UNIVERSITÀ DEGLI STUDI DI ROMA
"LA SAPIENZA"

Piani proiettivi finiti e neo-insiemi di differenze

Dina Ghinelli - Dieter Jungnickel

Quaderni Elettronici del Seminario di Geometria Combinatoria
13E (Febbraio 2004)

http://www.mat.uniroma1.it/~combinat/quaderni

Dipartimento di Matematica "Guido Castelnuovo"
P.le Aldo Moro, 2 - 00185 Roma - Italia

Piani proiettivi finiti e neo-insiemi di differenze.

Al Professor Adriano Barlotti per il suo ottantesimo compleanno

Dina Ghinelli
Dipartimento di Matematica
Università di Roma "La Sapienza"
Piazzale Aldo Moro, 2
I–00185 Roma, Italy
dina@mat.uniroma1.it

Dieter Jungnickel
Lehrstuhl für Diskrete Mathematik, Optimierung
und Operations Research
Universität Augsburg
D–86135 Augsburg, Germany
jungnickel@math.uni-augsburg.de

Sommario

In questo articolo si chiariscono i legami tra le seguenti nozioni, apparse in letteratura in contesti diversi:

- piani proiettivi finiti con un gruppo di collineazioni di tipo Lenz-Barlotti I.3 o I.4;
- piani parzialmente transitivi di tipo (3) considerati da Hughes;
- piani con un gruppo di collineazioni quasiregolare di tipo (g) nella classificazione di Dembowski-Piper;
- un certo tipo di insiemi di differenze relativi a sottogruppi disgiunti nel senso di Hiramine, che noi chiamiamo "neo-insiemi di differenze", in quanto il caso abeliano corrisponde ai neocorpi.

In particolare, si stabilisce che gruppi di tipo Lenz-Barlotti I.4 sono equivalenti a gruppi quasiregolari di tipo (g) (necessariamente abeliani) e a neo-insiemi di differenze abeliani. Si fa poi una una rassegna delle restrizioni possibili per piani di classe I.4 nella classificazione di Lenz-Barlotti, usando le tecniche dei neo-insiemi di differenze. Ciò fa ri-ottenere, per tali piani, tutte le restrizioni note e anche alcune nuove

restrizioni. Usare le tecniche standard degli anelli di gruppo permette, non solo di evitare per quasi tutta la trattazione l'uso dei neocorpi, ma anche di dare, in molti casi, dimostrazioni più semplici e trasparenti, evidenziando l'analogia agli insiemi di differenze planari e affini. Come risultato a latere, si ottiene anche una nuova costruzione sintetica per triangoli proiettivi in piani desarguesiani.

1 Introduzione

Assumiamo che il lettore abbia familiarità con le nozioni di base della teoria dei piani proiettivi, in particolare, con le nozioni di elazione, omologia, (p, L)-transitività e con l'idea della classificazione di Lenz-Barlotti, rinviando a Dembowski [4], Hughes e Piper [17] o Pickert [25], per tali nozioni.

In questo articolo ci occupiamo di alcuni concetti, tra loro strettamente legati, che si ritrovano nella letteratura in contesti diversi:

- piani proiettivi finiti con un gruppo di collineazioni di tipo Lenz-Barlotti I.3 o I.4;
- piani parzialmente transitivi di tipo (3) considerati da Hughes [16];
- piani con un gruppo di collineazioni quasiregolare di tipo (g) nella classificazione di Dembowski-Piper [5];
- un certo tipo di insiemi di differenze relativi a sottogruppi disgiunti nel senso di Hiramine [12], che noi chiamiamo "neo-insiemi di differenze", in quanto il caso abeliano corrisponde ai neocorpi.

Guardando alla letteratura, può sorgere una certa confusione, in quanto le relazioni tra queste nozioni non sono mai state precisate. Il nostro primo scopo è chiarire queste connessioni. In particolare dimostriamo che gruppi di tipo Lenz-Barlotti I.4 sono equivalenti a gruppi quasiregolari di tipo (g) (necessariamente abeliani) e a neo-insiemi di differenze abeliani; in ogni caso, gli unici esempi noti si trovano in piani desarguesiani. Similmente, proviamo che gruppi di tipo Lenz-Barlotti I.3 sono equivalenti a neo-insiemi di differenze non abeliani, e gli unici esempi vengono dai piani sopra quasicorpi.

Una volta stabilite le equivalenze di base, passiamo in rassegna le restrizioni note e ne dimostriamo alcune nuove, per piani di classe I.4 nella classificazione di Lenz-Barlotti. Ciò permette, non solo di evitare la coordinatizzazione mediante un neocorpo per la maggior parte dell'esposizione, ma anche di dare, in molti casi, dimostrazioni più semplici e trasparenti, che usano le tecniche standard degli anelli di gruppo. Si accentua in tal

modo l'analogia al caso degli insiemi di differenze planari e affini. In particolare, otteniamo una dimostrazione breve e trasparente del teorema del moltiplicatoro per neo-insiemi di differenze.

Concludiamo questa introduzione ricordando alcune nozioni e dando qualche breve riferimento bibliografico. Un gruppo di permutazioni G si dice *quasiregolare* se induce un'azione regolare su ciascuna orbita, ossia se ciascun elemento del gruppo fissa o nessuno o tutti gli elementi dell'orbita. Questa condizione è soddisfatta, in particolare, quando G è abeliano. Più in generale, si vede facilmente che G ha un'azione quasiregolare su un insieme se, e solo se, ogni stabilizzatore è un sottogruppo normale.

Diamo, infine, alcuni riferimenti bibliografici. Per quanto riguarda la famosa classificazione di Lenz-Barlotti, dovuta a [1, 21]; oltre a Dembowski [4], vale ancora la pena di leggere una rassegna del 1967, dovuta a Yaqub [29] o il lavoro [7] che è in italiano e il cui aggiornamento in lingua inglese è attualmente in preparazione e uscirà in questa stessa collana elettronica. Un resoconto aggiornato della situazione, per quanto riguarda la classificazione di Dembowski-Piper [5], è stato dato dai presenti autori in [8]. Per le necessarie nozioni su insiemi di differenze e anelli di gruppo si rinvia al capitolo VI di Beth, Jungnickel e Lenz [2]. Una versione ridotta dei risultati qui illustrati è pubblicata in [9]

2 Gruppi di tipo almeno I.3

Nella classificazione di Lenz-Barlotti i gruppi di collineazioni dei piani proiettivi sono classificati secondo la configurazione F formata dalle coppie punto-retta (p, L) per le quali il dato gruppo G è (p, L)-transitivo; nel caso particolare in cui $G = \operatorname{Aut}\Pi$ sia il gruppo totale degli automorfismi del piano Π, si parla della *classe di Lenz-Barlotti* di Π. Per un gruppo di tipo I.4, F è costituita dai tre vertici e dai tre lati a loro opposti di un triangolo; per il tipo I.3 manca una di queste transitività.

Consideriamo gruppi di tipo almeno I.3. Esiste quindi un triangolo di vertici o, x, e y tale che che Π è un piano proiettivo finito di ordine n simultaneamente (y, ox)- e (x, oy)-transitivo. Si può pensare Π come il piano proiettivo ottenuto per ampliamento del piano affine avente $L_\infty = xy$ come retta all'infinito, o come origine e le rette ox e oy come assi x e y, rispettivamente.

I punti non appartenenti ai lati del triangolo si chiameranno *punti ordinari*; dualmente, le rette non appartenenti all'unione dei tre fasci di centro un vertice del triangolo si diranno *rette ordinarie*. Indicati con X il gruppo di tutte le omologie di centro x ed asse oy (in breve: (x, oy)-omologie) e

con Y il gruppo di tutte le (y, ox)-omologie, si può assumere, senza ledere la generalità, che il gruppo G in esame sia il gruppo generato da X ed Y.

Lemma 2.1 *Con le notazioni sopra introdotte, G è il prodotto diretto di X e Y; inoltre, G agisce regolarmente sia sull'insieme dei punti ordinari che sull'insieme delle rette ordinarie.*

Dimostrazione. Cominciamo con il dimostrare che G è transitivo sui punti ordinari. A tale scopo, scegliamo arbitrariamente un punto ordinario u (che possiamo pensare come punto unità del riferimento). Per ogni punto ordinario p, siano $p_x = ox \cap yp$ e $p_y = oy \cap xp$ le sue proiezioni sugli assi (cfr. Figura 1). Sia $\xi \in X$ l'unica (x, oy)-omologia che trasforma u_x in p_x e sia $\psi \in Y$ l'unica (y, ox)-omologia che trasforma u_y in p_y. Si vede facilmente che sia $\xi\psi$ che $\psi\xi$ trasformano u in p; pertanto G è transitivo sui punti ordinari. Data l'arbitrarietà della scelta di u, la stessa argomentazione prova che le immagini tramite $\xi\psi$ e $\psi\xi$ coincidono per ogni punto ordinario u, il che implica che $\xi\psi = \psi\xi$ per ogni $\xi \in X$ e $\psi \in Y$. Si ha dunque che X e Y commutano, di conseguenza $G = X \times Y$. Essendo X e Y gruppi di ordine $n-1$, il gruppo G risulta di ordine $(n-1)^2$. Ma questo è esattamente il numero dei punti ordinari, per cui G agisce regolarmente su tali punti. Per dualità, G agisce regolarmente anche sulle rette ordinarie. □

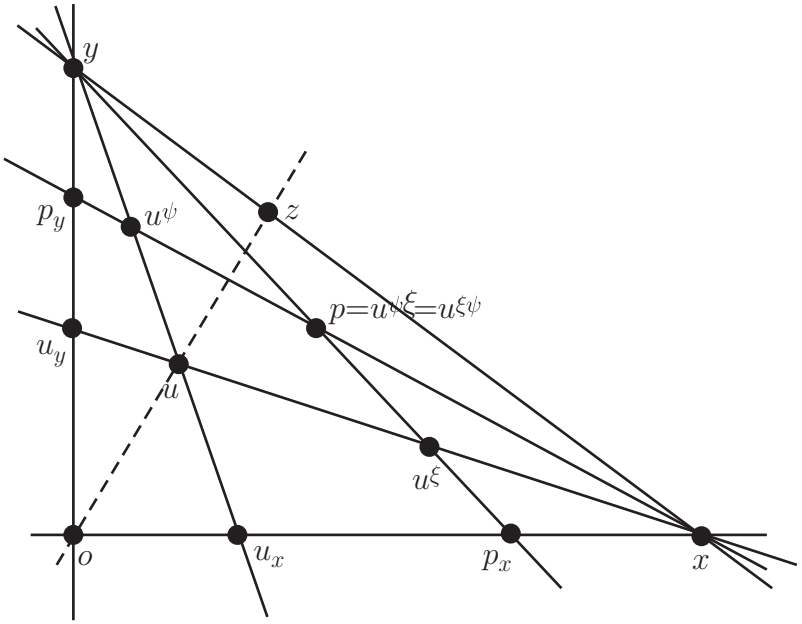

Figura 1: L'azione di G

Posto $z = ou \cap xy$, sia Z lo stabilizzatore di ou. Poiché G fissa o e, per il Lemma 2.1, è regolare sui punti ordinari, Z è un ulteriore sottogruppo di

ordine $n-1$ di G. Osserviamo in primo luogo il seguente fatto che si trova già nel lavoro di Hughes [16].

