Università Cattolica del Sacro Cuore
Sede di Brescia
Facoltà di Scienze Matematiche Fisiche e Naturali

———

Tesi di Laurea in Matematica

Gruppi di Frobenius
e
strutture geometriche associate

Relatore:
Ch.ma prof.ssa Silvia Pianta

Laureando:
Luca Giuzzi
Matricola: 2262553

Anno Accademico 1995-96

Introduzione

Sia $\mathbb{K}$ un campo, e sia $(\mathfrak{P}, \mathfrak{R}) = \mathrm{AG}(n, \mathbb{K})$ lo spazio affine di dimensione n costruito su di esso. Per come è stato costruito $\mathrm{AG}(n, \mathbb{K})$, a partire dallo spazio vettoriale $\mathbb{K}^n$, è immediato verificare che la somma $+$ di $\mathbb{K}^n$ trasforma $(\mathfrak{P}, +)$ in un gruppo abeliano. Inoltre $\forall x \in \mathfrak{P}$:

$$x^+ : \begin{cases} \mathfrak{P} \to \mathfrak{P} \\ a \to x + a \end{cases}$$

è una collineazione di $(\mathfrak{P}, \mathfrak{R})$, e

$$\forall R \in \mathfrak{R} : 1 \in R \Rightarrow R \leq \mathfrak{P}.$$

La nozione di gruppo di incidenza nasce come generalizzazione di questa situazione: si considerano infatti strutture $(\mathfrak{P}, \mathfrak{R}, \cdot)$ tali che:

1. $(\mathfrak{P}, \mathfrak{R})$ sia uno spazio di incidenza proprio,
2. $(\mathfrak{P}, \cdot)$ sia un gruppo
3. e $\forall x \in \mathfrak{P}$:

   $$x_l : \begin{cases} \mathfrak{P} \to \mathfrak{P} \\ a \to x \cdot a \end{cases}$$

   sia una collineazione.

Un gruppo di incidenza si dice *fibrato* se vale la condizione:

$$\forall R \in \mathfrak{R} : 1 \in R \Rightarrow R \leq \mathfrak{P},$$

e *bilatero* se anche le applicazioni del tipo:

$$x_r : \begin{cases} \mathfrak{P} \to \mathfrak{P} \\ a \to a \cdot x \end{cases}$$

sono tutte collineazioni. Un gruppo di incidenza fibrato e bilatero viene detto *spazio cinematico*

In effetti, come si vedrà nel seguito, il concetto di spazio cinematico costituisce una buona generalizzazione di quello di spazio affine e risulta addirittura possibile introdurre una relazione di parallelismo sull'insieme $\mathfrak{R}$.

Scopo di questo lavoro è studiare gli spazi cinematici in cui il gruppo $(\mathfrak{P}, \cdot)$ è finito e di Frobenius.

Il **capitolo 1** richiama alcune nozioni algebriche di base, quali la definizione di gruppo nilpotente od i teoremi di Sylow, che saranno impiegate massicciamente in seguito.

Nel **capitolo 2**, *nozioni algebriche sui gruppi di Frobenius* viene introdotto il concetto di gruppo di Frobenius. Si forniscono alcune definizioni diverse e se ne dimostra l'equivalenza. A questo proposito viene dimostrato il "teorema di Frobenius", dopo aver richiamato alcune nozioni di teoria dei caratteri.

Altri risultati notevoli che vengono presentati sono la nilpotenza del nucleo e la caratterizzazione dei sottogruppi di un gruppo di Frobenius che sono ancora di Frobenius.

La condizione che $(\mathfrak{P}, \mathfrak{R}, \cdot)$ sia uno spazio cinematico è piuttosto forte. Infatti, posto $\mathfrak{F} := \{R \in \mathfrak{R} : 1 \in R\}$, abbiamo che le seguenti condizioni devono essere soddisfatte:

- $$\mathfrak{F} \neq \{\mathfrak{P}\}$$
- $$\mathfrak{P} = \bigcup_{R \in \mathfrak{F}} R$$
- $$\forall H, K \in \mathfrak{F} : H \neq K \Rightarrow H \cap K = \{1\}$$
- $$\forall x \in \mathfrak{P}, \forall H \in \mathfrak{F} : H^x \in \mathfrak{F}.$$

Questi fatti equivalgono a richiedere che il gruppo $(\mathfrak{P}, \cdot)$ ammetta una partizione normale non banale.

Nel **capitolo 3** si presenta il teorema di classificazione dei gruppi finiti con partizione e si indaga su alcune proprietà elementari delle partizioni stesse. Si verifica inoltre che ogni gruppo di Frobenius ammette almeno una partizione normale, la cosiddetta *partizione di Frobenius*.

Il **capitolo 4** ha carattere eminentemente geometrico. Dapprima vi si introduce la nozione di struttura di incidenza, e si presentano alcune configurazioni notevoli. Successivamente vengono enunciati i concetti di gruppo di incidenza e di spazio cinematico, mostrando come questi possano essere caratterizzati dalla esistenza di opportune configurazioni.

Nel **capitolo 5** si indaga sugli spazi cinematici derivanti da gruppi di Frobenius. In particolare si mostra che gli spazi cinematici costruiti a partire dalla partizione di Frobenius sono sempre di scambio ed hanno dimensione *di incidenza* due oppure tre[1]. Successivamente si dimostra, in modo originale[2], che se $(\mathfrak{P}, \mathfrak{R}, \cdot)$ è uno spazio cinematico in cui il gruppo $\mathfrak{P}$ è strettamente 2-transitivo[3], allora $(\mathfrak{P}, \mathfrak{R})$ è, in realtà, un piano affine poroso (stripe plane).

Nella conclusione si introduce la nozione di *partizione lineare*, e si mostra una famiglia di gruppi di Frobenius che ammettono una partizione di questo tipo[4].

[1] la dimensione affine è sempre 2
[2] il risultato è già noto; vedi [**Kar73**]
[3] e quindi di Frobenius, per un risultato dimostrato nel capitolo 2
[4] bisogna osservare che la partizione di Frobenius non è *mai* lineare

CAPITOLO 1

Preliminari algebrici

Scopo di questo capitolo è presentare alcune nozioni algebriche che verranno ampiamente utilizzate in seguito. Le dimostrazioni dei risultati qui esposti possono trovarsi su un qualsiasi testo di teoria dei gruppi. In particolare si può far riferimento al primo capitolo di [**Rob82**].

Ove non indicato diversamente nel seguito con $\mathcal{G}$ si intenderà sempre un gruppo scritto con notazione moltiplicativa.

1. Richiami di teoria dei gruppi

Definizione 1.1. Sia $\mathcal{G}$ un gruppo. Diremo **automorfismo di** $\mathcal{G}$ ogni biiezione α

$$\alpha : \begin{cases} \mathcal{G} \to \mathcal{G} \\ x \to \alpha(x) \end{cases}$$

Tale che

$$\forall x_1, x_2 \in \mathcal{G} : \alpha(x_1 {x_2}^{-1}) = \alpha(x_1)\alpha(x_2)^{-1}$$

Si verifica facilmente che tali biiezioni costituiscono gruppo. Indicheremo tale gruppo col simbolo $\mathrm{Aut}(\mathcal{G}, \cdot)$.

Definizione 1.2. Sia $\mathcal{G}$ un gruppo, e siano $x, y \in \mathcal{G}$; chiamiamo allora **coniugato di** y **mediante** x l'elemento

$$y^x := x^{-1} y x$$

Vale il seguente risultato:

Teorema 1.1. *Per ogni $x \in \mathcal{G}$ l'applicazione $\cdot^x$, che associa ad ogni $y \in \mathcal{G}$ il suo coniugato tramite x, cioè tale che:*

$$\cdot^x := \begin{cases} \mathcal{G} \to \mathcal{G} \\ g \to g^x := x^{-1} g x \end{cases}$$

è un automorfismo di $\mathcal{G}$. L'insieme di tutti tali automorfismi costituisce gruppo e viene chiamato **gruppo degli automorfismi interni di $\mathcal{G}$.** *Nel seguito esso sarà indicato col simbolo* $\operatorname{Inn}\mathcal{G}$.

Definizione 1.3. Sia $(\mathcal{G}, \cdot)$ un gruppo. Chiamiamo **centro** di $\mathcal{G}$ l'insieme così definito:

$$\mathrm{Z}(\mathcal{G}) := \{x \in \mathcal{G} : \forall y \in \mathcal{G} : xy = yx\}.$$

Evidentemente 1 appartiene a $\mathrm{Z}(\mathcal{G})$ per qualsiasi gruppo $\mathcal{G}$. Tale insieme dunque non è mai vuoto. Il seguente teorema ci consente di immergere alcuni gruppi nel gruppo dei loro automorfismi:

Teorema 1.2. *Sia $(\mathcal{G}, \cdot)$ un gruppo con centro banale*[1]*, allora:*

$$\operatorname{Inn}(\mathcal{G}, \cdot) \simeq \mathcal{G}$$

Dimostrazione. Sia

$$\theta : \begin{cases} \mathcal{G} \to \operatorname{Inn}(\mathcal{G}) \\ x \to \theta(x) : \begin{cases} \mathcal{G} \to \mathcal{G} \\ h \to h^x \end{cases} \end{cases}$$

Ora, θ è evidentemente un epimorfismo. Sia $k \in \ker\theta$. Allora

$$\forall x \in \mathcal{G} : (\theta(k))(x) = x^k = x,$$

cioè

$$\forall x \in \mathcal{G} : xk = kx,$$

ovvero $k \in \mathrm{Z}(\mathcal{G}) = \{1\}$. Segue la tesi. □

In generale esistono automorfismi di $\mathcal{G}$ che non sono interni; ha dunque senso fornire le seguenti definizioni:

Definizione 1.4. Sia $\mathcal{G}$ un gruppo, e $N \subseteq \mathcal{G}$.

- Diciamo che l'insieme N è **normale** in $\mathcal{G}$ se

$$\forall \tau \in \operatorname{Inn}\mathcal{G} : \tau(N) = N;$$

[1] i.e. $\mathrm{Z}(\mathcal{G}) = \{1\}$

- diciamo che N è **caratteristico** in $\mathcal{G}$ se
$$\forall \tau \in \operatorname{Aut} \mathcal{G} : \tau(N) = N;$$
- diciamo che N è **pienamente invariante** in $\mathcal{G}$ se
$$\forall \tau \in \operatorname{End} \mathcal{G} : \tau(N) = N.$$

Se $N \leq \mathcal{G}$, allora si parla di sottogruppo rispettivamente **normale**, etc.

La normalità, a differenza dell'essere caratteristico o pienamente invariante, non è transitiva; è quindi ragionevole formulare il seguente concetto:

Definizione 1.5. Sia $\mathcal{G}$ un gruppo e $N \leq \mathcal{G}$. Allora N si dice **subnormale** in $\mathcal{G}$ se e solo se esiste una successione finita di sottogruppi di $\mathcal{G}$ $G_1, \dots, \mathcal{G}_n$, tale che
$$N \lhd \mathcal{G}_1 \lhd \mathcal{G}_2 \ldots \lhd \mathcal{G}_n$$
In tale caso si scrive $N \lhd\lhd \mathcal{G}$.

Definizione 1.6. Sia $\mathcal{G}$ un gruppo e $N \lhd\lhd \mathcal{G}$; allora chiamata n la lunghezza minima di una successione tale che
$$N \lhd \mathcal{G}_1 \lhd \mathcal{G}_2 \ldots \lhd \mathcal{G}_n$$
si dice che $n-1$ è il **difetto di subnormalità** di N in $\mathcal{G}$.

Definizione 1.7. Un gruppo $\mathcal{G}$ si dice **semplice** se non ammette sottogruppi normali non banali; si dice **caratteristicamente semplice** se non ammette sottogruppi caratteristici propri diversi da $\{1\}$.

Definizione 1.8. Sia $\mathcal{G}$ un gruppo agente su di un insieme P, e $X \subseteq P$; allora diciamo **stabilizzante di X in $\mathcal{G}$** il sottogruppo di $\mathcal{G}$:
$$\operatorname{St}_{\mathcal{G}}(X) := \{g \in \mathcal{G} : \forall x \in X : g(x) = x\}.$$

Definizione 1.9. Sia $\mathcal{G}$ un gruppo; e $X \subseteq \mathcal{G}$ un suo sottoinsieme; chiamiamo **centralizzante di X in $\mathcal{G}$** l'insieme
$$\operatorname{C}_{\mathcal{G}}(X) := \{y \in \mathcal{G} : \forall x \in X : xy = yx\}.$$

Si può facilmente verificare che

$$\forall x \in \mathcal{G} : \mathrm{C}_{\mathcal{G}}(x) := \mathrm{St}_{\mathrm{Inn}\,\mathcal{G}}(x);$$

tale relazione non vale però fra i centralizzanti e gli stabilizzanti di insiemi.

Teorema 1.3. *Sia $\mathcal{G}$ un gruppo e $X \leq \mathcal{G}$; allora $\mathrm{C}_{\mathcal{G}}(X) < \mathcal{G}$.*

DIMOSTRAZIONE. Evidentemente $1 \in \mathrm{C}_{\mathcal{G}}(X)$; D'altro canto se $c, d \in \mathrm{C}_{\mathcal{G}}(X)$, allora

$$\forall x \in X : cx = xc \& dx = xd \Rightarrow d^{-1}xd = c^{-1}xc$$
$$\Rightarrow cd^{-1}x = xcd^{-1} \Rightarrow cd^{-1} \in \mathrm{C}_{\mathcal{G}}(X).$$

da cui la tesi. □

Definizione 1.10. Sia $\mathcal{G}$ un gruppo e $M \subseteq \mathcal{G}$; diciamo **normalizzante di M in $\mathcal{G}$** il sottogruppo di $\mathcal{G}$

$$\mathrm{N}_{\mathcal{G}}(M) := \{g \in \mathcal{G} : M^x = M\}$$

È possibile dimostrare che il normalizzante in $\mathcal{G}$ di un gruppo M è il più grande sottogruppo N di $\mathcal{G}$ tale che $M \lhd N$.

Definizione 1.11. Sia $\mathcal{G}$ un gruppo e sia $H \leq \mathcal{G}$. Diciamo **laterale sinistro** contenente x di H in $\mathcal{G}$ l'insieme

$$xH := \{xh : h \in H\}.$$

Similmente diciamo **laterale destro**, contentente x di H in $\mathcal{G}$ l'insieme

$$Hx := \{hx : h \in H\}.$$

Si verifica che

Definizione 1.12. Nelle stesse ipotesi della definizione precedente diciamo **trasversale destro di H in $\mathcal{G}$** ogni insieme T tale che

$$\bigcup_{t \in T} Ht = \mathcal{G}$$

e

$$\forall t_1, t_2 \in T : Ht_1 = Ht_2 \Leftrightarrow t_1 = t_2.$$

Analogamente si può definire un **trasversale sinistro di H in $\mathcal{G}$** S

In generale esistono numerosi trasversali (destri o sinistri) distinti, ma la loro cardinalità è costante. La seguente definizione è quindi ben posta:

Definizione 1.13. Sia $\mathcal{G}$ un gruppo e $H \leq \mathcal{G}$. Diciamo **indice di H in $\mathcal{G}$** la cardinalità di un qualsiasi trasversale K di H in $\mathcal{G}$. Indicheremo tale numero col simbolo

$$|\mathcal{G} : H|$$

Vale il seguente risultato:

Teorema 1.4. *Sia $\mathcal{G}$ un gruppo e $\mathcal{N} \leq \mathcal{G}$. Se $|\mathcal{N} : \mathcal{G}| = 2$, allora $\mathcal{N} \lhd \mathcal{G}$.*

2. Prodotto di due gruppi

Definizione 1.14. Siano $(K, \star_K)$, e $(H, \star_H)$ due gruppi; diciamo **prodotto diretto esterno** di K ed H il gruppo $(G, \star) := K \times H$ i cui elementi sono quelli del prodotto cartesiano degli insiemi H e K, e la cui operazione è definita nel seguente modo:

$$(k_1, h_1) \star (k_2, h_2) := (k_1 \star_K k_2, h_1 \star_H h_2).$$

Definizione 1.15. Sia $\mathcal{G}$ un gruppo, e siano $H, K \leq G$. Diciamo che $\mathcal{G}$ è **prodotto diretto interno** di H e K se:

1. $H, K \lhd \mathcal{G}$;
2. $H \cap K = \{1\}$;
3. $\mathcal{G} = HK$.

Spesso è utile una generalizzazione della nozione di prodotto diretto:

Definizione 1.16. Sia $\mathcal{G}$ un gruppo, e siano $H, N \leq G$. Diciamo che $\mathcal{G}$ è **prodotto semidiretto interno** di H e K se:

1. $N \lhd \mathcal{G}, H \leq \mathcal{G}$;
2. $N \cap H = \{1\}$;

3. $\mathcal{G} = NH$.

In tale caso scriveremo $\mathcal{G} = N \rtimes H$.

Come nel caso del prodotto diretto, esiste anche una variante "esterna" di questo tipo di prodotto:

Definizione 1.17. Siano H,N due gruppi, e $\alpha : H \to \mathrm{Aut}(N)$ un omomorfismo. Chiamiamo **prodotto semidiretto esterno** $G := N \rtimes_\alpha H$ il gruppo avente per elementi le coppie ordinate di $N \times H$, e per operazione la seguente:

$$(h_1, n_1) \star (h_2, n_2) = (h_1 h_2, n_1^{\alpha(h_2)} n_2)$$

ove si è indicato con la notazione $n_1^{\alpha(h_2)}$ il trasformato di n_1 mediante l'automorfismo $\alpha(h_2)$.

Osservazione. A rigore si dovrebbe sempre parlare di "prodotto semidiretto esterno di H e N rispetto un automorfismo α,"

3. Il teorema di Sylow

Definizione 1.18. Sia p un numero primo. Allora un gruppo $\mathcal{G}$ si dice p-**gruppo** se $\forall x \in \mathcal{G}$, l'ordine di x è potenza di p.

Definizione 1.19. Sia $\mathcal{G}$ un gruppo finito. Sia p un primo, ed α un numero naturale (0 incluso!) tale che

$$p^\alpha \mid |\mathcal{G}|,$$

ma non

$$p^{\alpha+1} \mid |\mathcal{G}|.$$

Diciamo che un sottogruppo $P \leq \mathcal{G}$ è un p-**sottogruppo di Sylow di** $\mathcal{G}$ (o, più semplicemente, un p-**Sylow di** $\mathcal{G}$), se $|P| = p^\alpha$. Indicheremo l'insieme di tutti i p-Sylow di $\mathcal{G}$ col simbolo

$$\mathrm{Syl}_p(\mathcal{G}).$$

Da tale definizione scende che, se esistono, i p-Sylow di un gruppo $\mathcal{G}$ sono suoi p-gruppi massimali. In effetti vale il seguente risultato:

Teorema 1.5. (Teorema di Sylow) *Sia $\mathcal{G}$ un gruppo finito, α un intero non negativo e p un numero primo tali che $|G| = p^\alpha m$ con $p \not| m$. Allora*

1. *Ogni p-sottogruppo di $\mathcal{G}$ è contenuto in un sottogruppo di ordine p^α; in particolare, poichè $\{1\}$ è un p-sottogruppo per ogni p, i p-Sylow esistono sempre;*
2. *Se n_p è il numero dei p-sottogruppi di Sylow, allora*
$$n_p \equiv 1 \mod p;$$
3. *Per p fissato, tutti i p-Sylow sono coniugati in $\mathcal{G}$.*

Osservazione. Dal punto 1. del teorema precedente discende in particolare che i p-Sylow di $\mathcal{G}$ sono *i* suoi p-gruppi massimali.

4. Gruppi risolubili e nilpotenti

Per questa sezione si può far riferimento al capitolo 5 di [**Rob82**].

Definizione 1.20. Sia $\mathcal{G}$ un gruppo; una successione di sottogruppi $\mathcal{G}_0, \mathcal{G}_1, \dots, \mathcal{G}_n$ si dice **serie normale di $\mathcal{G}$** se:

$$\{1\} = \mathcal{G}_0 \lhd \mathcal{G}_1 \lhd \dots \lhd \mathcal{G}_n = \mathcal{G}$$

e

$$\forall 0 \leq i \leq n : \mathcal{G}_i \lhd \mathcal{G}$$

Definizione 1.21. Un gruppo $\mathcal{G}$ si dice **risolubile** se ammette una *serie abeliana*, ovvero esistono un intero positivo n e dei sottogruppi $\mathcal{G}_0, \mathcal{G}_1, \dots, \mathcal{G}_n \leq \mathcal{G}$ tali che

$$\{1\} = \mathcal{G}_0 \lhd \mathcal{G}_1 \lhd \dots \lhd \mathcal{G}_n = \mathcal{G}$$

e

$$\forall i : 0 \leq i \leq n-1 \Rightarrow \mathcal{G}_{i+1}/\mathcal{G}_i \text{ è abeliano}$$

Definizione 1.22. Un gruppo $\mathcal{G}$ si dice **nilpotente** se ammette una *serie centrale*, ovvero se ammette una serie normale finita

$$\{1\} = \mathcal{G}_0 \lhd \mathcal{G}_1 \lhd \dots \lhd \mathcal{G}_n = \mathcal{G}$$

tale che

$$\forall i : 0 \leq i \leq n-1 \Rightarrow \mathcal{G}_{i+1}/\mathcal{G}_i \leq \mathrm{Z}(\mathcal{G}/\mathcal{G}_i).$$

Definizione 1.23. Sia $\mathcal{G}$ un gruppo nilpotente; La lunghezza della più corta fra le serie centrali di $\mathcal{G}$ viene detta **classe di nilpotenza** di $\mathcal{G}$.

È possibile caratterizzare i gruppi nilpotenti finiti in modo molto forte:

Teorema 1.6. *Sia $\mathcal{G}$ un gruppo finito; allora le seguenti proprietà sono equivalenti:*

1. *$\mathcal{G}$ è nilpotente,*
2. *Ogni sottogruppo di $\mathcal{G}$ è subnormale in $\mathcal{G}$,*
3. *Per ogni $H < \mathcal{G}$ si ha $H \neq \mathrm{N}_{\mathcal{G}}(H)$,*
4. *Per ogni $H \leq \mathcal{G}$: H massimale in $\mathcal{G}$ implica $H \lhd \mathcal{G}$,*
5. *$\mathcal{G}$ è il prodotto diretto dei suoi Sylow.*

Osservazione. Nel caso $\mathcal{G}$ infinito la condizione 1. è più forte di tutte le altre, e dunque il teorema non vale.

Esempi importanti di gruppi nilpotenti sono i gruppi abeliani[2], o i p-gruppi.

La definizione di classe di nilpotenza richiede di calcolare una serie centrale di lunghezza minima per $\mathcal{G}$. In effetti esiste un metodo standard per ottenere serie con tale proprietà.

Definizione 1.24. Sia $\mathcal{G}$ un gruppo, e siano $x_1, x_2 \in \mathcal{G}$. Si dice **commutatore** di x_1 e x_2 l'elemento di $[x_1, x_2] \in \mathcal{G}$ tale che

$$[x_1, x_2] := x_1^{-1} x_2^{-1} x_1 x_2.$$

Se $X_1, X_2 \leq \mathcal{G}$ si dice **commutatore** dei sottogruppi X_1 e X_2 il sottogruppo $[X_1, X_2]$ di $\mathcal{G}$ generato da

$$\{[x_1, x_2] : x_1 \in X_1, x_2 \in X_2\}.$$

[2]in effetti il concetto di nilpotenza nasce come generalizzazione di quello di abelianità

Definizione 1.25. Sia $\mathcal{G}$ un gruppo; si dice **sottogruppo derivato** di $\mathcal{G}$ il sottogruppo

$$\mathcal{G}' := [\mathcal{G}, \mathcal{G}].$$

Si dice **serie derivata di** $\mathcal{G}$ la serie

$$\mathcal{G}^{(0)} \geq \mathcal{G}^{(1)} \geq \dots$$

tale che $\mathcal{G}^{(0)} = \mathcal{G}$ e $\mathcal{G}^{(i)} = (\mathcal{G}^{(i-1)})'$.

Osservazione. Non è detto che la serie derivata debba necessariamente terminare.

Definizione 1.26. Sia $\mathcal{G}$ un gruppo; sia $\gamma_1\mathcal{G} = \mathcal{G}$. Allora posto

$$\gamma_i\mathcal{G} := [\gamma_{i-1}\mathcal{G}, \mathcal{G}]$$

la serie normale

$$\mathcal{G} = \gamma_1\mathcal{G} \geq \gamma_2\mathcal{G} \geq \dots$$

si dice **serie centrale discendente di** $\mathcal{G}$.

Definizione 1.27. Sia $\mathcal{G}$ un gruppo; chiamiamo $\zeta_0\mathcal{G} := 1$; allora la serie normale

$$1 = \zeta_0\mathcal{G} \leq \zeta_1\mathcal{G} \leq \dots$$

definita da

$$\zeta_{i+1}\mathcal{G}/\zeta_i\mathcal{G} := \mathrm{Z}\,(\mathcal{G}/\zeta_i\mathcal{G})$$

si dice **serie centrale ascendente di** $\mathcal{G}$.

Vale il seguente risultato:

Teorema 1.7. *Sia $\mathcal{G}$ un gruppo; allora:*

- *la serie derivata di $\mathcal{G}$ termina con $\{1\}$ dopo un numero finito di passi se e solo se $\mathcal{G}$ è risolubile.*
- *la serie centrale discendente di $\mathcal{G}$ termina con $\{1\}$ dopo un numero finito di passi se e solo se $\mathcal{G}$ è nilpotente*
- *la serie centrale ascendente raggiunge $\mathcal{G}$ in un numero finito di passi se e solo se $\mathcal{G}$ è nilpotente.*

- *se $\mathcal{G}$ è nilpotente la serie centrale ascendente e la serie centrale discendente hanno la medesima lunghezza, pari alla classe di nilpotenza di $\mathcal{G}$.*

Esistono numerosi criteri per determinare se un gruppo è nilpotente.

Teorema 1.8. (P.Hall) *Sia $\mathcal{G}$ un gruppo, e $N \lhd \mathcal{G}$. Supponiamo che sia N che $\mathcal{G}/\mathcal{N}'$ siano nilpotenti; allora $\mathcal{G}$ è nilpotente.*

Definizione 1.28. Sia $\mathcal{G}$ un gruppo; chiamiamo **sottogruppo di Frattini di** $\mathcal{G}$ l'intersezione di tutti i sottogruppi massimali di $\mathcal{G}$. Indicheremo tale sottogruppo come

$$\mathrm{Frat}\,\mathcal{G}.$$

Osservazione. Il sottogruppo di Frattini di un gruppo è sempre nilpotente.

Teorema 1.9. (Wielandt) *Sia $\mathcal{G}$ un gruppo finito; allora $\mathcal{G}$ è nilpotente se e solo se $\mathcal{G}' \leq \mathrm{Frat}\,\mathcal{G}$.*

Nel corso della dimostrazione di questo teorema (per cui rimandiamo a [**Rob82**], pag. 132) si sfrutta un risultato, notevole di per sè, che prende il nome di **argomento di Frattini**:

Teorema 1.10. (Frattini) *Sia $\mathcal{G}$ un gruppo, ed H un suo sottogruppo normale finito. Sia $P \in \mathrm{Syl}_p(H)$; allora $\mathcal{G} = \mathrm{N}_{\mathcal{G}}(P)H$.*

DIMOSTRAZIONE. Sia $g \in \mathcal{G}$; allora, per la normalità di H: $P^g \leq H$ è un p-Sylow di H. Ma per il teorema di Sylow tutti i p-Sylow di H devono essere coniugati *in* H, e quindi $P^g = P^h$ per qualche $h \in \mathcal{H}$. Per conseguenza $gh^{-1} \in \mathrm{N}_{\mathcal{G}}(P)$, da cui

$$g \in \mathrm{N}_{\mathcal{G}}(P)H$$

che è la tesi. □

5. Sottogruppi di Hall

Per questa sezione si può fare riferimento al capitolo 9 di [**Rob82**], oppure di [**Sco64**].

Definizione 1.29. Sia π un insieme di primi; un numero intero n si dice **π-numero** se nella sua fattorizzazione compaiono solamente primi appartenenti a π; al contrario n si dice **π'-numero** se nella sua fattorizzazione *non* compaiono primi di π.

Definizione 1.30. Sia π un insieme di primi; un gruppo $\mathcal{G}$ si dice **π-gruppo** se e solo se per ogni numero primo p vale:

$$p \mid |\mathcal{G}| \Rightarrow p \in \pi.$$

Definizione 1.31. Sia $\mathcal{G}$ un gruppo; chiamiamo π-Sylow di $\mathcal{G}$ ogni π-sottogruppo massimale di $\mathcal{G}$.

L'insieme dei π-Sylow di un gruppo $\mathcal{G}$ non è mai vuoto; d'altro canto se $|\pi| > 1$ i π-Sylow non godono delle medesime proprietà dei p-Sylow: ad esempio non è detto che essi siano per un insieme π fissato tutti coniugati fra loro.

Un concetto più forte e maggiormente significativo è il seguente:

Definizione 1.32. Sia $\mathcal{G}$ un gruppo e sia $H \leq \mathcal{G}$; sia $\mathcal{P}$ l'insieme dei divisori primi di $|\mathcal{G}|$, e sia $\pi \subseteq \mathcal{P}$. Diciamo che H è un **π-Hall** di $\mathcal{G}$ se e solo se H è un π-sottogruppo di $\mathcal{G}$ e $|\mathcal{G} : H|$ è un π'-numero.

Definizione 1.33. Sia $\mathcal{G}$ un gruppo, e sia $H \leq \mathcal{G}$; diciamo che H è un **sottogruppo di Hall** di $\mathcal{G}$ se e solo se il suo ordine e il suo indice in $\mathcal{G}$ sono coprimi.

Osservazione. Tale definizione è ben posta in quanto è immediato convincersi che in effetti ogni π-Hall è un sottogruppo di Hall di $\mathcal{G}$.

I gruppi di Hall rivestono una certa importanza in quanto si può dimostrare (con una certa difficoltà) il seguente risultato:

Teorema 1.11. (Schur-Zassenhaus) *Sia $\mathcal{G}$ un gruppo finito, e sia $N \lhd \mathcal{G}$ un suo sottogruppo di Hall; se poniamo $m := |\mathcal{G} : N|$, allora $\mathcal{G}$ contiene sottogruppi di ordine m. Inoltre i sottogruppi così ottenuti sono a due a due coniugati.*

Osservazione. L'enunciato di tale teorema è equivalente ad affermare che se π è l'insieme dei divisori primi di m, allora esistono dei π-Hall, sottogruppi di $\mathcal{G}$, che costituiscono un complemento per N. Inoltre tali π-Hall sono tutti coniugati fra loro.

CAPITOLO 2

Nozioni algebriche sui gruppi di Frobenius

1. Definizioni

Teorema 2.1. *Sia $\mathcal{G}$ un gruppo finito; allora le seguenti proprietà sono equivalenti:*

1. *esiste $\mathcal{M} \lhd \mathcal{G}$ non banale tale che:*

$$\forall x \in \mathcal{M} \setminus \{1\} : \mathrm{C}_{\mathcal{G}}(x) \leq \mathcal{M}$$

2. *esiste $\mathcal{H} < \mathcal{G}$, non banale, tale che:*

$$\forall x \in \mathcal{G} \setminus \mathcal{H} : \mathcal{H}^x \cap \mathcal{H} = \{1\}$$

Per poter svolgere la dimostrazione di tale teorema è necessario il seguente risultato fondamentale, che sarà dimostrato in seguito:

Teorema 2.2. (Frobenius) *Se $\mathcal{G}$ è un gruppo finito con un sottogruppo $\mathcal{H}$ tale che $\mathcal{H} \cap \mathcal{H}^x = \{1\}$ per ogni $x \in \mathcal{G} \setminus \mathcal{H}$, allora l'insieme*

$$\mathcal{N} := \mathcal{G} \setminus (\bigcup_{x \in \mathcal{G}} H^x \setminus \{1\})$$

è un sottogruppo normale di $\mathcal{G}$ tale che $\mathcal{G} := \mathcal{H}\mathcal{N}$ e $\mathcal{H} \cap \mathcal{N} = \{1\}$.

È bene premettere anche il seguente lemma:

Lemma 2.1. *Se $\mathcal{G}$ è un gruppo finito e $\mathcal{M}$ è un suo sottogruppo soddisfacente le ipotesi del punto* 1. *del teorema 2.1, allora $\mathcal{M}$ è un sottogruppo di Hall di $\mathcal{G}$.*

DIMOSTRAZIONE. Ragionando per assurdo.

Supponiamo che $\mathcal{M}$ non sia un sottogruppo di Hall; allora esiste un p, numero primo, che divide l'ordine di $\mathcal{G}$e tale che

$$\exists P \in \mathrm{Syl}_p(\mathcal{M}), Q \in \mathrm{Syl}_p(\mathcal{G}) : \{1\} < P < Q.$$

Ora, $\mathrm{Z}(Q)$, essendo il centro di un p-gruppo non è banale e dunque contiene almeno un elemento x di ordine p.

Abbiamo due possibilità:

- $x \in P$, da cui seguirebbe $Q \subseteq \mathrm{C}_{\mathcal{G}}(x)$ con $Q \nsubseteq \mathcal{M}$, contro l'ipotesi.
- $x \notin P$, ma allora dovremmo avere per qualche $y \in P \setminus \{1\}$, $x \in \mathrm{C}_{\mathcal{G}}(y) \setminus \mathcal{M}$, assurdo.

