}^3$. Un vettore $\mathbf{v}_S$, non nullo, corrispondente al punto S, si può scrivere quindi nella forma $\mathbf{v}_S = x\mathbf{u}_P + y\mathbf{u}_Q + z\mathbf{u}_R$, con x, y, z non nulli perché S non è allineato né con P e Q, né con P ed R, né con Q ed R. Ne segue che, assunti come nuovi rappresentanti dei tre punti P, Q, R i vettori $\mathbf{v}_P = x\mathbf{u}_P$, $\mathbf{v}_Q = y\mathbf{u}_Q$, $\mathbf{v}_R = z\mathbf{u}_R$ e scelta $\{\mathbf{v}_P, \mathbf{v}_Q, \mathbf{v}_R\}$ come base di $\mathcal{K}^3$, si ha $\mathbf{v}_S = \mathbf{v}_P + \mathbf{v}_Q + \mathbf{v}_R$. Allo stesso modo si possono scegliere i vettori $\mathbf{v}_{P'}, \mathbf{v}_{Q'}, \mathbf{v}_{R'}$ e $\mathbf{v}_{S'}$ che rappresentino, rispettivamente, i punti P', Q', R', S' in modo tale che $\{\mathbf{v}_{P'}, \mathbf{v}_{Q'}, \mathbf{v}_{R'}\}$ sia una base di $\mathcal{K}^3$ e $\mathbf{v}_{S'} = \mathbf{v}_{P'} + \mathbf{v}_{Q'} + \mathbf{v}_{R'}$. Dall'algebra lineare sappiamo che esiste una ed una sola applicazione lineare α che trasforma la base $\{\mathbf{v}_P, \mathbf{v}_Q, \mathbf{v}_R\}$ nella base $\{\mathbf{v}_{P'}, \mathbf{v}_{Q'}, \mathbf{v}_{R'}\}$. Tale applicazione è non singolare e $\mathbf{v}_S^\alpha = (\mathbf{v}_P + \mathbf{v}_Q + \mathbf{v}_R)^\alpha = \mathbf{v}_P^\alpha + \mathbf{v}_Q^\alpha + \mathbf{v}_R^\alpha = \mathbf{v}_{P'} + \mathbf{v}_{Q'} + \mathbf{v}_{R'} = \mathbf{v}_{S'}$. Pertanto esiste una ed una sola collineazione α tale che $P^\alpha = P', Q^\alpha = Q', R^\alpha = R', S^\alpha = S'$. ■

Dalla transitività di $Aut(\Pi)$ sui quadrangoli segue la 2-transitività sui punti e sulle rette.

Si noti che $Aut(\Pi)$ non può essere 3-transitivo perchè tre punti non allineati non possono essere trasformati in tre punti allineati.

Ricordiamo che un piano proiettivo Π è detto (V, l)-transitivo se, per ogni scelta di due punti distinti A, B allineati con V, distinti da V e non giacenti sull'asse l, esiste una (V, l)-prospettività α in $Aut(\Pi)$ con $A^\alpha = B$.

Proposizione 5.3 *Il piano desarguesiano è (V, l)-transitivo.*

Dim. Proviamo l'asserto per una opportuna scelta della coppia (V, l) considerando separatamente i casi $V \notin l$ e $V \in l$. Dalla transitività di $Aut(\Pi)$ sulle coppie punto-retta seguirà quindi la tesi.

I caso: $V \notin l$, sia $V = (0, 0, 1)$ e $l = [0, 0, c]$ e sia $r = [a, b, 0]$ una generica retta per V. Consideriamo due punti distinti A e B di r diversi da V: sia $A = (-b, a, c)$ e $B = (b, -a, c')$. Vogliamo provare che esiste una (V, l)-omologia α in $Aut(\Pi)$ tale che $A^\alpha = B$. Se consideriamo l'omologia α rappresentata dalla matrice $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & \frac{c'}{c} \end{pmatrix}$ sia ha che

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & \frac{c'}{c} \end{pmatrix} \begin{pmatrix} -b \\ a \\ c \end{pmatrix} = \begin{pmatrix} b \\ -a \\ c' \end{pmatrix}$$

e quindi $A^\alpha = B$. Osserviamo che α, per come è stata scelta, è effettivamente una omologia di centro V e asse l.