Lemma 2.2 *X, Y e Z sono tre sottogruppi di ordine $n-1$ di $G = X \times Y$ a due a due disgiunti e isomorfi. Inoltre, G è abeliano se e solo se anche Z è un sottogruppo normale.*

Il Lemma 2.2 è una conseguenza immediata del Lemma 2.1 e del seguente risultato generale, dimostrato da Sprague [27] nel contesto delle reti di traslazione; dato che lo useremo nel seguito, ne riportiamo la dimostrazione per comodità del lettore.

Lemma 2.3 *Sia G un gruppo di ordine s^2 con tre sottogruppi X, Y e Z di ordine s a due a due disgiunti. Se X e Y sono normali in G, i tre sottogruppi risultano necessariamente a due a due isomorfi. Inoltre, G è abeliano se e solo se anche Z è un sottogruppo normale.*

Dimostrazione. L'ipotesi implica, ovviamente, che $G \cong X \times Y$. Poiché Z interseca sia X che Y banalmente, ciascun elemento $\zeta \in Z$ si può scrivere, in modo unico, nella forma $\zeta = (\xi, f(\xi))$, ove f è un'applicazione biunivoca tra X e Y. Se $\xi, \eta \in X$, risulta

$$(\xi, f(\xi))(\eta, f(\eta)) \;=\; (\xi\eta, f(\xi)f(\eta)) \;=\; (\xi\eta, f(\xi\eta)),$$

essendo Z un gruppo. Ciò prova che f è un isomorfismo tra X e Y e quindi $\xi \mapsto (\xi, f(\xi))$ è un isomorfismo tra X e Z. Si ha poi che G è abeliano se e solo se X è abeliano e, in tal caso, Z è banalmente normale. Viceversa, se si assume che Z sia normale e che $\xi, \eta \in X$, si ha

$$(\xi^{-1}, 1)(\eta, f(\eta))(\xi, 1) \;=\; (\xi^{-1}\eta\xi, f(\eta)) \;\in\; Z$$

da cui $f(\eta) = f(\xi^{-1}\eta\xi)$ e quindi $\eta = \xi^{-1}\eta\xi$, il che mostra appunto che X è abeliano. □

Osserviamo poi che il nostro gruppo di collineazioni G ha su Π la stessa struttura in orbite di un gruppo quasiregolare di tipo (g) nella classificazione di Dembowski-Piper: le sette orbite sui punti sono

- l'orbita dei punti ordinari, sui quali G agisce regolarmente;
- i tre punti fissi o, x, e y;
- gli $n-1$ punti $z' \neq x, y$ su xy, e, similmente, sugli altri due lati del triangolo oxy.

Le orbite sulle rette si dànno dualmente. È spontaneo chiedersi sotto quali condizioni G risulti effettivamente quasiregolare. Il risultato che segue è in parte contenuto nel lavoro di Hughes (cfr. [16, Theorem 10]) in cui G viene chiamato *gruppo di collineazioni parzialmente transitivo di tipo* (3) in cui due dei tre sottogruppi speciali sono normali.

Proposizione 2.4 *Con le notazioni precedenti, le condizioni che seguono sono equivalenti:*

1. *G è un gruppo di collineazioni di tipo Lenz-Barlotti I.4.*
2. *Z è costituito da omologie di centro o ed asse xy.*
3. *Z è un sottogruppo normale di G.*
4. *G è quasiregulare.*
5. *X è abeliano.*
6. *G è abeliano.*

Dimostrazione. Poiché Z è lo stabilizzatore di z in G e agisce regolarmente sui punti ordinari della retta oz, è chiaro che G è di tipo I.4 se e solo se tutte le collineazioni in Z sono omologie di centro o ed asse xy. Ciò significa che ciascun elemento che fissa z deve fissare ogni punto della retta xy; ma G è transitivo sui punti $z' \neq x, y$ di xy e lo stabilizzatore di z^γ è $\gamma^{-1}Z\gamma$; pertanto, ciò succede se, e solo se, Z è un sottogruppo normale di G. A sua volta, ciò equivale a dire che G è quasiregolare in quanto, essendo X e Y costituiti da omologie, è chiaro che G induce un'azione regolare su tutte le altre orbite. Infine, X è abeliano se e solo se G lo è; per il Lemma 2.3, ciò accade se e solo se Z è normale. □

Ne segue che un gruppo quasiregolare di tipo almeno I.3 ha in effetti tipo I.4; pertanto, in questo caso, Π è di classe di Lenz-Barlotti almeno I.4. Si noti, tuttavia, che a questo punto non è affatto chiaro che valga il viceversa, ossia che ogni gruppo di tipo I.4 sia quasiregolare. A priori si potrebbe pensare che esista un terzo gruppo transitivo U (necessariamente non abeliano) di (o, xy)-omologie che non è contenuto nel gruppo $G = X \times Y$ generato dagli altri due gruppi di omologie X e Y. Questo non è possibile, come vedremo nel prossimo paragrafo. Sfortunatamente, non siamo in grado di trovare una dimostrazione diretta semplice di questo fatto che non faccia uso di un risultato di Kantor e Pankin [20] sui neocorpi.

Concludiamo questo paragrafo illustrando gli esempi noti di piani che ammettono un gruppo di tipo almeno I.3. Gli unici piani finiti noti che sono simultaneamente (y, ox)- e (x, oy)-transitivi, con o, x, y vertici di un

triangolo, sono quelli definiti sopra un quasicorpo finito. Un quasicorpo proprio, essenzialmente, si può pensare come un corpo con una sola proprietà distributiva. Più precisamente, un *quasicorpo* finito è un insieme K su cui sono definite due operazioni, addizione $(+)$ e moltiplicazione $(\cdot)$, tali che

(N1) $(K, +)$ è un gruppo abeliano con elemento neutro 0.
(N2) $(K^*, \cdot)$, ove $K^* = K \backslash \{0\}$, è un gruppo.
(N3) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$, per ogni $a, b, c \in K$;
(N4) $a \cdot 0 = 0$, per ogni $a \in K$.

Osserviamo che i quasicorpi finiti sono stati completamente classificati da Zassenhaus [31]; si veda anche Dembowski [4, §5.2]. I gruppi di omologie assegnati X e Y sono isomorfi al gruppo moltiplicativo K^*. Si hanno ora due possibilità:

- Se K è proprio, ossia non è un campo, K^* è non-commutativo. In tal caso, Π ha classe di Lenz-Barlotti IVa.2 tranne quando K è il quasicorpo eccezionale di ordine 9 (allora Π ha classe IVa.3). In questo caso, il gruppo $G = X \times Y$ è di tipo I.3 e, pertanto, non è quasiregolare.

- Se K è un campo e quindi K^* è abeliano, allora Π è desarguesiano e pertanto è nella classe di Lenz-Barlotti VII.2. In questo caso, il gruppo $G = X \times Y$ è di tipo I.4 ed è quasiregolare.

Gli esempi precedenti sono già citati da Hughes in [16] usando la terminologia dei suoi piani parzialmente transitivi; Hughes non poteva, ovviamente, discutere ancora della connessione con la classificazione di Lenz-Barlotti, in quanto l'articolo di Barlotti è apparso un anno dopo. Questi esempi compaiono di nuovo in diversi articoli successivi, di solito senza un riferimento ad Hughes. Sembra che il suo articolo sia stato ignorato anche se spesso è citato in un modo generale molto vago. Ci teniamo a citarlo qui, in quanto anticipa molte delle idee della successiva classificazione di Dembowski-Piper.

Non si conoscono, comunque, esempi di piani proiettivi finiti nelle classi I.3 o I.4 di Lenz-Barlotti, e si congettura che tali piani non esistano. Parleremo in seguito del problema di esistenza. Osserviamo infine che Hughes [16] ha considerato anche piani con un gruppo parzialmente transitivo di tipo (3) (i.e. con la stessa struttura in orbite di un gruppo quasiregolare di tipo (g)) ma senza l'ipotesi che almeno due dei sottogruppi speciali coinvolti siano normali. Abbiamo deciso di non considerare questo caso, per non appesantire la trattazione con troppi dettagli tecnici, anche perché non sembrano noti esempi di gruppi siffatti.

3 Piani di classe almeno I.4 e neocorpi

In questo paragrafo, illustriamo l'approccio standard allo studio di piani appartenenti alla classe di Lenz-Barlotti almeno I.4, precisamente l'introduzione delle coordinate e l'uso dei neocorpi. Iniziamo con una breve descrizione della coordinatizzazione come viene data in Dembowski [4],si veda la Figura 2; tale descrizione segue essenzialmente Hall [11]. Osserviamo che questo metodo di coordinatizzazione non è l'unico usato (cfr. Hughes e Piper [17] e Pickert [25]).

Sia R un insieme avente la stessa cardinalità di una retta di Π, con due elementi distinti, che denotiamo con $0, 1$; fissato un triangolo oxy in Π, scegliamo arbitrariamente un punto $u \in \Pi$ che non sia su ox,oy o su xy.

Consideriamo il quadrangolo ordinato $ouxy$ e, detto ∞ un simbolo non in R, indichiamo con $[\infty]$ la retta xy e con (∞) il punto y. A ciascun punto non su $[\infty]$ della retta ou associamo un elemento di R in modo tale che al punto o corrisponda $0 \in R$ e al punto u corrisponda $1 \in R$. Se ad un punto p su ou corrisponde $a \in R$ diremo che p ha coordinate (a, a). Ad ogni punto q su oy tale che $qx \cap ou = (b, b)$ si associano le coordinate $(0, b)$, mentre se r è un punto di ox tale che $ry \cap ou = (a, a)$ le coordinate di r saranno $(a, 0)$. Ad ogni punto p non appartenente ad alcun lato del triangolo oxy e tale che $px \cap oy = (0, b)$ e $py \cap ox = (a, 0)$ si assegnano le coordinate (a, b). In tal modo, si sono assegnate delle coordinate a tutti i punti del piano non appartenenti alla retta $[\infty] = xy$. Al punto z sulla retta $[\infty]$, $z \neq y$, che si trova sulla retta congiungente o al punto di coordinate $(1, m)$ associamo la coordinata (m). Le rette del piano sono coordinatizzate come segue. Per ogni $m \in R$, $[m, k]$ è la retta congiungente (m) a $(0, k)$; la retta congiungente $y = (\infty)$ ad $(a, 0)$ è $[a]$; infine $xy = [\infty]$. Questo metodo di coordinatizzare il piano ci assicura che i punti del tipo (a, a), quando a varia in R, sono allineati.

Introduciamo un'operazione ternaria T su R mediante la

$$(3.1)\quad T(a, m, k) = b \qquad \text{se e solo se} \qquad (a, b) \in [m, k].$$

Ogni insieme R con una tale operazione ternaria si chiama *anello planare ternario di Hall*. L'addizione e la moltiplicazione in R sono definite tramite le

$$(3.2)\quad a + b = T(a, 1, b) \qquad \text{e} \qquad ab = T(a, b, 0).$$

Rispetto all'addizione R è un cappio (si veda V.4 in [17]) con elemento neutro 0, mentre l'insieme $R^* = R \setminus \{0\}$ è, rispetto alla moltiplicazione, un cappio con elemento neutro 1. Un anello planare ternario si dice *lineare* se $T(a, m, k) = am + k$ per ogni $a, m, k \in R$.