Si ha dunque la tesi per $\mathcal{M}$. □

Dimostrazione. (Teorema)

- $(1 \Rightarrow 2)$ Per il lemma precedente $\mathcal{M}$ è un sottogruppo di Hall di $\mathcal{G}$. Il teorema di Schur-Zassenhaus[1] ci garantisce allora l'esistenza di un complemento $\mathcal{H}$ tale che
$$\mathcal{G} = \mathcal{M} \rtimes \mathcal{H}$$
Sia ora $x \in \mathcal{G} \setminus \mathcal{H}$ e studiamo $\mathcal{H} \cap \mathcal{H}^x$. Poichè $\mathcal{G} = \mathcal{H}\mathcal{M}$, x si potrà scrivere come $x = hm$ con $h \in \mathcal{H}, m \in \mathcal{M}$; per conseguenza
$$\mathcal{H}^x = \mathcal{H}^{hm} = \mathcal{H}^m.$$
Supponiamo esista $y \in (\mathcal{H} \cap \mathcal{H}^x) \setminus \{1\}$. Allora $m^{-1}ym \in \mathcal{H}$, ma, essendo $\mathcal{M}$ normale, $y^{-1}m^{-1}ym \in \mathcal{H} \cap \mathcal{M} = \{1\}$. Allora $y \in \mathcal{H}$ centralizza $m \in \mathcal{M}$, contro l'ipotesi.
- $(2 \Rightarrow 1)$ Poniamo
$$\mathcal{M} = \mathcal{G} \setminus (\bigcup_{x \in \mathcal{G}} H^x \setminus \{1\})$$
L'insieme $\mathcal{M}$ così definito non è necessariamente un gruppo; il teorema di Frobenius (Th. 2.2) ci garantisce che in effetti, nelle nostre ipotesi, $\mathcal{M} \lhd \mathcal{G}$.

  Ragioniamo per assurdo: sia $x \in \mathcal{M}$ tale che $\mathrm{C}_{\mathcal{G}}(x) \nsubseteq \mathcal{M}$; esiste allora un elemento $y \in \mathrm{C}_{\mathcal{G}}(x) \setminus \{1\}$ che appartiene anche a un qualche coniugato di $\mathcal{H}$, diciamo $\mathcal{H}^t$. Consideriamo ora gli elementi $z = txt^{-1}$ e $h = tyt^{-1}$. Ovviamente $h \in \mathcal{H}^{tt^{-1}} = \mathcal{H}$, mentre per la normalità di $\mathcal{M}$ si ha $z \in \mathcal{M} \setminus \{1\}$; inoltre

[1] vedi Th.1.11

$h \in \mathrm{C}_{\mathcal{G}}(z)$. Ma allora, poichè z centralizza h, dovrebbe essere $h \in \mathcal{H} \cap \mathcal{H}^z$, contro l'ipotesi, dal che segue 1.

□

Definizione 2.1. Un gruppo $\mathcal{G}$ che soddisfi una qualsiasi delle proprietà enunciate nel teorema 2.1 viene chiamato **gruppo di Frobenius**. I due sottogruppi $\mathcal{M}$ e $\mathcal{H}$ che compaiono in tale teorema sono detti rispettivamente **nucleo** e **complemento di Frobenius**.

Definizione 2.2. In un qualsiasi gruppo $\mathcal{G}$, se $\mathcal{H} < \mathcal{G}$, l'insieme

$$\mathcal{M} = \mathcal{G} \setminus (\bigcup_{x \in \mathcal{G}} H^x \setminus \{1\})$$

introdotto nel corso della dimostrazione del teorema precedente viene detto **insieme residuo di $\mathcal{G}$ rispetto $\mathcal{H}$**.

Osservazione. Nel caso di gruppi di Frobenius parliamo semplicemente di **insieme residuo**, intendendo l'insieme residuo di $\mathcal{G}$ rispetto un qualsiasi complemento di Frobenius $\mathcal{H}$.

Si può dimostrare il seguente risultato:

Teorema 2.3. *Sia $\mathcal{G}$ un gruppo finito; $\mathcal{G}$ é un gruppo Frobenius se e solo se esiste un insieme X su cui $\mathcal{G}$ agisce transitivamente e valgono le seguenti due proprietà:*

1. $\forall g \in \mathcal{G} : \ |\operatorname{Fix}(g)| > 1 \Rightarrow g = 1_{\mathcal{G}}$
2. $\forall x \in X : \operatorname{St}(x) \neq \{1_{\mathcal{G}}\}$.

ovvero se e solo $\mathcal{G}$ è un gruppo transitivo di grado n (cioè agente su di un insieme di n punti) e grado minimo[2] *$n-1$.*

Dimostrazione.

- ($\Leftarrow$) Sia $\mathcal{G}$ di Frobenius con complemento $\mathcal{H}$; ha senso considerare l'azione di $\mathcal{G}$ sulle classi laterali destre di $\mathcal{H}$. Ovviamente tale azione è transitiva e lo stabilizzante di un qualsiasi laterale non

[2]si dice **grado minimo** il numero minimo di punti spostati da una permutazione diversa dall'identità

è banale. Supponiamo ora che $g \in \mathcal{G}$ fissi due laterali distinti, diciamo $\mathcal{H}x$ e $\mathcal{H}y$; allora $\mathcal{H}xg = \mathcal{H}x$ e $\mathcal{H}yg = \mathcal{H}y$, da cui scende $g \in \mathcal{H}^x \cap \mathcal{H}^y$; d'altro canto $yx^{-1} \notin \mathcal{H}$ implica $\mathcal{H}^x \cap \mathcal{H}^y = \{1_\mathcal{G}\}$ da cui la tesi $g = 1_\mathcal{G}$.

- ($\Rightarrow$) Sia $a \in X$ e poniamo

$$\mathcal{H} := \mathrm{St}_\mathcal{G}(a)$$

Se $g \in \mathcal{G} \setminus \mathcal{H}$ allora $\mathcal{H} \cap \mathcal{H}^g$ consiste di tutti gli elementi di $\mathcal{G}$ che fissano i due punti distinti a e $g(a)$; allora $\mathcal{H} \cap \mathcal{H}^g = \{1\}$ e quindi $\mathcal{G}$ è di Frobenius.

La seconda parte della tesi è conseguenza immediata della prima, in quanto la condizione sul grado minimo implica:

1. Se $\tau \in \mathcal{G}$ ha grado $n-1$, allora $\exists x \in X : \tau(x) = x$, ma essendo gli stabilizzatori tutti fra loro coniugati (siamo in un gruppo transitivo!) da questo scende che:

$$\forall x \in X : \mathrm{St}(x) \neq \{1_\mathcal{G}\}$$

2. Se $g \in \mathcal{G}$ fissa un elemento, allora g deve avere o grado $n-1$, e allora $|\operatorname{Fix}(g)| = 1$, oppure essere l'identità, che è la seconda condizione.

$\square$

Corollario 2.1. *Sia $\mathcal{G}$ un gruppo di Frobenius; supponiamo $\mathcal{G}$ agisca transitivamente su di un insieme X; allora il nucleo di $\mathcal{G}$ coincide con l'insieme costituito da tutti gli elementi di $\mathcal{G}$ con azione priva di punti fissi assieme con l'identità.*

DIMOSTRAZIONE. Poichè l'azione di $\mathcal{G}$ su X è transitiva tutti gli stabilizzanti risultano essere coniugati; allora, se $\mathcal{H} = \mathrm{St}_\mathcal{G}(a)$:

$$H^x = \mathrm{St}_\mathcal{G}(x(a)).$$

Per conseguenza

$$\mathcal{N} = \mathcal{G} \setminus (\bigcup_{g \in \mathcal{G}} H^g \setminus \{1\}) = (\mathcal{G} \setminus \bigcup_{x \in X} \mathrm{St}_\mathcal{G}(x)) \cup \{1\}$$

Ovvero $\mathcal{N}$ consta dell'insieme degli elementi di $\mathcal{G}$ che non fissano alcun elemento di X unito con $\{1\}$. $\square$

Corollario 2.2. *Il nucleo $\mathcal{N}$ di un gruppo di Frobenius $\mathcal{G}$ è caratteristico in $\mathcal{G}$.*

Dimostrazione. $\mathcal{N} \setminus \{1\}$ consta di tutti gli elementi di $\mathcal{G}$ che posseggono azione priva di punti fissi. D'altro canto deve essere

$$\forall \alpha \in \mathrm{Aut}(\mathcal{G}), \forall x \in \mathcal{G} : |\,\mathrm{Fix}(x)| = |\,\mathrm{Fix}(x^\alpha)|.$$

Allora $\mathcal{N}$ deve essere invariante per ogni $\alpha \in \mathrm{Aut}(\mathcal{G})$, che è la tesi. $\square$

Osservazione. Un gruppo di Frobenius $\mathcal{G}$ si può sempre vedere come gruppo di permutazioni sul suo nucleo $\mathcal{N}$. Si verifica che l'azione indotta da

$$\sigma(x) := \begin{cases} n \to xn \text{ se } x \in \mathcal{N} \\ n \to n^x \text{ se } x \in \mathcal{H} \end{cases}$$

trasforma $\mathcal{G}$ in un gruppo di grado $n = |\mathcal{N}|$, e grado minimo $n-1$, in quanto $\mathcal{H} = \mathrm{St}_{\mathcal{G}}(1)$.

Alla luce del risultato del corollario 2.1 è possibile fornire la seguente generalizzazione[3] del concetto di nucleo:

Definizione 2.3. Sia $\mathcal{G}$ un gruppo di permutazioni agente su di un insieme X; chiamiamo allora **nucleo di Frobenius** di $\mathcal{G}$ l'insieme[4] $\mathcal{N}$ così definito:

$$\mathcal{N} := \{g \in \mathcal{G} : \mathrm{Fix}(g) = \emptyset\} \cup \{1\}$$

Osservazione. Si verifica che tale insieme coincide con l'insieme residuo di $\mathcal{G}$ rispetto $\mathcal{H} = \mathrm{St}_{\mathcal{G}}(x)$

[3] Vedi [**Rot95**], pag. 252

[4] in generale **non** è un gruppo

2. Il teorema di Frobenius

Teorema 2.4. (Wielandt) *Sia $\mathcal{G}$ un gruppo finito, e siano $\mathcal{K} < \mathcal{G}$; $\mathcal{H} \lhd \mathcal{G}$ due suoi sottogruppi tali che*

$$\forall x \in \mathcal{G} \setminus \mathcal{H} : \mathcal{H} \cap \mathcal{H}^x \leq \mathcal{K}$$

Allora, posto

$$\mathcal{N} := \mathcal{G} \setminus (\bigcup_{x \in \mathcal{G}} H^x \setminus \mathcal{K})$$

si ha che:

1. $\mathcal{N} \lhd \mathcal{G}$
2. $\mathcal{G} = \mathcal{H}\mathcal{N}$
3. $\mathcal{H} \cap \mathcal{N} = \mathcal{K}$.

Evidentemente il teorema di Frobenius (Th 2.2) è una conseguenza pressochè immediata del teorema di Wielandt 2.4 ove si ponga $\mathcal{K} = \{1\}$.

D'altro canto la dimostrazione tradizionale del fatto che $\mathcal{N}$ è sottogruppo normale di $\mathcal{G}$ necessita di strumenti piuttosto tecnici di teoria dei caratteri. Essa puó trovarsi sia su [**Rob82**], pagg. 241-243 (ove si mostra il più generale teorema di Wielandt), che su [**Sco64**], pagg. 345-347.

Vogliamo presentare qui una dimostrazione diversa che, pur non riuscendo ad evitare l'uso dei caratteri, ciò nonostante risulta sotto certi punti di vista molto meno "tecnica" della precedente[5].

Prima di procedere è necessario il seguente fondamentale lemma:

Lemma 2.2. (Lemma induttivo) *Sia $\mathcal{G}$ un gruppo di Frobenius con complemento $\mathcal{H}$, e sia $\mathcal{N}$ l'insieme residuo; allora se esiste un sottogruppo proprio L di G contenente $\mathcal{N}$, si ha $\mathcal{N} < \mathcal{G}$.*

Dimostrazione. Per induzione sull'ordine di $\mathcal{G}$. Sia $\mathcal{N} \subseteq L < \mathcal{G}$;

- se $\mathcal{N} = L$, allora $\mathcal{N}$ è sottogruppo e non vi è nulla da aggiungere;

[5] sono grato per questa dimostrazione al professor Virgilio Pannone dell'università di Firenze, che l'ha presentata in una conferenza tenuta presso l'Università Cattolica di Brescia l'11-5-1995

- se $\mathcal{N} \subset L$, allora posto $\mathcal{H}_1 = \mathcal{H} \cap L$ si ha che L é un gruppo di Frobenius di complemento H_1 con insieme residuo $\mathcal{N}$; per induzione segue la tesi.

$\square$

2.1. Richiami di teoria dei caratteri. Richiamiamo ora alcuni risultati fondamentali di teoria dei caratteri che saranno utili anche in seguito.

Per una trattazione più esauriente degli argomenti qui accennati si rimanda a [**Sco64**],[**Rob82**], oppure [**JL93**].

Definizione 2.4. Sia $\mathcal{G}$ un gruppo; chiameremo **funzione di classe** ogni applicazione avente come dominio $\mathcal{G}$ e costante sulle classi di coniugio. Indicheremo l'insieme delle funzioni di classe di $\mathcal{G}$ a valori complessi con il simbolo $\mathbf{cla}(\mathcal{G})$.

Teorema 2.5. *Sia $\mathcal{G}$ un gruppo; allora l'insieme* $\mathbf{cla}(\mathcal{G})$ *è una algebra hermitiana su* $\mathbb{C}$.

DIMOSTRAZIONE. Siano $\alpha, \beta \in \mathbf{cla}(\mathcal{G})$ e $c \in \mathbb{C}$; allora $\forall g \in \mathcal{G}$ poniamo

$$(\alpha + \beta)(g) := \alpha(g) + \beta(g)$$

e inoltre

$$(c\alpha)(g) := c(\alpha(g)),$$

$$(\alpha\beta)(g) := \alpha(g)\beta(g).$$

È facile vedere che la somma il prodotto ed il prodotto per uno scalare di due funzioni di classe è ancora una funzione di classe, e per conseguenza $\mathbf{cla}(\mathcal{G})$ è una algebra su $\mathbb{C}$.

Se definiamo

$$[\alpha, \beta]_{\mathcal{G}} := \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} \alpha(g)\overline{\beta(g)}.$$

si verifica rapidamente che $[\alpha, \beta]_{\mathcal{G}}$ soddisfa tutte le proprietà di un prodotto hermitiano, e si ha dunque la tesi. $\square$

Definizione 2.5. Sia $\mathcal{G}$ un gruppo; per ogni funzione di classe α chiamiamo **preimmagine principale** l'insieme

$$\mathbf{prep}(\alpha) := \{g \in \mathcal{G} : \alpha(g) = \alpha(1_{\mathcal{G}})\}.$$

Osservazione. La preimmagine principale di una funzione di classe *non* è sempre un sottogruppo di $\mathcal{G}$, anche se costituisce sempre un sottoinsieme normale[6].

Definizione 2.6. Sia $\mathcal{G}$ un gruppo R un anello; si dice **anello gruppo** di $\mathcal{G}$ su R l'anello

$$R\mathcal{G}$$

definito come l'insieme di tutte le serie formali del tipo $\sum_{x \in \mathcal{G}} r_x x$, ove $r_x \in R$ e $r_x = 0$ tranne che in un numero finito di casi, fornito delle seguenti due operazioni:

$$\left(\sum_x r_x x\right) + \left(\sum_x r'_x x\right) = \sum_x (r_x + r'_x) x$$

e

$$\left(\sum_x r_x x\right) \left(\sum_x r'_x x\right) = \sum_x \left(\sum_{yz=x} (r_y r'_z)\right) x.$$

Definizione 2.7. Se $\mathbb{F}$ è un campo, e $\mathcal{G}$ è un gruppo allora l'anello gruppo $\mathbb{F}\mathcal{G}$ è dotato di una struttura naturale di $\mathbb{F}$-modulo fornita da:

$$\forall f \in \mathbb{F} : f\left(\sum_x f_x x\right) = \sum_x (f f_x) x,$$

ed inoltre, se $f \in \mathbb{F}$, $r, s \in \mathbb{F}\mathcal{G}$ allora

$$f(rs) = (fr)s = r(fs).$$

$\mathbb{F}\mathcal{G}$ è dunque una algebra che chiameremo **algebra gruppo** di $\mathcal{G}$ su $\mathbb{F}$.

Definizione 2.8. Sia $\mathcal{G}$ un gruppo e $\mathbb{F}$ un campo; chiamiamo **rappresentazione lineare di grado n di $\mathcal{G}$ su $\mathbb{F}$**[7] ogni omomorfismo $\rho : \mathcal{G} \leftarrow \mathrm{GL}(n, \mathbb{F})$; una $\mathbb{F}$-rappresentazione ρ si dice **fedele** se $\ker \rho = 1$.

[6] i.e. invariante per automorfismi interni

[7] oppure **$\mathbb{F}$-rappresentazione di grado n di $\mathcal{G}$**

Osservazione. Sia $\rho : G \leftarrow \mathrm{GL}(n, \mathbb{F})$ una $\mathbb{F}$-rappresentazione del gruppo $\mathcal{G}$ e sia M lo spazio vettoriale di dimensione n sul campo $\mathbb{F}$. Allora M può essere trasformato in un $\mathbb{F}\mathcal{G}$-modulo sinistro per mezzo del "prodotto":

$$\forall a \in M : a\left(\sum_{x\in\mathcal{G}} f_x x\right) := \sum_{x\in\mathcal{G}} f_x(ax^\rho).$$

Viceversa per ogni $\mathbb{F}\mathcal{G}$-modulo sinistro M di dimensione finita n esiste una $\mathbb{F}$-rappresentazione ρ di grado n definita da:

$$\forall a \in M : ag^\rho = ag.$$

Definizione 2.9. Sia $\mathcal{G}$ un gruppo. Se ϕ,ρ sono due sue $\mathbb{F}$-rappresentazioni. ϕ e ρ si dicono **equivalenti** se i due $\mathbb{F}\mathcal{G}$-moduli cui danno luogo sono isomorfi.

Definizione 2.10. Sia $\mathcal{G}$ un gruppo e sia ϕ una sua $\mathbb{F}$-rappresentazione. Tale rappresentazione ϕ si dice **irriducibile** se l'$\mathbb{F}\mathcal{G}$-modulo ad essa associato non ha $\mathbb{F}\mathcal{G}$-sottomoduli propri.

Definizione 2.11. Sia $\mathcal{G}$ un gruppo, e ϕ una rappresentazione di grado n di $\mathcal{G}$ sul campo $\mathbb{F}$; chiamiamo **carattere di $\mathcal{G}$ offerto dalla rappresentazione** ϕ l'applicazione

$$\chi_\phi : \mathcal{G} \to \mathbb{F}$$

che associa ad ogni $g \in \mathcal{G}$ la traccia della matrice $\phi(x)$. Un carattere si dice **irriducibile** se la rappresentazione ϕ è irriducibile.

L'importanza dei caratteri discende dal fatto che due rappresentazioni hanno il medesimo carattere se e solo se esse sono equivalenti.

Nel seguito, per "rappresentazioni" e "caratteri" di un gruppo, si intenderanno sempre delle $\mathbb{C}$-rappresentazioni con i caratteri ad esse associati, ove $\mathbb{C}$ è il campo complesso.

È facile convincersi che i caratteri sono sempre funzioni di classe; in effetti nel caso particolare delle $\mathbb{C}$-rappresentazioni godono di una proprietà molto particolare:

Teorema 2.6. *I caratteri irriducibili di $\mathcal{G}$ costituiscono una base ortonormale per* $\mathbf{cla}(\mathcal{G})$.

Teorema 2.7. *Sia $\mathcal{G}$ un gruppo, e sia ϕ un carattere di $\mathcal{G}$. Allora*

$$\ker(\phi) := \mathbf{prep}(\phi) \lhd \mathcal{G}$$

Tale sottogruppo normale viene detto anche **nucleo** *del carattere.*

Teorema 2.8. *Per ogni gruppo finito $\mathcal{G}$ esiste almeno un suo carattere irriducibile ϕ tale che*

$$\{1\} \leq \ker(\phi) < \mathcal{G}$$

Osserviamo che mentre la somma ed il prodotto di caratteri sono ancora caratteri, altrettanto non si può dire della differenza; ha quindi senso la seguente definizione:

Definizione 2.12. Si dicono **caratteri generalizzati** tutte le funzioni di classe che sono differenza di due caratteri.

2.2. La dimostrazione. Sia ora $\mathcal{G}$ un gruppo di Frobenius con complemento $\mathcal{H}$. Chiamato ϕ un carattere irriducibile di $\mathcal{H}$ tale che, a norma del teorema 2.8, $\{1\} \leq \ker(\phi) < \mathcal{H}$. L'idea da applicare per dimostrare il teorema di Frobenius è quella di costruire un carattere $\phi^\star$ di $\mathcal{G}$ tale che:

1. $\mathcal{N} \subseteq \ker(\phi^\star)$
2. $\phi^\star_{\mathcal{H}} = \phi$.

Dalla condizione 2. segue $\ker(\phi^\star) < \mathcal{G}$, e dunque, posto $L = \ker(\phi^\star)$ si ottiene grazie al lemma 2.2 la tesi.

Osservazione. Esiste una ed una sola funzione di classe $\phi^\star$ che soddisfa le condizioni sopra enunciate.

Dimostrazione. Il fatto che $\phi^\star$ sia di classe implica che essa debba essere costante all'interno di ogni singola classe di coniugio; d'altro canto $\phi^\star$ é assegnata per la condizione 2. su tutti i coniugati del complemento, mentre su $\mathcal{N}$, per la 1. deve assumere il medesimo valore che su $1_{\mathcal{G}}$. Poichè

$$\mathcal{G} = \bigcup_{x\in\mathcal{G}} \mathcal{H}^x \cup \mathcal{N}$$

si ha la tesi □

Dimostrazione. (Teorema di Frobenius)

Sia ϕ come sopra; poniamo allora per ogni $g \in \mathcal{G}$:

$$\phi^\star(g) := \begin{cases} \phi(1) & \text{se } g \in \mathcal{N} \\ \phi(g^{x^{-1}}) & \text{se } g \in \mathcal{H}^x \end{cases}$$

Per costruzione $\phi^\star$ è una funzione di classe di $\mathcal{G}$ e

$$\mathcal{N} \subseteq \mathbf{prep}(\phi^\star) \subseteq \mathcal{G}.$$

Resta da dimostrare che $\phi^\star$ è un carattere di $\mathcal{G}$. Per il teorema 2.6, chiamati $\chi_1, \ldots, \chi_s$ i caratteri irriducibili di $\mathcal{G}$, si ha il seguente sviluppo in serie di Fourier:

$$\phi^\star = [\phi^\star, \chi_1]_{\mathcal{G}} \cdot \chi_1 + \ldots + [\phi^\star, \chi_s]_{\mathcal{G}} \cdot \chi_s = \sum_{i=1}^{s} [\phi^\star, \chi_i]_{\mathcal{G}} \cdot \chi_i.$$

Ove con $[\cdot,\cdot]_{\mathcal{G}}$ si intende il prodotto hermitiano standard fra due funzioni di classe di $\mathcal{G}$ a valori in $\mathbb{C}$. Se tutti i coefficienti di Fourier di $\phi^\star$ sono interi e positivi, allora esso è certamente un carattere. Ci basta dunque dimostrare questo ultimo fatto per poter dedurre la tesi. Procediamo in due passi:

- Dimostriamo dapprima che i coefficienti di Fourier sono numeri interi.

  Poichè in ogni gruppo di Frobenius vale[8] per ogni funzione di classe α la relazione:

$$\sum_{g\in\mathcal{G}} \alpha(g) = \sum_{g\in\mathcal{N}} \alpha(g) + |\mathcal{N}| \sum_{g\in\mathcal{H}} \alpha(g) - |\mathcal{N}|\alpha(1_{\mathcal{G}})$$

[8] la dimostrazione è banale e scende dal fatto che vi sono esattamente $|\mathcal{N}|$ gruppi coniugati distinti di $\mathcal{H}$ in $\mathcal{G}$, ed essi hanno tutti intersezione ridotta ad $\{1\}$

abbiamo, per ogni carattere irriducibile χ di $\mathcal{G}$:

$$
\begin{aligned}
[\phi^\star, \chi]_{\mathcal{G}} &= \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} \phi^\star(g)\overline{\chi(g)} = \\
&= \frac{1}{|\mathcal{G}|} \left\{ \sum_{g \in \mathcal{N}} \phi^\star(g)\overline{\chi(g)} + |N| \sum_{g \in \mathcal{H}} \phi^\star(g)\overline{\chi(g)} - |N|\phi(1)\chi(1) \right\} = \\
&= \frac{|\mathcal{N}|}{|\mathcal{G}|} \sum_{g \in \mathcal{H}} \phi^\star(g)\overline{\chi(g)} + \left[\frac{\phi(1_{\mathcal{G}})}{|\mathcal{G}|} \sum_{g \in \mathcal{N}} \overline{\chi(g)} - \frac{\phi(1)}{|\mathcal{H}|}\chi(1) \right] = \\
&= [\phi, \chi_{\mathcal{H}}]_{\mathcal{H}} + \frac{|\mathcal{N}|\phi(1)}{|\mathcal{G}|} \sum_{g \in \mathcal{H}} \overline{\chi(g)} - \frac{\phi(1)}{|\mathcal{H}|} \sum_{g \in \mathcal{H}} \overline{\chi(g)} + \\
&\quad + \left[\frac{\phi(1_{\mathcal{G}})}{|\mathcal{G}|} \sum_{g \in \mathcal{N}} \overline{\chi(g)} - \frac{\phi(1)}{|\mathcal{H}|}\chi(1) \right] = \\
&= [\phi, \chi_{\mathcal{H}}]_{\mathcal{H}} + \phi(1) \left\{ [1, \chi]_{\mathcal{G}} + \frac{|\mathcal{N}|}{|\mathcal{G}|}\chi(1) \right\} - \frac{\phi(1)}{|\mathcal{H}|} \sum_{g \in \mathcal{H}} \overline{\chi(g)} - \frac{\phi(1)\chi(1)}{|\mathcal{H}|} = \\
&= [\phi, \chi_{\mathcal{H}}]_{\mathcal{H}} + \phi(1)[1, \chi]_{\mathcal{G}} - \phi(1)[1, \chi_{\mathcal{H}}]_{\mathcal{H}}
\end{aligned}
$$

che è evidentemente un intero in quanto consta di somme e differenze di numeri interi positivi.

- Verifichiamo che $\forall i : [\phi^\star, \chi_i]_{\mathcal{G}} \geq 0$ In primo luogo, poichè ϕ è carattere irriducibile di $\mathcal{H}$ abbiamo:

$$
\begin{aligned}
[\phi^\star, \phi^\star]_{\mathcal{G}} &= \frac{1}{\mathcal{G}} \sum_{g \in \mathcal{G}} |\phi^\star(g)|^2 = \frac{1}{\mathcal{G}} \left\{ \sum_{g \in \mathcal{N}} |\phi^\star(g)|^2 + \sum_{g \notin \mathcal{N}} |\phi^\star(g)|^2 \right\} = \\
&= \frac{|\mathcal{N}|\phi(1)^2}{|\mathcal{G}|} + \frac{|\mathcal{N}|}{|\mathcal{G}|} \sum_{g \in \mathcal{H}} |\phi^\star(g)|^2 - \frac{|\mathcal{N}|}{|\mathcal{G}|}\phi(1)^2 = \\
&= \frac{1}{|\mathcal{H}|} \sum g \in \mathcal{H} |\phi(g)|^2 = [\phi, \phi]_{\mathcal{H}} = 1
\end{aligned}
$$

Ma in una algebra hermitiana la norma al quadrato coincide sempre con la somma dei coefficienti di Fourier elevati al quadrato, per cui:

$$[\phi^\star, \phi^\star] = \sum_{i=1}^{s} [\phi^\star, \chi_i]_{\mathcal{G}}^2$$

Abbiamo verificato, nel punto precedente, che tali coefficienti sono tutti interi; da questo segue che di essi uno e uno solo solo può (e deve) essere diverso da zero e possedere modulo unitario.

Allora esiste un j tale che $\forall g \in \mathcal{G} : \phi^\star(g) = \pm\chi_j(g)$. D'altro canto $\phi^\star(1) = \phi(1) > 0$, e, al contempo $\chi_j(g) > 0$; allora necessariamente $\phi^\star = \chi_j$; quindi $\phi^\star$ è un carattere (irriducibile), dal che segue finalmente la tesi $\mathcal{N} < \mathcal{G}$.

A questo punto è immediato rendersi conto che $\mathcal{N}$ deve essere normale in $\mathcal{G}$; infatti

$$\bigcup_{x \in \mathcal{G}} \mathcal{H}^x$$

costituisce un sottoinsieme normale di $\mathcal{G}$; conseguentemente anche

$$\mathcal{N} := \{1\} \cup \left(\mathcal{G} \setminus \bigcup_{x \in \mathcal{G}} H^x \right) \lhd \mathcal{G}.$$

□

3. Il teorema di Thompson

Se $\mathcal{G}$ è un gruppo di Frobenius finito, allora, per quanto visto in precedenza, esso non può essere semplice e risulta sempre possibile scriverlo come

$$\mathcal{G} = \mathcal{N} \rtimes \mathcal{H}$$

ove $\mathcal{N}$ è il suo nucleo ed $\mathcal{H}$ un complemento. In effetti la struttura di $\mathcal{G}$ determina le proprietà di $\mathcal{N}$ in modo molto forte.

Premettiamo una definizione ed un lemma di carattere generale.

Definizione 2.13. Sia $\mathcal{G}$ un gruppo e α un automorfismo di $\mathcal{G}$. Diciamo che α è **privo di punti fissi** se l'unico elemento fissato da α è $1_{\mathcal{G}}$.

Lemma 2.3. *Sia $\mathcal{G}$ un gruppo finito. Supponiamo che α sia un suo automorfismo di ordine 2 privo di punti fissi; allora $\mathcal{G}$ è abeliano di ordine dispari e $\forall g \in \mathcal{G} : g^\alpha = g^{-1}$.*

DIMOSTRAZIONE. Sia β definito nel seguente modo:

$$\forall g \in \mathcal{G} : g^\beta := g^{-1}(g^\alpha).$$

Allora β è una biiezione di $\mathcal{G}$ in $\mathcal{G}$, infatti essa è iniettiva:

$$g^{\beta} = h^{\beta} \Leftrightarrow g^{-1}(g^{\alpha}) = h^{-1}(h^{\alpha}) \Leftrightarrow$$
$$\Leftrightarrow hg^{-1} = (hg^{-1})^{\alpha} \Leftrightarrow hg^{-1} = 1 \Leftrightarrow h = g$$

ed essendo $\mathcal{G}$ finito risulta automaticamente anche suriettiva.

Ora sia $x \in \mathcal{G}$; per quento sopra osservato $x = g^{\beta}$ per esattamente un $g \in \mathcal{G}$; quindi:

$$x^{\alpha} = (g^{\beta})^{\alpha} = (g^{-1}(g^{\alpha}))^{\alpha} = (g^{\alpha})^{-1}g =$$
$$= (g^{-1}(g^{\alpha})^{-1} = x^{-1}$$

Ma l'invertire è un antiautomorfismo[9], e non un automorfismo, se $\mathcal{G}$ non è abeliano, contro l'ipotesi su α. Ne segue necessariamente la tesi.

Il fatto che l'ordine di $\mathcal{G}$ debba essere dispari segue dalla considerazione che α, visto come permutazione sugli elementi di $\mathcal{G}$, deve fissare la sola identità ed essere il prodotto disgiunto di, diciamo n 2-cicli, e quindi:

$$|G| = 2n + 1$$

che è la tesi. □

Teorema 2.9. *Sia $\mathcal{G}$ un gruppo di Frobenius; allora gli elementi del complemento $\mathcal{H}$ diversi dall'identità inducono per coniugio sul nucleo $\mathcal{N}$ degli automorfismi privi di punti fissi.*

Dimostrazione. Poichè $\mathcal{N} \lhd \mathcal{G}$ il coniugio mediante elementi di $\mathcal{H}$ ristretto ad $\mathcal{N}$ è effettivamente un automorfismo di $\mathcal{N}$. Supponiamo ora $h \in \mathcal{H} \setminus \{1\}$ e che sia $n \in \mathcal{N}$ tale che $n^h = n$. Allora, poichè

$$n^h = h^{-1}nh = k \Leftrightarrow nhn^{-1} = h \Leftrightarrow h^n = n^{-1}hn = h$$

si ha $1 \neq h^n = h \in \mathcal{H} \cap \mathcal{H}^x$ da cui segue $k \in \mathcal{H} \cap \mathcal{N} = \{1\}$, da cui segue quanto richiesto[10]. □

---

[9] $\forall x, y \in \mathcal{G} : (xy)^{-1} = y^{-1}x^{-1}$

[10] si può fornire una dimostrazione alternativa di questo fatto tenuto conto del fatto che

$$n^h = n \Leftrightarrow h \in \mathrm{C}_{\mathcal{G}}(n) < \mathcal{N},$$

e che dunque deve essere $h \in \mathrm{C}_{\mathcal{G}}(n) \cap \mathcal{H} < \mathcal{N} \cap \mathcal{H}$, da cui segue, come sopra, la tesi

Teorema 2.10. *Sia $\mathcal{G}$ un gruppo di Frobenius con complemento $\mathcal{H}$. Se la cardinalità di $\mathcal{H}$ è pari allora il nucleo $\mathcal{N}$ deve essere abeliano.*

DIMOSTRAZIONE. Se esiste un numero naturale n tale che $|\mathcal{H}| = 2n$, allora esiste almeno un elemento $x \in \mathcal{H} \setminus \{1\}$ tale che $x^2 = 1$. Tale elemento induce a norma del teorema 2.9 un automorfismo di periodo 2 privo di punti fissi sul nucleo $\mathcal{N}$. A questo punto la tesi segue dal lemma 2.3. $\square$

In generale, se $|\mathcal{H}|$ non è pari, non è possibile dire nulla riguardo l'eventuale abelianità del nucleo.