II caso: $V \in l$, sia $V = (0,1,0)$ e $l = [0,0,c]$ e sia $r = [a,0,c]$ una generica retta per V. Consideriamo due punti distinti A e B di r diversi da V: sia $A = (-c, y, a)$ e $B = (-c, y', a)$. Vogliamo provare che esiste una (V,l)-elazione β in $Aut(\Pi)$ tale che $A^\beta = B$. Se consideriamo l'elazione β rappresentata dalla matrice $\begin{pmatrix} -\frac{a}{y-y'} & 0 & 0 \\ 0 & -\frac{a}{y-y'} & 1 \\ 0 & 0 & -\frac{a}{y-y'} \end{pmatrix}$ sia ha che

$$\begin{pmatrix} -\frac{a}{y-y'} & 0 & 0 \\ 0 & -\frac{a}{y-y'} & 1 \\ 0 & 0 & -\frac{a}{y-y'} \end{pmatrix} \begin{pmatrix} -c \\ y \\ a \end{pmatrix} = \begin{pmatrix} \left(-\frac{a}{y-y'}\right)(-c) \\ \left(-\frac{a}{y-y'}\right) y' \\ \left(-\frac{a}{y-y'}\right) a \end{pmatrix}$$

e quindi $A^\beta = B$. Osserviamo che β, per come è stata scelta, è effettivamente una elazione di centro V e asse l. ■

5.2 Automorfismi Semilineari di $\mathcal{K}^3$

Sia $\mathcal{K} = GF(q)$ con $q = p^m$. Si dimostra che:

1. Le funzioni $\varphi_h : \mathcal{K} \to \mathcal{K}$, $\varphi_h(x) = x^{p^h}$, $h \in N$, sono automorfismi di $\mathcal{K}$.
2. $Aut(\mathcal{K})$ è ciclico, generato da φ_1, ed ha m elementi.
3. Se $\varphi_h \in Aut(\mathcal{K})$ allora φ_h muta in sé il sottocampo $GF(p^{(h,m)})$.

Definizione 5.4 *Un'applicazione semilineare non singolare di $\mathcal{K}^3$ in sé è un automorfismo del gruppo additivo $(\mathcal{K}^3, +)$ per il quale esiste $\sigma \in Aut(\mathcal{K})$, tale che per ogni $\mathbf{v} \in \mathcal{K}^3, k \in \mathcal{K}$ si ha $f(\lambda \mathbf{v}) = \lambda^\sigma f(\mathbf{v})$. Chiamiamo f automorfismo semilineare associato a σ.*

Indichiamo con $\Gamma L(\mathcal{K}^3)$ l'insieme degli automorfismi semilineari di $\mathcal{K}^3$. Valgono le seguenti proprietà:

a) *Gli automorfismi semilineari di $\mathcal{K}^3$ formano un gruppo.*

Infatti, siano f e g automorfismi semilineari associati rispettivamente ad $\alpha, \beta \in Aut(\mathcal{K})$. Allora naturalmente $f \circ g$ è ancora un automorfismo del gruppo $(\mathcal{K}^3, +)$, ed è tale che che per ogni $\mathbf{v} \in \mathcal{K}^3$, $k \in \mathcal{K}$ si ha:

$$f \circ g(k\mathbf{v}) = f(g(k\mathbf{v})) = f(k^\beta g(\mathbf{v})) = (k^\beta)^\alpha f(g(\mathbf{v})) = k^{\alpha\circ\beta} f \circ g(\mathbf{v}) \tag{9}$$

quindi $f \circ g \in \Gamma L(\mathcal{K}^3)$ perchè è associato ad $\alpha \circ \beta \in Aut(\mathcal{K})$. L'identità di $\mathcal{K}^3$ è associata all'identità di $Aut(\mathcal{K})$, quindi è semilineare. Proviamo che l'automorfismo inverso f^{-1} di f è semilineare. Poichè f ed α sono biiettive, per ogni $\mathbf{v} \in \mathcal{K}^3$, $k \in \mathcal{K}$ esistono $\mathbf{w} \in \mathcal{K}^3$, $\lambda \in \mathcal{K}$ tali che $\mathbf{v} = f(\mathbf{w})$, $k = \lambda^\alpha$. Ne segue:

$$f^{-1}(k\mathbf{v}) = f^{-1}(\lambda^\alpha f(\mathbf{w})) = f^{-1}(f(\lambda\mathbf{w})) = \lambda\mathbf{w} = \lambda^{\alpha^{-1}} f^{-1}(\mathbf{w}) \tag{10}$$

e dunque f^{-1} è l'automorfismo semilineare associato ad α^{-1}.

b) *Ad ogni automorfismo semilineare f è associato un solo automorfismo α di $\mathcal{K}$.*

Infatti, siano α, β tali che per ogni ogni $\mathbf{v} \in \mathcal{K}^3$, $k \in \mathcal{K}$ si ha $f(k\mathbf{v}) = k^\alpha f(\mathbf{v}) = k^\beta f(\mathbf{v})$. Allora si ha $(k^\alpha - k^\beta) f(\mathbf{v}) = 0$, e scelto $\mathbf{v} \neq \mathbf{0}$, si ha $f(\mathbf{v}) \neq 0$ e dunque $(k^\alpha - k^\beta) = 0$ per ogni $k \in K$.

c) $\Gamma L(\mathcal{K}^3)/GL(\mathcal{K}^3) \simeq Aut(\mathcal{K})$.