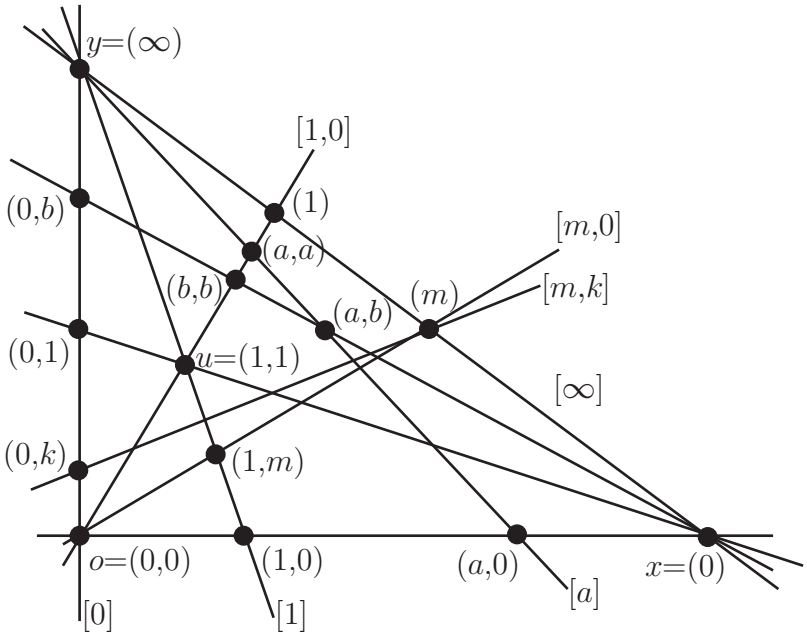

Figura 2: Coordinatizzazione di Π

Supponiamo ora che Π sia (y, ox)-, (x, oy)- e (o, xy)-transitivo, ossia che sia di classe di Lenz-Barlotti almeno I.4. La coordinatizzazione suindicata dà luogo ad un anello planare ternario (R, T) tale che

- (R, T) è lineare;
- $(R^*, \cdot)$, ove $R^* = R \setminus \{0\}$, è un gruppo;
- Valgono in $(R, +, \cdot)$ entrambe le proprietà distributive: $(a + b)c = ac + bc$, $c(a + b) = ca + cb$ per ogni $a, b, c \in R$.

Seguendo Kantor [19], chiameremo *neocorpo* ogni anello planare ternario siffatto. Precedentemente, Hughes [14, 15] ha usato per tale struttura la terminologia *Neo-anello di divisione planare* (in inglese: PDNR, abbreviazione per Planar Division Neo-Ring). Il cambiamento di terminologia è motivato dal fatto che i neocorpi finiti hanno le seguenti ulteriori proprietà.

Teorema 3.1 *Se (R, T) è un neocorpo finito, allora*

1. *$(R, +)$ è commutativo;*
2. *$(a + b) + (-b) = a$ per ogni $a, b \in R$;*

3. $(R^*, \cdot)$ *è commutativo.*

Le prime due proprietà nel Teorema 3.1 sono state dimostrate da Hughes estendendo risultati precedenti dovuti a Paige [22], mentre la terza è un teorema di Kantor e Pankin [20], analogo al teorema di Wedderburn. Si vede così che ogni neocorpo finito soddisfa tutti gli assiomi di un campo, ad eccezione dell'associatività dell'addizione, che è rimpiazzata dalla proprietà 2 del Teorema 3.1, che chiamiamo *proprietà associativa dell'opposto* (in inglese, semplicemente: "inverse property").

Viceversa, ogni neocorpo finito coordinatizza un piano proiettivo che è o di tipo I.4 (quando il neocorpo è *proprio*, ossia non è un campo), oppure è desarguesiano. Per ogni neocorpo R, la struttura di incidenza $\Sigma = \Sigma(R)$ definita come segue è un piano affine:

- I punti di Σ sono le coppie ordinate (a, b) con $a, b \in R$.
- Le rette sono gli insiemi di punti

$$(3.3)\ [m,k] \ = \ \{(r, rm+k) : r \in R\} \quad \text{e} \quad [a] \ = \ \{(a,b) : b \in R\}.$$

Nel piano proiettivo Π ottenuto per ampliamento del piano affine Σ, siano $o = (0,0)$, $u = (1,1)$, $x = (0)$ e y il punto improprio della retta $[0]$. Il quadrangolo ordinato $ouxy$ dà luogo ad un anello planare ternario essenzialmente identico a quello di partenza R.

Siamo ora in grado di dimostrare il risultato annunciato nella discussione che segue la Proposizione 2.4.

Teorema 3.2 *Se* Π *è un piano proiettivo finito, le condizioni che seguono sono equivalenti:*

1. Π *è almeno nella classe di Lenz-Barlotti I.4.*
2. Π *ha un gruppo di collineazioni abeliano di tipo Lenz-Barlotti I.4.*
3. Π *ha un gruppo di collineazioni quasiregolare di tipo (g).*

Dimostrazione. Assumiamo che Π sia almeno nella classe di Lenz-Barlotti I.4, ossia che esista un triangolo oxy tale che Π è (y, ox)-, (x, oy)- ed (o, xy)-transitivo. Indicato con X il gruppo di tutte le omologie di centro x e asse oy (in breve: (x, oy)-omologie) e con Y il gruppo di tutte le (y, ox)-omologie, per il Lemma 2.1, il gruppo $G = X \times Y$ è un gruppo di collineazioni di tipo Lenz-Barlotti almeno I.3. Coordinatizziamo Π tramite un neocorpo R, come indicato sopra. Dalla descrizione della parte affine Σ, si vede facilmente che l'applicazione $(a, b) \mapsto (ac, b)$ è, per ogni $c \in R$, una (x, oy)-omologia. Quindi, il gruppo X di tutte queste omologie è isomorfo a R^* e, come tale, è

abeliano, per il Teorema 3.1. Pertanto, G è abeliano e la Proposizione 2.4 mostra che G ha tipo di Lenz-Barlotti I.4. Sempre per la Proposizione 2.4, ciò implica che Π ha un gruppo di collineazioni quasiregolare di tipo (g). Assumendo, infine, che G sia un gruppo siffatto, la regolarità delle azioni indotte sulle tre orbite sui punti corrispondenti ai lati del triangolo oxy implica, immediatamente, che lo stabilizzatore di ogni punto di una di queste orbite è costituito da omologie, e quindi Π è ovviamente almeno nella classe di Lenz-Barlotti I.4. □

4 Neo-insiemi di differenze

In questo paragrafo, illustriamo come un piano proiettivo finito, che sia almeno nella classe di Lenz-Barlotti I.3, possa rappresentarsi mediante un certo tipo di insieme di differenze relativo a sottogruppi disgiunti nel senso di Hiramine [12]; chiameremo un tale insieme "neo-insieme di differenze", in quanto il caso abeliano corrisponde a piani che sono almeno nella classe di Lenz-Barlotti I.4 e, pertanto, corrisponde a neocorpi. Osserviamo che Hughes [14, 15, 16], per primo, ha considerato quelli che noi chiamiamo neo-insiemi di differenze, usando la terminologia "insiemi di differenze parziali" per un piano parzialmente transitivo di tipo (3).

Come al solito, nello studio di ogni tipo di insieme di differenze è opportuno usare $\mathbb{Z}G$, l'anello di gruppo sugli interi. Richiamiamo le necessarie notazioni. Se $A = \sum a_g g \in \mathbb{Z}G$ e $t \in \mathbb{Z}$ scriviamo $A^{(t)} = \sum a_g g^t$ e $[A]_g = a_g$ (il coefficiente di g in A). Per abuso di notazioni, se $r \in \mathbb{Z}$ e $S \subseteq G$, indichiamo ancora con r e S, rispettivamente, l'elemento $r \cdot 1$ e il sottoinsieme $\sum_{g \in S} g$ dell'anello di gruppo. Sarà utile il semplice lemma seguente, che mostra come si calcolino gli ordini delle intersezioni usando $\mathbb{Z}G$.

Lemma 4.1 *Se A e B sono due sottoinsiemi del gruppo finito G, risulta* $|A \cap Bg| = [AB^{(-1)}]_g$. □

Usando le notazioni dell'anello di gruppo, un *neo-insieme di differenze* di ordine n si può definire come un sottoinsieme D, di un gruppo G di ordine $(n-1)^2$ avente tre sottogruppi a due a due disgiunti X, Y, e Z di ordine $n-1$, che soddisfa in $\mathbb{Z}G$ l'equazione

$$(4.1)\quad DD^{(-1)} = n + G - X - Y - Z.$$

Quindi ogni elemento γ, che non sia nell'unione N dei tre *sottogruppi proibiti* X, Y, e Z, si può rappresentare in modo unico come "differenza" $\gamma = \delta\varepsilon^{-1}$ di elementi $\delta, \varepsilon \in D$. Nel seguito, considereremo solo neo-insiemi di differenze *normali* nel senso che almeno due dei tre sottogruppi, siano X ed Y, sono

normali. In tal caso sussiste il Lemma 2.3. Iniziamo costruendo un neo-insieme di differenze normale da ogni piano proiettivo finito che sia almeno nella classe di Lenz-Barlotti I.3; per comodità del lettore accenneremo al ragionamento del tutto standard necessario.

Proposizione 4.2 *Se* Π *è un piano proiettivo finito di ordine* n *simultaneamente* (y, ox)- *e* (x, oy)*-transitivo, essendo* o*,* x*, e* y *un triangolo, e* G*,* X*,* Y*, e* Z *sono definiti come nel paragrafo 2, allora esiste in* G *un neo-insieme di differenze normale di ordine* n*, relativo ai sottogruppi proibiti* X*,* Y *e* Z*.*

Dimostrazione. Come nella dimostrazione del Lemma 2.1, possiamo identificare l'immagine, mediante la collineazione $(\xi, \psi) \in G = X \times Y$, del punto base u con l'elemento del gruppo (ξ, ψ). Scelta una retta ordinaria come "retta base", per l'identificazione fatta, si può considerare D come un $(n-2)$-sottoinsieme di G; le rette ordinarie assumono dunque la forma $D\gamma$ with $\gamma \in G$. Si verifica ora facilmente che il numero delle rette di questo tipo che uniscono due punti ordinari assegnati (ξ_1, ψ_1) e (ξ_2, ψ_2) è il numero delle rappresentazioni come differenze

$$(\xi_1, \psi_1)(\xi_2, \psi_2)^{-1} \;=\; (\delta_1, \delta_2)(\varepsilon_1, \varepsilon_2)^{-1}$$

con $(\delta_1, \delta_2), (\varepsilon_1, \varepsilon_2) \in D$. Essendo Π un piano proiettivo, tale numero risulta uguale a 0 quando (ξ_1, ψ_1) e (ξ_2, ψ_2) sono su una retta passante per uno dei vertici o, x, e y del triangolo, mentre è sempre uguale ad uno in tutti gli altri casi. Si controlla facilmente – tramite l'identificazione dei punti con gli elementi di G illustrata sopra – che le rette per i vertici sono esattamente le classi laterali destre dei tre sottogruppi proibiti. Quindi due punti la cui congiungente passa per uno dei vertici o, x e y hanno una differenza in uno dei tre sottogruppi X, Y e Z. Pertanto, D risulta effettivamente un neo-insieme di differenze e, per il Lemma 2.2, D è normale. □

Stabiliamo ora il viceversa della Proposizione 4.2. Sia D un neo-insieme di differenze normale di ordine n, come sopra definito. Per semplificare, faremo alcune ipotesi. In primo luogo, dato che $X \cong Y$, possiamo usare l'isomorfismo f costruito nella dimostrazione del Lemma 2.3 per sostituire Y con X. In tal modo, $G = X \times X$, i tre sottogruppi proibiti assumono la forma

$$U_1 = X \times \{1\}, \;\; U_2 = \{1\} \times X, \;\; U_3 = \{(\xi, \xi) : \xi \in X\},$$

e l'equazione (4.1) diventa

$$(4.2) \;\; DD^{(-1)} \;=\; n + G - U_1 - U_2 - U_3.$$

A questo punto osserviamo che vale la seguente restrizione su X, dimostrata da Paige [22] nel contesto dei neo-corpi.