Nel 1959 Thompson (vedi [**Tho59**]) ha pubblicato il seguente criterio di nilpotenza, per la cui dimostrazione (tutt'altro che elementare) rimandiamo a [**Rob82**], pagg. 289-298, oppure al capitolo 10 di [**Gor80**]:

Teorema 2.11. (Thompson) *Sia $\mathcal{G}$ un gruppo finito e sia p un numero primo; se $\mathcal{G}$ possiede un automorfismo α di ordine p privo di punti fissi, allora $\mathcal{G}$ è nilpotente.*

Procedendo in modo analogo alla dimostrazione del teorema 2.10, sfruttando al posto del lemma 2.3 quanto appena enunciato, si ottiene il seguente risultato fondamentale:

Teorema 2.12. *Sia $\mathcal{G}$ un gruppo di Frobenius finito di nucleo $\mathcal{N}$. Allora $\mathcal{N}$ è nilpotente.*

4. Proprietà elementari

Un modo standard per costruire gruppi di Frobenius è offerto dal seguente teorema:

Teorema 2.13. *Sia $\mathcal{N}$ un gruppo, e sia $\mathcal{H}$ un sottogruppo di* $\operatorname{Aut}\mathcal{N}$ *tale che*

$$\forall x \in \mathcal{N}, \forall \tau \in \mathcal{H} \setminus \{\mathrm{Id}\} : \tau(x) = x \Rightarrow x = 1.$$

Allora il prodotto semidiretto esterno $\mathcal{G} = \mathcal{N} \rtimes \mathcal{H}$, ove $\mathcal{H}$ agisce su $\mathcal{N}$ in modo naturale, è un gruppo di Frobenius.

DIMOSTRAZIONE. Sia $x \in \mathcal{N}$, e sia $h \in \mathcal{H} \setminus \{1\}$. Allora

$$xh = hx \Leftrightarrow \forall p \in \mathcal{N} : xh(p) = h(xp).$$

D'altro canto, per l'ipotesi:

$$xh(p) = h(xp) = h(x)h(p) \Rightarrow x = h(x) \Rightarrow x = 1.$$

Se ora $t \in \mathcal{G} \setminus \mathcal{N}$, si ha $t = nh$ con $h \in \mathcal{H} \setminus \{1\}$, e quindi:

$$xt = tx \Rightarrow \forall p \in \mathcal{N} : (xt)(p) = (tx)(p) = t(xp),$$

cioè:

$$xnh(p) = nh(xp) \Leftrightarrow xnh(p) = nh(x)h(p) \Leftrightarrow xn = nh(x) \Leftrightarrow h(x) = x^n.$$

D'altro canto in questo caso $h(n) = n^n = n$, e dunque $h = 1$, per l'ipotesi che esso sia un automorfismo privo di punti fissi, assurdo. Da queste considerazioni segue che:

$$\forall x \in \mathcal{N} : \mathrm{C}_{\mathcal{G}}(x) \leq \mathcal{N},$$

ovvero che $\mathcal{G}$ è un gruppo di Frobenius. □

Osservazione. Il richiedere l'esistenza di un gruppo di automorfismi privi di punti fissi è una condizione piuttosto restrittiva per la struttura di $\mathcal{N}$, come si è visto nel teorema di Thompson.

La classe dei gruppi di Frobenius gode di alcune proprietà che, pur essendo conseguenze pressochè immediate della definizione, non risultano di per sè evidenti.

Scopo del prosieguo di questa sezione è presentare alcuni di questi risultati.

Teorema 2.14. *Sia $\mathcal{G}$ un gruppo di Frobenius; allora $\mathrm{Z}(\mathcal{G})$ è banale.*

DIMOSTRAZIONE. Consideriamo $\mathcal{G}$ come gruppo di permutazioni agente su di un insieme X. Siano $g, h \in \mathcal{G}$ due elementi tali che $\mathrm{Fix}(g) = \{a\}$ e $\mathrm{Fix}(h) = \{b\}$, con $a \neq b$. Prendiamo $\theta \in \mathrm{Z}(\mathcal{G})$. Poichè

θ si trova nel centro di $\mathcal{G}$, esso è fissato da ogni automorfismo interno di $\mathcal{G}$, ed in particolare

$$g^{-1}\theta g = \theta = h^{-1}\theta h.$$

Calcoliamo ora $\theta(a)$:

$$\theta(a) = g^{-1}\theta g(a) = g^{-1}\theta(a)$$

D'altro canto, per ipotesi g, e di conseguenza g^{-1}, fissa solamente a, per cui deve necessariamente essere:

$$\theta(a) = a.$$

Ragionando similmente con h e b si ottiene che deve valere anche:

$$\theta(b) = b,$$

da cui, per il teorema 2.3, $\theta = 1_{\mathcal{G}}$, che è la tesi. □

Osservazione. Il centro di $\mathcal{G}$ non è da confondersi col centro di $\mathcal{N}$, gruppo nilpotente. I gruppi nilpotenti infatti hanno sempre centro non banale.

Teorema 2.15. *Sia $\mathcal{G}$ un gruppo di Frobenius, e siano $\mathcal{N}$ ed $\mathcal{H}$ il suo nucleo ed il suo complemento rispettivamente; allora:*

$$|\mathcal{H}| \mid |\mathcal{N}| - 1$$

Dimostrazione. Sia $k \in \mathcal{N} \setminus \{1\}$ fissato, e consideriamo l'orbita di k sotto l'azione di $\mathcal{H}$

$$\Gamma_k := \{g \in \mathcal{G} : g = k^h, h \in \mathcal{H}\}.$$

Per la normalità di $\mathcal{N}$, Γ_k è interamente contenuta nel nucleo, e per il teorema 2.9, la sua cardinalità deve essere esattamante $m = |\mathcal{H}|$. (Altrimenti esisterebbero $h_1, h_2 \in \mathcal{H}$ con $h_1 \neq h_2$ e tali che $k^{h_1} = k^{h_2}$, da cui seguirebbe $k^{h_1 h_2{}^{-1}} = k$, ovvero $h_1 = h_2$, per il teorema citato)

D'altro canto due orbite o coincidono, o sono disgiunte e, ovviamente,

$$\mathcal{N} \setminus \{1\} = \bigcup_{k \in \mathcal{N} \setminus \{1\}} \Gamma_k.$$

Da questo segue che $|\mathcal{N} \setminus \{1\}| = |\mathcal{N}| - 1$ è un multiplo di $m = |\mathcal{H}|$, che è quanto richiesto. □

Lemma 2.4. *Sia $\mathcal{G}$ un gruppo di Frobenius, di nucleo $\mathcal{N}$ e complemento $\mathcal{H}$; allora:*

$$|\mathcal{N}| = |\mathcal{G} : \mathcal{H}|;$$

inoltre anche $\mathcal{H}$ è un sottogruppo di Hall di $\mathcal{G}$.

DIMOSTRAZIONE. Poichè $\mathcal{G} = \mathcal{N}\mathcal{H}$ (prodotto semidiretto interno) e $\mathcal{N} \cap \mathcal{H} = \{1\}$, allora $|\mathcal{G}| = |\mathcal{N}||\mathcal{H}|$. Ne segue la prima parte della tesi. Tenuto conto che l'indice di $\mathcal{H}$ coincide con l'ordine di $\mathcal{N}$, e che l'ordine di $\mathcal{H}$deve allora necessariamente essere uguale all'indice di $\mathcal{N}$, e che questi due devono essere coprimi, si ha che $\mathcal{H}$ è di Hall in $\mathcal{G}$. □

Teorema 2.16. *Sia al solito $\mathcal{G}$ un gruppo di Frobenius di nucleo $\mathcal{N}$ e complemento $\mathcal{H}$. Allora $\mathcal{N}$ agisce in modo regolare*[11] *sull'insieme dei complementi*

$$\mathcal{F} := \{\mathcal{H}^x : x \in \mathcal{G}\}.$$

DIMOSTRAZIONE. Siano $\mathcal{H}^{x_1}$ ed $\mathcal{H}^{x_2}$ due elementi distinti di $\mathcal{F}$. Poichè $G = \mathcal{H}\mathcal{N}$ si potrà sempre scrivere $x_i = h_i n_i$ con $i = 1, 2$ e $n_i \in \mathcal{N}$ e $h_i \in \mathcal{H}$. Allora:

$$\mathcal{H}^{x_i} = \mathcal{H}^{h_i n_i} = \mathcal{H}^{n_i},$$

per cui

$$\mathcal{H}^{x_1} = \mathcal{H}^{x_2} \Leftrightarrow \mathcal{H}^{n_1} = \mathcal{H}^{n_2},$$

cioè $\mathcal{F}$ si può scrivere come:

$$\mathcal{F} = \{\mathcal{H}^n : n \in \mathcal{N}\}.$$

Allora l'applicazione ϕ che associa ad un elemento del nucleo il coniugato mediante quell'elemento del complemento $\mathcal{H}$ induce una azione di $\mathcal{N}$ transitiva su $\mathcal{F}$. La stretta 1-transitività scende a questo

[11] i.e. strettamente 1-transitivo

punto da considerazioni di ordine, in quanto per il lemma precedente $|\mathcal{F}| = |\mathcal{N}|$. □

Corollario 2.3. *Sia $\mathcal{G}$ un gruppo di Frobenius; se $x \in \mathcal{G} \backslash \mathcal{N}$, allora*

$$\mathrm{C}_{\mathcal{G}}(x) \cap \mathcal{N} = \{1\}$$

DIMOSTRAZIONE. Se $x \in \mathcal{G} \setminus \mathcal{N}$, allora $\exists n \in \mathcal{N}$ tale che $x^n \in \mathcal{H}$. Ora, per il teorema precedente [12].

$$\mathrm{C}_{\mathcal{G}}(x^n) \cap \mathcal{N} = \{1\}.$$

Ma $\mathrm{C}_{\mathcal{G}}(x^n) = (\mathrm{C}_{\mathcal{G}}(x))^n$, e allora:

$$\mathrm{C}_{\mathcal{G}}(x) \cap \mathcal{N} = (\mathrm{C}_{\mathcal{G}}(x^n))^{n^{-1}} \cap \mathcal{N} = (\mathrm{C}_{\mathcal{G}}(x^n) \cap \mathcal{N})^{n^{-1}} = \{1\}^{n^{-1}} = \{1\}.$$

□

5. Sottogruppi di un gruppo di Frobenius

È possibile caratterizzare abbastanza bene le proprietà cui devono soddisfare i sottogruppi di un gruppo di Frobenius. Abbiamo i seguenti risultati:

Teorema 2.17. *Sia $\mathcal{G}$ un gruppo finito di Frobenius, e sia $M \lhd \mathcal{G}$ un suo sottogruppo. Allora, chiamato $\mathcal{N}$ il nucleo di $\mathcal{G}$, si ha $M \lhd \mathcal{N}$ oppure $\mathcal{N} \lhd M$.*

DIMOSTRAZIONE. Sia $\mathcal{H}$ un complemento di $\mathcal{N}$, e supponiamo $\exists x \in M \setminus \mathcal{N}$. Allora, per il corollario 2.3 $\mathrm{C}_{\mathcal{G}}(x) \cap \mathcal{N} = \{1\}$.

Se poniamo $\mathrm{Cl}_{\mathcal{G}}(x) := \{x^g : g \in \mathcal{G}\}$, ne segue[13]

$$|\mathcal{N}| = |G : H| \Big| |Cl_x|$$

Ma $Cl_x \subseteq M$, dal che segue

$$|\mathcal{N}| \Big| |M|.$$

[12]in quanto $h \in \mathrm{C}_{\mathcal{G}}(x) \Leftrightarrow x^h = x$ e $\mathcal{N}$agisce in modo strettamente 1-transitivo sugli H^i

[13]basta considerare che $\mathrm{Cl}_{\mathcal{G}}(x)$ è un sottoinsieme normale di $\mathcal{G}$, ed $\mathcal{N}$ agisce su di esso in modo privo di punti fissi, in quanto ha intersezione banale col centralizzante di un qualsiasi suo elemento. La tesi segue da un ragionamento affine a quello esposto nella dimostrazione del teorema 2.15.

Poichè $\mathcal{N}$ è un sottogruppo di Hall in $\mathcal{G}$ si ha che ogni suo p-sylow deve essere anche un p-sylow di M, e $\mathcal{N}$ stesso, essendo nilpotente[14], deve coincidere con il prodotto diretto di tali p-sylows. Per conseguenza $\mathcal{N} < M$. □

Teorema 2.18. *Sia $\mathcal{G}$ un gruppo di Frobenius con nucleo $\mathcal{N}$ e complemento $\mathcal{H}$; allora valgono i seguenti fatti:*

1. *Se esiste H_1 tale che $\{1\} < H_1 < \mathcal{H}$, allora $H_1\mathcal{N}$ è un gruppo di Frobenius di nucleo $\mathcal{N}$.*
2. *Se esiste $K \lhd \mathcal{G}$ tale che $\{1\} < K < \mathcal{N}$, allora $\mathcal{G}/K$ è di Frobenius con nucleo $\mathcal{N}/K$.*
3. *Se esistono K e H_1 tali che $\{1\} < K \subseteq \mathcal{N}$ e $\{1\} < H_1 \subseteq \mathcal{H}$ con inoltre la condizione $H_1 \subseteq \mathrm{N}_{\mathcal{G}}(K)$ allora H_1K è un gruppo di Frobenius con nucleo K.*

DIMOSTRAZIONE.

- Evidentemente la proprietà 1. è conseguenza della 3.
- Dimostriamo dunque la 3:

  sicuramente $H_1K \subseteq \mathcal{G}$; se $x \in K \setminus \{1\}$, allora

$$\mathrm{C}_{H_1K}(x) \subseteq \mathcal{H}_1K \cap \mathcal{N} = K$$

  da cui scende la tesi H_1K di Frobenius con nucleo K.
- Verifichiamo ora la 2 (per assurdo).

  Siano $x \in \mathcal{H} \setminus \{1\}$ e $yK \in \mathcal{N}/K$, tali che $x \in \mathrm{C}_{\mathcal{G}/K}(yK)$. Possiamo supporre senza perdere in generalità che l'ordine di x sia un numero primo p. Ora: il coniugio mediante x induce una permutazione sull'insieme yK, in quanto K è normale; d'altro canto il numero degli elementi di yK non può essere divisibile per p poichè $\mathcal{H}$ è un sottogruppo di Hall di $\mathcal{G}$; allora la permutazione indotta da x dovrebbe fissare almeno un elemento di $\mathcal{N}$ diverso dall'identità, contro l'ipotesi che $\mathcal{G}$ sia di Frobenius. Dunque

[14]per il teorema di Thompson

deve essere

$$\forall yK \in \mathcal{N}/K : \mathrm{C}_{\mathcal{G}/K}(yK) \subseteq \mathcal{N}/K$$

che è la tesi.

$\square$

Teorema 2.19. *Se $\mathcal{G}$ è un gruppo di Frobenius, allora esiste un sottogruppo di Frobenius $B < \mathcal{G}$ con nucleo K, p-gruppo abeliano elementare, e complemento L di ordine primo.*

Dimostrazione. Supponiamo che $\mathcal{G}$ non abbia sottogruppi propri di Frobenius. Chiamiamo allora $\mathcal{N}$ il nucleo di $\mathcal{G}$, ed $\mathcal{H}$ un complemento per $\mathcal{N}$.

Se esiste un A tale che $\{1\} < A < \mathcal{H}$, allora, per il teorema precedente $\mathcal{N}A$ sarebbe un sottogruppo proprio di Frobenius di $\mathcal{G}$, contro l'ipotesi. Dunque $\mathcal{H}$ deve essere di ordine primo.

Sia ora $\{1\} \neq P \in \mathrm{Syl}(\mathcal{N})$. Per l'argomento di Frattini (Teorema 1.10)

$$\mathcal{G} = \mathrm{N}_{\mathcal{G}}(P)\mathcal{N}.$$

D'altro canto se $\mathcal{H}$ è di ordine primo, allora esso deve essere non solo di Hall, ma anche di Sylow in $\mathcal{G}$. Dunque

$$|\mathcal{H}| \,\big|\, |\mathrm{N}_{\mathcal{G}}(\mathcal{N})|$$

e qualche coniugato di $\mathcal{H}$, diciamo $\mathcal{H}$ stesso, deve essere contenuto in $\mathrm{N}_{\mathcal{G}}(P)$. Per il teorema precedente $P\mathcal{H}$ è un gruppo di Frobenius, ma, per l'ipotesi che $\mathcal{G}$ non ammetta sottogruppi propri di Frobenius, allora dobbiamo avere $P = \mathcal{N}$, e $\mathcal{N}$ è un p-gruppo per qualche primo p.

Ora se $\mathcal{N}$ ha un qualche sottogruppo caratteristico non banale Q, allora $Q \lhd \mathcal{G}$ e, per conseguenza, $Q\mathcal{H}$ sarebbe un gruppo di Frobenius più piccolo di $\mathcal{G}$. Dunque $\mathcal{N}$ deve essere caratteristicamente semplice e quindi risulta un p-gruppo abeliano elementare. $\square$

Osserviamo che il nucleo $\mathcal{N}$ di un gruppo di Frobenius non può contenere a sua volta gruppi di Frobenius; infatti $\mathcal{N}$ è, per il teorema di Thompson, nilpotente, e, come conseguenza, ha centro non banale, come pure tutti i suoi sottogruppi propri; d'altro canto il teorema 2.14 ci assicura che per ogni gruppo $\mathcal{G}$ di Frobenius $Z(\mathcal{G}) = \{1\}$, da cui scende la tesi.

Si può dimostrare che nemmeno un complemento $\mathcal{H}$ di $\mathcal{N}$ può contenere sottogruppi di Frobenius. Per procedere a ciò abbiamo bisogno di due lemmata:

Definizione 2.14. Una rappresentazione A di un gruppo finito $\mathcal{G}$ su di un campo $\mathbb{F}$ si dice **assolutamente irriducibile** se e solo se è irriducibile su ogni estensione di grado finito di $\mathbb{F}$.

Lemma 2.5. *Sia $\mathbb{F} = \mathbb{R}$ oppure $\mathbb{F} = \mathbb{C}$. Sia D una rappresentazione di un gruppo finito $\mathcal{G}$ su $\mathbb{F}$, e supponiamo che la caratteristica di $\mathbb{F}$ non divida $|\mathcal{G}|$. Allora esiste un campo $\mathbb{K}$, estensione di dimensione finita di $\mathbb{F}$, tale che $D = \sum_i D_i$ ove ogni D_i è una rappresentazione assolutamente irriducibile di $\mathcal{G}$ su $\mathbb{K}$.*

Dimostrazione. (Per induzione sul grado della rappresentazione)

Se D è assolutamente irriducibile, allora non c'è nulla da dimostrare; altrimenti esiste una estensione finita $\mathbb{F}_1$ di $\mathbb{F}$ su cui D è riducibile. Per il teorema di Maschke[15] si ha $D = D' + D''$ su $\mathbb{F}_1$ con $\deg(D') < \deg(D)$. Per ipotesi induttiva esiste una estensione finita $\mathbb{F}_2$ di $\mathbb{F}_1$ tale che su di essa $D' = \sum_i D_i$, e i D_i sono assolutamente irriducibili. Ancora per l'ipotesi induttiva esiste una estensione finita $\mathbb{K}$ di $\mathbb{F}_2$ tale che su essa $D'' = \sum_j D''_j$, con i D''_j assolutamente irriducibili. Allora $\mathbb{K}$ è una estensione finita di $\mathbb{F}$, e D è somma diretta di rappresentazioni assolutamente irriducibili su di esso. □

Lemma 2.6. *Se D è una rappresentazione assolutamente irriducibile di un gruppo abeliano finito $\mathcal{G}$ su di un campo $\mathbb{F}$ la cui caratteristica non divide $|\mathcal{G}|$, allora* $\deg(D) = 1$.

[15]tale teorema afferma che se V è un $\mathbb{F}\mathcal{G}$-modulo e $U < V$ è un suo $\mathbb{F}\mathcal{G}$-sottomodulo, allora esiste $W < V$, W $\mathbb{F}\mathcal{G}$-sottomodulo, tale che

$$V = U \oplus W.$$

Per ulteriori dettagli si può vedere [**JL93**], cap.8.

Omettiamo la dimostrazione[16].

Teorema 2.20. *Sia $\mathcal{G}$ un gruppo di Frobenius con nucleo $\mathcal{N}$. Se $\mathcal{H}$ è un complemento di $\mathcal{N}$, allora $\mathcal{H}$ non contiene gruppi di Frobenius.*

DIMOSTRAZIONE. (per assurdo)

Sia $\mathcal{G}$ un controesempio di ordine minimo; per il teorema 2.19 $\mathcal{H}$ deve essere di Frobenius con nucleo Q abeliano elementare e un complemento K (di Q in $\mathcal{H}$) di ordine primo. Sia $P \in \mathrm{Syl}(\mathcal{N})$, tale che $P \neq \{1\}$; allora, per l'argomento di Frattini (Th. 1.10):

$$|\mathcal{H}| \,\big|\, |\mathrm{N}_{\mathcal{G}}(P)|.$$

Ora: $\mathrm{N}_{\mathcal{G}}(P) \cap \mathcal{N}$ è un sottogruppo normale di Hall di $\mathrm{N}_{\mathcal{G}}(P)$; allora, per il teorema di Schur-Zassenhaus, deve ammettere un complemento S, tale che

$$\mathrm{N}_{\mathcal{G}}(P) = (\mathrm{N}_{\mathcal{G}}(P) \cap \mathcal{N})S,$$

e, evidentemente, $|S| = |\mathcal{H}|$ e $\mathcal{N}S = \mathcal{G}$. Inoltre

$$S \simeq \mathcal{G}/\mathcal{N} \simeq \mathcal{H},$$

e dunque è di Frobenius. Consideriamo ora il gruppo PS. Poichè $P < \mathcal{N}$

$$\forall x \in P : \mathrm{C}_{PS}(x) \subseteq (PS \cap \mathcal{N}) = P$$

anche PS deve essere di Frobenius. Per la minimalità di $\mathcal{G}$, si deve allora verificare che $\mathcal{N} = P$; $\mathcal{N}$ risulta allora essere un p-gruppo, per qualche p. Ma $\mathcal{N}$ deve anche essere caratteristicamente semplice[17], ed è dunque un p-gruppo abeliano elementare e, per la medesima ragione risulta anche un sottogruppo normale minimo di $\mathcal{G}$.

Ora: $\mathcal{H}$ ammette una rappresentazione fedele A, come gruppo irriducibile di trasformazioni lineari su $\mathcal{N}$, ove si consideri il p-gruppo abeliano elementare $\mathcal{N}$ come spazio vettoriale sul campo finito $\mathbb{Z}_p$.

[16] essa può trovarsi su [**Sco64**], pagg.352,353

[17] altrimenti a norma del teorema 2.18 dovrebbe essere possibile costruire un gruppo di Frobenius con la medesima proprietà di $\mathcal{G}$, ma di esso strettamente più piccolo

Per il lemma 2.5 deve esistere un campo finito $\mathbb{F}$, estensione di $\mathbb{Z}_p$ tale che A è somma diretta di rappresentazioni assolutamente irriducibili di $\mathcal{H}$ su $\mathbb{F}$. Sia B una di tali rappresentazioni irriducibili, e chiamiamo V lo $\mathbb{F}$-spazio vettoriale su cui essa agisce.

A meno di una ulteriore estensione di $\mathbb{F}$ possiamo assumere che

$$V = V_1 + \ldots + V_n$$

ove i singoli V_i sono tutti Q-spazi irriducibili. Per il lemma 2.6 dobbiamo avere

$$\forall i : \dim(V_i) = 1,$$

sicchè per $x \in Q$, $B(x)$ deve essere una matrice "scalare" su ogni V_i. Combinando assieme diversi V_i, possiamo scrivere:

$$V = W_1 + \ldots + W_r$$

ove ogni W_i è un sottospazio massimale di V tale che $B(x)$ è una matrice scalare per ogni $x \in Q$.

Se $K = \langle y \rangle$ (K è di ordine primo!), $x \in Q$, e $v \in W_i$, facendo agire gli elementi mediante la rappresentazione B, tenuto conto che $yxy^{-1} \in Q$:

$$v(yx) = v(yxy^{-1}y) = cvy$$

con $c \in \mathbb{F}$ (i.e. c si può vedere come matrice scalare), e c non dipendente da v. Ne segue che per ogni i deve esistere un j tale che

$$W_i y \subseteq W_j.$$

D'altro canto se per qualche i fosse $W_i y < W_j$, allora $Vy < V$, assurdo in quanto nessuna delle trasformazioni lineari che appaiono in una rappresentazione può essere singolare. Ne discende:

$$W_i y = W_j.$$

Ora, poichè

$$\mathcal{H} = QK = \langle Q, K \rangle = \langle Q, y \rangle$$

e V è Q-irriducibile, ne segue che y deve permutare ciclicamente tutti i W_i. Allora, fissato $w \in W_1 \setminus \{1\}$, e posto $r = |K|$, si ha che l'elemento

$$v = w + wy + \ldots + wy^{r-1}$$

deve essere fissato mediante y e diverso da 0. Per conseguenza la trasformazione lineare $B(y)$ deve avere almeno un autovalore pari ad 1. D'altro canto gli autovalori sono invarianti per coniugio, e B è (equivalente ad) un addendo diretto di A. Per conseguenza $A(y)$ ha un autovalore pari ad 1. Esiste allora un autovettore $z \in \mathcal{N}$ tale che per $y \in K \setminus \{1\} < \mathcal{H}$

$$y^{-1}zy = z,$$

assurdo, contro la definizione di gruppo di Frobenius. Segue la tesi.

□

Sinora si è sempre parlato "del" nucleo di un gruppo di Frobenius, ma non ne si è mai dimostrata l'effettiva unicità. Il seguente risultato è finalizzato a colmare tale lacuna.

Teorema 2.21. *Un gruppo di Frobenius ammette un unico nucleo.*

Dimostrazione. Sia $\mathcal{G}$un gruppo di Frobenius. Supponiamo che $\mathcal{N}$ e $\mathcal{N}_1$ siano due suoi nuclei, e chiamiamo $\mathcal{H}$ un complemento per $\mathcal{N}$. A norma del teorema 2.17 possiamo supporre senza perdere generalità $\mathcal{N} \subseteq \mathcal{N}_1$. Allora: $\mathcal{N}_1 = \mathcal{M}K$ ove

$$K = \mathcal{H} \cap \mathcal{N}_1 \lhd \mathcal{H}.$$

Ora, se $x \in K$, allora $\mathrm{C}_{\mathcal{H}}(x) \subseteq \mathcal{H} \cap \mathcal{N}_1 = K$. Per conseguenza se $\mathcal{N} < \mathcal{N}_1$ si ha che $\mathcal{H}$ deve essere di Frobenius con nucleo K, contro il teorema precedente. Allora necessariamente $\mathcal{N} = \mathcal{N}_1$, che è la tesi. □

È possibile caratterizzare i p-Sylow del complemento $\mathcal{H}$. Sono necessarii un teorema ed alcuni lemmata preliminari:

Lemma 2.7. *Sia H un gruppo di automorfismi di un gruppo abeliano finito A; supponiamo che H sia il prodotto semidiretto $M \rtimes \langle\sigma\rangle$*

ove $\beta\sigma$ è di ordine p (con p numero primo) e privo di punti fissi per ogni $\beta \in M$. Se inoltre $|A|$ e $|M|$ risultano essere coprimi, allora

$$M = \{1\}$$

La dimostrazione può essere ritrovata su [**Rob82**], pag.296.

Definizione 2.15. Un gruppo finito si dice di essere un **gruppo di quaternioni generalizzati** se e solo se esso ammette una presentazione del tipo

$$\langle x, y | x^{2n-1} = 1, y^2 = x^{2n-2}, y^{-1}xy = x^{-1} \rangle.$$

In tale caso lo si indicherà col simbolo Q_{2^n}.

Definizione 2.16. Un gruppo D_{2n} si dice **gruppo diedrale** se ammette la seguente presentazione:

$$D_{2n} := \langle a, b | a^2 = 1; b^n = 1, aba = b^{-1} \rangle$$

Si verifica che tale gruppo coincide con quello delle simmetrie dello n-agono regolare.

Teorema 2.22. *Un gruppo di ordine p^n possiede un sottogruppo ciclico massimale se e solo se appartiene ad uno dei seguenti tipi:*

1. *è un gruppo ciclico di ordine p^n;*
2. *è il prodotto diretto di un gruppo ciclico di ordine p con uno di ordine p^{n-1};*
3. *è il gruppo diedrale D_{2^n}, con $n > 2$;*
4. *è il gruppo di quaternioni generalizzati Q_{2^n}, con $n > 2$;*
5. *è il gruppo semidiedrale $\left\langle x, a | x^2 = 1 = a^{2n-1}; a^x = a^{2^{n-2}-1} \right\rangle$, con $n > 2$;*
6. *ha la presentazione $\left\langle x, a | x^p = 1 = a^{p^{n-1}}, a^x = a^{1+p^{n-2}} \right\rangle$, con $n > 2$.*

Per la dimostrazione vedi [**Rob82**], pagg. 136-138.

Lemma 2.8. *Un p-gruppo finito $\mathcal{G}$ ammette un unico sottogruppo di ordine p se e solo se $\mathcal{G}$ è ciclico o di quaternioni generalizzati*

DIMOSTRAZIONE. In primo luogo è vero che i p-gruppi ciclici e i gruppi di quaternioni generalizzati godono della proprietà richiesta.

Supponiamo ora che $\mathcal{G}$ abbia ordine p^n e supponiamo che esista solo un sottogruppo di $\mathcal{G}$ avente ordine p.

- Se $\mathcal{G}$ è abeliano, il teorema di Frobenius-Stickelberger[18] implica che esso deve essere anche ciclico.
- Supponiamo che $\mathcal{G}$ non sia abeliano e che p sia dispari. Sia H un sottogruppo massimale di $\mathcal{G}$. Ragionando per induzione sull'ordine, si vede che H deve essere ciclico; $\mathcal{G}$ ha quindi un sottogruppo ciclico massimale. Esaminando la classificazione dei p-gruppi con sottogruppi ciclici massimali (teorema 2.22) si verifica che un $\mathcal{G}$ con tali proprietà non può esistere, e che dunque $p = 2$.
- Sia dunque $\mathcal{G}$ non abeliano e $p = 2$. Sia A un sottogruppo abeliano normale massimale in $\mathcal{G}$. Allora A deve essere ciclico (diciamo $A = \langle a \rangle$) e, per la nilpotenza di $\mathcal{G}$, $A = \mathrm{C}_{\mathcal{G}}(A)$.

  Sia $xA \in \mathcal{G}/A$ un elemento di ordine 2. Per la massimalità di A, $\langle A, x \rangle$ non può essere abeliano ed ha un unico sottogruppo ciclico di indice 2; allora per il teorema 2.22 deve essere un gruppo di quaternioni generalizzati, in quanto in tutti altri casi esiste più di sottogruppo di ordine 2. Da questo scende $a^x = a^{-1}$, il che implica che $\mathcal{G}/A$ possieda un unico elemento di ordine 2.

  Ora $\mathcal{G}/A$ è isomorfo con un sottogruppo di $\mathrm{Aut}(A)$, che a sua volta risulta isomorfo al gruppo costituito degli elementi unitari di $\mathbb{Z}_{2^m}$ ove $2^m = |A|$. Ma allora $\mathcal{G}/A$ deve essere abeliano, e quindi ciclico.

  Si verifica che -1 non è un quadrato modulo 2^m, tranne nel caso $m = 1$, che nelle nostre ipotesi non può verificarsi (implicherebbe $A < \mathrm{Z}(\mathcal{G})$). Allora xA genera $\mathcal{G}/A$ che risulta dunque avere ordine 2; per conseguenza $\mathcal{G}$ è un gruppo di quaternioni generalizzati.

[18] Teorema di struttura per i gruppi abeliani finiti: asserisce che un gruppo $\mathcal{G}$ è abeliano e finito se e solo se è la somma diretta di un numero finito di gruppi ciclici aventi ordine primo; la dimostrazione può essere ritrovata su [**Rob82**], pagg.99-100.

□

Lemma 2.9. *Sia $\mathcal{G}$ un gruppo finito, e sia $\mathcal{H}$ un gruppo di automorfismi di $\mathcal{G}$ privi di punti fissi. Allora ogni sottogruppo di $\mathcal{H}$ di ordine pq ove p e q sono primi, non necessariamente distinti, è ciclico; inoltre i p-Sylow di $\mathcal{H}$ sono ciclici se $p \neq 2$, ciclici o quaternioni generalizzati se $p = 2$.*

DIMOSTRAZIONE. Supponiamo che S sia un sottogruppo di $\mathcal{H}$ di ordine pq e che S non sia ciclico. Allora S ammette certamente un q-sylow Q, tale che $Q \lhd S$[19]. Chiaramente $S = QP$, ove $P < S$ è di ordine p. Sia ora R un r-Sylow non banale di $\mathcal{G}$; sappiamo per il teorema 2.11 che $\mathcal{G}$ deve essere nilpotente; quindi $R \lhd \mathcal{G}$. Evidentemente $R^S = R$.

- Se fosse anche $r = q$, allora $R \rtimes Q$ sarebbe nilpotente[20], e avrebbe centro non banale, cosa che renderebbe impossibile per $\mathcal{H}$ l'avere una azione priva di punti fissi su $\mathcal{G}$.
- Supponiamo allora $r \neq q$. Sia $P = \langle \alpha \rangle$, e supponiamo $\beta \in Q$.I Allora l'ordine di $\alpha\beta$ non può coincidere con pq, in quanto $|S| = pq$ e S è per ipotesi non ciclico. Allora $|\alpha\beta| = p$. Poichè il centro di R è caratteristico in R, possiamo considerare S come gruppo di automorfismi privi di punti fissi del gruppo abeliano $\mathrm{Z}(R)$; il lemma 2.7 implica $Q = \{1\}$, assurdo.

In tale modo abbiamo dimostrato la prima parte della tesi.

Sia ora $P \in \mathrm{Syl}_p(\mathcal{H})$. Per quanto appena verificato P non può contenere sottogruppi di ordine p^2 che non siano ciclici; d'altro canto,

---

[19]in quanto, supponendo $p < q$, otteniamo, a norma dei teoremi di Sylow, che il numero n_q dei q-Sylow di S deve essere tale che

$$n_q \equiv 1 \mod q \& n_q | pq \Rightarrow n_q | p,$$

ma p è primo. Non può essere $n_q = p \neq 1$, poichè ciò implicherebbe

$$q | (p-1),$$

assurdo, contro l'ipotesi $q > p$, quindi $n_q = 1$, che è la tesi, essendo tutti i q-Sylow coniugati fra loro; se $p = q$ non c'è nulla da dimostrare.