Consideriamo l'applicazione ρ che ad ogni automorfismo semilineare f associa l'automorfismo α di K a cui è associato. Si è gia visto che a $f \circ g \in \Gamma L(\mathcal{K}^3)$ è associato $\alpha \circ \beta \in Aut(\mathcal{K})$, dunque $\rho : \Gamma L(\mathcal{K}^3) \to Aut(\mathcal{K})$ è un omomorfismo. Si verifica facilmente che ρ è suriettivo.

Il nucleo di ρ è costituito dal sottogruppo $GL(\mathcal{K}^3)$ degli automorfismi lineari, coincidenti con gli automorfismi semilineari associati all'identità di $\mathcal{K}$. Si ha quindi $\Gamma L(\mathcal{K}^3)/GL(\mathcal{K}^3) \simeq Aut(\mathcal{K})$.

Abbiamo già osservato che il gruppo $GL(\mathcal{K}^3)$ è isomorfo al gruppo $GL(3, \mathcal{K})$ delle matrici non singolari di ordine 3 sul campo $\mathcal{K}$. Se $A \in GL(3, \mathcal{K})$, le sue colonne formano una base (ordinata) dello spazio vettoriale $\mathcal{K}^3$; viceversa, incolonnando i vettori di una base ordinata di $\mathcal{K}^3$ si ha una matrice invertibile. Pertanto, c'è una biiezione fra $GL(3, \mathcal{K})$ e l'insieme delle basi ordinate di $\mathcal{K}^3$. Se $\mathcal{K} = GF(q)$, è un campo finito d'ordine q, allora $\mathcal{K}^3$ ha q^3 elementi e non è difficile contare le sue basi. Se infatti vogliamo costruire una base $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$, possiamo scegliere $\mathbf{v}_1$ in $\mathcal{K}^3 \setminus \{\mathbf{0}\}$, cioè in $q^3 - 1$ modi. Scelto $\mathbf{v}_1$, si deve scegliere un vettore $\mathbf{v}_2$ in modo tale che $\mathbf{v}_1$,$\mathbf{v}_2$ siano indipendenti, ossia $\mathbf{v}_2 \in \mathcal{K}^3 \setminus L(\mathbf{v}_1)$, per cui vi sono per $\mathbf{v}_2$ solo $q^3 - q$ scelte. Analogamente, dovrà essere $\mathbf{v}_3 \in \mathcal{K}^3 \setminus L(\mathbf{v}_1, \mathbf{v}_2)$, quindi per $\mathbf{v}_3$ ci sono solo $q^3 - q^2$ scelte. In conclusione, in $\mathcal{K}^3$ ci sono $(q^3-1)(q^3-q)(q^3-q^2)$ basi ordinate, quindi il gruppo $GL(3, \mathcal{K})$, ha in definitiva $\prod_{i=o}^{2}(q^3 - q^i)$ elementi.

Ora, $q = p^m$, p primo, implica $|Aut(\mathcal{K})| = m$, quindi

$$\left|\Gamma L(\mathcal{K}^3)\right| = m \prod_{i=o}^{2} (q^3 - q^i).$$

Ripetendo un discorso analogo a quello fatto per gli automorfismi lineari, possiamo dire che ogni automorfismo semilineare trasforma punti proiettivi in punti proiettivi e rette proiettive in rette proiettive conservando l'inclusione. Pertanto, ogni automorfismo semilineare f induce una collineazione α su $PG(2, \mathcal{K})$. Si ha, allora, un omomorfismo Φ dal gruppo $\Gamma L(\mathcal{K}^3)$, indicato anche con $\Gamma L(3, \mathcal{K})$, al gruppo G delle collineazioni di $PG(2, \mathcal{K})$ il cui nucleo è il centro $Z(GL(3, \mathcal{K}))$ di $GL(3, \mathcal{K})$. Il quoziente si denota con $P\Gamma L(3, \mathcal{K}) = \Gamma L(3, \mathcal{K}) / Z(GL(3, \mathcal{K}))$ ed è isomorfo quindi ad un sottogruppo del gruppo delle collineazioni di $PG(2, \mathcal{K})$.

In realtà oltre a queste non ce ne sono altre, si dimostra infatti che:

$$Aut(PG(2, \mathcal{K})) = P\Gamma L(3, \mathcal{K}) = Aut(\mathcal{K}) \frac{GL(3, \mathcal{K})}{Z(GL(3, \mathcal{K}))}$$

essendo $\mathcal{K} = GF(q)$, $q = p^m$, si ha:

$$|Aut(PG(2, q))| = |P\Gamma L(3, q)| = \frac{m}{q-1} \prod_{i=o}^{2} (q^3 - q^i).$$

References

[1] Dembowski, P.: *Finite Geometries*. Springer-Verlag, Berlin-Heidelberg-New York 1968

[2] Hughes, P. and Piper, F.C.: *Projective Planes*, Springer-Verlag, Berlin-Heidelberg-New York 1973

[3] Lüneburg, H., *Translation Planes,Springer-Verlag, Berlin-Heidelberg-New York 1980*

[4] Wielandt, H. : *Finite permutation groups*. New York: Academic Press 1964