Lemma 4.3 *Il gruppo X contiene al più un'involuzione.*

Dimostrazione. Se, per assurdo, esistesse un'involuzione γ di G tale che $\gamma \notin N = U_1 \cup U_2 \cup U_3$ si avrebbe non solo la rappresentazione $\gamma = \delta\varepsilon^{-1}$ with $\delta, \varepsilon \in D$, ma anche la seconda rappresentazione $\gamma = \gamma^{-1} = \varepsilon\delta^{-1}$, il che è una contraddizione. Ne segue che tutte le involuzioni di G sono contenute in N. Siano ora κ e λ involuzioni di X. L'applicazione (κ, λ) è un'involuzione di G e, come tale, deve stare in N; ciò è possibile se e solo se $\kappa = \lambda$. □

Continuando con le nostre ipotesi semplificative, osserviamo che, per ogni $i = 1, 2, 3$, esiste esattamente una classe laterale di U_i che non interseca D, mentre ogni altra classe laterale ha una sola intersezione con D, in quanto nessun elemento di N si può rappresentare come "differenza" di elementi di D. Sostituendo eventualmente a D un suo traslato opportunamente scelto, possiamo supporre, senza perdere di generalità, che sia U_1 che U_2 non incontrino D. Scriviamo l'unica classe laterale di U_3 che non interseca D nella forma $U_3(1, \theta)$ con $\theta \in X$; in seguito saremo in grado di determinare il valore di θ nel caso che G sia abeliano. Con tali ipotesi si può scrivere

$$(4.3)\quad D \;=\; \sum_{\xi \in X \setminus \{1\}} (\xi, g(\xi)),$$

ove $g\colon X \setminus \{1\} \to X \setminus \{1\}$ è biunivoca. Si noti che l'elemento $(\xi, g(\xi))$ è nella classe $U_3(1, \xi^{-1}g(\xi))$, pertanto

$$(4.4)\quad \Delta \;:=\; \{\xi^{-1}g(\xi) : \xi \in X\} \;=\; X \setminus \{\theta\}.$$

Possiamo ora dare una descrizione esplicita del piano proiettivo $\Pi = \Pi(D)$ in termini di D (cfr. Figura 3). A tale scopo, scegliamo un elemento $0 \notin X$ e immergiamo X nel semigruppo $\overline{X} = X \cup \{0\}$, ove $0\xi = \xi 0 = 0$ per ogni $\xi \in X$. Sia, inoltre, ∞ un simbolo non appartenente a $\overline{X}$. I punti di Π sono

- gli n^2 elementi $(\xi, \psi) \in \overline{G} = \overline{X} \times \overline{X}$;
- n punti (ξ), con $\xi \in \overline{X}$, e un punto (∞).

Le rette di Π sono

- $(n-1)^2$ rette

  $$[\xi, \psi] \;=\; D(\xi, \psi) \cup \{(\xi, 0), (0, \psi), (\theta\psi\xi^{-1})\},$$

  ove $\xi, \psi \in X$;
- n rette $[U_1\psi] = \{(\xi, \psi) : \xi \in \overline{X}\} \cup \{(0)\}$, ove $\psi \in \overline{X}$;

- n rette $[U_2\xi] = \{(\xi, \psi) : \psi \in \overline{X}\} \cup \{(\infty)\}$, ove $\xi \in \overline{X}$;
- $n-1$ rette $[U_3\psi] = \{(\xi, \xi\psi) : \xi \in \overline{X}\} \cup \{(\psi)\}$, ove $\psi \in X$;
- una retta $[\infty] = \{(\xi) : \xi \in \overline{X}\} \cup (\infty)$.

La costruzione precedente è ispirata da un lato al lavoro di Hughes, cf. [16, pp. 660–662], anche se la situazione più particolare considerata qui rende possibili alcune semplificazioni, dall'altro alla rappresentazione, illustrata nel paragrafo precedente, dei piani di tipo I.4 mediante neocorpi; è anche analoga – ma in un certo senso più contorta – alla presentazione dei piani con un gruppo quasiregolare di tipo (f) data dai presenti autori in collaborazione con de Resmini in [6].

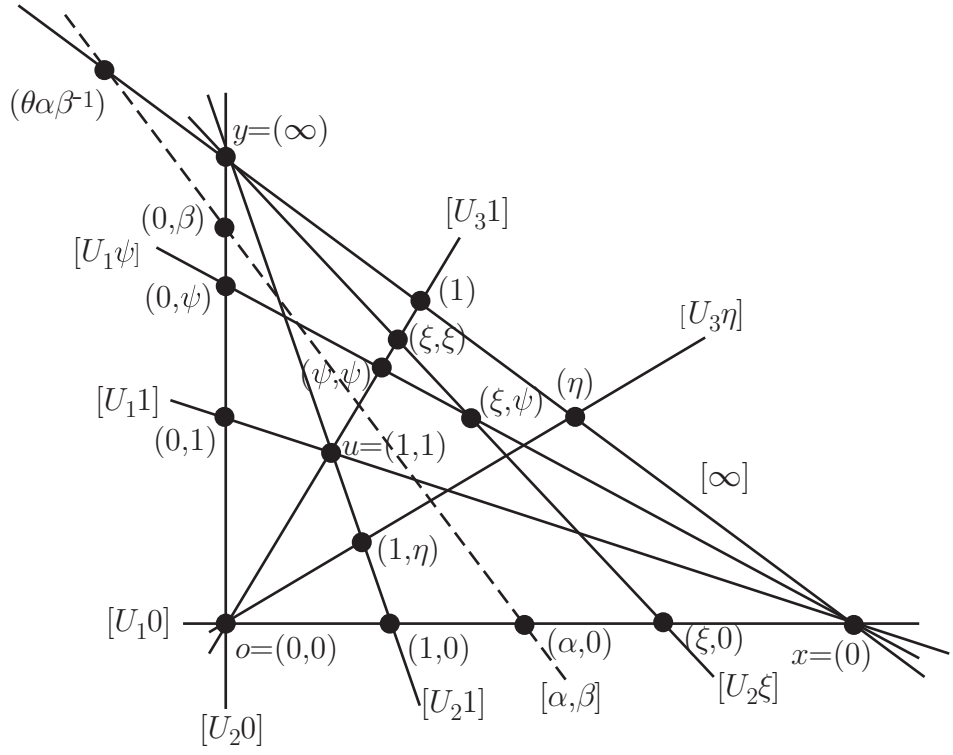

Figura 3: Il piano $\Pi(D)$

Proposizione 4.4 *La struttura di incidenza $\Pi = \Pi(D)$ sopra definita è un piano proiettivo di ordine n su cui G agisce come gruppo di collineazioni di tipo Lenz-Barlotti almeno I.3.*

Dimostrazione. Notiamo, in primo luogo, che G agisce su Π per traslazioni destre. Poniamo $o = (0, 0)$, $x = (0)$ e $y = (\infty)$ e chiamiamo *ordinari* i punti

$(\xi, \psi) \in X \times X$. La struttura in orbite di G sui punti è come quella descritta nel paragrafo 2. Osserviamo, poi, che Π ha $n^2 + n + 1$ punti e $n^2 + n + 1$ rette ciascuna contenente $n + 1$ punti. Resta da verificare che ogni coppia di punti p, q di Π è congiunta da almeno una retta. In diversi casi questo è banale, precisamente

- se uno dei punti è $o = (0, 0)$, $x = (0)$ o $y = (\infty)$;
- se entrambi i punti hanno una delle forme $(\xi, 0)$, $(0, \psi)$ e (ξ).

Possiamo, quindi, assumere che p sia un punto ordinario. Per la transitività di G sui punti ordinari, si può anche assumere $p = (1, 1)$. In tali ipotesi, p è unito ad ogni punto della forma $(\xi, 1)$ dalla retta $[U_1 1]$, ad ogni punto della forma $(1, \psi)$ dalla retta $[U_2 1]$, e ad ogni punto della forma (ξ, ξ) dalla retta $[U_3 1]$. Se $q = (\xi, \psi)$ è un punto ordinario non appartenente ad alcuna di queste tre rette, la "differenza" $(\xi, \psi)(1, 1)^{-1}$ individuata da q e p è in $G \setminus N$. Essendo D un neo-insieme di differenze, l'argomentazione data nella dimostrazione della Proposizione 4.2 mostra che, p e q sono su un'unica retta *ordinaria*, i.e. una retta del tipo $[\alpha, \beta]$. Resta da esaminare il caso in cui q sia su uno dei lati del triangolo oxy. Usiamo ora la forma di D data nell'equazione (4.3) e osserviamo che la retta $[\xi^{-1}, g(\xi)^{-1}]$ contiene sia $p = (1, 1)$ che i punti $(\xi^{-1}, 0)$, $(0, g(\xi)^{-1})$ e $(\theta g(\xi)^{-1}\xi)$. Poiché $g \colon X \setminus \{1\} \to X \setminus \{1\}$ è biunivoca, si vede che p è unito ad ogni punto di ox diverso da $(1, 0)$ e ad ogni punto di oy diverso da $(0, 1)$ da una di queste rette. Inoltre, p è unito ad ogni punto di xy diverso da (1), in quanto l'insieme degli elementi $\xi^{-1} g(\xi) \theta^{-1}$ è $X \setminus \{1\}$, per l'equazione (4.4). Ma i tre punti eccezionali si trovano sulle rette $[U_i 1]$ per p. È poi banale verificare che gli elementi in U_1 e U_2 agiscono come omologie su Π che pertanto è (y, ox)- e (x, oy)-transitivo. □

La struttura di incidenza $\mathcal{D}$ formata dai punti ordinari e dalle rette ordinarie è ciò che possiamo chiamare un *semipiano triangolare* che ammette $G = X \times X$ come gruppo di Singer. Come si è visto, Π può essere univocamente ricostruito da $\mathcal{D}$. Più in generale, è noto che una geometria che si ottiene da un piano proiettivo rimuovendo un triangolo è necessariamente una tale struttura a patto che l'ordine sia almeno 25 (cfr. Ralston [26]).

Esempio 4.5 Sia K un quasicorpo finito di ordine n. Allora l'insieme

$$D \;=\; \{(\xi, \psi) \in K^* \times K^* : \xi + \psi = 1\}$$

è un neo-insieme di differenze normale di ordine n in $G = K^* \times K^*$, come è semplice verificare direttamente usando gli assiomi di quasicorpo. Questo esempio è dovuto a Hughes [16, pp.656–657] ed è stato riscoperto da Hiramine [12, Example 4.2.(iv)]. Si noti che D è abeliano se e solo se K è un campo

finito. Dunque il piano proiettivo associato a D nella proposizione 4.4 risulta essere o desarguesiano o un piano sopra un quasicorpo. In questo modo si ottengono i piani noti che ammettono un gruppo di tipo di Lenz-Barlotti almeno I.3 discussi alla fine del paragrafo 2.