[20]in quanto q-gruppo

essendo P un p-gruppo,

$$\exists K < Z(P) : |K| = p.$$

Se P contenesse un altro sottogruppo L di ordine p, allora $KL = K+L$ sarebbe non ciclico, assurdo. Dunque P contiene solo un sottogruppo di ordine p; allora per il lemma 2.8 si ha la seconda parte della tesi.

$\square$

Osservazione. Per una dimostrazione differente di questo lemma che non richiede il teorema di Thompson, ma è limitata al caso in cui $\mathcal{G} \rtimes \mathcal{H}$ è di Frobenius vedi [**Sco64**], pag.355.

Teorema 2.23. *Sia $\mathcal{G}$ un gruppo di Frobenius avente complemento $\mathcal{H}$ e nucleo $\mathcal{N}$. Se $P \in \mathrm{Syl}_p(\mathcal{H})$ valgono i seguenti fatti:*

1. *se $p \neq 2$, allora P è ciclico;*
2. *se $p = 2$, allora P è ciclico oppure un gruppo di quaternioni generalizzati.*

DIMOSTRAZIONE. $\mathcal{H}$ agisce come gruppo di automorfismi privo di punti fissi su $\mathcal{N}$. Dal lemma precedente scende la tesi. $\square$

6. Il caso 2-transitivo

Definizione 2.17. Sia $\mathcal{G}$ un gruppo di permutazioni su di un insieme X. $\mathcal{G}$ si dice **transitivo** (o **1-transitivo**) su X se

$$\forall x, y \in X : \exists g \in \mathcal{G} : g(x) = y$$

Definizione 2.18. Sia k un numero naturale diverso da 0. Un gruppo $\mathcal{G}$ si dice k-transitivo su di un insieme finito X se e solo se per ogni coppia di k-ple ordinate di elementi di X $(\alpha_1, \dots, \alpha_k)$, $(\beta_1, \dots, \beta_k)$ tali che

$$i \neq j \Rightarrow \alpha_i \neq \alpha_j \& \beta_i \neq \beta_j$$

esiste sempre almeno un $g \in \mathcal{G}$ tale che

$$\forall i : 1 \leq i \leq k : \beta_i = g(\alpha_i).$$

Teorema 2.24. *Sia $\mathcal{G}$ un gruppo di permutazioni su di un insieme X finito, con $|X| > 2$; supponiamo che $\mathcal{G}$ sia strettamente 2-transitivo; allora $\mathcal{G}$ è di Frobenius.*

DIMOSTRAZIONE. Poichè $\mathcal{G}$ è strettamente due transitivo, una permutazione è individuata dalla sua azione su due elementi distinti di X. Allora se

$$\alpha \in \mathcal{G} \& |\operatorname{Fix}(\alpha)| > 1 \Rightarrow \alpha = 1.$$

Lo stabilizzante di un elemento $x \in X$, d'altro canto consta di esattamente $|X| - 1$ elementi[21]. e dunque non è banale; per il teorema 2.3 $\mathcal{G}$ è un gruppo di Frobenius. □

Caratterizziamo ora i gruppi strettamente 2-transitivi.

Teorema 2.25. *Un gruppo $\mathcal{G}$ di Frobenius con nucleo $\mathcal{N}$ e complemento $\mathcal{H}$ possiede una azione strettamente 2-transitiva se e solo se $|\mathcal{H}| = |\mathcal{N}| - 1$.*

DIMOSTRAZIONE. Sia X un insieme su cui $\mathcal{G}$ possiede una azione fedele e poniamo $n = |X|$.

- Se $\mathcal{G}$ è strettamente 2-transitivo, allora, $|\mathcal{G}| = n(n-1)$ e, per quanto visto nel teorema precedente, $|\mathcal{H}| = n - 1$; per conseguenza, poichè $\mathcal{N} \cap \mathcal{H} = \{1\}$, deve essere anche $|\mathcal{N}| = n$, da cui segue la tesi.
- $\mathcal{G}$ può avere al più azione strettamente 2-transitiva su X[22]; per motivi di ordine si ha la tesi.

□

Si è già dimostrato che se in un gruppo di Frobenius $\mathcal{G}$ uno dei complementi $\mathcal{H}$ ha cardinalità pari, allora il nucleo deve essere abeliano. Verifichiamo che nel caso 2-transitivo vale il seguente teorema:

Teorema 2.26. *Sia $\mathcal{G}$ un gruppo di Frobenius tale che $|\mathcal{H}| = |\mathcal{N}| - 1$; allora il nucleo $\mathcal{N}$ è abeliano.*

[21] $\mathcal{G}$ deve essere regolare su $X \setminus \{x\}$

[22] altrimenti esisterebbe almeno un elemento $\gamma \in \mathcal{G} \setminus \{1\}$ tale che $\operatorname{Fix} \gamma > 1$

DIMOSTRAZIONE. Sia $n \in \mathcal{N} \setminus \{1\}$,e poniamo $C = \mathrm{C}_{\mathcal{G}}(x)$. Allora $C \leq \mathcal{N}$ e

$$|\mathcal{G} : C| \geq |\mathcal{G} : \mathcal{N}| = |\mathcal{H}| = n - 1.$$

D'altro canto l'indice del centralizzante di un elemento in $\mathcal{G}$ deve coincidere con la cardinalità dell'orbita di quello stesso elemento in $\mathcal{G}$, per cui:

$$|\mathcal{G} : C| = |x^{\mathcal{G}}| \leq n - 1.$$

Ma allora

$$|\mathcal{G} : C| = n - 1$$

da cui segue immediatamente

$$|C| = n = |\mathcal{N}|.$$

Quindi

$$\forall x \in \mathcal{N} \setminus \{1\} : C = C_{\mathcal{G}}(x) = \mathcal{N},$$

condizione equivalente all'abelianità di $\mathcal{N}$. $\square$

7. Il caso $\frac{3}{2}$-transitivo

Abbiamo visto che tutti i gruppi strettamente 2-transitivi sono di Frobenius con nucleo abeliano; un gruppo strettamente 1-transitivo, d'altro canto non può essere di Frobenius, in quanto lo stabilizzante di un qualsiasi punto sarebbe banale.

Forniamo alcune definizioni:

Definizione 2.19. Un gruppo di permutazioni si dice **$\frac{1}{2}$-transitivo** se tutte le sue orbite hanno la medesima cardinalità $n > 1$.

Definizione 2.20. Similmente un gruppo di permutazioni si dice **$(k + \frac{1}{2})$-transitivo**, con $k > 1$ numero naturale, se è transitivo, e lo stabilizzante di un punto è $(k - \frac{1}{2})$-transitivo.

Si verifica[23] che un gruppo k-transitivo è anche $(k-\frac{1}{2})$-transitivo, mentre, ovviamente, ogni gruppo $(k+\frac{1}{2})$-transitivo è anche k-transitivo: le definizioni sopra fornite hanno dunque un senso.

Sappiamo già che un gruppo, se è di Frobenius, deve essere almeno 1-Transitivo e non regolare. In effetti:

Teorema 2.27. *Sia $\mathcal{G} = \mathcal{N} \rtimes \mathcal{H}$ un gruppo di Frobenius, agente su di un insieme X; allora $\mathcal{G}$ è almeno $\frac{3}{2}$-transitivo.*

DIMOSTRAZIONE. Sappiamo che il complemento $\mathcal{H}$ può essere visto come lo stabilizzante di un punto $x \in X$. Poichè il grado minimo di $\mathcal{G}$ è $n-1$, $\mathcal{H}$ deve agire in modo semiregolare su $X \setminus \{x\}$. Questo implica[24] in particolare:

$$\forall y \in X \setminus \{x\} : |y^{\mathcal{H}}| = |\mathcal{H}|,$$

che è la tesi. $\square$

Definizione 2.21. Sia $\mathcal{G}$ un gruppo di permutazioni sull'insieme Ω. Chiamiamo **blocco** di $\mathcal{G}$ un insieme $\Psi \subseteq \Omega$ tale che $\forall g \in \mathcal{G} : \Psi^g = \Psi$ oppure $\Psi^g \cap \Psi = \emptyset$.

Evidentemente l'intero insieme Ω, $\emptyset$, ed ogni singoletto $\{\alpha\} \subseteq \Omega$ sono blocchi per ogni gruppo $\mathcal{G}$; chiamiamo tali blocchi **blocchi banali**.

Definizione 2.22. Ogni blocco non banale di un gruppo $\mathcal{G}$ viene detto **insieme di imprimitività**.

Definizione 2.23. Un gruppo $\mathcal{G}$ si dice **primitivo** se non ammette insiemi di imprimitività, i.e. se possiede solo i blocchi banali. In caso contrario $\mathcal{G}$ si dice **imprimitivo**.

Differentemente dal caso 2-transitivo prima esaminato, non è vero che tutti i gruppi $\frac{3}{2}$-transitivi siano di Frobenius; giovandoci delle precedenti definizioni possiamo però enunciare il seguente teorema:

[23] vedi [**Wie64**], pag.24
[24] vedi, ad esempio [**Wie64**], pag. 9

Teorema 2.28. *Ogni gruppo $\frac{3}{2}$-transitivo o è primitivo, oppure è di Frobenius.*

DIMOSTRAZIONE. Sia Ω un insieme con $n = |\Omega| > 2$, e sia $\mathcal{G}$ un gruppo $\frac{3}{2}$-transitivo su Ω. Poniamo $\mathcal{H} = \mathrm{St}_{\mathcal{G}}(1)$, con $1 \in \Omega$, e chiamiamo m la lunghezza di tutte le orbite di Ω sotto l'azione di $\mathcal{H}$. Supponiamo che $\mathcal{G}$ abbia un blocco di lunghezza k con $1 < k < n$ e sia dunque imprimitivo.

In queste ipotesi possiamo disporre i punti $1, \ldots, n$ di Ω in una matrice α_{ij} tale che ogni riga Ψ_i sia un blocco di $\mathcal{G}$ con lunghezza k, e, poniamo $\alpha_{11} = 1$. Ora, Ψ_1 è fissato da $\mathcal{H}$ come blocco (poichè $\mathcal{H}$ fissa 1), e dunque

$$k \equiv 1 \mod m,$$

cioè k ed m sono coprimi. Per ogni $i > 1$, $\Psi_i^{\mathcal{H}}$ è fissato da $\mathcal{H}$ e non contiene 1; per conseguenza

$$km \Big| |\Psi_i^{\mathcal{H}}|.$$

D'altro canto $|\alpha_{ij}^{\mathcal{H}}| = m$, e, per conseguenza, $|\Psi_i^{\mathcal{H}}| \leq km$, da cui

$$|\Psi_i^{\mathcal{H}}| = km,$$

che implica

$$\forall i \neq m : \alpha_{ij}^{\mathcal{H}} \cap \alpha_{im}^{\mathcal{H}} = \emptyset,$$

cioè

$$i > 1 \Rightarrow \alpha_{ij}^{\mathcal{H}} \cap \Psi_i = \alpha_{ij}.$$

Allora:

- Se $i > 1$ e $\alpha \in \Psi_i$, allora $\mathrm{St}_{\mathcal{H}}(\alpha) = \mathrm{St}_{\mathcal{G}}(1, \alpha) \leq \mathrm{St}_{\mathcal{G}}(\Psi_i)$, in quanto $\forall a \in \mathrm{St}_{\mathcal{H}}(\alpha)$:

$$\alpha_{ij}^{a} = (\alpha_{ij}^{\mathcal{H}} \cap \Psi_i)^{a} = \alpha_{ij}^{\mathcal{H}} \cap \Psi_i^{a} = \alpha_{ij}^{\mathcal{H}} \cap \Psi_i = \alpha_{ij}$$

- Sotto le stesse ipotesi del punto precedente $\mathrm{St}_{\mathcal{G}}(1, \alpha) \leq \mathrm{St}_{G}(\Psi_1)$ (basta scambiare 1 con α nel ragionamento).

- Sempre nelle ipotesi del primo punto:
$$\mathrm{St}_{\mathcal{G}}(1, \alpha) = \mathrm{St}_{\mathcal{G}}(1, \alpha_{12}) = \cdots = \mathrm{St}_{\mathcal{G}}(1, \alpha_{1k})$$
in quanto $\mathrm{St}_{\mathcal{G}}(1, \alpha) \leq \mathrm{St}_{\mathcal{G}}(\Psi_1) \leq \mathrm{St}_{\mathcal{G}}(1, \alpha_{1i})$, e dunque, per motivi di ordine[25], essi devono coincidere.
- Dal punto precedente deduciamo per l'arbitrarietà di α fuori da Ψ_1 che $\mathrm{St}_{\mathcal{G}}(1, \alpha_1 2) = \{1\}$.
- Per tutto quando visto sinora si ottiene:
$$\forall \alpha \in \Omega, \alpha \neq 1 : \mathrm{St}_{\mathcal{G}}(\alpha, 1) = \{1\}.$$

In tale modo abbiamo mostrato che il grado minimo di $\mathcal{G}$ deve essere maggiore od uguale a $n - 1$, ove n è il grado di $\mathcal{G}$. D'altro canto se $n \neq 2$ la $\frac{3}{2}$-transitività implica che $\mathcal{G}$ non possa essere regolare (i.e. di grado minimo n), dunque $\deg_{\min}(G) = n - 1$, e per il teorema 2.3, $\mathcal{G}$ deve essere di Frobenius. Se $n = 2$, si verifica che $\mathcal{G}$ è primitivo, e quindi la tesi è soddisfatta in ogni caso.

□

[25]Evidentemente nelle nostre ipotesi $|\alpha^{\mathcal{H}}| = |\alpha_{1i}^{\mathcal{H}}| = m$; un risultato generale asserisce poi che
$$|\mathcal{G}| = |\,\mathrm{St}_{\mathcal{G}}(a)||a^{\mathcal{G}}|.$$

CAPITOLO 3

Gruppi Fibrati

Definizione 3.1. Sia $\mathcal{G}$ un gruppo e $\pi(\mathcal{G})$ un insieme di sottogruppi di $\mathcal{G}$. Allora $\pi(\mathcal{G})$ si dice **partizione** o **fibrazione** di $\mathcal{G}$ se

1.
$$\{1\} \notin \pi(\mathcal{G})$$

2.
$$\bigcup_{H \in \pi(\mathcal{G})} H = \mathcal{G}$$

3.
$$\forall H_1, H_2 \in \pi(\mathcal{G}) : H_1 \neq H_2 \Rightarrow H_1 \cap H_2 = \{1\}$$

Gli elementi di $\pi(\mathcal{G})$ si diranno **componenti** della partizione, oppure **fibre** di $\mathcal{G}$.

Ogni gruppo possiede ovviamente la **partizione banale** $\{\mathcal{G}\}$.

Definizione 3.2. Un gruppo $\mathcal{G}$ si dice **fibrato** se ammette una partizione non banale.

1. Gruppi finiti con partizione

Si verifica che la proprietà di possedere una partizione per un gruppo $\mathcal{G}$ dipende solamente dalla struttura del reticolo dei suoi sottogruppi.

I risultati presentati in questa sezione, ove non diversamente indicato, sono tratti da [**Sch94**], cap 3.5, pagg. 145-156.

Per un gruppo finito la condizione di possedere una partizione non banale è molto forte; un teorema fondamentale pubblicato nel 1961 da Suzuki ([**Suz61**]) ha consentito di classificarli in modo completo.

Premettiamo alcune definizioni.

1.1. Gruppi di Hughes-Thompson.

Definizione 3.3. Sia $\mathcal{G}$ un gruppo finito, e p un numero primo; chiamiamo **sottogruppo di Hughes di $\mathcal{G}$ relativo a p** il gruppo

$$H_p(\mathcal{G}) := \langle \{x \in \mathcal{G} : x^p \neq 1\} \rangle$$

generato da tutti gli elementi di $\mathcal{G}$ di ordine diverso da p.

Relativamente ai sottogruppi di Hughes vale il seguente risultato:

Teorema 3.1. *Se $H_p(\mathcal{G}) < \mathcal{G}$, allora $H_p(G)$ è nilpotente.*

Dimostrazione. Supponiamo $H_p(\mathcal{G}) < \mathcal{G}$; allora $\mathcal{G} \setminus H_p(\mathcal{G})$ è non vuoto, ed ogni suo elemento ha ordine p. Fissiamo ora $a \in \mathcal{G} \setminus \mathcal{H}_p(\mathcal{G})$. Per ogni $x \in H_p(\mathcal{G})$ si ottiene ovviamente che $xa^{-1} \notin \mathcal{H}_p(\mathcal{G})$; allora

$$\forall x \in \mathcal{H}_p(\mathcal{G}) \setminus \{1\} : (x^a)^p = a^{-1}xa \ldots a^{-1}xa = a^{-1}x^p a \neq \{1\}.$$

per cui $x^a \in \mathcal{H}_p(\mathcal{G})$, ed a induce un automorfismo su $H_p(\mathcal{G})$. Inoltre si verifica che

$$1 = (xa^{-1})^p = xx^a \ldots x^{a^{p-1}} a^{-p} = xx^a \ldots x^{a^{p-1}}.$$

Conseguenza di questo ultimo fatto è che x^a deve essere diverso da x per ogni $x \in \mathcal{G}$. Infatti se così non fosse avremmo $x = x^a = x^{a^2} = \ldots = x^{a^{p-1}}$ e dunque

$$1 = (xa^{-1})^p = xx^a \ldots x^{a^{p-1}} = x^p$$

contro l'ipotesi $x \in H_p(\mathcal{G})$. Dunque a induce un automorfismo privo di punti fissi e di ordine primo p su $H_p(\mathcal{G})$. A questo punto applicando il teorema di Thompson (Th.2.11) si deduce immediatamente che $H_p(\mathcal{G})$ deve essere nilpotente. □

Definizione 3.4. Sia $\mathcal{G}$ un gruppo; diciamo che $\mathcal{G}$ è un **p-Hughes-Thompson gruppo** se e solo se $H_p(\mathcal{G}) \neq \mathcal{G}$. Indicheremo l'insieme dei p-Hughes-Thompson gruppi col simbolo $\mathrm{HT}(p)$.

1.2. Gruppi di Suzuki. Una importante famiglia di gruppi semplici che ammettono partizione è costituita dai **gruppi di Suzuki**, introdotti per la prima volta da M.Suzuki in [**Suz60**], e esaminati più diffusamente in [**Suz62**].

Sia n un numero intero, e poniamo $q = 2^{2n+1}$ e $r = 2^n$. Chiamiamo $\mathbb{F}$ il campo di Galois con q elementi, e sia $\theta : \mathbb{F} \to \mathbb{F}$ l'applicazione tale che

$$\forall \alpha \in \mathbb{F} : \alpha^\theta := \alpha^r.$$

Un noto risultato di Frobenius assicura che θ è in effetti un automorfismo del campo F.

Sia $\mathcal{M}$ il gruppo delle matrici 4×4 su F.

Sotto queste ipotesi forniamo le seguenti definizioni:

Definizione 3.5. Chiamiamo $S(\alpha, \beta)$ la matrice (a_{ij}) di $\mathcal{M}$ tale che

1. $i < j \Rightarrow a_{ij} = 0$
2. $\forall i : a_{i,i} := 1$
3. $a_{21} = a_{43} = \alpha^\theta$
4. $a_{31} = \beta$
5. $a_{32} = \alpha$
6. $a_{41} = \alpha^{2\theta+1} + \alpha^\theta \beta + \beta^{2\theta}$
7. $a_{42} = \alpha^{\theta+1} + \beta$

Definizione 3.6. Sia $\zeta \in \mathbb{F}$. Chiamiamo $M(\zeta)$ la matrice diagonale

$$M(\zeta) := \mathrm{Diag}(\zeta^\theta, \zeta^{1-\theta}, \zeta^{\theta-1}, \zeta^{-\theta})$$

Definizione 3.7. Siano q, M, S come sopra. Sia

$$J := \begin{bmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 0&1&0&0 \\ 1&0&0&0 \end{bmatrix}$$

Chiamiamo **gruppo di Suzuki** $\mathrm{Sz}(q)$ il sottogruppo di $\mathcal{M}$ generato nel seguente modo:

$$\mathrm{Sz}(q) := \langle \{ M(\zeta), S(\alpha, \beta), J : \zeta, \alpha, \beta \in \mathbb{F} \} \rangle$$

Si verifica che il gruppo $\mathrm{Sz}(q)$ sopra definito per q potenza dispari di 2 è un gruppo di Zassenhaus[1], semplice, ed avente ordine $q^2(q-1)(q^2+1)$.

La costruzione dei gruppi di Suzuki tosto fornita è puramente algebrica. È comunque possibile costruirli anche in modo più "geometrico", come gruppi di proiettività. Nel realizzare questa costruzione seguiremo il capitolo 4, The Suzuki Groups and their geometries, di [**Lün80**].

Per le nozioni di geometria proiettiva si può fare riferimento a [**Art57**] e [**Bae52**].

Teorema 3.2. *Sia $\mathcal{K} = \mathrm{GF}(2^t)$, con $t > 1$. Allora $\mathcal{K}$ ammette un automorfismo σ tale che*

$$\forall x \in \mathrm{GF}(2^t) : x^{\sigma^2} = x^2$$

se e solo se t è dispari. In tale caso detto automorfismo è unico.

Dimostrazione. Supponiamo $\mathrm{GF}(4) \subseteq \mathcal{K}$. È immediato verificare che il gruppo moltiplicativo $\mathrm{GF}(4)^\star$ deve constare di tutte e sole le radici cubiche in $\mathcal{K}$ dell'unità. Per conseguenza, $\forall \sigma \in \mathrm{Aut}(\mathcal{K})$:

$$\mathrm{GF}(4)^\sigma = \mathrm{GF}(4),$$

e dunque $\sigma_{|\mathrm{GF}(4)} \in \mathrm{Aut}(\mathrm{GF}(4))$. D'altro canto $|\mathrm{Aut}(\mathrm{GF}(4))| = 2$, e per conseguenza

$$\forall \sigma \in \mathrm{Aut}(\mathcal{K}), \forall x \in \mathrm{GF}(4) : x^{\sigma^2} = x.$$

Dunque $\sigma^2 \neq 2$, assurdo. Allora è condizione necessaria che $\mathrm{GF}(4) \not\subseteq \mathcal{K}$, ovvero che esista un r numero naturale maggiore di 1 tale che $t = 2r+1$.

Supponiamo ora $\mathcal{K} \simeq \mathrm{GF}(2^{2r+1})$. Sia $\sigma = 2^{r+1}$. Allora

$$x^{\sigma^2} = x^{2^{2r+2}} = x^2$$

e dunque $\mathcal{K}$ ammette un automorfismo del tipo richiesto.

[1] cioè due transitivo in cui la sola identità fissi tre elementi distinti e tale che lo stabilizzante di due punti non sia banale

Per concludere supponiamo $\alpha \in \mathrm{Aut}(\mathcal{K})$ tale che $x^{\alpha^2} = x^2$ per ogni x in $\mathcal{K}$. Per la caratterizzazione degli automorfismi dei campi di Galois, allora deve essere $x^\alpha = x^{2^t}$ con $1 \leq t < 2r+1$. Allora $\forall x \in \mathcal{K} : x^2 = x^{2^{2t}}$, da cui

$$2t \equiv 1 \mod 2r+1,$$

ovvero $2t = 2r+1+1$ cioè $t = r+1$ che è la tesi. □

Sia $\mathcal{K}$ un campo[2] di caratteristica 2 con $|\mathcal{K}| > 2$ tale che esista un automorfismo σ di $\mathcal{K}$ tale che

$$\forall x \in \mathcal{K} : x^{\sigma^2} = x^2.$$

Sia $\mathfrak{B} := PG(3, \mathcal{K})$ lo spazio proiettivo 3-dimensionale su $\mathcal{K}$, costruito, al solito, come:

$$PG(3, \mathcal{K}) := \frac{\mathcal{K}^{4\star}}{\mathcal{K}^\star}$$

ove $\mathcal{K}^{4\star} := \mathcal{K}^4 \setminus \{(0,0,0,0)\}$. Indichiamo le coordinate omogenee del generico punto $x \in \mathfrak{B}$ con (x_0, x_1, x_2, x_3).

Sia E il piano $x_0 = 0$. Se $x \in \mathfrak{B} \setminus E$, possiamo associare ad x le sue coordinate non omogenee x, y, z date da:

$$x := x_2 {x_0}^{-1}, \qquad y := x_3 {x_0}^{-1}, \qquad z = x_1 {x_0}^{-1}$$

Definizione 3.8. Diciamo **ovoide di Tits** l'insieme $\mathfrak{T}$ dei punti di $\mathfrak{B} \setminus E$ le cui coordinate non omogenee soddisfano la seguente equazione:

$$z = xy + x^{\sigma+2} + y^\sigma$$

unito al punto $(0,1,0,0)\mathcal{K}^\star$.

Definizione 3.9. Nelle medesime ipotesi della definizione precedente chiamiamo $\mathrm{Sz}(\mathcal{K}, \sigma)$ il gruppo di tutte le proiettività di $\mathfrak{B}$ che fissano $\mathfrak{T}$.

Si verifica (Tits, 1962) che il gruppo[3] così definito è semplice e agisce in modo due transitivo su $\mathfrak{T}$, e non ammette collineazioni diverse

[2]non necessariamente finito
[3]non necessariamente finito

dall'identità che fissino più di tre punti di $\mathfrak{T}$ stesso. Nel caso finito, $\mathrm{Sz}(\mathcal{K}, \sigma)$ è dunque un gruppo di Zassenhaus su $\mathfrak{T}$, e coincide con il gruppo di Suzuki $\mathrm{Sz}(|\mathcal{K}|)$. La definizione 3.9 è quindi, se $|\mathcal{K}|$ non è infinito, equivalente alla 3.7.

Nel caso $\mathcal{K}$ finito vale inoltre il seguente teorema:

Teorema 3.3. (Suzuki,1961) *Sia q una potenza dispari di 2, e sia r tale che $r^2 = 2q$. Allora il gruppo $\mathcal{G} = \mathrm{Sz}(q)$ ammette una partizione normale π. Tale partizione consta delle seguenti classi di gruppi coniugati:*

1. *la classe dei 2-Sylow di $\mathcal{G}$;*
2. *una classe di gruppi ciclici di ordine $q-1$;*
3. *una classe di gruppi ciclici di ordine $q+r+1$*
4. *una classe di gruppi ciclici di ordine $q-r+1$*

Dunque i gruppi $\mathrm{Sz}(q)$ ammettono partizione.

1.3. Gruppi di Frobenius. Sia $\mathcal{G} = \mathcal{N} \rtimes \mathcal{H}$ un gruppo di Frobenius. Sia $\mathfrak{F}$ la seguente famiglia di sottogruppi di $\mathcal{G}$:

$$\mathfrak{F}(\mathcal{G}) := \{\mathcal{N}\} \cup \bigcup_{x \in \mathcal{G}} \{H^x\}.$$

Vale allora il seguente teorema:

Teorema 3.4. *$\mathfrak{F}$ è una partizione normale di $\mathcal{G}$.*

Dimostrazione. Per definizione di gruppo di Frobenius

$$\forall X, Y \in \mathfrak{F}(\mathcal{G}) : X \neq Y \Rightarrow X \cap Y = \{1\}.$$

D'altro canto il teorema di Frobenius ci garantisce che

$$\mathcal{N} = \mathcal{G} \setminus (\bigcup_{g \in \mathcal{G}} \mathcal{H}^x)$$

per cui

$$\bigcup_{X \in \mathfrak{F}(\mathcal{G})} X = \mathcal{N} \cup (\bigcup_{x \in \mathcal{G}} \mathcal{H}^x) = \mathcal{G}$$

e dunque $\mathfrak{F}(\mathcal{G})$ è una partizione di $\mathcal{G}$. Il fatto che essa sia normale è immediato. $\square$

Definizione 3.10. Chiameremo la partizione $\mathfrak{F}(\mathcal{G})$ sopra introdotta per i gruppi di Frobenius **partizione di Frobenius**[4].

Osservazione. Dall'unicità del nucleo di Frobenius e dal teorema di Schur-Zassenhaus, che asserisce che tutti i complementi debbono essere coniugati fra loro, discende l'unicità della partizione di Frobenius.

In generale un gruppo di Frobenius può ammettere altre partizioni non banali oltre a quella appena introdotta: in [**Zap69**] si dimostra il seguente risultato:

Teorema 3.5. *Sia $\mathcal{G} = \mathcal{N} \rtimes \mathcal{H}$ un gruppo di Frobenius. Allora $\mathcal{G}$ ammette una partizione non banale diversa da quella di Frobenius se e solo se il nucleo $\mathcal{N}$ ammette una partizione non banale.*

D'altro canto per il teorema di Thompson il nucleo $\mathcal{N}$ deve essere nilpotente. Scorrendo la lista dei gruppi finiti con partizione, presentata nel teorema di classificazione 3.11, si vede che i soli gruppi nilpotenti che possono ammettere partizione sono tutti p-gruppi. Da questo segue:

Corollario 3.1. *Sia $\mathcal{G}$ un gruppo di Frobenius di nucleo $\mathcal{N}$. Se $\mathcal{G}$ ammette una partizione non banale diversa di $\mathfrak{F}(G)$, allora $\mathcal{N}$ è un p-gruppo.*

1.4. Proprietà delle partizioni.

Teorema 3.6. *Sia $\pi(\mathcal{G})$ una partizione di un gruppo finito $\mathcal{G}$, e siano $a, b \in \mathcal{G}$ due elementi tali che $ab = ba$. Indicato con $o(x)$ l'ordine del generico $x \in \mathcal{G}$, supponiamo valga inoltre una delle due seguenti condizioni:*

1. *$o(a) \neq o(b)$ oppure*
2. *$o(a) = o(b)$ non è un numero primo.*

Allora esiste una componente $X \in \pi(\mathcal{G})$ tale che $a, b \in X$.

[4] talvolta si trova anche la dicitura **partizione principale di Frobenius**

DIMOSTRAZIONE. Supponiamo $1 \notin \{a, b\}$, e consideriamo $X, Y \in \pi(\mathcal{G})$ tali che $a \in X$ e $b \in Y$. La nostra tesi è $X = Y$.

1. Supponiamo dapprima $o(a) \neq o(b)$, e sia $Z \in \pi(\mathcal{G})$ tale che $ab \in$ Z. Possiamo anche supporre senza perdere in generalità che sia $o(a) > o(b)$. Poichè a e b commutano si ha
$$1 \neq a^{o(b)} = (ab)^{o(b)} \in X \cap Z$$
Per la definizione di partizione deve allora essere $X = Z$. Allora $a, ab \in Z$, da cui, essendo Z gruppo, $b \in Z$. Segue la tesi $X = Z = Y$.
2. Siano ora $o(a) = o(b)$, e sia p un primo tale che $p|o(a)$. Ovviamente si avrà $p \neq o(a)$. Dunque $a^p \neq 1$, $a^p b = ba^p$ e $o(a^p) \neq o(b)$. Applicando il punto precedente si ottiene che a^p e b debbono giacere nella medesima componente di $\pi(\mathcal{G})$. Poichè $a^p \in X$ allora $X = Y$.

$\square$

Osservazione. Dal teorema appena dimostrato discende che un gruppo abeliano finito ammette una partizione non banale se e solo se è un p-gruppo abeliano elementare.

Più in generale vale il seguente corollario:

Corollario 3.2. *Se $\pi(\mathcal{G})$ è una partizione di $\mathcal{G}$ e $H \leq \mathcal{G}$ è un sottogruppo nilpotente di $\mathcal{G}$ non contenuto in alcuna componente di $\pi(\mathcal{G})$, allora H è un p-gruppo per qualche primo p.*

DIMOSTRAZIONE. Essendo H nilpotente esso è il prodotto diretto dei suoi Sylow. D'altro canto se H non è un p-gruppo, allora vi sono almeno due primi q, r tali che esistano un q-Sylow Q ed un r-Sylow R non banali. Siano $a' \in \mathrm{Z}(Q) \setminus \{1\}$ e $a'' \in \mathrm{Z}(R) \setminus \{1\}$. Allora $a = a'a'' \in \mathrm{Z}(Q)\,\mathrm{Z}(R) \leq \mathrm{Z}(H)$, e $o(a)$ non è un numero primo (in quanto $pq|o(a)$. Consideriamo adesso $X \in \pi(\mathcal{G})$ tale che $a \in X$. Ogni elemento $b \in \mathrm{C}_{\mathcal{G}}(a)$ soddisfa una delle due condizioni del teorema 3.6, e dunque $b \in X$. In particolare si avrà $H \leq \mathrm{C}_{\mathcal{G}}(a) \leq X$, contro l'ipotesi. □

Definizione 3.11. Sia $\mathcal{G}$ un gruppo, e sia $\pi(\mathcal{G})$ una sua partizione. Supponiamo $H \leq \mathcal{G}$. H si dice $\pi(\mathcal{G})$**-ammissibile** se e solo se

$$\forall X \in \pi(\mathcal{G}) : X \cap H \neq \{1\} \Rightarrow X \leq H.$$

Ovviamente ogni componente di $\pi(\mathcal{G})$ è $\pi(\mathcal{G})$-ammissibile. Vogliamo dimostrare il seguente teorema:

Teorema 3.7. (Kegel,1961) *Sia $\mathcal{G}$ un gruppo e $\pi(\mathcal{G})$ una sua partizione. Supponiamo che $H \leq \mathcal{G}$ sia $\pi(\mathcal{G})$-ammissibile; allora $H = \mathrm{N}_{\mathcal{G}}(H)$ oppure H è nilpotente.*

Abbiamo bisogno di un lemma preliminare:

Lemma 3.1. (Hughes, Thompson, 1959) *Se $H_p(\mathcal{G}) < \mathcal{G}$ e $\mathcal{G}$ non è un p-gruppo, allora $|\mathcal{G} : H_p(\mathcal{G})| = p$.*

Dimostrazione. Per induzione su $|\mathcal{G}|$. Poniamo $H = H_p(\mathcal{G})$ e sia $P \in \mathrm{Syl}_p(\mathcal{G})$. Allora $G = HP$, e, poichè H è nilpotente[5] esso deve essere il prodotto diretto dei suoi Sylows. Sia ora Q un complemento di P in $\mathcal{G}$ (tale complemento esiste certamente a norma del teorema di Schur-Zassenhaus) e non è banale poichè $\mathcal{G}$ non è p-gruppo. Allora è facile verificare che deve essere $H = Q \times (P \cap H)$.