Le due proposizioni 4.2 e 4.4 dimostrano il primo tra i risultati principali di questo paragrafo:

Teorema 4.6 *Un piano proiettivo finito* Π *ammette un gruppo di collineazioni* G *di tipo di Lenz-Barlotti almeno I.3 se e solo se può essere rappresentato da un neo-insieme di differenze normale.*

Usando questo teorema assieme al teorema 3.2, otteniamo anche il secondo tra i risultati principali:

Teorema 4.7 *Sia* Π *un piano proiettivo finito. Le seguenti affermazioni sono equivalenti:*

1. Π *è di classe di Lenz-Barlotti almeno I.4.*
2. Π *ammette un gruppo di collineazioni abeliano di tipo di Lenz-Barlotti almeno I.4.*
3. Π *ammette un gruppo di collineazioni quasiregolare di tipo (g).*
4. Π *può essere rappresentato da un neo-insieme di differenze abeliano.*

Usando l'approccio del paragrafo 3 otteniamo anche la seguente interessante proposizione come conseguenza. Per la dimostrazione siamo comunque costretti ad usare i neocorpi. Sarebbe auspicabile riuscire a darne una dimostrazione più diretta che non faccia uso del neocorpo associato.

Proposizione 4.8 *Se* D *un neo-insieme di differenze abeliano di ordine* n *come nell'equazione (4.2), si può supporre che* D *sia* simmetrico, *nel senso che* $(\xi, \psi) \in D$ *implica* $(\psi, \xi) \in D$*; in altri termini: se* D *è abeliano, si può supporre che l'applicazione* g *nell'equazione (4.3) sia un'involuzione. Inoltre,* g *soddisfa l'ulteriore restrizione*

$$(4.5)\quad g(\xi^{-1}) \;=\; \varepsilon\xi^{-1}g(\xi) \qquad \textit{per ogni} \quad \xi \in X,$$

dove ε *è l'unica involuzione in* X *se* n *è dispari, mentre* $\varepsilon = 1$ *negli altri casi (cfr. Lemma 4.3).*

Dimostrazione. Dalla proposizione 4.4 segue che D dà luogo ad un piano proiettivo Π di classe di Lenz-Barlotti almeno I.4 su cui il gruppo G agisce per traslazioni destre. Se coordinatizziamo Π come nella dimostrazione della proposizione 4.2 e usiamo $[1,1]$ come retta base, possiamo ritrovare D. D'altro canto possiamo anche coordinatizzare Π usando un neocorpo R, come discusso nel paragrafo 3. Ora i gruppi di omologie X e Y possono essere identificati con i sottogruppi $R^* \times \{1\}$ e $\{1\} \times R^*$ di $R^* \times R^* \cong G \cong X \times X$. Dunque, le coordinate dei punti ordinari coincidono sia nel caso del neocorpo che in quello del neo-insieme di differenze, se identifichiamo X con R^*. Consideriamo ora la retta affine

$$L \;=\; [-1,1] \;=\; \{(r,-r+1) : r \in R\} \;=\; \{(\xi,\psi) \in R \times R : \xi + \psi = 1\};$$

cfr. (3.3) e l'esempio 4.5. Se scegliamo L come retta base nel determinare D (il che vuol dire sostituire D, se necessario, con un suo traslato opportuno), la commutatività dell'addizione in R implica immediatamente la simmetria di D. Infine, si noti che L contiene i punti $(1,0)$ e $(0,1)$, dunque sia $R^* \times \{1\}$ che $\{1\} \times R^*$ non incontrano D. Dunque D è della forma data in (4.3), e questo prova la seconda affermazione.

Per provare l'ultima affermazione osserviamo dapprima che $1+(-1)=0$ in R implica $\alpha + (-1)\alpha = 0$ e dunque $-\alpha = (-1)\alpha$ per ogni $\alpha \in R$, come ci aspettavamo; in particolare, $(-1)^2 = 1$. Questo, sempre identificando X con R^*, mostra che -1 è proprio l'elemento ε definito nell'enunciato. Da quanto già dimostrato si ha che g può essere determinato dall'equazione $\xi + g(\xi) = 1$ in R. Moltiplicando questa per ξ^{-1} otteniamo $1 + \xi^{-1} g(\xi) \;=\; \xi^{-1}$, che è equivalente a

$$\xi^{-1} + \varepsilon \xi^{-1} g(\xi) \;=\; 1,$$

usando $\varepsilon = -1$ e la proprietà 2 del Teorema 3.1; questo prova (4.5). □

Più avanti avremo bisogno del seguente risultato:

Corollario 4.9 *Nelle ipotesi della proposizione 4.8, un elemento $\alpha \in X$ ha ordine* 3 *se e solo se valgono le seguenti condizioni:*

(4.6) $g(\varepsilon\alpha) \;=\; \varepsilon\alpha^2 \quad e \quad g(\varepsilon\alpha^2) \;=\; \varepsilon\alpha.$

Dimostrazione. Si noti in primo luogo che le due equazioni in (4.6) sono equivalenti per la proposizione 4.8. Assumendo che valgano queste equazioni, calcoliamo

$$\alpha^2 g(\varepsilon\alpha^2) \;=\; \alpha^2 \varepsilon\alpha \;=\; \alpha\varepsilon\alpha^2 \;=\; \alpha g(\varepsilon\alpha) \;=\; \alpha^2 g(\varepsilon\alpha^{-1}),$$

dove l'ultima equazione segue dall'applicare l'equazione (4.5) all'elemento $\xi = \varepsilon\alpha$. Essendo g biunivoca, concludiamo immediatamente che $\alpha^2 = \alpha^{-1}$ e dunque α ha ordine 3.

Viceversa, sia α un elemento di ordine 3. Applicando l'equazione (4.5) all'elemento $\xi = \varepsilon\alpha$, otteniamo l'identità

$$(4.7)\quad g(\varepsilon\alpha^2) \;=\; \alpha^2 g(\varepsilon\alpha).$$

Osserviamo ora che D contiene i quattro elementi $(\varepsilon\alpha, g(\varepsilon\alpha))$, $(\varepsilon\alpha^2, g(\varepsilon\alpha^2))$, $(g(\varepsilon\alpha), \varepsilon\alpha)$ e $(g(\varepsilon\alpha^2), \varepsilon\alpha^2)$. Ma questi portano ad una "differenza" ripetuta:

$$\begin{aligned}(\varepsilon\alpha, g(\varepsilon\alpha)) \cdot (g(\varepsilon\alpha^2), \varepsilon\alpha^2)^{-1} &= (\varepsilon\alpha g(\varepsilon\alpha^2)^{-1}, g(\varepsilon\alpha)\varepsilon\alpha)\\ &= (\varepsilon\alpha^2 g(\varepsilon\alpha)^{-1}, g(\varepsilon\alpha^2)\varepsilon\alpha^2)\\ &= (\varepsilon\alpha^2, g(\varepsilon\alpha^2)) \cdot (g(\varepsilon\alpha), \varepsilon\alpha),\end{aligned}$$

immediata usando (4.7). Poiché $\varepsilon\alpha \neq \varepsilon\alpha^2$, abbiamo

$$(\varepsilon\alpha g(\varepsilon\alpha^2)^{-1}, g(\varepsilon\alpha)\varepsilon\alpha) \;=\; (1,1)$$

che è proprio la condizione (4.6). □

5 Ovali associate a neo-insiemi di differenze abeliani

In questo paragrafo mostreremo che un piano finito associato a un neo-insieme di differenze abeliano ammette un sistema di ovali che forma una configurazione interessante. Questo risultato somiglia a ciò che abbiamo dimostrato sulle ovali nei piani che ammettono un gruppo quasiregolare di tipo (f) in [6], dove si citava la possibilità di un simile approccio ma, considerando le difficoltà tecniche connesse, non lo si considerava sufficientemente interessante da essere portato fino in fondo. Come vedremo, in realtà emergono alcune conseguenze interessanti; inoltre, a questo punto abbiamo tutti gli strumenti che ci servono.

Proposizione 5.1 *Sia Π un piano proiettivo di ordine n rappresentato da un neo-insieme di differenze D in un gruppo abeliano G, come nel paragrafo 4, e assumiamo che D abbia la forma (4.3). Allora, gli $(n-2)$-insiemi $A_\gamma = D^{(-1)}\gamma$ con $\gamma = (\alpha, \beta) \in G$ sono archi in Π, e la retta $[\xi^{-2}\alpha, g(\xi)^{-2}\beta]$ è la tangente ad A_γ nel suo punto $(\xi, g(\xi))^{-1}\gamma$. Inoltre l'$(n-2)$-arco A_γ può essere esteso a un'ovale di Π, e precisamente $O_\gamma = A_\gamma \cup \{(0,0), (0), (\infty)\}$. Infine, se n è pari, il nucleo di O_γ è il punto ordinario γ.*

Dimostrazione. La dimostrazione usa ragionamenti standard, come segue. Prima si verifica che ogni insieme $D\kappa$ interseca $A_\gamma = D^{(-1)}\gamma$ al più due volte. Assumiamo che α sia un punto di intersezione,

$$\alpha = \delta\kappa = \varepsilon^{-1}\gamma, \quad \text{cosicché} \quad \delta\varepsilon = \gamma\kappa^{-1},$$

con $\delta, \varepsilon \in D$. Se β è un secondo punto di intersezione, analogamente

$$\beta = \mu\kappa = \nu^{-1}\gamma, \quad \text{cosicché} \quad \mu\nu = \gamma\kappa^{-1},$$

con $\mu, \nu \in D$. Da queste due equazioni, $\delta\mu^{-1} = \nu\varepsilon^{-1}$ e perciò $\delta = \nu$ e $\mu = \varepsilon$, poiché D è un neo-insieme di differenze. Quindi β è univocamente determinato da α, il che mostra che $D\kappa$ interseca A_γ al più due volte. Inoltre, nessuna classe laterale di uno dei tre sottogruppi proibiti U_i interseca un traslato di D in più di un punto e così A_γ è un arco in Π. Visto che possiamo sempre riscrivere $\delta\kappa = \varepsilon^{-1}\gamma$ come $\varepsilon\kappa = \delta^{-1}\gamma$, è ovvio che il traslato $D\kappa$ interseca A_γ in due punti (ordinari) a meno che $\delta = \varepsilon$. Quindi la retta $[\kappa]$ associata a $D\kappa$ è una tangente a A_γ nel punto $\delta^{-1}\gamma$ se e solo se $\delta = \varepsilon$, cosicché $\kappa = \delta^{-2}\gamma$. Questo dimostra la prima affermazione. Ora, una retta di Π per uno dei punti $o = (0,0)$, $x = (0)$ e $y = (\infty)$ interseca A_γ al più una volta, il che mostra che O_γ è un'ovale. Infine, assumiamo che n sia pari, di modo che tutte le tangenti di O_γ passano per uno stesso punto (il *nucleo* dell'ovale). Poniamo dapprima $\gamma = (1,1)$. In base alle nostre ipotesi nel paragrafo 4, le rette $[U_1 1]$ e $[U_2 1]$ non incontrano $D^{(-1)}$, cioè sono tangenti a $O_{(1,1)}$. Dato che queste due rette si incontrano nel punto ordinario $(1,1)$, questo punto deve essere il nucleo di $O_{(1,1)}$. In generale ne segue che γ è il nucleo di O_γ. □

Osserviamo due interessanti conseguenze della Proposizione 5.1. La prima di esse è stata dimostrata da Kantor [19] in modo diverso, e la seconda è la determinazione dell'elemento eccezionale θ del gruppo, definito nel paragrafo 4.

Corollario 5.2 *Se $n \neq 2$ è pari, n è necessariamente un multiplo di 4.*

Dimostrazione. Si osservi che D è disgiunto da ogni traslato della forma $D\gamma$ con $1 \neq \gamma \in N$. Per un γ siffatto, le iperovali che completano $O_{(1,1)}$ e O_γ si intersecano esattamente nei tre punti speciali $(0,0)$, (0) e (∞). Ma in un piano di ordine $n \equiv 2 \pmod 4$, due iperovali qualsiansi si devono intersecare in un numero pari di punti: si veda per esempio [18, Lemma 3.3]. □

Proposizione 5.3 *Sia D un neo-insieme di differenze di ordine n in un gruppo abeliano $G = X \times X$, come in (4.3), e assumiamo che D non intersechi la classe laterale $U_3(1,\theta)$, cosicché θ soddisfa l'equazione (4.4). Allora $\theta = 1$ se n è pari; altrimenti, θ è l'unica involuzione in X.*

Dimostrazione. Consideriamo l'ovale $O = O_{(1,1)}$. Se n è pari, il nucleo di O è il punto $(1,1)$, per la proposizione 5.1. Ovviamente, la retta $[U_3\theta]$ è l'unica tangente a O nel punto $(0,0)$; pertanto, la classe laterale $U_3\theta$ deve contenere $(1,1)$, e quindi $\theta = 1$. Supponiamo ora che n sia dispari. Notiamo in primo luogo che in questo caso $\theta \neq 1$, poiché il punto $(1,1)$ si trova sulle due tangenti $[U_1 1]$ e $[U_2 1]$ e non può trovarsi su un'ulteriore tangente. Ne

segue che D incontra U_3, e quindi O contiene un (unico) punto della forma (ξ^{-1}, ξ^{-1}), ossia g fissa un unico elemento $\xi_0 \in X$. Per la proposizione 5.1, quando ξ varia in $X \setminus \{1\}$, la retta $L_\xi = [\xi^{-2}, g(\xi)^{-2}]$ è l'unica tangente a O nel punto $(\xi, g(\xi))$. Per definizione, L_ξ interseca $[\infty] = xy$ nel punto $(\theta g(\xi)^{-2}\xi^2)$. In particolare, la tangente L_{ξ_0} interseca ∞ in (θ). Ma la tangente $[U_3\theta]$ contiene anche (θ), e quindi (θ) non può trovarsi su ulteriori tangenti. Assumiamo ora che θ non sia l'unica involuzione $\tau \in X$, cosicché $\tau = \xi^{-1}g(\xi)$ per qualche $\xi \in X$. Allora, la tangente corrispondente L_ξ interseca $[\infty]$ in $(\theta g(\xi)^{-2}\xi^2) = (\theta\tau^{-2}) = (\theta)$ e abbiamo trovato una terza tangente passante per (θ), il che dà una contraddizione. □

Citiamo anche il seguente risultato costruttivo che è conseguenza immediata della proposizione 5.1.

Proposizione 5.4 *Sia* Π *un piano proiettivo di ordine n rappresentato da un neo-insieme di differenze D in un gruppo abeliano G, come nel paragrafo 4; in particolare, possiamo prendere* $\Pi = PG(2, n)$. *Allora* Π *contiene una famiglia* $\mathcal{O}$ *di* $(n-1)^2$ *ovali, ognuna delle quali contiene il triangolo speciale oxy, che hanno, a due a due, al più un ulteriore punto di intersezione.* □

La dimostrazione della proposizione 5.3 suggerisce un'ulteriore applicazione geometrica interessante. Ricordiamo che un *triangolo proiettivo di lato k* in un piano di ordine n è un insieme B di $3(k-1)$ punti con le seguenti proprietà:

(a). B contiene un triangolo speciale oxy.

(b). Su ogni lato di oxy ci sono esattamente k punti di B.

(c). Se i punti $q \in ox$ e $r \in oy$ appartengono a B, allora anche $qr \cap xy$ appartiene a B.

Mostreremo ora che i piani con un gruppo di tipo almeno I.4 contengono triangoli proiettivi che formano blocking set piccoli (cfr. Hirschfeld [13, Chapter 13]).

Proposizione 5.5 *Sia* Π *un piano proiettivo di ordine dispari n rappresentato da un neo-insieme di differenze D in un gruppo abeliano G, come nel paragrafo 4. Denotiamo con O l'ovale* $D^{(-1)} \cup \{o, x, y\}$, *dove* $o = (0, 0)$, $x = (0)$ *e* $y = (\infty)$ *(si veda la proposizione 5.1). Definiamo B come l'insieme di tutti i punti che si possono ottenere come intersezione di qualche lato di oxy con qualche tangente ad O. Allora B è un triangolo proiettivo di lato* $\frac{1}{2}(n+3)$*; inoltre, B è un blocking set minimale per* Π.

Dimostrazione. Useremo la proposizione 5.3 e quanto osservato nella sua dimostrazione. La retta L_ξ incontra l'asse x, ox, in $(\xi^{-2}, 0)$, l'asse y, oy, in $(0, g(\xi)^{-2})$ e la retta all'infinito xy in $(\theta g(\xi)^{-2}\xi^2)$. Così

$$B \;=\; \{o, x, y\} \cup \{(\xi, 0) : \xi \in X^\square\} \cup \{(0, \psi) : \psi \in X^\square\} \cup \{(\theta\eta) : \eta \in X^\square\},$$

dove $X^\square$ indica l'insieme dei quadrati in X. Poiché X contiene un'unica involuzione, in virtù del lemma 4.3, $X^\square$ ha indice 2 in X, il che mostra che la condizione (b) che precede è soddisfatta. Consideriamo poi un punto $q = (\xi, 0) \in ox$ e un punto $r = (0, \psi) \in oy$. La qr è la retta $[\xi, \psi]$ e pertanto $z = qr \cap xy = (\theta\psi\xi^{-1})$. È ora immediato che $q, r \in B$ implica $z \in B$, il che dimostra che B è effettivamente un triangolo proiettivo. D'altro canto, se la retta $L = [\xi, \psi]$ non interseca né ox né oy in un punto di B, allora sia ξ che ψ devono essere non-quadrati. Dato che $X^\square$ ha indice 2 in X, vediamo che $\theta\psi\xi^{-1}$ è a sua volta un non-quadrato. Quindi L interseca xy in un punto di B, cosicché B è effettivamente un blocking set che è ovviamente minimale. □

Nel caso speciale dei piani desarguesiani, la proposizione 5.5 è, naturalmente, ben nota, anche se la nostra dimostrazione e la descrizione geometrica che diamo sono nuove anche in questo caso. Più precisamente, otteniamo la seguente costruzione sintetica per triangoli proiettivi:

Corollario 5.6 *Sia $\Pi = PG(2, q)$, con q dispari, sia C una conica in Π, e sia oxy un triangolo contenuto in C. Definiamo B come l'insieme di tutti i punti che si ottengono come intersezione di qualche lato di oxy con qualche tangente a C. In tali ipotesi B è un triangolo proiettivo di lato $\frac{1}{2}(q + 3)$; inoltre, B è un blocking set minimale per Π.* □

6 Risultati di nonesistenza

In questo paragrafo raccogliamo alcuni risultati di nonesistenza per neo-insiemi di differenze abeliani; le dimostazioni qui presentate differiscono da quelle esistenti nella letteratura in quanto non utilizzano i neocorpi associati. Poiché questi metodi non si applicano al caso non abeliano, per risultati di nonesistenza relativi a piani con un gruppo di tipo di Lenz-Barlotti I.3, rinviamo il lettore alla letteratura (cfr. ad esempio Kantor [19] e Yaqub [30]).

Iniziamo con la seguente restrizione strutturale dovuta a Paige [22], Hughes [15] e Kantor [19].

Teorema 6.1 *Se D è un neo-insieme di differenze abeliano in $G = X \times X$, i 2- e 3-sottogruppi di Sylow di X sono ciclici.*

Dimostrazione. Il 2-sottogruppo di Sylow di X è ciclico per il Lemma 4.3. Supponiamo ora che $\alpha, \beta \in X$ siano due elementi di ordine 3. Dal Corollario 4.9 segue

$$g(\varepsilon\alpha) = \varepsilon\alpha^2, \;\; g(\varepsilon\alpha^2) = \varepsilon\alpha, \;\; g(\varepsilon\beta) = \varepsilon\beta^2, \;\; g(\varepsilon\beta^2) = \varepsilon\beta.$$

Usando questo, abbiamo che D contiene i quattro elementi $(\varepsilon\alpha, \varepsilon\alpha^2)$, $(\varepsilon\alpha^2, \varepsilon\alpha)$, $(\varepsilon\beta, \varepsilon\beta^2)$ e $(\varepsilon\beta^2, \varepsilon\beta)$. Ma ciò porta ad una "differenza" ripetuta:

$$(\varepsilon\alpha, \varepsilon\alpha^2) \cdot (\varepsilon\beta, \varepsilon\beta^2)^{-1} \;=\; (\alpha\beta^2, \beta\alpha^2) \;=\; (\varepsilon\beta^2, \varepsilon\beta) \cdot (\varepsilon\alpha^2, \varepsilon\alpha)^{-1},$$

e dunque $\beta \in \{\alpha, \alpha^2\}$. Quindi X può contenere al più un sottogruppo di ordine 3. □

Passiamo a considerare i moltiplicatori. Definiremo, come al solito nella teoria degli insiemi di differenze, un *moltiplicatore* di un neo-insieme di differenze abeliano D di ordine n come un automorfismo α del gruppo G che induce una collineazione del piano proiettivo associato Π. Un moltiplicatore della forma $\alpha : x \mapsto tx$ per qualche intero t con $(t, (n-1)^2) = 1$ è detto *moltiplicatore numerico*; con abuso di linguaggio, t stesso è detto anche moltiplicatore. È chiaro che $\alpha \in \operatorname{Aut} G$ è un moltiplicatore se e solo se $\alpha(D) = D\gamma$ per qualche $\gamma \in G$.

Poiché i risultati che seguono corrispondono ad analoghe affermazioni per insiemi di differenze planari e affini (cfr. [8]), abbiamo conservato la terminologia corrispondente. Ad esempio, imitando la dimostrazione di [2, Lemma VI.2.5], possiamo usare argomentazioni standard per ottenere il semplice risultato seguente.

Lemma 6.2 *Se D è un neo-insieme di differenze abeliano in G, esiste un elemento $\gamma \in G$ tale che $D\gamma$ è fissato da ogni moltiplicatore.* □

Dimostriamo ora un teorema del moltiplicatore originariamente dovuto a Hughes [15]. La dimostrazione di Hughes, che usa i neocorpi, è lunga, molto tecnica e non molto illuminante. In analogia al caso degli insiemi di differenze planari e affini discusso in [8], presentiamo qui una nuova dimostrazione, molto più corta e anche più trasparente. Di fatto la nostra dimostrazione costruirà esplicitamente moltiplicatori che fissano il dato neo-insieme di differenze.