Supponiamo sia $x \in P$ e che esista $y \in \mathrm{C}_Q(x) \setminus \{1\}$. Allora l'ordine di xy non può essere p, e dunque $xy \in H$. Ma, poichè $y \in H$, allora si deve avere anche $x \in P \cap H$. Distinguiamo ora due casi:

- Se $H \cap P = \{1\}$, allora tutto P (meno l'identità) opera in modo privo di punti fissi su H e, per un corollario del teorema di Thompson[6] P deve essere o ciclico o di quaternioni generalizzati. D'altro canto poichè ogni elemento in $\mathcal{G} \setminus H$ deve avere ordine p ne segue che $|P| = p$ e dunque $|G : H| = p$ che è la tesi.

[5]vedi teorema 3.1
[6]vedi [**Rob82**], pag 298, th. 10.5.5

- Se $H \cap P \neq \{1\}$ allora, poichè $H \cap P$ è nilpotente, esiste un sottogruppo $N \leq H \cap \mathrm{Z}(P)$ tale che $|N| = p$. Evidentemente $N \lhd \mathcal{G}$ ed ogni elemento di $\mathcal{G}/N$ non contenuto in H/N ha ordine p. Allora $H_p(\mathcal{G}/N) \leq H/N$ e, per induzione $|\mathcal{G}/N : H_p(\mathcal{G}/N)| = p$, da cui segue $H_p(\mathcal{G}/N) = H/N$ e finalmente $|\mathcal{G} : H| = p$.

$\square$

DIMOSTRAZIONE. (teorema) Supponiamo $H < \mathrm{N}_{\mathcal{G}}(H)$. Allora esiste un sottogruppo $M < \mathrm{N}_{\mathcal{G}}(H)$ tale che $|M : H| = p$ per qualche numero primo p. Sia $x \in M \setminus H$, e consideriamo l'unico $X \in \pi(\mathcal{G})$ tale che $x \in X$. Poichè H è $\pi(\mathcal{G})$-ammissibile, $X \cap H = 1$, ma poichè $M = H\langle x \rangle$ ne segue che $\langle x \rangle \simeq M/H$, da cui si deduce che l'ordine di x deve essere proprio p. Allora $H_p(M) \leq H$. Ora, se H è un p-gruppo allora esso è necessariamente nilpotente.

Viceversa se H non è un p-gruppo, allora, per il lemma precedente, $|M : H_p(M)| \leq p$, da cui $H_p(M) = H < \mathrm{N}_{\mathcal{G}}(H) \leq \mathcal{G}$. La tesi scende allora dal teorema 3.1. $\square$

Definizione 3.12. Sia $\mathcal{G}$ un gruppo e $\pi(\mathcal{G})$ una sua partizione; allora $\pi(\mathcal{G})$ si dice:

- **abeliana** se tutti i suoi elementi sono gruppi abeliani;
- **ciclica** se tutti i suoi componenti sono ciclici;
- **normale** se
$$\forall x \in \mathcal{G}, H \in \pi(\mathcal{G}) : H^x \in \pi(\mathcal{G});$$
- **caratteristica** se
$$\forall \alpha \in \mathrm{Aut}(\mathcal{G}, \cdot), H \in \pi(\mathcal{G}) : \alpha(H) \in \pi(\mathcal{G}).$$

La ragione per cui **non** si dice partizione normale quella tale che $\forall H \in \pi(\mathcal{G}) : H \lhd \mathcal{G}$ risiede nel seguente teorema:

Teorema 3.8. (Kontorovič) *Sia $\mathcal{G}$ un gruppo. Se $\mathcal{G}$ ammette una partizione non banale $\pi(\mathcal{G})$ i cui componenti sono tutti normali in $\mathcal{G}$, allora $\mathcal{G}$ è abeliano.*

DIMOSTRAZIONE. • Siano $g \in \mathcal{G}$, e $X \in \pi(\mathcal{G})$ tali che $g \in X$. Poichè $\pi(\mathcal{G})$ è non banale esiste certamente $Y \in \pi(\mathcal{G})$ tale che $Y \subseteq \mathcal{G} \setminus X$. Sia $h \in Y$. Da $Y \lhd \mathcal{G}$ segue

$$h \in Y \Rightarrow g^{-1}hg \in Y \Rightarrow h^{-1}g^{-1}hg = [h,g] \in Y.$$

Similmente, poichè anche $X \lhd \mathcal{G}$:

$$g^{-1} \in X \Rightarrow h^{-1}g^{-1}h \in X \Rightarrow h^{-1}g^{-1}hg = [h,g] \in X.$$

Tenuto conto che $X \cap Y = \{1\}$ si ha:

$$\forall g \in X, h \in Y : [h,g] = 1,$$

cioè, per l'arbitraretà di Y:

$$\forall g \in X : \mathcal{G} \setminus X \subseteq \mathrm{C}_{\mathcal{G}}(g).$$

Poichè $\mathrm{C}_{\mathcal{G}}(g)$ è un gruppo, ovviamente si ha l'includsione:

$$\langle \mathcal{G} \setminus X \rangle \leq \mathrm{C}_{\mathcal{G}}(g).$$

• Verifichiamo ora che $\mathcal{G} = \langle \mathcal{G} \setminus X \rangle$. Ovviamente $\mathcal{G} = X \cup (\mathcal{G} \setminus X)$. Siano ora $x \in X$ e $y \in \mathcal{G} \setminus X$. È immediato verificare che in tale caso $h = xy \in \mathcal{G} \setminus X$, dal che segue

$$x = hy^{-1}$$

con $h, y \in \langle \mathcal{G} \setminus X \rangle$, da cui:

$$\forall x \in X : x \in \langle \mathcal{G} \setminus X \rangle,$$

cioè

$$\mathcal{G} = \langle \mathcal{G} \setminus X \rangle.$$

• A questo punto, per l'arbitrarietà di $g \in \mathcal{G}$:

$$\forall g \in \mathcal{G} : \mathrm{C}_{\mathcal{G}}(g) = \mathcal{G},$$

cioè $\mathcal{G}$ è abeliano.

□

Di tale risultato forniremo in seguito[7] una dimostrazione condotta solamente a partire da considerazioni di natura geometrica.

[7] vedi teorema 4.16

Possiamo definire alcune operazioni fra partizioni:

Definizione 3.13. Se $\pi(\mathcal{G})$ è una partizione non banale di un gruppo $\mathcal{G}$e $g \in \mathcal{G}$, allora anche

$$\pi^g(\mathcal{G}) := \{X^g : X \in \pi(\mathcal{G})\}$$

è una partizione non banale di $\mathcal{G}$. Tale partizione si dirà **coniugata** di π^g mediante g.

Siano ora $H \leq \mathcal{G}$ tale che $H \neq \{1\}$, e sia $\pi(\mathcal{G})$ definita come sopra. Allora, posto

$$H \cap \pi(\mathcal{G}) := \{H \cap X : X \in \pi(\mathcal{G}), H \cap X \neq \{1\}\}$$

si verifica immediatamente che $H \cap \pi(\mathcal{G})$ è una partizione[8] di $\mathcal{H}$.

Supponiamo adesso che $\pi(\mathcal{G})$ e $\sigma(\mathcal{G})$ siano due partizioni non banali di $\mathcal{G}$. Diciamo **intersezione** di $\pi(\mathcal{G})$ e $\sigma(\mathcal{G})$ la partizione (che si verifica essere a sua volta non banale)

$$\pi(\mathcal{G}) \cap \sigma(\mathcal{G}) := \{X \cap Y : X \in \pi(\mathcal{G}), Y \in \sigma(\mathcal{G}), X \cap Y \neq \{1\}\} =$$

$$= \bigcap_{Y \in \sigma(\mathcal{G})} (\pi(\mathcal{G}) \cap Y)$$

Ovviamente non tutte le partizioni di un gruppo sono normali, ma è facile verificare che se $\mathcal{G}$ è un gruppo e $\pi(\mathcal{G})$ è una sua partizione non banale, allora

$$\Sigma_{\mathcal{G}} := (\bigcap_{x \in \mathcal{G}} \pi^x(G))$$

ove intersezione e coniugio sono definiti come sopra è una partizione normale non banale di $\mathcal{G}$.

Non ha dunque senso domandarsi quali gruppi ammettano partizioni normali non banali.

Aggiungendo una ipotesi è però possibile giungere al seguente importante teorema di classificazione:

[8]eventualmente banale

Teorema 3.9. (Baer,1961) *Sia $\mathcal{G}$ un gruppo finito con una partizione normale $\pi(\mathcal{G})$, e supponiamo che $N \lhd \mathcal{G}$ sia un sottogruppo proprio non banale $\pi(\mathcal{G})$-ammissibile. Allora vale una delle due seguenti condizioni:*

1. *$\mathcal{G}$ è un gruppo di Frobenius in cui N è contenuto nel nucleo $\mathcal{N}$ e tutti i possibili complementi di $\mathcal{N}$ sono elementi di $\pi(\mathcal{G})$.*
2. *Esiste un primo p tale che tutti gli elementi di $\mathcal{G} \setminus N$ hanno ordine p. Inoltre se $\mathcal{G}$ non è un p-gruppo, allora $N = H_p(\mathcal{G})$, $|\mathcal{G} : N| = p$ e $N \in \pi(\mathcal{G})$.*

Onde poter condurre a termine la dimostrazione di tale teorema è necessario richiamare preliminarmente il seguente risultato generale.

Teorema 3.10. (Hölder, Burnside, Zassenhaus) *$\mathcal{G}$ è un gruppo finito in cui tutti i sottogruppi di Sylow sono ciclici, se e solo $\mathcal{G}$ ammette una presentazione del tipo:*

$$G := \left\langle a, b | a^m = 1 = b^n, b^{-1}ab = a^r \right\rangle$$

ove $r^n \equiv 1 \mod m$, m è dispari, $0 \leq r < m$ e m e $n(r-1)$ sono coprimi.

In particolare un gruppo con tali proprietà è sempre risolubile.

Per la dimostrazione di tale risultato si rimanda a [**Rob82**], pag. 281-282.

Dimostriamo ora il teorema di Baer:

Dimostrazione. • Supponiamo dapprima che esista $X \in \pi(\mathcal{G})$ tale che $X \not\leq N$ e $\mathrm{C}_N(X) = \{1\}$. Allora, poichè N è $\pi(\mathcal{G})$-ammissibile, $X \cap N = \{1\}$, sicchè X e $N \cap \mathrm{N}_{\mathcal{G}}(X)$ sono sottogruppi normali di $\mathrm{N}_{\mathcal{G}}(X)$ con intersezione banale. Per conseguenza anche il loro prodotto diretto $(N \cap \mathrm{N}_{\mathcal{G}}(X)) \times X$ sarà sottogruppo di $\mathrm{N}_{\mathcal{G}}(X)$. D'altro canto se abbiamo un prodotto diretto $A \times B \leq C$ è sempre vero che

$$\forall a \in A, \forall b \in B : ab = ba,$$

ovvero

$$A \leq \mathrm{C}_C(B) \& B \leq \mathrm{C}_C(A)$$

cioè A e B si centralizzano a vicenda. Questo fatto nel nostro caso implica in particolare:

$$N \cap \mathrm{N}_{\mathcal{G}}(X) \leq \mathrm{C}_N(X) = \{1\}.$$

Applicando ora la legge modulare di Dedekind si ottiene:

$$\mathrm{N}_{NX}(X) := NX \cap \mathrm{N}_{\mathcal{G}}(X) = (N \cap \mathrm{N}_{\mathcal{G}}(X))X = X$$

Allora se consideriamo l'azione di N sulle classi laterali destre di X in NX possiamo verificare facilmente che NX deve essere un gruppo di Frobenius di nucleo N e complemento X. Ne segue

$$NX = N \cup (\bigcup_{g \in NX} X^g)$$

e dunque NX deve essere $\pi(\mathcal{G})$-ammissibile, in quanto, essendo $\pi(\mathcal{G})$ una partizione normale $\forall g \in \mathcal{G} : X^g \in \pi(\mathcal{G})$.

D'altro canto i gruppi di Frobenius non sono nilpotenti; allora per il teorema 3.7 dobbiamo avere $\mathrm{N}_{\mathcal{G}}(NX) = NX$. Ma poichè $N \lhd \mathcal{G}$, si ha $\mathrm{N}_{\mathcal{G}}(X) \leq \mathrm{N}_{\mathcal{G}}(NX)$ e dunque $\mathrm{N}_{\mathcal{G}}(X) = X$. Da ciò, ragionando come sopra, si deduce che anche $\mathcal{G}$ deve essere un gruppo di Frobenius con complemento X e nucleo $\mathcal{N}$. Ora, per il teorema 2.18 si ha $N \leq \mathcal{N}$ che conclude la tesi.

- Supponiamo ora

$$\forall X \in \pi(\mathcal{G}) : X \nleq N \Rightarrow \mathrm{C}_N(X) \neq \{1\}$$

Siano $a \in \mathrm{C}_N(X) \setminus \{1\}$ e $b \in X \setminus \{1\}$. Allora a e b giacciono in componenti distinte di $\pi(\mathcal{G})$ e, per il teorema 3.6 si deve avere che $o(a) = o(b) = p$ con p numero primo. Inoltre ogni elemento diverso da 1 in X o in $\mathrm{C}_N(X)$ deve avere ordine p. In particolare p divide $|N|$ e deve coincidere con l'esponente[9] di X.

Conseguenza di ciò è che ogni elemento di $\mathcal{G} \setminus N$ deve avere ordine primo. La tesi vale sicuramente se $\mathcal{G}$ è un p-gruppo.

[9] i.e. il minimo comune multiplo degli ordini

Supponiamo ora che $\mathcal{G}$ non sia un p-gruppo per nessun p. Allora, per quanto visto sopra nemmeno N può essere un p-gruppo. Sia ora p un numero primo che divida $|\mathcal{G} : N|$ e sia P un p-Sylow di $\mathcal{G}$. Allora $|NP : N|$ è necessariamente una potenza di p e dunque ogni elemento di $NP \setminus N$ deve avere ordine p. Dunque

$$H_p(NP) \leq N < NP.$$

A questo punto per il lemma 3.1 si ottiene $|NP : H_p(NP)| = p$ da cui

$$H_p(NP) = N \& |NP : N| = p.$$

Ne segue che tutti i sottogruppi di Sylow di $\mathcal{G}/N$ devono essere ciclici di ordine primo. Per il teorema 3.10 $\mathcal{G}/N$ deve essere risolubile. Allora esisterà certamente un gruppo $M/N \lhd \mathcal{G}/N$ di indice primo p. Di nuovo ogni elemento $G \setminus M$ avrà ordine p e dunque, applicando ancora una volta il lemma 3.1 avremo $H_p(\mathcal{G}) = M$. Per il lemma 3.1 M deve essere nilpotente e di ordine non primo in quanto $N \leq M$. Da questo discende per il corollario 3.2 che M deve essere una componente di $\pi(\mathcal{G})$, e per la $\pi(\mathcal{G})$-ammissibilità di N abbiamo $M = N$. Segue la tesi.

□

1.5. Il teorema fondamentale. Servendosi di quanto sin qui dimostrato e di alcune ulteriori caratterizzazioni è possibile provare il seguente teorema:

Teorema 3.11. (Miller, Kotorovič, Baer, Kegel, Thompson, Suzuki) *Un gruppo finito $\mathcal{G}$ ammette una partizione non banale se e solo se esso è il gruppo simmetrico S_4 oppure appartiene ad una delle seguenti classi:*

1. $\mathrm{PGL}(2, p^h)$ *con p numero primo e $p^h \geq 4$;*
2. $\mathrm{PSL}(2, p^h)$ *con p numero primo e $p^h \geq 4$;*
3. $\mathrm{Sz}(2^{2k+1})$ *con $k \geq 1$;*

4. *gruppi di Frobenius;*
5. *gruppi di Hughes-Thompson.*

In particolare se $\mathcal{G}$ è un gruppo risolubile, allora (Baer):

1. $\mathcal{G}$ *è un p-gruppo per qualche primo p, e* Σ *contiene una componente* X *tale che ogni elemento di* $\mathcal{G} \setminus X$ *ha ordine p; inoltre* $|\Sigma| \equiv 1 \mod p$.
2. $\mathcal{G}$ *possiede un sottogruppo normale nilpotente* N *tale che* $N \in \Sigma$, $|\mathcal{G} : N| = p$, *p numero primo, e ogni elemento di* $\mathcal{G} \setminus N$ *ha ordine* p.
3. $\mathcal{G}$ *è un gruppo di Frobenius.*
4. $\mathcal{G} \simeq \mathrm{S}_4$;

Se invece $\mathcal{G}$ non è risolubile vale una delle seguenti possibilità (Suzuki):

1. $\mathcal{G}$ *è un gruppo di Frobenius;*
2. $\mathcal{G} \simeq \mathrm{PGL}(2, p^h)$ *con* $p^h \geq 4$;
3. $\mathcal{G} \simeq \mathrm{PSL}(2, p^h)$ *con* $p^h \geq 4$;
4. $\mathcal{G} \simeq \mathrm{S}_4$.

Osservazione.

- La classe dei gruppi di Frobenius non è disgiunta da quella dei gruppi di Hughes-Thompson.
- I gruppi delle classi 1 e 2 nel caso risolubile sono di Hughes-Thompson.

Non è nostra intenzione presentare la dimostrazione di tale risultato per cui rimandiamo al già citato [**Sch94**].

CAPITOLO 4

Strutture di incidenza

In questo capitolo seguiremo per le definizioni relative le strutture di incidenza [**KSW73**].

1. Nozioni di base

Definizione 4.1. Sia $\mathfrak{P}$ un insieme, e sia $\mathfrak{R} \subseteq 2^{\mathfrak{P}}$. Diciamo che la coppia $(\mathfrak{P}, \mathfrak{R})$ è uno **spazio lineare** o **spazio di incidenza** se

1. $\forall a, b \in \mathfrak{P}$ con $a \neq b : \exists! R \in \mathfrak{R}$ con $\{a, b\} \subseteq R$
2. $\forall R \in \mathfrak{R} : |R| \geq 2$.

Gli elementi di $\mathfrak{P}$ verranno detti **punti** e quelli di $\mathfrak{R}$ **rette**. Dati due punti distinti $a, b \in \mathfrak{P}$ indicheremo con il simbolo $\overline{a, b}$ l'unica retta di $\mathfrak{R}$ che li contiene.

Osservazione. La coppia $(\emptyset, \emptyset)$ è, per la definizione precedente, uno spazio di incidenza banale.

Definizione 4.2. Sia $(\mathfrak{P}, \mathfrak{R})$ uno spazio di incidenza. Si dice **collineazione** di $(\mathfrak{P}, \mathfrak{R})$ ogni biiezione $\phi : \mathfrak{P} \to \mathfrak{P}$ tale che:

$$\forall R \in \mathfrak{R} : \phi(R) \in \mathfrak{R}$$

L'insieme di tutte le collineazioni di uno spazio di incidenza costituisce gruppo. Indicheremo tale gruppo col simbolo $\mathrm{Aut}(\mathfrak{P}, \mathfrak{R})$.

Definizione 4.3. Uno spazio di incidenza $(\mathfrak{P}, \mathfrak{R})$ si dice **proprio** se e solo se $|\mathfrak{R}| > 1$.

Nel seguito supporremo sempre che i nostri spazi di incidenza siano propri.

Definizione 4.4. Diciamo che una coppia $(\mathfrak{P}, \mathfrak{R})$ con $\mathfrak{R} \subseteq 2^{\mathfrak{P}}$ è uno **spazio parziale** se

1. $\forall R \in \mathfrak{R} : |R| \geq 2$
2. $\forall a, b \in \mathfrak{P}$ esiste al più una retta $R \in \mathfrak{R}$ tale che $a, b \in R$.

Un esempio di spazio di incidenza è offerto dal **piano di fano**, in cui $\mathfrak{P} = \{a, b, c, d\}$ ed $\mathfrak{R} = \binom{\mathfrak{P}}{2}$, ove con $\binom{X}{n}$ si intende l'insieme di tutti i sottoinsiemi di X aventi cardinalità n.

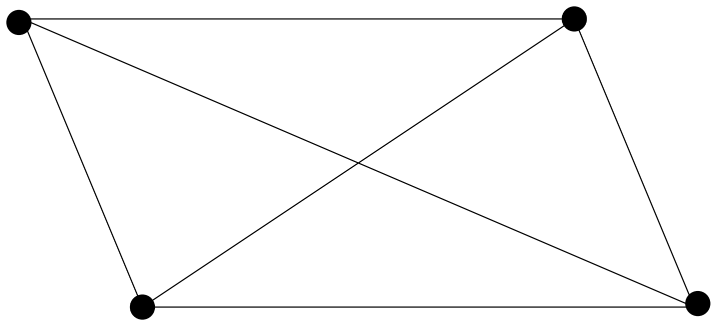

FIGURA 1. Piano di fano

La definizione di spazio di incidenza è piuttosto debole. Un modo per caratterizzare delle strutture geometriche interessanti può consistere nell'aggiungere alcuni assiomi.

Definizione 4.5. Uno spazio di incidenza $(\mathfrak{P}, \mathfrak{R})$ si dice **piano affine** se e solo se sono soddisfatte le seguenti condizioni:

1. $(\mathfrak{P}, \mathfrak{R})$ è proprio
2. (Assioma delle parallele)

$$\forall (x, R) \in \mathfrak{P} \times \mathfrak{R} \text{ con } x \notin R :$$
$$\exists! S \in \mathfrak{R} \text{ tale che } x \in S \& S \cap R = \emptyset.$$

Dato un piano affine $(\mathfrak{P}, \mathfrak{R})$ ed una retta $R \in \mathfrak{R}$ diciamo **parallela** ad R ogni retta $S \in \mathfrak{R}$ tale che $S \cap R = \emptyset$ oppure $S = R$. Indicheremo tale fatto scrivendo $S \parallel_{\mathrm{A}} R$.

Il piano di Fano è un esempio di piano affine.

Osservazione. È facile verificare che la relazione $\parallel_{\mathrm{A}}$ sopra definita è di equivalenza.

Spesso è utile fornire una nozione più generale ed astratta di parallelismo:

Definizione 4.6. Sia $(\mathfrak{P}, \mathfrak{R})$ uno spazio di incidenza. Una relazione $\| \subseteq \mathfrak{R} \times \mathfrak{R}$ si dice **parallelismo** se e solo se sono soddisfatti i seguenti due assiomi:

1. $\|$ è di equivalenza;
2. $\forall x \in \mathfrak{P}, \forall R \in \mathfrak{R} : \exists! H \in \mathfrak{R}$ tale che $x \in \mathcal{H} \& H \parallel R$.

La retta H cui al punto 2. si dirà **parallela ad** R **per** x e verrà indicata col simbolo $H := (x \parallel R)$.

Osservazione. È pressochè immediato dimostrare che $\|_{\mathrm{A}}$ è, nel caso di un piano affine, un parallelismo.

D'altro canto la definizione di $\|$ implica immediatamente che se $R, S \in \mathfrak{R}$ e $R \neq S$, allora $R \cap S = \emptyset$. Infatti se fosse $R \cap S = \{x\}$, allora per x passerebbero *due* rette distinte fra loro parallele, contro il punto 2 della definizione.

Definizione 4.7. Una terna $(\mathfrak{P}, \mathfrak{R}, \|)$ si dice **spazio di incidenza con parallelismo** o **struttura di André**[1] (o, in breve, **A-Struttura**) se e solo se $(\mathfrak{P}, \mathfrak{R})$ è uno spazio di incidenza e $\|$ è un parallelismo.

Definizione 4.8. Sia $(\mathfrak{P}, \mathfrak{R}, \|)$ una A-struttura. Si dice **collineazione affine** ogni collineazione ϕ di $(\mathfrak{P}, \mathfrak{R})$ tale che:

$$\forall A, B \in \mathfrak{R} : A \parallel B \Rightarrow \phi(A) \parallel \phi(B)$$

L'insieme delle collineazioni affini di $(\mathfrak{P}, \mathfrak{R})$ è un sottogruppo del gruppo $\mathrm{Aut}(\mathfrak{P}, \mathfrak{R})$. Indicheremo tale sottogruppo col simbolo $\mathrm{Aut}(\mathfrak{P}, \mathfrak{R}, \|)$.

Definizione 4.9. Sia $(\mathfrak{P}, \mathfrak{R}, \|)$ una A-struttura. Si dice **dilatazione** di $(\mathfrak{P}, \mathfrak{R}, \|)$ ogni collineazione affine ϕ di $(\mathfrak{P}, \mathfrak{R})$ tale che

$$\forall R \in \mathfrak{R} : \phi(R) \parallel R.$$

[1] in quanto introdotta per la prima volta in [**And61**]

Si dice **dilatazione forte** di $(\mathfrak{P}, \mathfrak{R}, \|)$ ogni dilatazione τ tale che

$$\forall R \in \mathfrak{R} \dim \overline{R \cup \tau(R)} \leq 2.$$

Si dimostra facilmente che l'insieme di tutte le dilatazioni $(\mathfrak{P}, \mathfrak{R}, \|)$ è un sottogruppo del gruppo $\mathrm{Aut}(\mathfrak{P}, \mathfrak{R}, \|)$ di tutte le collineazioni affini. Indicheremo tale sottogruppo col simbolo $\mathfrak{D}(\mathfrak{P}, \mathfrak{R}, \|)$.

Osservazione. La nozione di collineazione affine, come tutte quelle da essa derivate, dipende strettamente dalla relazione di parallelismo definita sullo spazio di incidenza $(\mathfrak{P}, \mathfrak{R})$. Se su $(\mathfrak{P}, \mathfrak{R})$ sono definiti due parallelismi distinti $\|_l$ e $\|_r$ è possibile che una collineazione τ possa essere, ad esempio una dilatazione rispetto $\|_l$ ma al contempo non appartenga nemmeno ad $\mathrm{Aut}(\mathfrak{P}, \mathfrak{R}, \|_r)$.

È importante notare che le due definizioni di parallelismo fornite in 4.5 e 4.6 non sono equivalenti, nemmeno nel caso in cui la dimensione[2] è 2. Tutti i piani affini sono spazi di incidenza con parallelismo, ma il viceversa è falso.

Un esempio grazioso è il seguente:

Esempio 4.1. Siano $R := \{a_0, a_1, a_2\}$ ed $S := \{b_0, b_1, b_2\}$; poniamo:

$$\mathfrak{P} := R \cup S$$

$$\mathfrak{R} = \{R, S\} \cup \{\{x, y\} : x \in R, y \in S\}$$

Definiamo ora una relazione di equivalenza $\|$ fra gli elementi di $\mathfrak{R}$ richiedendo:

- $R \parallel S$;
- $\forall i, j, k \in \mathrm{GF}(3) : \{a_i, b_{i+k}\} \parallel \{a_j, b_{j+k}\}$
- $\forall i, k \in \mathrm{GF}(3) : R \nparallel \{a_i, b_{i+k}\}$.

È facile vedere che $(\mathfrak{P}, \mathfrak{R}, \|)$ è uno spazio lineare con parallelismo. D'altro canto, diversamente da quanto accade nel caso affine $\{a_0, b_0\} \nparallel \{a_1, b_2\}$ ma la loro intersezione è vuota.

[2]vedi definizione 4.14

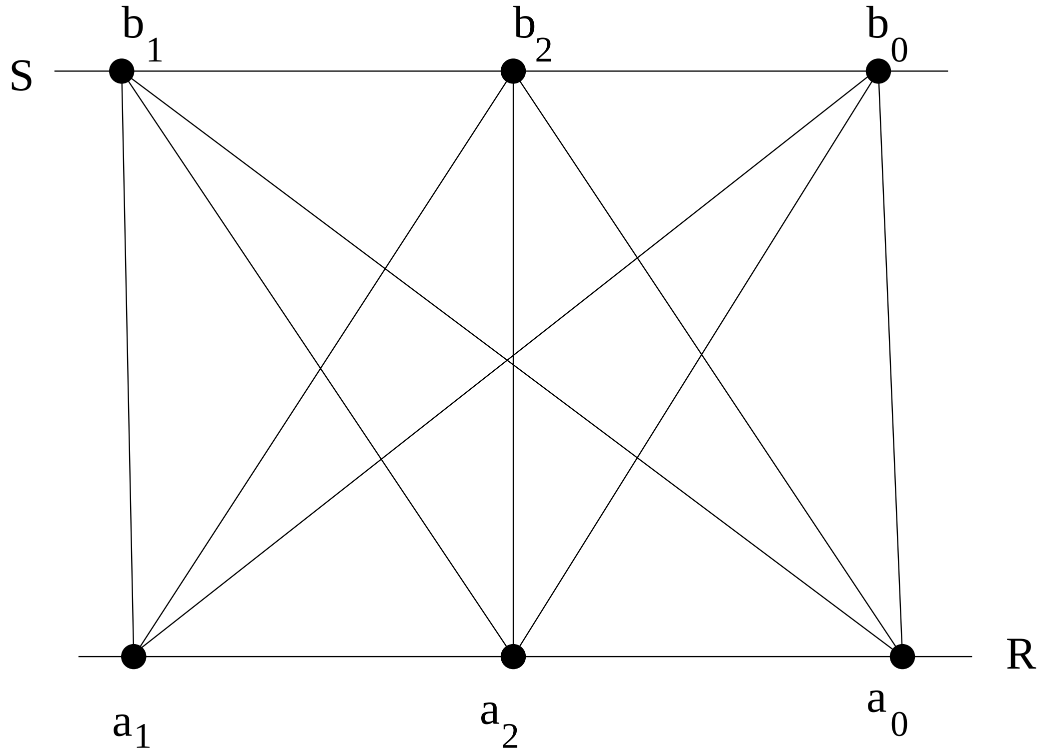

FIGURA 2

1.1. Sottospazi e spazi traccia.

Definizione 4.10. Sia $(\mathfrak{P}, \mathfrak{R})$ uno spazio di incidenza. Un insieme $\mathfrak{Q} \subseteq \mathfrak{P}$ si dice **spazio traccia** se e solo se posto

$$\mathfrak{R}' := \{R \cap \mathfrak{Q} : R \in \mathfrak{R}; |R \cap \mathfrak{Q}| > 1\},$$

la coppia $(\mathfrak{Q}, \mathfrak{R}')$ è uno spazio di incidenza.

Definizione 4.11. Sia $(\mathfrak{P}, \mathfrak{R})$ uno spazio di incidenza, e sia $Q \subseteq \mathfrak{P}$. Q si dice **sottospazio** di $(\mathfrak{P}, \mathfrak{R})$ se e solo se

$$\forall p, q \in Q : p \neq q : \{p, q\} \in R \in \mathfrak{R} \Rightarrow R \subseteq Q.$$

Indicheremo l'insieme di tutti i sottospazi di uno spazio di incidenza col simbolo $\mathfrak{S}(\mathfrak{P}, \mathfrak{R})$, ovvero, ove sia chiaro quale è lo spazio ambiente più brevemente con $\mathfrak{S}$.

Teorema 4.1. *Sia* $(\mathfrak{P}, \mathfrak{R})$ *uno spazio di incidenza. Allora* $\mathfrak{S}$ *è un insieme* $\cap$*-chiuso*[3]

[3] ovvero "chiuso per intersezioni"

DIMOSTRAZIONE. Siano $H, K \in \mathfrak{S}$. Se $H = K$, oppure $|H \cap K| < 2$ non c'è nulla da dimostrare.

Supponiamo $H \cap K = G$, e siano $g_1, g_2 \in G$ tali che $g_1 \neq g_2$. Allora abbiamo:

$$g_1, g_2 \in G \Rightarrow g_1, g_2 \in H \Rightarrow R = \overline{g_1, g_2} \subseteq H$$

$$g_1, g_2 \in G \Rightarrow g_1, g_2 \in K \Rightarrow R = \overline{g_1, g_2} \subseteq K$$

da cui finalmente

$$\forall g_1, g_2 \in G : R = \overline{g_1, g_2} \Rightarrow R \subseteq H \cap K = G$$

che è la tesi, cioè $G \in \mathfrak{S}$. □

Definizione 4.12. Sia X un insieme. Un operatore $\sigma : 2^X \to 2^X$ si dice **chiusura** se e solo se $\forall A, B \in 2^X$:

1. $\sigma(\sigma(A)) = \sigma(A)$;
2. $A \subseteq \sigma(A)$;
3. $A \subseteq B \Rightarrow \sigma(A) \subseteq \sigma(B)$.

Osservazione. Sia X un insieme e σ un operatore di chiusura su X. Si verifica che posto $\tau = \mathrm{Im}(\sigma)$:

$$\sigma : \begin{cases} 2^X \to \tau \subseteq 2^X \\ T \to \bigcap_{\substack{V \in \tau \\ X \subseteq V}} V. \end{cases}$$

Gli elementi di τ si diranno **chiusi** per σ.

Viceversa, assegnata una famiglia $\tau \subseteq 2^X$, chiusa per intersezione e tale che $X \in \tau$ l'operatore σ definito come sopra risulta essere di chiusura.

Definizione 4.13. Sia $(\mathfrak{P}, \mathfrak{R})$ uno spazio di incidenza, e sia $Q \subseteq \mathfrak{P}$. Poniamo per definizione:

$$\overline{Q} := \bigcap_{X \in \mathfrak{S} : Q \subseteq X} X.$$

Per l'osservazione precedente ed il teorema 4.1 si può rapidamente verificare che $\bar{\cdot}$ è un operatore di chiusura $2^{\mathfrak{P}} \to \mathfrak{S}$. Chiameremo il sottospazio $\overline{Q}$ **sottospazio generato da Q in** $(\mathfrak{P}, \mathfrak{R})$.

Osservazione. Siano $a, b \in \mathfrak{P}$ con $a \neq b$. Allora:

$$\overline{a,b} = \overline{\{a,b\}}.$$

Dimostrazione. Poichè $\overline{a,b} \in \mathfrak{S}$[4] , sicuramente:

$$T = \overline{\{a,b\}} \subseteq \overline{a,b}.$$

Viceversa, per definizione di S:

$$a, b \in T, a \neq b \Rightarrow \overline{a,b} \subseteq T = \overline{\{a,b\}},$$

e dunque si ha la tesi. □

Alla luce della precedente osservazione nel seguito scriveremo sempre $\overline{a,b}$ per indicare il sottospazio generato da a e da b.