Teorema 6.3 (Teorema del moltiplicatore) *Se D è un neo-insieme di differenze abeliano di ordine n, ogni divisore primo p di n è un moltiplicatore di D. Precisamente, si può supporre che si abbia $D = D^{(p)}$ in $\mathbb{Z}G$, per ogni primo p che divide n.*

Dimostrazione. Usiamo l'anello di gruppo $\mathbb{Z}G$ e assumiamo senza ledere la generalità che D soddisfi l'equazione (4.2) e sia della forma (4.3). Dapprima osserviamo che valgono le seguenti equazioni ausiliarie:

$$DG = (n-2)G, \;\; DU_1 = G - U_1, \;\; DU_2 = G - U_2 \;\text{ e }\; DU_3 = G - U_3\theta,$$

dove θ è come nell'equazione (4.4) ed è stata determinata esplicitamente nella Proposizione 5.3. Affermiamo ora che, posto con $N = U_1 \cup U_2 \cup U_3$, si ha

$$(6.1)\;\; |D^{(p)} \cap Dg| \;\geq\; 1 \qquad \text{per ogni } g \in G \setminus N.$$

Ciò segue banalmente dalla congruenza

$$(6.2)\;\; |D^{(p)} \cap Dg| \;\equiv\; 1 \mod p \qquad \text{per ogni } g \in G \setminus N,$$

che dimostreremo applicando il Lemma 4.1. Dobbiamo dunque calcolare l'elemento dell'anello di gruppo $D^{(p)}D^{(-1)}$ modulo p. Usando l'ipotesi $p \mid n$, l'equazione (4.2), le equazioni ausiliarie scritte sopra ed il ben noto fatto

$$(6.3)\;\; D^p \;\equiv\; D^{(p)} \mod p \qquad \text{per } D \in \mathbb{Z}_p,$$

che segue dal teorema multinomiale (si veda [2, Lemma VI.3.7]), In $\mathbb{Z}_pG$ si ha:

$$\begin{aligned} D^{(p)}D^{(-1)} &= D^pD^{(-1)} \;=\; D^{p-1}(DD^{(-1)}) \\ &= D^{p-1}(G - U_1 - U_2 - U_3) \\ &= D^{p-2}(-2G - (U_1 - G) - (U_2 - G) - (U_3\theta - G)) \\ &= D^{p-2}(G - U_1 - U_2 - U_3\theta) \\ &= \dots \\ &= G - U_1 - U_2 - U_3\theta^{p-1} \;=\; G - U_1 - U_2 - U_3, \end{aligned}$$

il che implica appunto la congruenza (6.2) e dunque anche (6.1). Abbiamo così stabilito che ogni retta $[\xi, \psi]$ con $\gamma = (\xi, \psi) \notin N$ incontra l'insieme $D^{(p)}$. Osserviamo ora che

- ogni retta $[\xi, 1]$ contiene il punto $(0, 1)$;
- ogni retta $[1, \psi]$ contiene il punto $(1, 0)$;
- ogni retta $[\xi, \xi]$ contiene il punto (θ),

e dunque ogni retta ordinaria incontra l'insieme

$$L \;:=\; D^{(p)} \cup \{(0,1),(1,0),(\theta)\}.$$

Inoltre, ciascuna delle tre rette $[U_1 1]$, $[U_2 1]$ e $[U_3\theta]$ contiene uno dei punti $(0,1)$, $(1,0)$ e (θ); per ogni altra classe laterale di uno dei tre sottogruppi proibiti la retta corrispondente $[U_i\xi]$ interseca D e dunque anche $D^{(p)}$. In conclusione, l'insieme L definito sopra ha $n+1$ punti e incontra ogni retta di Π. Quindi, per un noto risultato di Lander (si veda [2, Lemma VI.4.2]), Lo stesso insieme L è una retta di Π. Questo implica ovviamente che $L = [1,1]$ e dunque $D = D^{(p)}$. □

Come mostrano i cinque risultati seguenti, i moltiplicatori di ordine pari rivestono una particolare importanza. Questi risultati sono essenzialmente contenuti in Kantor [19], ove si usa il linguaggio dei neocorpi; le nostre dimostrazioni risulteranno pertanto alquanto diverse. Il risultato centrale è la seguente caratterizzazione dei moltiplicatori di ordine 2; l'argomentazione geometrica che presentiamo è stata ispirata dalla dimostrazione dell'analogo enunciato per gli insiemi di differenze planari dovuta a Blokhuis, Brouwer e Wilbrink [3].

Teorema 6.4 *Sia D un neo-insieme di differenze abeliano di ordine n in G. Se D ammette un moltiplicatore t di ordine 2 allora n è un quadrato perfetto $n = m^2$, e si ha necessariamente $t = m$.*

Dimostrazione. Sia t un qualsiasi moltiplicatore di ordine 2 di D. La collineazione π del piano proiettivo associato Π descritta nel paragrafo 4 è un'involuzione il cui insieme dei punti fissi contiene il quadrangolo $oxyu$, con $u = (1,1)$. Quindi π è un'involuzione di Baer, ossia gli elementi fissi di π formano un sottopiano di Baer Π_0 (cfr. Hughes e Piper [17]). In particolare, n deve essere un quadrato, e sia $n = m^2$. Definiamo ora i sottogruppi A e B di X come segue:

$$A \;=\; \{\xi \in X : \xi^t = \xi^{-1}\}, \qquad B \;=\; \{\xi \in X : \xi^t = \xi\}.$$

Le applicazioni α e β definite da $\xi^\alpha = \xi^{1-t}$ e $\xi^\beta = \xi^{1+t}$ sono omomorfismi da X ad A e B rispettivamente, e $\xi^\alpha\xi^\beta \;=\; \xi^2$ per ogni $\xi \in X$; quindi $AB = X^\square$ è l'insieme dei quadrati di X e, per il Lemma 4.3, risulta un sottogruppo di indice al più 2. Dato che i punti ordinari di Π_0 non sono altro che le coppie (ξ,ψ) con $\xi,\psi \in B$, si ha che B è l'unico sottogruppo di ordine $m-1$ in X. Il fatto che $AB = X^\square$ implica che A deve essere l'unico sottogruppo di ordine $m+1$ di X. (Se m è pari, $A \cap B = \emptyset$, altrimenti, $A \cap B = \{1,\varepsilon\}$, dove ε è l'unica involuzione di X). Pertanto, ogni moltiplicatore di ordine 2 porta agli stessi sottogruppi A e B e agisce su di essi nello stesso modo di t. Questo vale, in particolare, per il moltiplicatore m di ordine 2 la cui esistenza è garantita dal Teorema 6.3. Dunque le collineazioni indotte da

t ed m coincidono su tutti i punti ordinari (ξ, ψ) con $\xi, \psi \in X^{\square}$, e quindi tm^{-1} deve essere l'identità. Questo prova che $t = m$. □

Corollario 6.5 *Se D è un neo-insieme di differenze abeliano in G, i 2-sottogruppi di Sylow del gruppo dei moltiplicatori di D sono ciclici.* □

Corollario 6.6 *Se D è un neo-insieme di differenze abeliano di ordine quadrato $n = m^2$ in G, esiste anche un neo-insieme di differenze abeliano di ordine m.*

Dimostrazione. Per il Teorema 6.3, D è fissato dal moltiplicatore m di ordine 2. Quindi, usando le stesse notazioni della dimostrazione del Teorema 6.4, D appartiene al sottopiano di Baer Π_0 formato dagli elementi fissi della collineazione π indotta da m. Ne segue che $D \cap B$ è un $(m-1)$-sottoinsieme di $B \times B$ che, come è facile verificare, risulta un sotto-neo-insieme di differenze di D. □

Come conseguenza del Teorema 6.4, otteniamo alcune utili restrizioni.

Teorema 6.7 (Test di Mann) *Sia D un neo-insieme di differenze abeliano di ordine n in $G = X \times X$. Allora o n è un quadrato oppure ogni moltiplicatore di D ha ordine dispari modulo l'esponente* exp G *di G. In particolare, ciascuna delle seguenti condizioni implica che n sia un quadrato:*

(a). D ha un moltiplicatore che ha ordine pari modulo q, dove q divide $n-1$ e o $q = 4$ oppure q è un primo dispari;

(b). se p e q sono divisori primi di n e di $n-1$, rispettivamente, allora p non è un residuo quadratico modulo q;

(c). $n \equiv 4$ *oppure* $6 \pmod 8$;

(d). $tp^f \equiv -1 \pmod q$ *per qualche divisore primo p di n, un opportuno intero non negativo f e qualche moltiplicatore t di D, dove q divide $n-1$ e o $q = 4$ oppure q è un primo dispari;*

(e). $(t+1, n-1) \geq 3$ *per qualche moltiplicatore t di D.*

Dimostrazione. Se t ha ordine pari, un'opportuna potenza di t ha ordine 2, e dunque la prima affermazione è conseguenza immediata del Teorema 6.4. Ogni moltiplicatore d'ordine pari (mod q) ha anche ordine pari modulo l'esponente di G; questo prova (a). Allora (b) segue dall'osservazione che ogni non residuo quadratico ha ordine pari modulo q. Supponiamo che si abbia $n \equiv 4$ o $6 \pmod 8$; in tali ipotesi n è pari e $n-1 \equiv 3$ o $5 \pmod 8$. Pertanto, 2 è un non residuo quadratico modulo $n-1$, e dunque esiste un divisore primo q di $n-1$ tale che 2 risulti anche un non residuo quadratico modulo q. Scegliendo $p = 2$ vediamo che (c) è un caso particolare di (b). Per quanto

riguarda (d), tp^f è un moltiplicatore che ha chiaramente ordine pari mod q; questo è evidente se q è un primo dispari, e segue per $q = 4$ dato che il 2-sottogruppo di Sylow di X è ciclico. Dunque (d) è un caso particolare di (a). Infine, (e) è conseguenza immediata di (d), dal momento che $(t+1, n-1)$ o è multiplo di 4 o ha un divisore primo dispari. □

I criterii del Teorema 6.7 sono analoghi a ben noti risultati per insiemi di differenze planari che sono solitamente dimostrati stabilendo dapprima una versione debole di (d), il cosiddetto *test di Mann* (si veda [2, Capitolo VI]). L'approccio geometrico usato qui, ispirato da alcune argomentazioni di Kantor [19], può essere anche applicato al caso planare, ed è certamente più elegante dell'usuale dimostrazione molto tecnica del test di Mann. Presentiamo ora due esempi che mostrano in che modo il test di Mann può essere applicato; ulteriori risultati dello stesso tipo si possono trovare nell'articolo di Kantor [19].

Esempio 6.8 Supponiamo che esista un neo-insieme di differenze abeliano di ordine $n \equiv 9 \pmod{12}$. Allora $t = 3$ è un moltiplicatore per cui $t+1$ divide $n-1$, e dunque n è un quadrato, come segue da (e).

Corollario 6.9 *Sia D un neo-insieme di differenze abeliano di ordine pari n. Allora $n = 2$, $n = 4$, oppure n è un multiplo di 8.*

Dimostrazione. Quando $n \neq 2$, per il Corollario 5.2, n risulta un multiplo di 4. Se $n \equiv 4 \pmod{8}$, per il Teorema 6.7, n è un quadrato perfetto, sia $n = m^2$. Per il Corollario 6.6, esiste anche un neo-insieme di differenze abeliano di ordine m. Poiché m è pari e non è un multiplo di 4, applicando il Corollario 5.2, si deduce che $m = 2$. Dunque n è divisibile per 8 se si ha $n \neq 2$ o 4. □

Un ulteriore risultato da noi ottenuto in [10] per neo-insiemi di differenze abeliani, è il seguente.

Teorema 6.10 *Sia D un neo-insieme di differenze abeliano di ordine n. Se n è un multiplo di 3, allora o $n = 3$ oppure n è un multiplo di 9.*

La dimostrazione del Teorema 6.10 usa sempre gli anelli di gruppo, ma è estremamente computazionale e, per tale motivo, non viene qui riportata ed è stata pubblicata separatamente in [10].

Citiamo anche un semplice criterio di nonesistenza dovuto a Pankin [23], da confrontarsi col criterio (d) del Teorema 6.7.

Proposizione 6.11 *Nessun neo-insieme di differenze abeliano di ordine $n > 4$ ammette come moltiplicatore -1. In particolare, non esiste un neo-insieme di differenze abeliano di ordine $n > 4$ se n ha un divisore p tale che $p^a \equiv -1 \pmod{n-1}$ per qualche a.*

Dimostrazione. Chiaramente -1 sarebbe un moltiplicatore di ordine 2, e dunque $-1 \equiv \sqrt{n} \pmod{n-1}$ per il Teorema 6.4, il che è impossibile per $n > 4$. La seconda affermazione segue allora usando il Teorema 6.3. □

L'osservazione che segue, semplice ma importante, è stata usata già da Hughes [14, 15], sebbene sembra sia stata esplicitamente enunciata per la prima volta solo nell'articolo di Kantor [19].

Lemma 6.12 *Se t_1, t_2, t_3, t_4 sono moltiplicatori di un neo-insieme di differenze abeliano di ordine n e se $t_1 - t_2 \equiv t_3 - t_4 \pmod{\exp G}$, allora $\exp G$ divide il minimo comune multiplo fra $t_1 - t_2$ e $t_1 - t_3$.*

Dimostrazione. Possiamo supporre, per il Lemma 6.2, che D sia fissato da ogni moltiplicatore numerico. Quindi $\delta \in D$ implica $t_i\delta \in D$ per $i = 1, \ldots, 4$. Per ipotesi, $t_1\delta - t_2\delta = t_3\delta - t_4\delta$ e questo vale solo se $t_1\delta = t_2\delta$ o $t_1\delta = t_3\delta$. Pertanto, l'ordine di ogni elemento di D divide il minimo comune multiplo fra $t_1 - t_2$ e $t_1 - t_3$; poiché D genera G, si ottiene l'asserto. □

Insieme al Teorema 6.3, questo porta al seguente risultato che rafforza il lavoro di Hughes [15, Theorem III.3] e impone forti restrizioni sui possibili ordini di neo-insiemi di differenze abeliani.

Teorema 6.13 *Non esiste un neo-insieme di differenze abeliano il cui ordine sia divisibile per una delle seguenti coppie di primi:* $(2,3)$, $(2,5)$, $(2,7)$, $(2,11)$, $(2,13)$, $(2,17)$, $(2,19)$, $(2,31)$, $(3,5)$, $(3,7)$, $(3,11)$, $(3,13)$, $(3,17)$, $(3,19)$, $(5,7)$, $(5,11)$, $(5,13)$, $(7,13)$.

Dimostrazione. La dimostrazione si basa sempre sul trovare una "differenza ripetuta" e poi applicare Lemma 6.12. Illustriamo ciò considerando i casi non contenuti nell'articolo di Hughes. Supponiamo dapprima che n sia un multiplo di $65 = 5 \cdot 13$; allora 5 e 13, e dunque anche 25, sono moltiplicatori. Ora $25 - 13 = 13 - 1 = 12$, e dunque per il Lemma 6.12 l'esponente di G divide 12. Il Teorema 6.1 implica che G è ciclico, quindi $n - 1$ divide 12, il che è assurdo. Il caso in cui n è un multiplo di 91 può essere trattato allo stesso modo. Supponiamo poi che n sia un multiplo di 34; allora 2 e 17 sono moltiplicatori di D. Poiché $17 - 16 = 2 - 1 = 1$, per il Lemma 6.12 l'esponente di G divide 15. Si noti che almeno uno dei primi 3 e 5 divide $n - 1$; essendo $p = 2$ d'ordine pari modulo q sia per $q = 3$ che per $q = 5$, il Teorema 6.7 implica che n deve essere un quadrato. Dal Corollario 6.6 abbiamo l'esistenza di un neo-insieme di differenze abeliano d'ordine $m = \sqrt{n}$. Chiaramente anche m è un multiplo di 34, e questo procedimento può essere ripetuto indefinitamente il che ci porta all'assurdo cercato. I casi in cui n è un multiplo di 38 o 62 vengono esclusi in modo analogo. □

Esiste un'ulteriore restrizione dovuta a Tanenbaum [28]; poichè non sembra sia posibile dimostrarla con i metodi qui esposti, non ne forniremo la dimostrazione rinviando all'articolo originale.

Teorema 6.14 *Non può esistere un neo-insieme di differenze abeliano di ordine* $n \equiv 15$ *o* $21 \pmod{24}$.

I risultati qui esposti assieme all'uso del computer sono stati usati per dimostrare che ogni neo-insieme di differenze abeliano di ordine ≤ 1000 ha ordine una potenza di un primo (cfr. [24]); la congettura è ovviamente che n sia sempre la potenza di un primo, e dovrebbe essere facile verificarla per molti altri valori di n.

Chiamiamo un neo-insieme di differenze in $G = X \times X$ *ciclico* se X è ciclico. Tali neo-insiemi di differenze (o più precisamente i corrispondenti neocorpi ciclici) sono stati studiati da Pankin [23, 24] che ha ottenuto i seguenti risultati di nonesistenza:

Teorema 6.15 *Supponiamo che* $n \geq 8$ *abbia un divisore* p *tale che l'esponente* r *di* p *modulo* $n-1$ *soddisfi*

- r *non è divisibile per* 3*;*
- $r > [(n-2)/6]$ *se* r *è dispari o rispettivamente* $r > 2[(n-2)/6]$ *se* r *è pari.*

In tali ipotesi, non esiste un neocorpo ciclico di ordine n.

Hughes [14], a mano, ha escluso l'esistenza di neocorpi ciclici proprii per gli ordini $9, 11, 13, 16, 27, 32$ e 64. Pankin [23] ha dato un algoritmo per la costruzione di un qualsiasi neocorpo ciclico; usando una ricerca al computer basata su questo algoritmo, ha aggiunto alla lista precedente gli ordini $17, 19, 23, 25, 29, 31, 37, 41, 43, 47, 49, 81$ e 128. Dunque gli unici neocorpi ciclici il cui ordine sia in una di queste due liste (che, per il Teorema 6.1, sono gli unici neocorpi di quell'ordine) sono campi. Ne segue che non esistono piani di classe di Lenz-Barlotti I.4 di questi ordini.

Ringraziamenti. Questo lavoro, compiuto nell'ambito del GNSAGA, è stato finanziato dal Ministero per l'Istruzione, l'Università e la Ricerca (Progetto: *Strutture geometriche, combinatoria e loro applicazioni*) e dall'Università di Roma "La Sapienza" (Progetto: *Gruppi, Grafi e Geometrie*). La ricerca si è principalmente svolta durante diverse visite presso l'Università di Roma "La Sapienza" del secondo autore, che ringrazia per l'ospitalità e per il supporto finanziario. Gli autori sono in debito con Yutaka Hiramine e Bill Kantor per gli utilissimi scambi di messaggi elettronici sugli argomenti qui trattati.

Riferimenti bibliografici

[1] A. Barlotti: Le possibili configurazioni del sistema delle coppie punto-retta (A, a) per cui un piano grafico risulta (A, a) transitivo. *Boll. Un. Mat. Ital.* **12** (1957), 212–226.

[2] T. Beth, D. Jungnickel and H. Lenz: *Design theory (2nd edition)*. Cambridge University Press, Cambridge (1999).

[3] A. Blokhuis, A.E. Brower and H.A. Wilbrink: Hermitian unitals are code words. *Discr. Math.* **97** (1991), 63–68.

[4] P. Dembowski: *Finite geometries*. Springer, Berlin (1968, Reprint 1997).

[5] P. Dembowski and F.C. Piper: Quasiregular collineation groups of finite projective planes. *Math. Z.* **99** (1967), 53–75.

[6] M.J. de Resmini, D. Ghinelli and D. Jungnickel: Arcs and ovals from abelian groups. *Designs, Codes and Cryptography* **26** (2002), 213–228.

[7] D. Ghinelli: Classificazione di Lenz-Barlotti e problemi aperti inerenti ad essa. *Ist. Mat. " G. Castelnuovo"* Roma (1969), 1–30.

[8] D. Ghinelli and D. Jungnickel: Finite projective planes with a large abelian group. In: Surveys in Combinatorics, Cambridge University Press 2003, 175–237.

[9] D. Ghinelli and D. Jungnickel: On finite projective planes in Lenz-Barlotti class at least I.3 *Advances in geometry*, Special Issue dedicated to A. Barlotti (2003), S28-S48.

[10] D. Ghinelli and D. Jungnickel: A non-existence result for finite projective planes in Lenz-Barlotti class I.4, *Combinatorica* (to appear).

[11] M. Hall: Projective planes. *Trans. Amer. Math. Soc.* **54** (1943), 229–277.

[12] Y. Hiramine: Difference sets relative to disjoint subgroups. *J. Comb. Th. (A)* **88** (1999), 205–216.

[13] J.W.P. Hirschfeld: *Projective geometries over finite fields (2nd edition)*. Oxford University Press, Oxford (1998).

[14] D.R. Hughes: *Planar division neo-rings*. Ph.D. Thesis, University of Wisconsin, Madison (1955).

[15] D.R. Hughes: Planar division neo-rings. *Trans. Amer. Math. Soc.* **80** (1955), 502–527.

[16] D.R. Hughes: Partial difference sets. *Amer. J. Math.* **78** (1956), 650–674.

[17] D.R. Hughes and F.C. Piper: *Projective planes (2nd edition)*. Springer (1982).

[18] D. Jungnickel and K. Vedder: On the geometry of planar difference sets. *European J. Comb.* **5** (1984), 143–148.

[19] W.M. Kantor: Projective planes of type I-4. *Geom. Ded.* **3** (1974), 335–346.

[20] W.M. Kantor and M.D. Pankin: Commutativity in finite planes of type I.4. *Arch. Math.* **23** (1972), 544–547.

[21] H. Lenz: Kleiner desarguesscher Satz und Dualität in projektiven Ebenen. *Jahresber. Deutsche Math. Ver.* **57** (1954), 20–31.

[22] L.J. Paige: Neofields. *Duke Math. J.* **16** (1949), 39–60.

[23] M.D. Pankin: *On finite planes of type I.4.* Ph.D. thesis, University of Illinois at Chicago Circle (1971).

[24] M.D. Pankin: On finite planes of type I.4. In: *Proc. Int. Conf. on projective planes,* pp. 215–218. Washington State Univ. Press, Pullman, Wash. (1973).

[25] G. Pickert: *Projektive Ebenen.* Springer, Berlin (1955).

[26] T. Ralston: On the embeddability of the complement of a complete triangle in a finite projective plane. *Ars Comb.* **11** (1981), 271–274.

[27] A.P. Sprague: Translation nets. *Mitt. Math. Sem. Giessen* **157** (1982), 46–68.

[28] P. Tanenbaum: On the nonexistence of certain finite projective planes of Lenz-Barlotti class I.4. *Boll. Un. Mat. Ital.* (5) **15-A** (1978), 137–139.

[29] J.C.D.S. Yaqub: The Lenz-Barlotti classification. *Proc. Proj. Geometry Conference,* pp. 129–160. Univ. of Illinois, Chicago (1967).

[30] J.C.D.S. Yaqub: On finite projective planes of Lenz-Barlotti class I3. In: *Number theory and algebra*, pp. 349–361 (1977).

[31] H. Zassenhaus: Über endliche Fastkörper. *Abh. Math. Sem. Hamburg* **11** (1935), 187–220.