Definizione 4.14. Sia $(\mathfrak{P}, \mathfrak{R})$ uno spazio di incidenza. Diciamo **dimensione** di $(\mathfrak{P}, \mathfrak{R})$ il numero

$$\dim(\mathfrak{P}, \mathfrak{R}) := \inf\{|X| : \overline{X} = \mathfrak{P}\} - 1.$$

Definizione 4.15. Sia $(\mathfrak{P}, \mathfrak{R})$ uno spazio di incidenza. Si dice **base** di $(\mathfrak{P}, \mathfrak{R})$ ogni insieme minimale di generatori.

Definizione 4.16. Sia $(\mathfrak{P}, \mathfrak{R})$ uno spazio di incidenza. Un insieme $Q \subseteq \mathfrak{P}$ si dice **indipendente** se e solo se

$$\forall q \in Q : \overline{Q} \neq \overline{Q \setminus \{q\}}$$

Osservazione. Sebbene le nozioni di dimensione e base così fornite siano applicabili ad ogni spazio di incidenza, in generale non valgono molte delle proprietà a cui si è abituati nel caso degli spazi vettoriali.

Un esempio interessante può essere offerto dalla struttura di incidenza rappresentata dalla figura 4.3.

Tutto lo spazio ha dimensione 2, in quanto

$$\mathfrak{P} := \overline{\{a,b,d\}},$$

ma si verifica immediatamente che $S = \{f, g, h\}$ costituisce un suo sottospazio proprio della medesima dimensione; inoltre S, è un insieme

[4]le rette sono sottospazi !

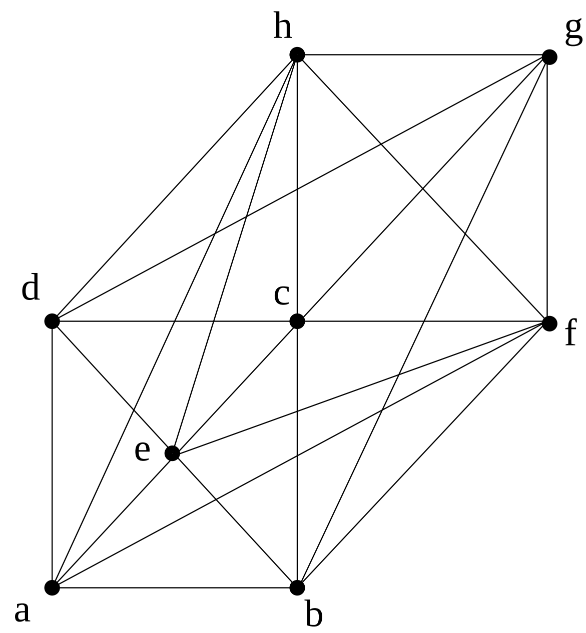

FIGURA 3

di punti indipententi che non può in alcun modo essere completato a base di tutto lo spazio.

È evidente dunque che le nozioni di "insieme massimale di punti indipendenti" e di "base" in questo ambiente non coincidono affatto.

Onde poter eliminare situazioni "patologiche" come quella presentata nell'osservazione precedente è utile la seguente definizione:

Definizione 4.17. Uno spazio di incidenza $(\mathfrak{P}, \mathfrak{R})$ si dice **spazio di scambio** se e solo se in esso vale il seguente assioma (**assioma di scambio**):

$$\forall S \subseteq \mathfrak{P}, \forall x, y \in \mathfrak{P} : x \in \overline{S \cup \{y\}} \setminus \overline{S} \Rightarrow y \in \overline{S \cup \{x\}}$$

Si verifica (vedi [**KSW73**], pagg. 50-52) che in uno spazio di scambio tutte le basi hanno la medesima cardinalità, vale il teorema del completamento della base, ed anche il concetto di dimensione gode delle abituali proprietà[5].

[5]non esistono sottospazi propri di dimensione pari (o superiore!) a quella dello spazio ambiente

2. Proprietà configurazionali

Un metodo per caratterizzare uno spazio di incidenza consiste nel chiedere siano soddisfatte determinate proprietà configurazionali.

2.1. La chiusura dei parallelogrammi.

Definizione 4.18. Sia $(\mathfrak{P}, \mathfrak{R})$ un piano affine. Diciamo **parallelogramma** ogni quaterna di punti distinti $P = (a, b, c, d)$ tale che

1. I punti a, b, c, d sono a 3 a 3 non allineati;
2. $\overline{a, b} \parallel \overline{c, d}$;
3. $\overline{a, d} \parallel \overline{b, c}$.

Tale definizione può estendersi in modo naturale ad ogni spazio di incidenza con parallelismo.

È però vero che, mentre nel caso affine è sempre possibile assegnati tre punti non allineati a, b, c costruire un parallelogramma avente fra i suoi vertici quei tre punti, in una generica A-struttura tale proprietà non risulta generalmente soddisfatta.

Definizione 4.19. Sia $(\mathfrak{P}, \mathfrak{R}, \parallel)$ una A-struttura, e siano $a, b, c \in \mathfrak{P}$ tre punti non allineati. Diciamo che **il parallelogramma di vertici** a, b, c **si chiude** se e solo se

$$\exists d \in (a \parallel \overline{b, c}) \cap (c \parallel \overline{a, b}),$$

cioè

$$\exists d \in \mathfrak{P} \text{ tale che } (a, b, c, d) \text{è un parallelogramma}$$

Esempio 4.2. Sia $(\mathfrak{P}, \mathfrak{R}) := \mathrm{AG}(2, 9)$ il piano affine di nove punti. Sia $x \in \mathfrak{P}$ un punto fissato, e poniamo:

$$\mathfrak{P}' := \mathfrak{P} \setminus \{x\},$$

$$\mathfrak{R}' := \{R \setminus \{x\} : R \in \mathfrak{R}\}.$$

In $(\mathfrak{P}', \mathfrak{R}')$ valgono ancora tutti gli assiomi degli spazi di incidenza.

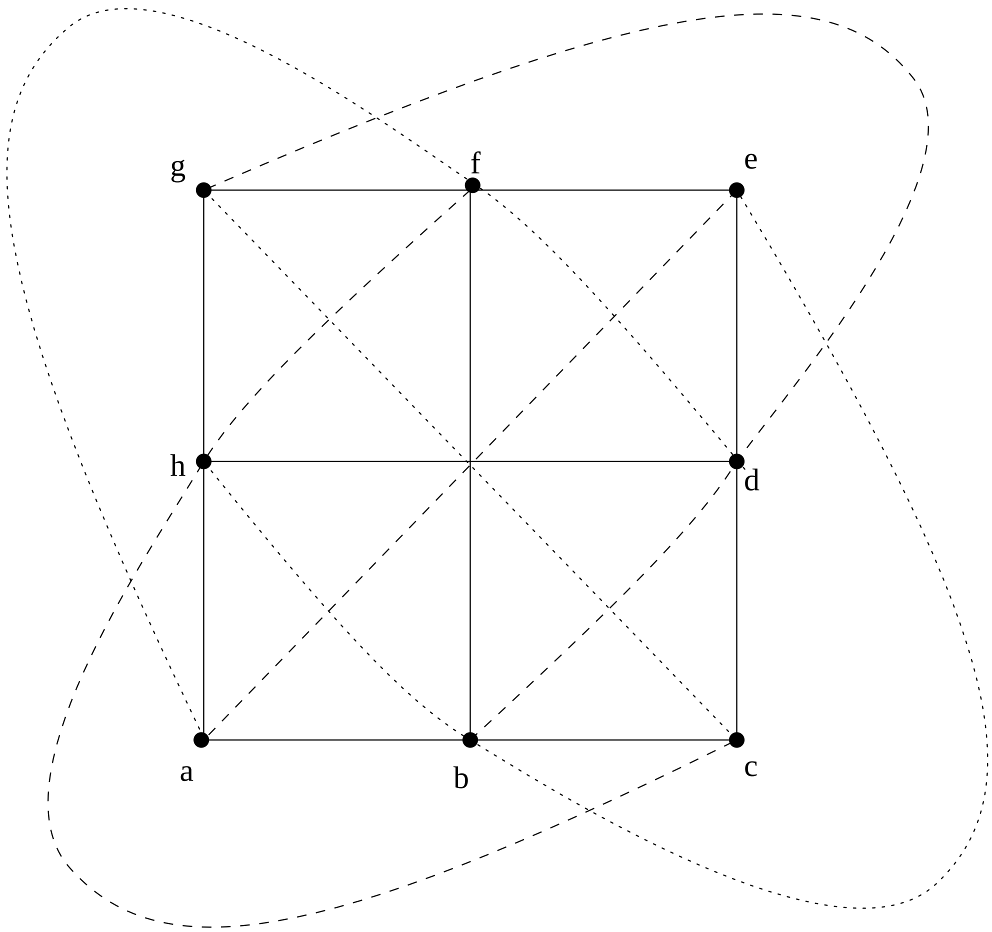

FIGURA 4. $(\mathfrak{P}', \mathfrak{R}')$

Inoltre si può definire in $\mathfrak{R}'$ una relazione di equivalenza $\|'$ nel seguente modo:

$$\forall H, K \in \mathfrak{R}' : H \|' K \Leftrightarrow \forall R, S \in \mathfrak{R} : H \subseteq R, K \subseteq S : R \| S$$

Si verifica banalmente che tale relazione, indotta da $\|$, è a sua volta un parallelismo per $(\mathfrak{P}', \mathfrak{R}')$. D'altro canto, chiamati i punti di $(\mathfrak{P}', \mathfrak{R}')$ come in figura 4.4.2 si vede immediatamente che che nessun parallelogramma di vertici a, b, h si chiude in $(\mathfrak{P}', \mathfrak{R}')$, ed abbiamo dunque il controesempio cercato.

Il pretendere la chiusura di tutti i parallelogrammi è una condizione piuttosto restrittiva per uno spazio di incidenza con parallelismo.

Risulta quindi naturale cercare di trovare una proprietà configurazionale più debole che sia soddifatta da una famiglia più ampia di A-strutture, e fornisca al contempo un utile strumento per poter dimostrare proprietà "simili" a quelle dei piani affini.

La seguente definizione si muove in tale direzione:

Definizione 4.20. Una terna $(\mathfrak{P}, \mathfrak{R}, \|_l, \|_r)$ si dice **spazio doppio** se e solo se:

1. $(\mathfrak{P}, \mathfrak{R})$ è uno spazio di incidenza;
2. sia $\|_l$ che $\|_r$ sono parallelismi[6] per $(\mathfrak{P}, \mathfrak{R})$;
3. (chiusura dei parallelogrammi misti)

$\forall A, B \in \mathfrak{R}$ tali che $A \cap B \neq \emptyset, \forall a \in A, b \in B$ vale

$$\forall X, Y \in \mathfrak{R} \text{ con } a \in X, b \in Y, X \|_l B, Y \|_r A : X \cap Y \neq \emptyset$$

2.2. La piccola configurazione di Desargues.

Definizione 4.21. Sia $(\mathfrak{P}, \mathfrak{R}, \|)$ uno spazio di incidenza con parallelismo. Siano per $i = 1, 2, 3$, $a_i, b_i \in \mathfrak{P}$ tali che, posto $R_i = \overline{a_i, b_i}$: $R_1 \parallel R_2 \parallel R_3$ e $|\{R_1, R_2, R_3\}| = 3$. Diciamo che tali punti soddisfano la **piccola configurazione di Desargues affine** se e solo se:

$$\overline{a_1, a_3} \parallel \overline{b_1, b_3}, \overline{a_2, a_3} \parallel \overline{b_2, b_3} \Rightarrow \overline{a_1, a_2} \parallel \overline{b_1, b_2}$$

Come è stato fatto per la chiusura dei parallelogrammi, è possibile generalizzare questa configurazione al caso degli spazi doppi:

Definizione 4.22. Sia $(\mathfrak{P}, \mathfrak{R}, \|_l, \|_r)$ uno spazio doppio. Siano per $i = 1, 2, 3$, $a_i, b_i \in \mathfrak{P}$ tali che, posto $R_i = \overline{a_i, b_i}$: $R_1 \|_l R_2 \|_l R_3$ e $|\{R_1, R_2, R_3\}| = 3$. Diciamo che tali punti soddisfano la **configurazione sinistra-destra di Desargues** se e solo se:

$$\overline{a_1, a_3} \|_r \overline{b_1, b_3}, \overline{a_2, a_3} \|_r \overline{b_2, b_3} \Rightarrow \overline{a_1, a_2} \|_r \overline{b_1, b_2}$$

[6] non necessariamente distinti

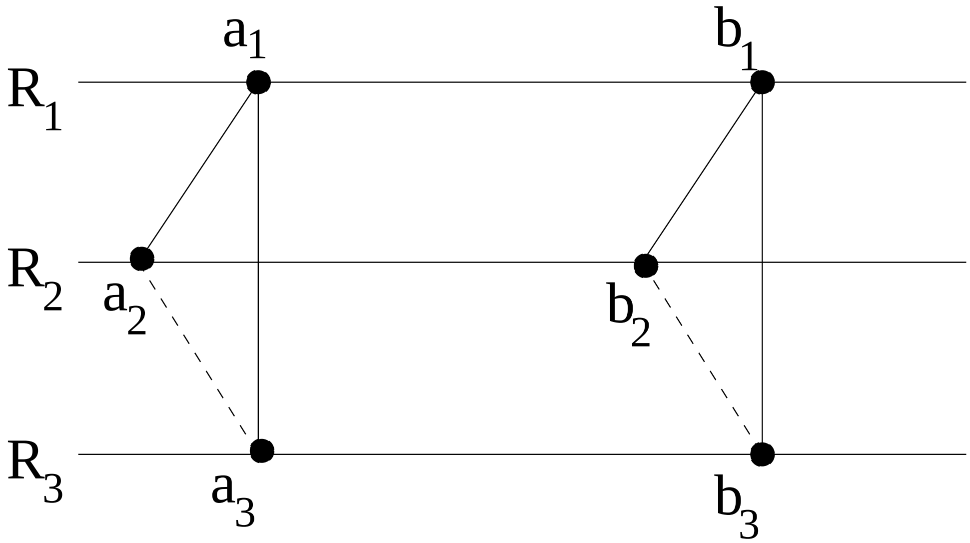

FIGURA 5. (Ad)

Uno spazio doppio in cui valga tale configurazione per ogni sestupla di punti soddisfacenti le ipotesi si dice **spazio prismatico destro**.

Simmetricamente si parla di **configurazione Destra-sinistra di Desargues** e di **spazio prismatico sinistro** se sono soddisfatte le medesime condizioni scambiando $\|_l$ con $\|_r$.

Definizione 4.23. Sia $(\mathfrak{P}, \mathfrak{R}, \|_l, \|_r)$ uno spazio doppio. Esso si dice **spazio prismatico** se e solo se è contemporaneamente uno spazio prismatico destro e sinistro.

Definizione 4.24. Sia $(\mathfrak{P}, \mathfrak{R}, \|)$ uno spazio di incidenza con parallelismo; una dilatazione τ si dice **traslazione** se essa è l'identità, oppure risulta priva di punti uniti.

Definizione 4.25. Una A-struttura $(\mathfrak{P}, \mathfrak{R}, \|)$ si dice **di traslazione**, o in breve **A-t-struttura** se ammette un gruppo di traslazioni transitivo su $\mathfrak{P}$.

Osservazione. Le traslazioni in generale non costituiscono gruppo. Indicheremo l'insieme di tutte le traslazioni col simbolo $\mathcal{T}(\mathfrak{P}, \mathfrak{R}, \|$).

Definizione 4.26. Nelle stesse ipotesi del teorema precedente, una traslazione τ si dice **centrale** se e solo se

$$\forall R, S \in \mathfrak{R} : \tau(R) = R \& S \parallel R \Rightarrow \tau(S) = S$$

Lo spazio $(\mathfrak{P}, \mathfrak{R}, \parallel)$ si dice **di traslazione centrale** se tutte le sue traslazioni sono centrali e costituiscono inoltre un gruppo transitivo su $\mathfrak{P}$.

Definizione 4.27. Sia $(\mathfrak{P}, \mathfrak{R}, \parallel_l, \parallel_r)$ uno spazio doppio. Si dice **traslazione sinistra** ogni collineazione $\tau \in \mathrm{Aut}(\mathfrak{P}, \mathfrak{R})$ tale che

1. τ è una dilatazione sinistra, cioè:

$$\forall R \in \mathfrak{R} : R \parallel_l \tau(R);$$

2.

$$\forall H \in \mathfrak{R} : \tau(H) = H \Rightarrow \forall K \in \mathfrak{R} : K \parallel_r H : \tau(K) = K.$$

Similmente si definiscono le **traslazioni destre**.

Tale definizione è consistente; infatti vale il seguente teorema:

Teorema 4.2. *Sia τ una traslazione sinistra*[7] *diversa dall'identità. Allora τ è priva di punti fissi.*

Dimostrazione. Sia τ una traslazione sinistra di $(\mathfrak{P}, \mathfrak{R}, \parallel_l, \parallel_r)$. Supponiamo $\exists x \in \mathfrak{P} : \tau(x) = x$. Allora in particolare:

$$\forall R \in \mathfrak{R} : x \in \mathfrak{R} \Rightarrow \tau(R) = R.$$

Dal punto 2 della definizione precedente e dall'esistenza della parallela destra per un punto ad una qualsiasi retta $H \in \mathfrak{R}$ segue:

$$\forall R \in \mathfrak{R} : \tau(R) = R.$$

Sia ora $y \in \mathfrak{P} \setminus \{x\}$ un generico punto. Sicuramente esistono due rette $A, B \in \mathfrak{R}$ tali che $\{y\} = A \cap B$. Essendo ogni traslazione una collineazione, sicuramente $\tau(A) \cap \tau(B) = \{\tau(y)\}$, ma

$$\tau(A) \cap \tau(B) = A \cap B = \{y\},$$

[7]Ovviamente il medesimo ragionamento si può applicare alle traslazioni destre

per cui y deve essere fissato. Da questo segue $\tau = 1$, che è la tesi. $\square$

Definizione 4.28. Sia $(\mathfrak{P}, \mathfrak{R}, \|_l, \|_r)$ uno spazio doppio, e sia τ una sua traslazione destra (sinistra) non identica. Si dice **direzione** di τ l'insieme $\mathrm{Dir}(\tau)$ delle rette fissate da τ:

$$\mathrm{Dir}(\tau) := \{R \in \mathfrak{R} : \tau(R) = R\} = \{\overline{a, \tau(a)} : a \in \mathfrak{P}\}.$$

Teorema 4.3. *Ove definita, la direzione di una traslazione destra è una classe di parallelismo per* $\|_l$*, mentre quella di una traslazione sinistra è una classe di parallelismo per* $\|_r$*.*

Dimostrazione. Per semplicità ragioniamo solo sulle traslazioni sinistre. Per ogni $A \in \mathfrak{R}$ indichiamo con $[A]_r$ la classe di parallelismo destro di A. Sia τ una traslazione sinistra di $(\mathfrak{P}, \mathfrak{R}, \|_l, \|_r)$. Evidentemente $\mathrm{Dir}(\tau) \neq \emptyset$. Sia $A \in \mathrm{Dir}(\tau)$. Per il punto 2 della definizione di traslazione sinistra

$$A \in \mathrm{Dir}(\tau) \Rightarrow [A]_r \subseteq \mathrm{Dir}(\tau).$$

Supponiamo ora esista $B \in \mathrm{Dir}(\tau)$ tale che $A \not\|_r B$. Allora

$$\forall x \in \mathfrak{P} : \{x\} = (x \|_r A) \cap (x \|_r B).$$

A questo punto, ragionando come nel teorema precedente, si verifica che x deve essere fissato, cioè che $\tau = 1$, contro l'ipotesi $\tau \neq 1$. Per conseguenza

$$\mathrm{Dir}(\tau) \subseteq [A]_r,$$

che è la tesi. $\square$

È possibile caratterizzare gli spazi prismatici mediante gli insiemi di traslazioni nel seguente modo:

Teorema 4.4. *Sia* $(\mathfrak{P}, \mathfrak{R}, \|_l, \|_r)$ *uno spazio doppio con almeno due rette. Allora chiamato* T_l *l'insieme delle sue traslazioni sinistre:*

1. $(\mathfrak{P}, \mathfrak{R}, \|_l, \|_r)$ *è uno spazio prismatico sinistro se e solo se* T_l *è un insieme transitivo su* $\mathfrak{P}$*.*

2. *Se T_l è transitivo su $\mathfrak{P}$ ed è un gruppo, allora $(\mathfrak{P}, \mathfrak{R}, \|_l, \|_r)$ è uno spazio prismatico.*

DIMOSTRAZIONE.

1.

- ($\Rightarrow$) Siano $p, q \in \mathfrak{P}$ con $p \neq q$, e sia $c \in \mathfrak{P} \setminus \overline{p,q}$. Poniamo

$$\tau' : \begin{cases} \mathfrak{P} \setminus \overline{p,q} \to \mathfrak{P} \setminus \overline{p,q} \\ x \to \{q \|_l \overline{p,x}\} \cap \{x \|_r \overline{p,q}\} \end{cases}$$

e

$$\tau : \begin{cases} \mathfrak{P} \to \mathfrak{P} \\ x \to \begin{cases} \tau'(x) & \text{se } x \notin \overline{p,q} \\ \overline{p,q} \cap \{\tau'(c) \|_l \overline{c,x}\} & \text{se } x \in \overline{p,q} \end{cases} \end{cases}$$

Si verifica che τ è una biiezione tale che $\tau(p) = q$. Inoltre per la configurazione destra-sinistra di Desargues l'applicazione τ è indipendente dalla scelta di c e $\forall R \in \mathfrak{R} : \tau(R) \| R$.

- ($\Leftarrow$) Siano assegnati sei punti $a_i, b_i \in \mathfrak{P}$ per $i = 1, 2, 3$ in modo tale che:

$$\forall i, j \in \{1, 2, 3\} : R_i = \overline{a_i, b_i} \|_r \overline{a_j, b_j} = R_j$$

$$\forall i \in \{1, 2\} : \overline{a_i, a_{i+1}} \|_l \overline{b_i, b_{i+1}}.$$

Poichè T_l è transitivo esiste $\tau \in \mathcal{T}_l$ tale che $\tau(a_2) = b_2$. Per conseguenza

$$\forall i \in \{1, 2, 3\} : \tau(R_i) = R_i.$$

Inoltre, essendo τ una traslazione sinistra

$$\tau(\overline{a_1, a_2}) \|_l \overline{a_1, a_2}$$

da cui scende in particolare

$$\tau(a_1) = R_1 \cap (b_2 \|_l \overline{a_1, a_2}) = b_1.$$

Similmente si verifica che $\tau(a_3) = b_3$, e dunque

$$\overline{a_1, a_3} \|_l \overline{\tau(a_1), \tau(a_3)} = \overline{b_1, b_3},$$

cioè la configurazione destra-sinistra di Desargues si chiude.

2. Per il punto precedente $(\mathfrak{P}, \mathfrak{R}, \|_l, \|_r)$ è uno spazio prismatico sinistro.

   Assegnati sei punti $a_i, b_i \in \mathfrak{P}$ per $i = 1, 2, 3$ in modo tale che:

$$\forall i, j \in \{1, 2, 3\} : R_i = \overline{a_i, b_i} \parallel_l \overline{a_j, b_j} = R_j$$

$$\forall i \in \{1, 2\} : \overline{a_i, a_{i+1}} \parallel_r \overline{b_i, b_{i+1}}.$$

   abbiamo che esistono certamente $\tau_1, \tau_2 \in T_l$ tali che $\tau_1(a_1) = a_2$ e $\tau_2(a_2) = a_3$, e dunque è vero che anche $\tau_1(b_1) = b_2$ e $\tau_2(b_2) = b_3$. Poichè T_l è un gruppo $\tau_2\tau_1 \in T_l$ ed inoltre:

$$\overline{a_1, a_3} = \overline{a_1, \tau_2\tau_1(a_1)} \parallel_r \overline{b_1, \tau_2\tau_1(b_1)} = \overline{b_1, b_3}.$$

   Questo dimostra che $(\mathfrak{P}, \mathfrak{R}, \|_l, \|_r)$ è anche uno spazio prismatico destro, da cui la tesi.

□

Teorema 4.5. *Sia $(\mathfrak{P}, \mathcal{G}, \|_l, \|_r)$ uno spazio prismatico sinistro, e sia T_r l'insieme delle sue traslazioni destre. Allora T_r è un gruppo.*

DIMOSTRAZIONE. Evidentemente $\tau \in T_r$ implica $\tau^{-1} \in T_r$. Supponiamo $\tau_1, \tau_2 \in T_r$ e $\tau_2 \neq {\tau_1}^{-1}$. Allora in primo luogo:

$$\forall R \in \mathcal{G} : \tau_2\tau_1(R) \parallel_r \tau_1(R) \parallel_r R.$$

Supponiamo ora $H \in \mathcal{G}$ tale che $\tau_2\tau_1(H) = H$, e sia $X \parallel_l H$. Allora abbiamo $\forall a \in H, \forall x \in X$:

$$\overline{a, x} \parallel_r \overline{\tau_1(a), \tau_1(x)} \parallel_r \overline{\tau_2\tau_1(a), \tau_2\tau_1(x)};$$

$$\overline{a, \tau_1(a)} \parallel_l \overline{x, \tau_1(x)}$$

e infine

$$\overline{\tau_1(a), \tau_2\tau_1(a)} \parallel_l \overline{\tau_1(x), \tau_2\tau_1(x)}.$$

A questo punto applicando la configurazione destra-sinistra di Desargues si ottiene

$$H = \overline{a, \tau_2\tau_1(a)} \parallel_l \overline{x, \tau_2\tau_1(x)}.$$

Da ciò segue $\tau_2\tau_1(x) \in (x \parallel_l H) = X$, e dunque $\tau_2\tau_1(X) = X$. Segue

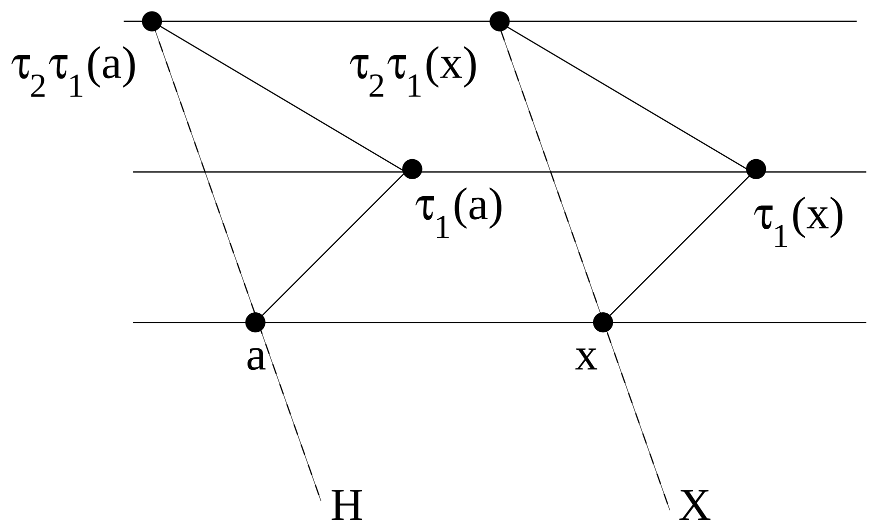

FIGURA 6. $\tau_2\tau_1(x) \in X$

la tesi. $\square$

Osservazione. I due teoremi precedenti asseriscono che in ogni spazio prismatico con più di una retta sia l'insieme delle traslazioni destre che quello delle traslazioni sinistre costituiscono gruppo.

Teorema 4.6. *Sia* $(\mathfrak{P}, \mathfrak{R}, \|_l, \|_r)$ *uno spazio doppio. Allora ogni traslazione sinistra (risp. destra) è univocamente determinata dalla sua azione su di un punto.*

DIMOSTRAZIONE. Sia $\tau \in T_l$, e sia $a \in \mathfrak{P}$ tale che $\tau(a) = b$. Allora Per ogni punto $p \in \mathfrak{P}$ si verifica che

$$\tau(p) = (b \,\|_l\, \overline{a, x}) \cap (x \,\|_r\, \overline{a, b}),$$

dal che discende immediatamente la tesi. $\square$

Definizione 4.29. Sia $(\mathfrak{P}, \mathfrak{R}, \|)$ uno spazio di incidenza con parallelismo, e sia $R \in \mathfrak{R}$ una retta. Diciamo che la direzione di R è **di traslazione centrale** se e solo se, indicato con Σ l'insieme[8] di tutte le traslazioni di $(\mathfrak{P}, \mathfrak{R}, \|)$

$$\forall \tau \in \Sigma; \forall S \in \mathfrak{R} : \tau(R) = R \& R \parallel S \Rightarrow \tau(S) = S$$

[8]non si tratta in generale di un gruppo

Definizione 4.30. Sia $(\mathfrak{P}, \mathfrak{R}, \|)$ una A-struttura. Esso viene chiamato **S-spazio**, o **spazio di Sperner** se e solo se:

$$\forall R, S \in \mathfrak{R} : |R| = |S|.$$

In [**Mar77**], pagg. 42-43 è dimostrato il seguente teorema:

Teorema 4.7. *Un S-spazio è di traslazione centrale se e solo se in esso vale l'assioma di chiusura dei parallelogrammi, ed inoltre è soddisfatta la configurazione (Ad) per ogni opportuna sestupla di punti.*

Osservazione. In effetti si verifica che la dimostrazione di tale risultato può essere estesa ad ogni A-struttura.

2.3. La piccola configurazione di Pappo.

Definizione 4.31. Sia $(\mathfrak{P}, \mathfrak{R}, \|)$ uno spazio di incidenza con parallelismo. Siano inoltre $R, S \in \mathfrak{R}$ tali che $R \parallel S$. Supponiamo inoltre siano assegnati sei punti $a_i \in R$,$b_i \in S$ per $i = 1, 2, 3$ tali che

$$\overline{a_1, b_3} \parallel \overline{b_1, a_3};$$

$$\overline{a_2, b_3} \parallel \overline{b_2, a_3}.$$

Diciamo che tali punti soddisfano la **piccola configurazione di**

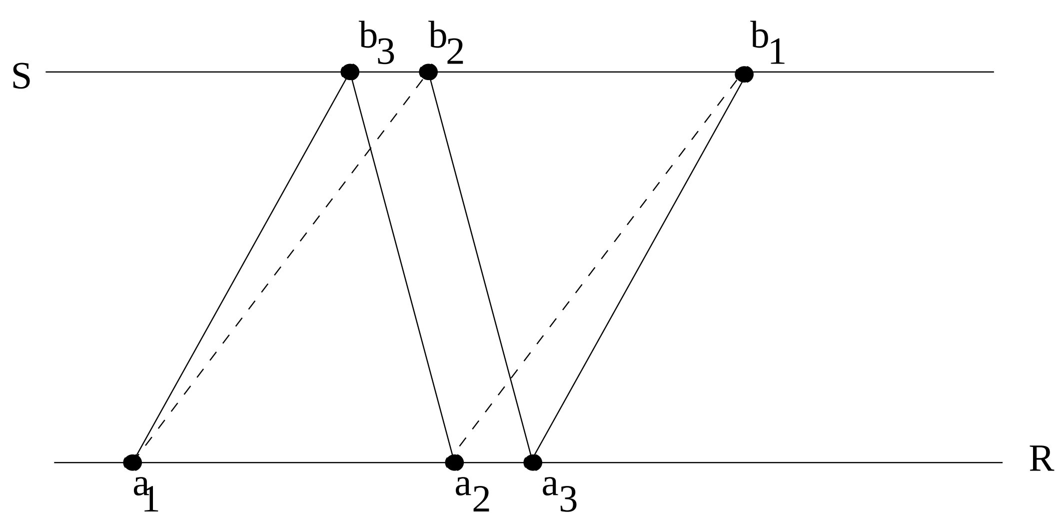

FIGURA 7. (Ap)

Pappo se è vero che

$$\overline{a_1, b_2} \parallel \overline{b_1, a_2}.$$

È logico fornire la seguente generalizzazione

Definizione 4.32. Sia $(\mathfrak{P}, \mathfrak{R}, \|_l, \|_r)$ uno spazio doppio. Siano inoltre $R, S \in \mathfrak{R}$ tali che $R \|_r S$. Supponiamo inoltre siano assegnati sei punti $a_i \in R$,$b_i \in S$ per $i = 1, 2, 3$ tali che

$$\overline{a_1, b_3} \|_l \overline{b_1, a_3};$$

$$\overline{a_2, b_3} \|_l \overline{b_2, a_3}.$$

Diciamo che tali punti soddisfano la **configurazione di Pappo Destra-sinistra** se è vero che

$$\overline{a_1, b_2} \|_l \overline{b_1, a_2}.$$

Similmente si definisce la **configurazione di Pappo Sinistra-destra**.

È stato mostrato da H.Karzel in [**Kar73**] che in generale, a differenza di quanto accade nel caso affine, la configurazione Destra-sinistra di Desargues *non* implica[9] la configurazione di Pappo Destra-sinistra.

3. Gruppi di incidenza

3.1. Strutture associate a gruppi fibrati.

Teorema 4.8. *Sia $(\mathcal{G}, \cdot)$ un gruppo. Supponiamo che $\mathcal{G}$ ammetta una partizione non banale $\pi(\mathcal{G})$. Allora posto:*

$$\mathfrak{R} := \{Yg : g \in \mathcal{G}; Y \in \pi(\mathcal{G})\}$$

e

$$\mathfrak{R}' := \{gY : g \in \mathcal{G}; Y \in \pi(\mathcal{G})\}$$

si ottiene che $(\mathcal{G}, \mathfrak{R})$ e $(\mathcal{G}, \mathfrak{R}')$ sono entrambi spazi di incidenza.

[9] si tratta di "piccole" configurazioni!

Dimostrazione. Evidentemente $\pi(\mathcal{G}) \subseteq \mathfrak{R}$, e dunque $|\mathfrak{R}| > 1$. Ragioniamo, per praticità, solo sui laterali destri. Siano $a, b \in \mathcal{G}$. Per definizione di partizione esiste esattamente uno ed un solo elemento Y di $\pi(\mathcal{G})$ tale che $ba^{-1} \in \pi(\mathcal{G})$. Consideriamo il laterale $Ya \in \mathfrak{R}$. Poichè $1 \in Y$, $a \in Ya$; da $ba^{-1} \in Y$ segue inoltre $b \in Ya$. Se esistesse un altro laterale $Zt \in \mathfrak{R}$ tale che $\{a, b\} \in Zt$, allora, dovremmo in primo luogo avere $Zt = Za$, in quanto

$$a \in Zt \Rightarrow a = zt \Rightarrow t = z^{-1}a \Rightarrow t \in Za.$$

A questo punto, per l'unicità dello $Y \in \pi(\mathcal{G})$ tale che $\{1, ba^{-1}\} \subseteq Y$, si ha immediatamente $Z = Y$, da cui scende l'unicità della retta per due punti.

Evidentemente il medesimo ragionamento si può appilicare anche sui laterali sinistri, e abbiamo dunque la tesi. □

Corollario 4.1. *Sia $\mathcal{G}$ un gruppo con partizione e sia $(\mathcal{G}, \mathfrak{R})$ lo spazio lineare costruito a partire dai laterali destri di una sua fissata partizione*[10] *$\pi(\mathcal{G})$ come nel teorema precedente. Sia $p \in \mathcal{G}$. Allora la generica retta di $(\mathcal{G}, \mathfrak{R})$ passante per p ha la forma Xp con $X \in \pi(\mathcal{G})$.*

Dimostrazione. Sia $H \in \mathfrak{R}$ tale che $p \in H$. Per definizione di $\mathfrak{R}$:

$$H \in \mathfrak{R} \Rightarrow \exists X \in \pi(\mathcal{G}), q \in \mathcal{G} : H = Xq$$

Dunque $\exists x \in H : p = xq$. D'altro canto $X < \mathcal{G} \Rightarrow x^{-1} \in X$, e per conseguenza $q = x^{-1}p$ e $q \in Xp$. Allora $\{p, q\} \subseteq Xp \cap Xq$ da cui la tesi $Xp = Xq = H$. □

Gli spazi di incidenza costruiti in questo modo risultano tutti essere A-strutture. Vale infatti il seguente teorema:

Teorema 4.9. *Sia $\mathcal{G}$ un gruppo con fibrazione $\pi(\mathcal{G})$, e sia $(\mathcal{G}, \mathfrak{R})$ lo spazio di incidenza destro ad esso associato, costruito come nel teorema 4.8. Allora $(\mathcal{G}, \mathfrak{R})$ ammette parallelismo.*

[10] evidentemente si può ragionare esattamente nel medesimo modo a partire dai laterali sinistri

Dimostrazione. Siano $R, S \in \mathfrak{R}$ due rette. Poniamo

$$R \parallel S \Leftrightarrow RR^{-1} = SS^{-1}.$$

Verifichiamo ora che $\parallel$ è un parallelismo:

- $\parallel$ è banalmente una relazione di equivalenza.
- d'altro canto data una retta R ed un punto h esiste sempre una retta S tale che $h \in S$ e $S \parallel R$. Infatti siccome $R \in \mathfrak{R}$ esiste certamente un $T \in \pi(\mathcal{G})$ tale che $R = Tg$ per qualche $g \in R$. Allora possiamo porre $S := Th$, ed è immediato verificare che $S \parallel R$.
- Supponiamo che esista una retta $H \in \mathfrak{R}$ ed un punto $h \in \mathcal{G}$ tale che $\exists A, B \in \mathfrak{R} : A \cap B = \{h\}$, e $H \parallel A$, $H \parallel B$. Ma A e B, si possono sicuramente scrivere a norma del corollario 4.1 come $A = Xh$, $B = Yh$ con $X, Y \in \pi(\mathcal{G})$. Allora

$$AA^{-1} = Xhh^{-1}X^{-1} = XX^{-1} = YY^{-1} = Yhh^{-1}Y^{-1} = BB^{-1},$$

  e, tenuto conto che $X, Y < \mathcal{G} \Rightarrow XX^{-1} = X \& YY^{-1} = Y$ si ha la tesi.

$\square$

Osservazione. La stessa dimostrazione può applicarsi allo spazio $(\mathcal{G}, \mathfrak{R}')$ del teorema 4.8, definendo però

$$\forall R, S \in \mathfrak{R}' : R \parallel S \Leftrightarrow R^{-1}R = S^{-1}S.$$

È possibile caratterizzare meglio la relazione di parallelismo:

Corollario 4.2. *Sia $\mathcal{G}$ un gruppo con partizione non banale $\pi(G)$, e sia $(\mathcal{G}, \mathfrak{R})$ lo spazio di incidenza associato a tale partizione costruito come nel teorema 4.8. Sia inoltre $\parallel$ definita come nel teorema precedente. Allora*

$$\forall R, S \in \mathfrak{R} : R \parallel S \Leftrightarrow \exists X \in \pi(G), r, s \in \mathcal{G} : R = Xr, S = Xs$$

Dimostrazione.

- $(\Leftarrow)$ $R = Xr \Rightarrow RR^{-1} = Xrr^{-1}X = X^2 = Xss^{-1}X = SS^{-1}$.

- ($\Rightarrow$) A norma del corollario 4.1 esistono $U, V \in \pi(\mathcal{G})$ tali che $R = Ur$, $S = Vs$ per $r \in R$ e $s \in S$. Ora

$$RR^{-1} = Urr^{-1}U^{-1} = UU^{-1} = U^2 = U$$

e similmente

$$SS^{-1} = Vss^{-1}V^{-1} = VV^{-1} = V^2 = V.$$

Allora necessariamente $U = V$ e quindi, posto $X = U$: $R = Xr$ ed $S = Xs$ che è la tesi.

□

Assegnato un gruppo fibrato $\mathcal{G}$ è possibile caratterizzare le sue partizioni che danno luogo a spazi doppi:

Teorema 4.10. *Sia $\mathcal{G}$ un gruppo fibrato con partizione $\pi(\mathcal{G})$, e siano $\mathfrak{R}$ ed $\mathfrak{R}'$ definiti come nel teorema 4.8. Supponiamo che inoltre $\mathfrak{R} = \mathfrak{R}'$, ovvero che come spazi di incidenza $(\mathcal{G}, \mathfrak{R})$ e $(\mathcal{G}, \mathfrak{R}')$ coincidano. Allora se poniamo*

$$\forall R, S \in \mathfrak{R} : R \parallel_r S \Leftrightarrow RR^{-1} = SS^{-1}$$

$$\forall R, S \in \mathfrak{R}' = \mathfrak{R} : R \parallel_l S \Leftrightarrow R^{-1}R = S^{-1}S$$

abbiamo che $(\mathcal{G}, \mathfrak{R}, \parallel_r, \parallel_l)$ è uno spazio doppio.

Dimostrazione. A norma del teorema 4.9 $(\mathcal{G}, \mathfrak{R}, \parallel_r)$ e $(\mathcal{G}, \mathfrak{R}, \parallel_l)$ sono due spazi di incidenza con parallelismo.

Siano ora (a, b, x) tre punti non allineati, e siano $A, B \in \pi(\mathcal{G})$ tali che:

$$xA = \overline{a, x}$$

$$Bx = \overline{b, x}.$$

Per il corollario 4.2 abbiamo allora:

$$b \in Bx \Rightarrow \exists \tilde{b} \in B : b = \tilde{b}x;$$

$$a \in xA \Rightarrow \exists \tilde{a} \in A : a = x\tilde{a}.$$

Dunque:

$$(b \parallel_r xA) = bA = \tilde{b}xA$$

e

$$(a \parallel_l Bx) = Ba = Bx\tilde{a}.$$

Poichè $\tilde{b} \in B$ e $\tilde{a} \in A$:

$$\tilde{b}x\tilde{a} \in Ba \cap bA \neq \emptyset$$

che è, per l'arbitrarietà di a, b, x la tesi. $\square$

Osservazione. Se $\mathcal{G}$ è un gruppo e $\pi(\mathcal{G})$ è una sua partizione allora gli spazi di incidenza $(\mathcal{G}, \mathfrak{R})$ e $(\mathcal{G}, \mathfrak{R}')$ derivati da tale partizione coincidono se e solo se $\pi(\mathcal{G})$ è normale.

Dimostrazione. Sia $Xa \in \mathfrak{R}$; poichè $\pi(\mathcal{G})$ è normale, allora

$$X \in \pi(G) \Rightarrow Y = X^{a^{-1}} = aXa^{-1} \in \pi(G).$$

Ma allora $Xa = aY \in \mathfrak{R}'$, e dunque $\mathfrak{R} \subseteq \mathfrak{R}'$. Ripetendo lo stesso ragionamento con gli elementi di $\mathfrak{R}'$ si ottiene la tesi $\mathfrak{R} = \mathfrak{R}'$.

Viceversa, supponiamo $\mathfrak{R} = \mathfrak{R}'$. Ciò significa che

$$\forall X \in \pi(\mathcal{G}), \forall x \in \mathcal{G} : \exists y \in \mathcal{G}, \exists Y \in \pi(\mathcal{G}) : Xx = yY$$

Da cui $xX^x = Xx = yY$, cioè $(y^{-1}x)X^x = Y \leq \mathcal{G}$. D'altro canto $1 \in X^x \cap Y$, e dunque

$$(y^{-1}x)^{-1} \in X^x \leq \mathcal{G} \Rightarrow X^x = Y.$$

Per conseguenza $\forall X \in \pi(\mathcal{G}), \forall x \in \mathcal{G} : X^x \in \pi(\mathcal{G})$, ovvero $\pi(\mathcal{G})$ è normale. $\square$

3.2. Spazi cinematici.

Definizione 4.33. Una struttura $(\mathfrak{P}, \mathfrak{R}, \cdot)$ di dice **gruppo di incidenza destro** se e solo se

- $(\mathfrak{P}, \mathfrak{R})$ è uno spazio di incidenza
- $(\mathfrak{P}, \cdot)$ è un gruppo

- $\forall a \in \mathfrak{P}$ l'applicazione

$$a_l : \begin{cases} \mathfrak{P} \to \mathfrak{P} \\ x \to a \cdot x \end{cases}$$

  è una collineazione di $(\mathfrak{P}, \mathfrak{R})$.

Similmente si possono definire gruppi di incidenza sinistri.

Definizione 4.34. Sia $(\mathfrak{P}, \mathfrak{R}, \cdot)$ un gruppo di incidenza. Supponiamo che 1 sia l'elemento neutro di $(\mathfrak{P}, \cdot)$. Allora $(\mathfrak{P}, \mathfrak{R}, \cdot)$ si dice **fibrato** se e solo se

$$\forall R \in \mathfrak{R} : 1 \in R \Rightarrow (R, \cdot) \leq (\mathfrak{P}, \cdot)$$

Definizione 4.35. Un gruppo di incidenza $(\mathfrak{P}, \mathfrak{R}, \cdot)$ si dice **bilatero** se e solo se è contemporaneamente un gruppo di incidenza destro e sinistro.

Definizione 4.36. Un gruppo di incidenza fibrato e bilatero si dice **spazio cinematico**.

Definizione 4.37. Sia $(\mathfrak{P}, \mathfrak{R}, \cdot)$ uno spazio cinematico. Si dice **sottospazio cinematico** di $(\mathfrak{P}, \mathfrak{R}, \cdot)$ ogni spazio cinematico $(\mathfrak{P}', \mathfrak{R}', \cdot)$ tale che $\mathfrak{P} \subseteq \mathfrak{P}'$ e $\mathfrak{R} \subseteq \mathfrak{R}'$.

Osservazione. È immediato verificare che affinchè un gruppo di incidenza $(\mathfrak{P}, \mathfrak{R}, \cdot)$ sia fibrato risulta indispensabile che il gruppo $(\mathfrak{P}, \cdot)$ sia fibrato. Inoltre, per l'esistenza e unicità della retta passante per due punti, tale gruppo deve ammettere una partizione $\pi(\mathfrak{P})$ tale che:

$$\forall R \in \mathfrak{R} : 1 \in R \Rightarrow R \in \pi(\mathfrak{P}),$$

e, viceversa

$$\forall R \in \pi(\mathfrak{P}) : R \in \mathfrak{R}.$$

Inoltre, essendo il prodotto a sinistra una collineazione, si verifica che

$$\forall R \in \mathfrak{R}, \forall r \in \mathfrak{R} : r^{-1}R \in \mathfrak{R} \& 1 \in r^{-1}R \Rightarrow R \in \pi(\mathfrak{P}).$$

Dunque la struttura geometrica dei gruppi di incidenza fibrati coincide con quella che era stata associata ai gruppi con partizione nel teorema 4.8.

In particolare ogni gruppo di incidenza è dotato naturalmente di un parallelismo.

Teorema 4.11. *Sia $(\mathfrak{P}, \mathfrak{R}, \cdot)$ uno spazio cinematico.*
Allora posto

$$\pi(\mathfrak{P}) := \{R \in \mathfrak{R} : 1 \in R\}$$

si verifica che $\pi(\mathfrak{P})$ è una partizione normale di $(\mathfrak{P}, \cdot)$.

Viceversa se $(\mathfrak{P}, \cdot)$ è un gruppo, $\pi(\mathfrak{P})$ è una sua partizione normale e $(\mathfrak{P}, \mathfrak{R})$ è lo spazio di incidenza costruito a partire da $\mathfrak{P}$ e da $\pi(\mathfrak{P})$ come nel teorema 4.8, allora $(\mathfrak{P}, \mathfrak{R}, \cdot)$ è uno spazio cinematico.

Dimostrazione. Per l'osservazione precedente $\pi(\mathfrak{P})$ deve essere una partizione di $\mathfrak{P}$. Supponiamo per assurdo che non sia normale. Allora in particolare esisteranno un $x \in \mathfrak{P}$ e un $N \in \pi(\mathfrak{P})$ tali che:

$$N^x = x^{-1}Nx \notin \pi(\mathfrak{P}).$$

D'altro canto:

$$1 \in \mathcal{N}^x \& N^x \notin \pi(\mathfrak{P}) \Rightarrow N^x \notin \mathfrak{R}.$$

Siccome $(\mathfrak{P}, \mathfrak{R}, \cdot)$ è bilatero abbiamo però che sia

$$x^{-1}{}_l : \begin{cases} \mathfrak{P} \to \mathfrak{P} \\ p \to x^{-1} \cdot p \end{cases}$$

che

$$x_r : \begin{cases} \mathfrak{P} \to \mathfrak{P} \\ p \to p \cdot x \end{cases}$$

sono collineazioni. In particolare abbiamo le seguenti implicazioni:

$$N \in \mathfrak{R} \Rightarrow x^{-1}{}_l(N) = x^{-1}N \in \mathfrak{R} \Rightarrow$$

$$\Rightarrow x_r(x^{-1}{}_l(N)) = x_r(x^{-1}N) = x^{-1}Nx = N^x \in \mathfrak{R}$$

contro l'ipotesi.

Il viceversa è ovvio. $\square$

Nel seguito quando tratteremo di spazi cinematici supporremo sempre assegnate le due relazioni di parallelismo destro e sinistro $\|_l$ e $\|_r$ canonicamente associate[11] al gruppo fibrato $(\mathfrak{P}, \cdot)$.

Conseguenza immediata del teorema precedente è che in ogni spazio cinematico è soddisfatto l'assioma di chiusura dei parallelogrammi misti. In effetti si può dimostrare molto di più:

Teorema 4.12. *Supponiamo che $(\mathfrak{P}, \mathfrak{R}, \cdot)$ sia uno spazio cinematico. Allora $(\mathfrak{P}, \mathfrak{R}, \|_l, \|_r)$ risulta essere in particolare uno spazio prismatico.*

Alla luce del teorema 4.4 ci basta provare il seguente enunciato:

Teorema 4.13. *Sia $(\mathfrak{P}, \mathfrak{R}, \cdot)$ uno spazio cinematico. Allora gli insiemi $\mathfrak{P}_l := \{x_l : x \in \mathfrak{P}\}$ e $\mathfrak{P}_r := \{x_r : x \in \mathfrak{P}\}$ sono due gruppi e contengono rispettivamente la totalità delle traslazioni sinistre ovvero destre di $(\mathfrak{P}, \mathfrak{R}, \|_l, \|_r)$.*

Dimostrazione. Per praticità ragioniamo solo su $\mathfrak{P}_l$.

- Che $\mathfrak{P}_l$ sia un gruppo transitivo su $\mathfrak{P}$ è ovvio.
- Sia $a_l \in \mathfrak{P}_l$. Se $a = 1$ non c'è nulla da dimostrare.

  Supponiamo dunque $a \neq 1$. Ma, per come è definito $\|_l$:

  $$\forall R, S \in \mathfrak{R} : R \|_l S \Leftrightarrow \exists r \in \mathfrak{P} : rR = S.$$

  e dunque $a_l(R) = aR \|_l R$.

  Sia ora $H \in \mathfrak{R}$, e supponiamo $a_l(H) = aH = H$. Se $S \in \mathfrak{R}$ e $S \|_r H$ allora esiste un $h \in \mathfrak{P}$ tale che $S = Hh$. Quindi

  $$a_l(S) = a_l(Hh) = aHh = Hh = S,$$

  da cui la tesi che $\mathfrak{P}_l$ sia un gruppo di traslazioni sinistre.
- Il fatto che $\mathfrak{P}_l$ consista di *tutte* le traslazioni sinistre è conseguenza del teorema 4.6.

  Infatti sia $a \in \mathfrak{P}$ e sia $\sigma \in T_l$. Allora $\exists b \in \mathfrak{P} : \sigma(a) = b$. Ma, poichè $\mathfrak{P}_l$ è regolare esiste certamente $\tau \in \mathfrak{P}_l$ tale che $\tau(a) = b$ e dunque per il teorema 4.6 $\sigma = \tau \in \mathfrak{P}_l$ che è la tesi.

[11] secondo il teorema 4.8

□

Tale risultato risulta essere invertibile. Infatti è stato dimostrato in [**KKS73**] il seguente importantissimo teorema:

Teorema 4.14. *Sia* $(\mathfrak{P}, \mathfrak{R}, \|_1, \|_2)$ *uno spazio prismatico. Allora esiste una operazione*

$$\cdot : \mathfrak{P} \times \mathfrak{P} \to \mathfrak{P}$$

tale che $(\mathfrak{P}, \mathfrak{R}, \cdot)$ *sia uno spazio cinematico e inoltre, chiamati* $\|_l$ *e* $\|_r$ *come in 4.10,* $\|_1 = \|_l$, $\|_2 = \|_r$.

Teorema 4.15. *Sia* $(\mathfrak{P}, \mathfrak{R}, \cdot)$ *uno spazio cinematico, e sia* $N \in \mathfrak{R}$ *tale che* $1 \in \mathcal{N}$. *La direzione di* N *è di traslazione centrale sinistra*[12] *se e solo se* $N \lhd \mathfrak{P}$.

Dimostrazione.

- $(\Rightarrow)$ Considerando la caratterizzazione delle traslazioni sinistre di $(\mathfrak{P}, \mathfrak{R}, \cdot)$ come nel teorema 4.13, e tenuto conto che $tN = N \Leftrightarrow t \in \mathcal{N}$ l'ipotesi diviene:

  $$\forall p \in \mathfrak{P}, \forall t \in \mathcal{N} : t(pN) = pN.$$

  Da questo segue:

  $$\forall p \in \mathfrak{P}, \forall t \in \mathcal{N} : p^{-1}tpN = N$$

  che equivale a:

  $$\forall p \in \mathfrak{P}, \forall t \in \mathcal{N} : p^{-1}tp \in N$$

  ovvero

  $$\forall p \in \mathfrak{P} : N^p = N \Rightarrow N \lhd \mathfrak{P}$$

  che è la tesi.
- $(\Leftarrow)$ Supponiamo $N \lhd \mathfrak{P}$. Visto che $\mathfrak{P}_l$ costituisce la totalità delle traslazioni sinistre di $(\mathfrak{P}, \mathfrak{R}, \cdot)$ ci basta mostrare che

  $$\forall p \in \mathfrak{P}, \forall n \in \mathcal{N} : npN = pN.$$

[12] tale ipotesi è superflua, ma necessaria per poter condurre a termine la dimostrazione

Ciò è banale, infatti

$$N \lhd \mathfrak{P} \Rightarrow \forall p \in \mathfrak{P} : pN = Np,$$

E dunque

$$npN = n(pN) = n(Np) = Np = pN,$$

che è la tesi.

$\square$

Osservazione. Evidentemente il medesimo ragionamento si può applicare alle traslazioni destre di $(\mathfrak{P}, \mathfrak{R}, \cdot)$. Inoltre la classe di parallelismo destra di $N \lhd \mathfrak{P}$ coincide con quella sinistra, per cui dal teorema precedente discende che in uno spazio doppio se una direzione è di traslazione centrale lo è sia per le traslazioni destre che per quelle sinistre.

La condizione che tutte le direzioni in uno spazio cinematico siano di traslazione centrale è in effetti molto forte:

Teorema 4.16. (Kontorovič) *Sia* $(\mathfrak{P}, \mathfrak{R}, \cdot)$ *uno spazio cinematico. Tutte le direzioni di* $\mathfrak{R}$ *sono di traslazione centrale se e solo se* $(\mathfrak{P}, \cdot)$ *è abeliano.*

DIMOSTRAZIONE.

- $(\Leftarrow)$ Se $(\mathfrak{P}, \cdot)$ è abeliano allora ogni suo sottogruppo è normale, da cui, mediante il teorema precedente, la tesi.
- $(\Rightarrow)$ Distinguiamo due situazioni possibili:
  1. Siano $R_1, R_2 \in \mathfrak{R}$ e $\tau_1, \tau_2 \in \mathfrak{P}_l \setminus \{1\}$ tali che $\tau_1(R_1) = R_1$; $\tau_2(R_2) = R_2$, ma $R_1 \not\parallel_l R_2$. Sia $x \in \mathfrak{P}$. Poniamo $x_1 := \tau_1(x)$ e $x_2 := \tau_2(x)$. Allora

$$\overline{x, x_1} \parallel_l R_1; \overline{x, x_2} \parallel_l R_2$$

ma

$$\overline{x, x_1} \not\parallel_l \overline{x, x_2}.$$

Ora, per l'ipotesi che le traslazioni siano centrali:

$$\tau_2(\overline{x,x_1}) = \overline{\tau_2(x),\tau_2\tau_1(x)} \parallel_l \overline{x,x_1}$$

$$\tau_1(\overline{x,x_2}) = \overline{\tau_1(x),\tau_1\tau_2(x)} \parallel_l \overline{x,x_2}.$$

Applicando τ_1 alla prima uguaglianza e τ_2 alla seconda si ottiene:

$$\tau_1\tau_2(\overline{x,x_1}) = \overline{\tau_1\tau_2(x),\tau_1\tau_2\tau_1(x)}$$

$$\tau_2\tau_1(\overline{x,x_2}) = \overline{\tau_2\tau_1(x),\tau_2\tau_1\tau_2(x)}.$$

Da questo si ottiene immediatamente:

$$\{\tau_1\tau_2(x),\tau_2\tau_1(x)\} \subseteq \tau_2(\overline{x,x_1}) \cap \tau_1(\overline{x,x_2}).$$

D'altro canto due rette possono intersecarsi al più in un punto, e dunque

$$\tau_1\tau_2(x) = \tau_2\tau_1(x).$$

Poichè una traslazione è individuata dalla sua azione su di un punto, segue la tesi.

2. Supponiamo ora che $R \in \mathfrak{R}$ e $\tau_1,\tau_2 \in \mathfrak{P}_l \setminus \{1\}$ tali che $\tau_1(R) = \tau_2(R) = R$. Supponiamo che

$$\forall x \in \mathfrak{P} : \tau_1(x) = a_1x \;\&\; \tau_2(x) = a_2x.$$

Se $\tau_1 = {\tau_2}^{-1}$ non c'è nulla da dimostrare. Sia altrimenti $b \in \mathfrak{P} \setminus R$. Allora la traslazione

$$\sigma : \begin{cases} \mathfrak{P} \to \mathfrak{P}; \\ x \to bx \end{cases}$$

possiede una direzione diversa da R, e dunque commuta sia con τ_1 che con τ_2. Inoltre la direzione di $\tau_1\sigma$ è diversa da quella di τ_1. Pertanto si desume che:

$$\tau_1\tau_2 = \tau_1\sigma\sigma^{-1}\tau_2 = \tau_1\sigma\tau_2\sigma^{-1} =$$

$$\tau_2\tau_1\sigma\sigma^{-1} = \tau_2\tau_1$$

che è la tesi.

□

Tenuto conto della corrispondenza esistente fra gli spazi cinematici e i gruppi fibrati dotati di partizione normale, l'enunciato appena dimostrato è equivalente al teorema 3.8. Vale la pena di osservare che la dimostrazione appena presentata è condotta con metodi puramente geometrici.

Relativamente i sottogruppi normali di una partizione è interessante dimostrare il seguente risultato:

Teorema 4.17. *Sia* $(\mathfrak{P}, \mathfrak{R}, \cdot)$ *uno spazio cinematico, derivato dalla partizione* $\pi(\mathfrak{P})$. *Supponiamo* $X \in \pi(\mathfrak{P})$ *tale che* $X \lhd \pi(\mathfrak{P})$. *Sia poi* $R \in \mathfrak{R}$ *tale che* $R \parallel_l X$. *Allora*

$$\forall S \in \mathfrak{R} : R \parallel_l S \Leftrightarrow R \parallel_r S$$

DIMOSTRAZIONE. Ovviamente R si può scrivere come rX, ma $X \lhd \mathfrak{P}$ implica in particolare che i laterali destri di X coincidono con i laterali sinistri, e dunque,

$$R \parallel_l S \Leftrightarrow R = rX \& S = sX \Leftrightarrow R = Xr \& S = Xs \Leftrightarrow R \parallel_r S$$

che è la tesi. □

In ogni struttura di André $(\mathfrak{P}, \mathfrak{R}, \parallel)$, e dunque anche in ogni spazio cinematico, si possono definire due diversi operatori di chiusura:

- uno è la chiusura di incidenza introdotta nella definizione 4.13,
- l'altro è la **chiusura affine**, che associa ad ogni sottoinsieme T di $\mathfrak{P}$ il più piccolo sottospazio di $(\mathfrak{P}, \mathfrak{R}, \parallel)$ contenente T e soddisfacente gli assiomi di spazio di incidenza con parallelismo.

Sebbene il tipo di chiusura "naturale" per uno spazio con parallelismo sia il secondo, per consistenza con le definizioni fornite in generale per gli spazi di incidenza indicheremo la chiusura affine di un insieme $S \subseteq P$ col simbolo $\overline{S}^A$, mentre la chiusura di incidenza resterà denotata con il simbolo $\overline{S}$. Osserviamo che in generale vale la relazione:

$$\forall S \subseteq \mathfrak{P} : \overline{S} \subseteq \overline{S}^A.$$

In generale uno spazio cinematico *non* è uno spazio di scambio rispetto la chiusura di incidenza. Vale comunque il seguente teorema (vedi [**KK80**]):

Teorema 4.18. (Karzel, Kroll) *Sia* $(\mathfrak{P}, \mathfrak{R}, \cdot)$ *uno spazio cinematico, e sia*

$$\mathfrak{R}_p := \{R \in \mathfrak{R} : \forall S \in \{A \in \mathfrak{R} : \exists p : A \subseteq \overline{R \cup \{p\}}\} : R \cap S \neq \emptyset\}$$

Allora $\forall R \in \mathfrak{R}_p, \forall p \in \mathfrak{P} \setminus \mathfrak{R}_p$ *il piano*

$$\Pi := \overline{R \cup \{p\}}$$

è di scambio.

Rammentiamo la seguente definizione:

Definizione 4.38. Sia $(\mathfrak{P}, \mathfrak{R})$ uno spazio di incidenza proprio. Esso si dice **piano proiettivo** se sono soddisfatte le seguenti condizioni:

- $\forall R \in \mathfrak{R} : |R| \geq 3$;
- (P): $\forall R, S \in \mathfrak{R} : R \cap S \neq \emptyset$.

Si nota subito che il piano Π definito nel teorema *non* è dotato di parallelismo; in effetti in esso vale la proprietà (P) tipica delle rette dei piani proiettivi. Non è vero però che tutte le rette abbiano cardinalità maggiore o uguale a 3. Dunque Π, come costruito nel teorema *non* è un propriamente piano proiettivo. Strutture di questo genere, vengono chiamate in [**Tei86**] **piani proiettivi generalizzati**.

Dimostrazione. Sia $R \in \mathfrak{R}_p$. Supponiamo $p \in \mathfrak{P} \setminus \mathfrak{R}_p$. Poniamo

$$\mathfrak{P}' := \overline{R \cup \{p\}}$$

e

$$\mathfrak{R}' := \{S \in \mathfrak{R} : S \subseteq \mathfrak{P}'\}.$$

La tesi del teorema è che $(\mathfrak{P}', \mathfrak{R}')$ è uno spazio di scambio, ovvero, tenuto conto che $(\mathfrak{P}', \mathfrak{R}')$ ha dimensione 2 che

$$\forall a, b, c \in \mathfrak{P}' : |\{a, b, c\}| = 3, c \notin \overline{a, b} \Rightarrow \overline{\{a, b, c\}} = \mathfrak{P}'.$$

- Se $a, b \in R$, $c = p$ non c'è niente da dimostrare.
- Supponiamo $a, b \in \mathfrak{R}$, $c \neq p$. Poichè $\{c, p\} \subseteq \mathfrak{P}'$ sicuramente $\overline{c, p} \in \mathfrak{R}'$. D'altro canto per definizione di $\mathfrak{R}_p$:

$$\overline{c, p} \cap R = \{m\} \neq \emptyset.$$

Ma allora

$$m \in R \Rightarrow \overline{m, c} \subseteq \overline{\{a, b, c\}} = \overline{R \cup \{c\}} \Rightarrow$$

$$\Rightarrow p \in \overline{\{a, b, c\}} \Rightarrow \mathfrak{P}' = \overline{R \cup \{p\}} \subseteq \overline{\{a, b, c\}}$$

che, essendo ovvia l'inclusione inversa, è la tesi.

- Supponiamo dunque che $|\{a, b, c\} \cap R| \leq 1$. Almeno uno dei punti a, b, c, diciamo c non appartiena ad R. Per la condizione su $\mathfrak{R}_p$ possiamo scrivere:

$$\overline{a, c} \cap R = \{a'\} \in R;$$

$$\overline{b, c} \cap R = \{b'\} \in R.$$

Dunque $R = \overline{a', b'} \subseteq \overline{\{a, b, c\}}$, e per conseguenza

$$\mathfrak{P}' = \overline{R \cup \{c\}} \subseteq \overline{\{a, b, c\}}.$$

Poichè il viceversa è ovvio, il teorema è così dimostrato.

□

CAPITOLO 5

Spazi cinematici derivati da Gruppi di Frobenius

Nel corso di questo capitolo si denoterà abitualmente con $\mathcal{G}$ un gruppo *finito* di Frobenius di nucleo $\mathcal{N}$. Con $\mathcal{H}$ si interà un complemento di $\mathcal{N}$ in $\mathcal{G}$ arbitrariamente fissato. Col simbolo $\mathfrak{F}(\mathcal{G})$ verrà indicata la partizione di Frobenius associata a $\mathcal{G}$, ovvero l'insieme:

$$\mathfrak{F}(\mathcal{G}) := \{H^x : \mathcal{G} := N \rtimes \mathcal{H}, x \in \mathcal{N}\} \cup \{\mathcal{N}\}.$$

1. Proprietà generali

Definizione 5.1. Sia $(\mathfrak{P}, \mathfrak{R})$ uno spazio di incidenza. Per ogni $p \in \mathfrak{P}$ si dice **grado di** p il numero di rette di $\mathfrak{R}$ passanti per p. Indicheremo tale numero col simbolo $\deg_{\mathfrak{R}} p$, o, più semplicemente, ove sia chiaro dal contesto a quale struttura lineare si sta facendo riferimento con $\deg p$.

Se S è un sottospazio di $(\mathfrak{P}, \mathfrak{R})$ useremo la notazione $\deg_S p$ per indicare il numero di rette incluse in S passanti per p, ovvero il numero $\deg_{\mathfrak{R}'} p$ ove

$$\mathfrak{R}' := \{R \in \mathfrak{R} : R \subseteq S\}.$$

Osservazione. Sia $(\mathfrak{P}, \mathfrak{R})$ uno spazio di incidenza, e sia $S \subseteq \mathfrak{P}$ un suo sottospazio. Se esiste $p \in S$ tale che

$$\deg_{\mathfrak{R}} p = \deg_S p < \infty,$$

allora $S = \mathfrak{P}$.

Dimostrazione. Per l'assioma che garantisce l'esistenza della retta per due punti di $\mathfrak{P}$ abbiamo

$$\mathfrak{P} = \bigcup_{x \in \mathfrak{P}} \overline{p, x} = \bigcup\nolimits_{p \in R_p}^{R_p \in \mathfrak{R}} R_p.$$

L'ipotesi $\deg_{\mathfrak{R}} p = \deg_S p < \infty$ implica che tutte le rette passanti per p in $(\mathfrak{P}, \mathfrak{R})$ sono interamente incluse in S, e dunque $\mathfrak{P} \subseteq S$. Essendo l'altra inclusione ovvia abbiamo la tesi. $\square$

È facile verificare che in uno spazio cinematico derivato da un gruppo di Frobenius si ha per ogni punto p:

$$\deg p = |\mathfrak{F}(\mathcal{G})| = |\mathcal{N}| + 1.$$

Teorema 5.1. *Sia $(\mathcal{G}, \mathfrak{R}, \cdot)$ lo spazio cinematico derivato dalla partizione $\mathfrak{F}(\mathcal{G})$ di un gruppo di Frobenius. Allora*

$$\forall A, B \in \mathfrak{R} : A \parallel_l B \& A \parallel_r B \Leftrightarrow A = B \mathit{oppure}\ A \parallel_l \mathcal{N}$$

DIMOSTRAZIONE.

- ($\Leftarrow$) Se $A = B$ non c'è nulla da dimostrare; se $A \parallel_l N$ si tratta del teorema 4.17.
- ($\Rightarrow$) Per il teorema di Kegel (Th 3.7) $\mathcal{H} = \mathrm{N}_{\mathcal{G}}(\mathcal{H})$, ovvero

  $$\forall x \in \mathcal{G} : \mathcal{H}x = x\mathcal{H} \Rightarrow x \in \mathcal{H},$$

  cosa che, per l'arbitrarietà di $\mathcal{H}$, si può anche scrivere come

  $$\forall a, x \in \mathcal{G} : \mathcal{H}^x a = a\mathcal{H}^x \Leftrightarrow a \in \mathcal{H}^x.$$

  Sia $p \in \mathcal{G}$, e sia $A \in \mathfrak{R}$. Supponiamo $a \in A$. Allora

  $$(p \parallel_l A) = pa^{-1}A$$

  e

  $$(p \parallel_r A) = Aa^{-1}p$$

  Ma

  $$pa^{-1}A = Aa^{-1}p \Leftrightarrow Aa^{-1}p = pa^{-1}Aa^{-1}a \Leftrightarrow$$

  $$\Leftrightarrow (Aa^{-1})(pa^{-1}) = (pa^{-1})(Aa^{-1}) \Leftrightarrow$$

  $$\Leftrightarrow pa^{-1} \in Aa^{-1} \Leftrightarrow pa^{-1} \in \mathrm{N}_{\mathcal{G}}\left(Aa^{-1}\right)$$

  Se $Aa^{-1} = \mathcal{N} \lhd \mathcal{G}$ la condizione è sempre soddisfatta; altrimenti per quanto osservato sopra

  $$pa^{-1} \in \mathrm{N}_{\mathcal{G}}\left(Aa^{-1}\right) \Leftrightarrow pa^{-1} \in Aa^{-1} \Leftrightarrow p \in A.$$

Da ciò discende che se $p \notin A$, e $A \not\parallel_l \mathcal{N}$ la parallela destra e la parallela sinistra per p ad A devono essere distinte, che è la tesi.

$\square$

Lemma 5.1. *Sia G un gruppo di Frobenius, e $(\mathcal{G}, \mathfrak{R}, \|_l, \|_r)$ lo spazio cinematico associato alla sua partizione $\mathfrak{F}(\mathcal{G})$. Posto*

$$[\mathcal{N}] := \{S \in \mathfrak{R} : S \parallel_l \mathcal{N}\}$$

si ha che

$$\forall R \in \mathfrak{R} \setminus [\mathcal{N}], \forall S \in [\mathcal{N}] : R \cap S \neq \emptyset$$

Dimostrazione. Sia $R \in \mathfrak{R} \setminus [\mathcal{N}]$ e $S \in [\mathcal{N}]$. Per definizione di spazio di incidenza, tenuto conto che $R \neq S$, si ha che:

$$\exists p \in R \setminus S.$$

Supponiamo per assurdo $R \cap S = \emptyset$. Si verifica immediatamente che:

$$\forall q_1, q_2 \in S : \overline{p, q_1} = \overline{p, q_2} \Leftrightarrow q_1 = q_2.$$

In tale modo abbiamo scritto n rette distinte, tutte passanti per p, e aventi intersezione non vuota con S. Per l'osservazione precedente abbiamo $\deg p = n + 1$, e dunque R deve essere l'unica retta per p che non può essere scritta in tale modo. D'altro canto $(\mathfrak{P}, \mathfrak{R}, \|_l)$ è uno spazio di incidenza con parallelismo. In particolare deve esistere una retta T tale che $p \in \mathcal{T}$ e $T \parallel_l R$. Per quanto visto nel capitolo 4:

$$T \neq S \& T \parallel_l S \Rightarrow T \cap S = \emptyset.$$

Ma allora, per l'unicità $R = T$ e dunque $R \in [\mathcal{N}]$, assurdo. Segue la tesi. $\square$

Osservazione. Dal lemma precedente discende immediatamente che $\forall R \in \mathfrak{R}$:

$$R \parallel_l \mathcal{N} \Leftrightarrow R \cap \mathcal{N} = \emptyset \text{ oppure } R = \mathcal{N} \Leftrightarrow$$

$$\Leftrightarrow R \parallel_A \mathcal{N} \Leftrightarrow R \parallel_r \mathcal{N},$$

ove con $\|_A$ si è inteso il parallelismo affine.

Il lemma precedente consente di dimostrare un risultato molto forte:

Teorema 5.2. *Sia $\mathcal{G}$ un gruppo di Frobenius e sia $(\mathcal{G}, \mathfrak{R})$ lo spazio cinematico associato alla sua partizione $\mathfrak{F}(\mathcal{G})$. Se*

$$|\mathcal{H}| > 2,$$

allora $(\mathcal{G}, \mathfrak{R})$ è uno spazio di scambio e

$$\dim(\mathcal{G}, \mathfrak{R}) = 2.$$

Dimostrazione. Siano a, b, c tre punti non allineati, e sia $\pi = \overline{\{a, b, c\}}$. Possiamo supporre senza perdere in generalità che $\{\overline{a, b}, \overline{a, c}\} \cap [\mathcal{N}] = \emptyset$.

Poniamo allora

$$T := (a \parallel \mathcal{N})$$

$$R := (c \parallel \mathcal{N}),$$

e sia $S \in [\mathcal{N}] \setminus \{T, R\}$. Per il lemma 5.1 siamo sicuri che

$$|R \cap \overline{a, b}| = 1$$

e dunque possiamo porre

$$\{d\} = R \cap \overline{a, b}.$$

Poichè $\overline{a, b} \notin [\mathcal{N}]$, $|\overline{a, b}| = |\mathcal{H}| > 2$. Esiste dunque

$$e \in \overline{a, b} \setminus \{a, d\}.$$

Poichè $d \in \overline{a, b} \subseteq \pi$, la retta $\overline{c, d} = R$ deve essere tutta inclusa in π. D'altro canto $e \in \overline{a, b} \subseteq \pi$ implica $\overline{c, e} \subseteq \pi$. Sempre per il lemma 5.1, $T \cap \overline{c, e} \neq \emptyset$, e sia

$$\{f\} = T \cap \overline{c, e}.$$

Evidentemente $f \in \pi$, e dunque $T = \overline{a, f} \subseteq \pi$.

Ora, per c passano n rette distinte che intersecano T. Poichè $T \subseteq \pi$ queste sono anche rette del sottospazio π. D'altro canto $c \in R \subseteq T$ e $R \cap T = \emptyset$, e dunqe R è una retta distinta dalle precedenti. Dunque

$$\deg_\pi c = n + 1 = \deg_{\mathfrak{R}} c,$$

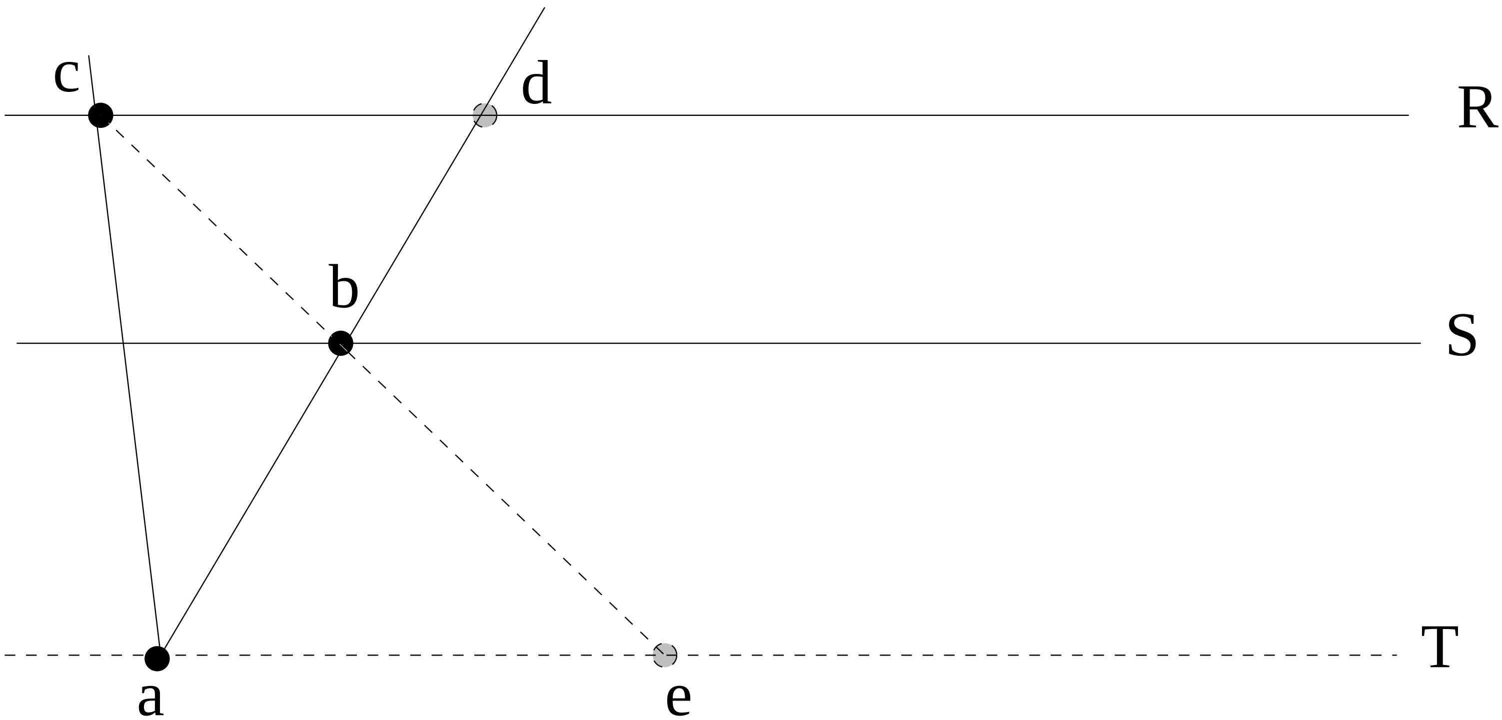

FIGURA 1

e per l'osservazione in calce alla definizione 5.1

$$\pi = \mathfrak{P},$$

da cui $\dim(\mathfrak{P}, \mathfrak{R}) = 2$. Dall'arbitrarietà di $a, b, c \in \mathfrak{P}$ segue ora la tesi. $\square$

Teorema 5.3. *Sia $\mathcal{G}$ un gruppo di Frobenius e sia $(\mathcal{G}, \mathfrak{R})$ lo spazio cinematico associato alla sua partizione $\mathfrak{F}(\mathcal{G})$. Se*

$$|\mathcal{H}| = 2,$$

allora $(\mathcal{G}, \mathfrak{R})$ è uno spazio di scambio e

$$\dim(\mathcal{G}, \mathfrak{R}) = 3.$$

DIMOSTRAZIONE.

- Se a, b, c, d sono 4 punti, a tre a tre non allineati, sicchè possiamo supporre:

$$a, b \in \mathcal{N}; c, d \in \mathcal{G} \setminus \mathcal{N}.$$

Ora, $|\mathcal{H}| = 2$ implica $|[\mathcal{N}]| = 2$, e dunque $(\mathcal{G} \setminus \mathcal{N}) \in \mathfrak{R}$, Per conseguenza:

$$\mathcal{G} = \mathcal{N} \cup (\mathcal{G} \setminus \mathcal{N}) = \overline{a, b} \cup \overline{c, d} \subseteq \overline{\{a, b, c, d\}} \subseteq \mathcal{G}$$

da cui segue

$$\dim \mathcal{G} \leq 3.$$

- Siano ora a, b, c tre punti non allineati. Poichè

$$\forall R \in \mathfrak{R} \setminus [\mathcal{N}] : |R| = 2,$$

possiamo supporre senza perdere in generalità $\overline{c, b} \in [\mathcal{N}]$. Sia

$$\pi = \bigcup_{x \in \overline{b,c}} \overline{a, x}.$$

Osserviamo che $(a \parallel_l \mathcal{N}) \not\subseteq \pi$, e dunque $\pi \neq \mathcal{G}$.

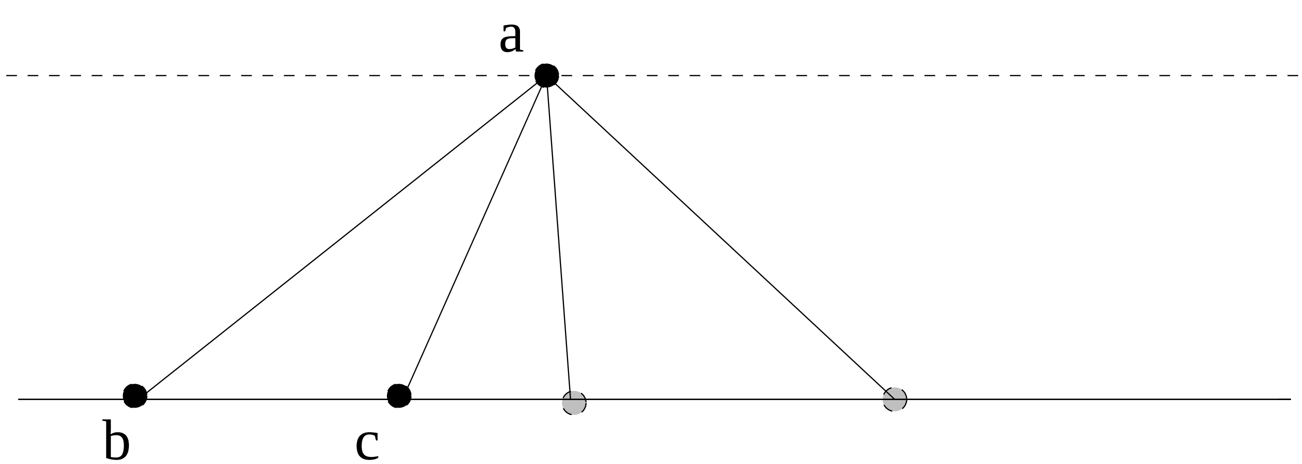

FIGURA 2. Near-pencil

D'altro canto è immediato verificare che π è il più piccolo sottospazio di $(\mathcal{G}, \mathfrak{R})$ contente $\{a, b, c\}$, ovvero

$$\pi = \overline{\{a, b, c\}}$$

Per l'arbitrarietà di $\{a, b, c\}$ segue:

$$\dim \mathcal{G} \geq 3$$

Segue la tesi. □

Osservazione. L'insieme π costruito nella dimostrazione del teorema precedente è un piano proiettivo generalizzato[1]. Esso viene detto **near-pencil**.

Tenuto conto del fatto che in un gruppo di Frobenius il complemento $\mathcal{H}$ non è mai banale e che:

$$|\mathcal{H}| \mid |\mathcal{N}| - 1 \Rightarrow |\mathcal{H}| < |\mathcal{N}|$$

si ha sempre:

$$|\mathcal{N}| \geq 3.$$

I due teoremi precedenti possono quindi essere riformulati nel seguente modo:

Teorema 5.4. *Sia $\mathcal{G}$ un gruppo di Frobenius, e sia $(\mathcal{G}, \mathfrak{R})$ lo spazio cinematico associato alla sua fibrazione $\mathfrak{F}(\mathcal{G})$. Allora*

1. $(\mathcal{G}, \mathfrak{R})$ *è uno spazio di scambio;*
2. $$\forall R \in \mathfrak{R} : |R| > 2 \Rightarrow \dim(\mathcal{G}, \mathfrak{R}) = 2,$$
3. $$\exists R \in \mathfrak{R} : |R| = 2 \Rightarrow \dim(\mathcal{G}, \mathfrak{R}) = 3.$$

1.1. Collineazioni di $(\mathcal{G}, \mathfrak{R})$.

Definizione 5.2. Sia $(\mathcal{G}, \mathfrak{R}, \|_l, \|_r)$ uno spazio doppio. Poniamo per definizione:

$$\mathrm{Aut}(\mathcal{G}, \mathfrak{R}, \|_l, \|_r) := \mathrm{Aut}(\mathcal{G}, \mathfrak{R}, \|_l) \cap \mathrm{Aut}(\mathcal{G}, \mathfrak{R}, \|_r).$$

Scriviamo inoltre

$$\mathrm{Aut}_1(\mathcal{G}, \mathfrak{R}, \|_l, \|_r) := \{\alpha \in \mathrm{Aut}(\mathcal{G}, \mathfrak{R}, \|_l, \|_r) : \alpha(1) = 1\}$$

In [**Pia87**] (pag.167)[2] si dimostra il seguente teorema:

[1] in effetti la condizione che le rette proiettive contengano almeno 3 punti serve proprio ad evitare questa situazione

[2] si veda anche [**MC80**], teorema 3

Teorema 5.5. *Sia* $(\mathcal{G}, \mathfrak{R}, \cdot)$ *uno spazio cinematico con fibrazione* $\mathfrak{F}$, *e sia* $\mathrm{Aut}(\mathcal{G}, \cdot, \mathfrak{F})$ *il gruppo di tutti gli automorfismi di* $(\mathcal{G}, \cdot)$ *compatibili*[3] *con la fibrazione* $\mathfrak{F}$. *Allora supposto* $|\mathfrak{F}| > 1$:

$$\mathrm{Aut}_1(\mathcal{G}, \mathfrak{R}, \|_l, \|_r) = \mathrm{Aut}(\mathcal{G}, \cdot, \mathfrak{F}).$$

Inoltre se $\mathcal{G}_l := \{a_l : a \in \mathcal{G}\}$ *si ottiene:*

$$\mathrm{Aut}(\mathcal{G}, \mathfrak{R}, \|_l, \|_r) = \mathcal{G}_l \rtimes \mathrm{Aut}(\mathcal{G}, \cdot, \mathfrak{F}).$$

Teorema 5.6. *Sia* $\mathcal{G}$ *un gruppo di Frobenius, e* $(\mathcal{G}, \mathfrak{R})$ *lo spazio cinematico associato alla sua partizione* $\mathfrak{F}(\mathcal{G})$. *Allora:*

$$\mathrm{Aut}(\mathcal{G}, \cdot) \leq \mathrm{Aut}_1(\mathcal{G}, \mathfrak{R}, \|_l, \|_r).$$

DIMOSTRAZIONE.

- Se $\mathfrak{F}(\mathcal{G})$ è una fibrazione caratteristica, allora abbiamo la tesi, infatti in tale caso:

  $$\forall \alpha \in \mathrm{Aut}(\mathcal{G}, \cdot), \forall T \in \mathfrak{F}(\mathcal{G}) : \alpha(T) \in \mathfrak{F}(\mathcal{G}).$$

  Sia $R \in \mathfrak{R}$, e $S \|_l R$. Allora esiste $H \in \mathfrak{F}(\mathcal{G})$, ed esistono $r, s \in \mathcal{G}$ tali che $R = rH$, e $S = sH$. Ora:

  $$\alpha(R) = \alpha(r)\alpha(H) \|_l \alpha(s)\alpha(H) = \alpha(sH) = \alpha(S).$$

  Similmente si ragiona sul parallelismo destro.
- Dimostriamo dunque che

  $$\forall T \in \mathfrak{F}(\mathcal{G}), \forall \alpha \in \mathrm{Aut}(\mathcal{G}, \cdot) : \alpha(T) \in \mathfrak{F}(\mathcal{G}).$$

  Sia $\alpha \in \mathrm{Aut}(\mathcal{G}, \cdot)$. Poichè per il corollario 2.2 $\mathcal{N}$ è caratteristico in $\mathcal{G}$:

  $$\alpha(\mathcal{N}) = \mathcal{N}.$$

  D'altro canto $\alpha(\mathcal{G}) = \mathcal{G}$. Se $\mathcal{H}$ è un complemento per $\mathcal{N}$, si ha $\mathcal{G} = \mathcal{N}\mathcal{H}$, e, come conseguenza:

  $$\alpha(\mathcal{G}) = \alpha(\mathcal{N}\mathcal{H}) = \alpha(\mathcal{N})\alpha(\mathcal{H}) = \mathcal{N}\alpha(\mathcal{H}),$$

[3] i.e. tali che

$$\forall \alpha \in \mathrm{Aut}(\mathcal{G}, \cdot, \mathfrak{F}), \forall T \in \mathfrak{F} : \alpha(T) \in \mathfrak{F}$$

da cui anche $\alpha(\mathcal{H})$ deve essere un complemento per $\mathcal{N}$. Poichè $\mathcal{N} \lhd \mathcal{G}$ è un sottogruppo di Hall, teorema di Schur-Zassenhaus (teorema 1.11) ci assicura che tutti i suoi complementi devono essere fra loro coniugati. Dunque esiste $t \in \mathcal{N}$ tale che:

$$\alpha(\mathcal{H}) = \mathcal{H}^t \in \mathfrak{F}(\mathcal{G}),$$

da cui la tesi.

□

Consideriamo ora particolari collineazioni di $(\mathcal{G}, \mathfrak{R})$:

Ogni gruppo di Frobenius ha centro banale. Allora, per il teorema 1.2:

$$\mathrm{Inn}(\mathcal{G}, \cdot) \simeq \mathcal{G},$$

e risulta dunque possibile, a norma del teorema 5.5, immergere $\mathcal{G}$ in $\mathrm{Aut}_1(\mathcal{G}, \mathfrak{R}, \|_l, \|_r)$.

Definizione 5.3. Supponiamo $\mathcal{G}$ sia un gruppo di Frobenius di nucleo $\mathcal{N}$ e complemento $\mathcal{H}$. Allora poniamo $\forall g \in \mathcal{G}$:

$$\rho_g : \begin{cases} \mathcal{G} \to \mathcal{G} \\ x \to x^g \end{cases} .$$

Indicheremo con Ω l'insieme:

$$\Omega := \{\rho_n : n \in \mathcal{N}\}.$$

Si può dimostrare con facilità che detta ρ l'applicazione

$$\rho : \begin{cases} \mathcal{G} \to \mathrm{Aut}\,\mathcal{G} \\ g \to \rho_g \end{cases} ,$$

tale ρ è un isomorfismo fra $\mathcal{G}$ ed $\mathrm{Inn}(\mathcal{G})$ e che $\Omega = \rho(\mathcal{N})$. Vogliamo indagare sulle collineazioni di Ω.

Osservazione. Si verifica che ogni $\rho_n \in \Omega$ precedente fissa oltre al punto 1 il punto n. Ciò non implica però che, ammesso $n \neq 1$ tutta la retta $\overline{1, n} = \mathcal{N}$ sia fissata punto per punto. In effetti

$$\mathcal{N} \subseteq \mathrm{Fix}(\rho_n) \Leftrightarrow n \in \mathrm{Z}(\mathcal{N}).$$

In questo caso parleremo di **rotazione attorno la retta $\mathcal{N}$**.

Poichè $\mathcal{N}$ è nilpotente, esso ha centro non banale. Da questo discende l'esistenza di rotazioni proprie attorno la retta $\mathcal{N}$.

In generale vale il seguente fatto:

Lemma 5.2. *Sia $\phi \in \mathrm{Aut}(\mathcal{G}, \mathfrak{R})$ una collineazione. Se $R \parallel_l \mathcal{N}$, allora $\phi(R) \parallel_l \mathcal{N}$.*

DIMOSTRAZIONE. Poichè ϕ è una biiezione:

$$\forall T \in \mathfrak{R} : |\phi(T)| = |T|.$$

D'altro canto è facile verificare che

$$\forall T \in \mathfrak{R} : |T| = n = |\mathcal{N}| \Leftrightarrow T \parallel_l \mathcal{N}.$$

Segue immediatamente la tesi. □

Le ρ_n godono in più della seguente proprietà:

Lemma 5.3. *Data $\rho_n \in \Omega$:*

$$\forall S \parallel \mathcal{N} : \rho_n(S) = S.$$

DIMOSTRAZIONE. Diciamo $S \parallel_l \mathcal{N}$. Allora $\exists h \in \mathcal{H}$ tale che $S = h\mathcal{N}$. Dunque

$$\rho_n(S) = h^n \mathcal{N}^n = h^n \mathcal{N} = n^{-1} h \mathcal{N} = {n^{-1}}_l(h)\mathcal{N} = {n^{(-1)}}_l(h\mathcal{N}).$$

Ma la traslazione sinistra ${n^{-1}}_l$ fissa la retta $\mathcal{N}$, e dunque deve fissare tutte le sue parallele *destre*. D'altro canto S è anche parallela destra di $\mathcal{N}$, e quindi la tesi. □

Corollario 5.1. *Sia $S \in \mathfrak{R}$ una retta fissata tale che $S \cap \mathcal{N} = \emptyset$. Allora Ω è regolare sui punti di S.*

DIMOSTRAZIONE. Poichè $S \cap \mathcal{N} = \emptyset$, necessariamente $S \parallel \mathcal{N}$. Per il lemma precedente, $\forall \rho_n \in \Omega$:

$$\rho_{n|S} : S \to S.$$

e, per definizione di ρ_n:

$$\rho_n(1) = 1.$$

D'altro canto le rette per 1 diverse da $\mathcal{N}$ sono incidenti ad S e dunque possono scriversi come

$$\overline{1, s}$$

per $s \in S$. Per costruzione dello spazio cinematico associato alla partizione di Frobenius $\mathfrak{F}(\mathcal{G})$, abbiamo che $\forall R \in \mathfrak{R} \setminus \{\mathcal{N}\}$:

$$1 \in R \Leftrightarrow R \in \mathfrak{F}(\mathcal{G}) \setminus \{\mathcal{N}\} \Leftrightarrow \exists t \in \mathcal{N} : R = \mathcal{H}^t = \rho_t(\mathcal{H})$$

Ma

$$|\mathfrak{F}(\mathcal{G}) \setminus \{\mathcal{N}\}| = |\mathfrak{F}(\mathcal{G})| - 1 = |\mathcal{N}| = |\Omega|,$$

e quindi Ω deve essere regolare sull'insieme delle rette passanti per 1. Ciò implica in particolare che

$$\forall s, t \in S : \exists n \in \mathcal{N} \text{ tale che } \rho_n(\overline{1, s}) = \overline{1, \rho(n)} = \overline{1, t}$$

cioè, tenuto conto che $s \in S \Rightarrow \rho_n(s) \in S$:

$$\rho_n(s) = t$$

che fornisce la 1-transitività. La regolarità può dedursi a questo punto da considerazioni di ordine. $\square$

Tenuto conto del fatto che in un gruppo di Frobenius

$$\forall n \in \mathcal{N} \setminus \{1\} : \mathrm{C}_{\mathcal{G}}(n) \subseteq \mathcal{N},$$

si ha immediatamente il seguente corollario:

Corollario 5.2. *Nelle stesse ipotesi del corollario precedente:*

$$\forall \rho_n \in \Omega \setminus \{\mathrm{Id}\} : \mathrm{Fix}(\rho_n) = \mathrm{C}_{\mathcal{N}}(n).$$

Vogliamo ora fornire una dimostrazione puramente geomentrica di questo fatto:

Dimostrazione. Ovviamente

$$\mathrm{C}_{\mathcal{N}}(n) \subseteq \mathrm{Fix}(\rho_n) = \mathrm{C}_{\mathcal{G}}(n).$$

Sia $g \in \mathcal{G} \setminus \mathcal{N}$, e consideriamo $S = (g \parallel_l \mathcal{N})$. Poichè Ω agisce regolarmente su S si ha

$$g = \rho_n(g) \Leftrightarrow \rho_n = \mathrm{Id}$$

da cui la tesi. □

2. Il caso 2-transitivo

Supponiamo che $\mathcal{G}$ sia un gruppo strettamente 2-transitivo su di un insieme X. Il teorema 2.24 ci garantisce che $\mathcal{G}$ è di Frobenius. Inoltre per il teorema 2.25 sappiamo che posto $n = |\mathcal{N}|$, abbiamo:

- $n = |\mathcal{N}| = |X|$
- $|\mathcal{H}| = n - 1$.

Sia ora $(\mathcal{G}, \mathfrak{R}, \cdot)$ lo spazio cinematico associato a $\mathfrak{F}(\mathcal{G})$, e siano p un punto e $R \in \mathfrak{R}$ una retta, tale che $p \notin R$. Vogliamo caratterizzare le rette passanti per p e aventi intersezione vuota con R.

Distinguiamo due casi.

- Supponiamo $R \parallel_l \mathcal{N}$, e sia $p \in S \in \mathfrak{R}$. Allora, per il lemma 5.1,
$$S \cap R = \emptyset \Leftrightarrow S \parallel_l \mathcal{N}$$
- Supponiamo allora $R \not\parallel \mathcal{N}$.

  Lo stesso metodo di conteggio applicato in precedenza mostra che stavolta esistono $(n+1)-(n-1) = 2$ rette passanti per p ed aventi intersezione vuota con R. Per il teorema 5.1 esistono due rette *distinte* H, K passanti per p tali che $H \parallel_l R$, $K \parallel_r R$. In particolare $H \cap R = K \cap R = \emptyset$. Dunque H e K devono essere le uniche due rette con intersezione vuota con R. Si ha quindi:
$$\forall R \not\parallel \mathcal{N}, \forall T \in \mathfrak{R} : T \cap R = \emptyset \Rightarrow T \parallel_l R \text{ oppure } T \parallel_r R.$$

Vogliamo dimostrare ora il seguente teorema di caratterizzazione:

Teorema 5.7. *Sia $\mathcal{G}$ un gruppo strettamente 2-transitivo di grado n. Allora $\mathcal{G}$ è un gruppo di Frobenius e lo spazio cinematico $(\mathcal{G}, \mathfrak{R}, \cdot)$ associato alla partizione $\mathfrak{F}(\mathcal{G})$ possiede la medesima struttura di incidenza di un* piano affine privato di una retta.

Dimostrazione. Per ogni retta $R \in \mathfrak{R}$ sia $[R]_r$ la classe di parallelismo destra di R, ovvero
$$[R]_r := \{S \in \mathfrak{R} : S \parallel_r \mathfrak{R}\}.$$

Siano

$$\mathfrak{P}' := \mathcal{G} \cup \{[R]_r : R \not\parallel \mathcal{N}\}$$

e

$$\mathfrak{R}' := [\mathcal{N}]_r \cup \{R \cup \{[R]_r\} : R \not\parallel \mathcal{N}\} \cup \{\mathcal{N}\infty = \{[R]_r : \mathfrak{R} \not\parallel \mathcal{N}\}\}.$$

Osserviamo che:

1. $\mathfrak{R}' \cap \mathfrak{R} = [\mathcal{N}]_r$;
2. $\mathcal{N}\infty \cap \mathcal{G} = \emptyset$;
3. $\mathcal{N}\infty = \mathfrak{P}' \setminus \mathcal{G}$;
4. $(R \cup \{[R]_r\}) \cap \mathcal{G} = R$;
5. $|(R \cup \{[R]_r\}) \cap \mathcal{N}\infty| = 1$.

Per praticità conviene estendere le relazioni di parallelismo destro e sinistro agli elementi di $\mathfrak{R}'$ nel seguente modo:

$$\forall R, S \in \mathfrak{R}' \setminus \{\mathcal{N}\infty\} : R \parallel_l S \Leftrightarrow (R \cap \mathcal{G}) \parallel_l (S \cap \mathcal{G})$$

e similmente

$$\forall R, S \in \mathfrak{R}' \setminus \{\mathcal{N}\infty\} : R \parallel_r S \Leftrightarrow (R \cap \mathcal{G}) \parallel_r (S \cap \mathcal{G}).$$

Poniamo inoltre

$$\forall N \in [\mathcal{N}]_r \cup \{\mathcal{N}\infty\} : N \parallel_l \mathcal{N}\infty \& N \parallel_r \mathcal{N}\infty.$$

Valgono alcuni fatti:

1. $(\mathfrak{P}', \mathfrak{R}')$ è uno spazio di incidenza.

   Ovviamente $\forall S \in \mathfrak{R}' : |S| \geq 2$. Resta da verificare l'esistenza ed unicità della retta per due punti.

   - Supponiamo $x, y \in \mathfrak{P}' \setminus \mathcal{G}$. Allora $x, y \in \mathcal{N}\infty$. Inoltre poichè

     $$\forall R \in \mathfrak{R}' \setminus \{\mathcal{N}\infty\} : |R \cap (P' \setminus \mathcal{G})| \leq 1$$

     si ha la tesi.
   - Sia $x \in \mathcal{G}$; $y \in \mathfrak{P}' \setminus \mathcal{G}$. Sia $T \in y$ e consideriamo l'elemento $U := (x \parallel_r T) \cup \{y\}$. Evidentemente $\{x, y\} \subseteq U \in \mathfrak{R}'$. Inoltre dall'esistenza ed unicità della parallela destra in $(\mathcal{G}, \mathfrak{R}, \cdot)$ discende la tesi.

- Siano $x, y \in \mathcal{G}$. Allora esiste una ed una sola retta $R \in \mathfrak{R}$ tale che $\{x, y\} \subseteq R$. Se $R \in \mathfrak{R}'$ non c'è nulla da dimostrare. Altrimenti poniamo $R' := \overline{\{x, y\}} \cup \{[\overline{x, y}]_r\}$. Allora $R' \in \mathfrak{R}$, e, per il punto precedente si ha la tesi.

2. $(\forall x \in \mathfrak{P}' : \deg(x) = n + 1)$: per quanto visto in precedenza dobbiamo dimostrare semplicemente che $\forall x \in \mathcal{N}\infty : \deg(x) = n+1$. Sia dunque $R \in \mathfrak{R}$ una retta non parallela a $\mathcal{N}$. Chiamata R' la retta di $\mathfrak{R}'$ tale che $R \subseteq R'$, sia $x \in R' \setminus R$. Ora, poichè

$$\forall T \in [R]_r : T \cap \mathcal{N} \neq \emptyset$$

è immediato verificare che

$$|[R]_l| = |[R]_r| = |\mathcal{N}| = n.$$

Ma allora si ha, per costruzione, che:

$$\deg(x) = |[R]_r| + 1 = n + 1,$$

cioè la tesi.

3. $(\mathfrak{P}', \mathfrak{R}', \|_l)$ è un piano affine.

Verifichiamo dapprima che

$$\forall R, S \in \mathfrak{R}' : R \neq S \& R \|_l S \Leftrightarrow R \cap S = \emptyset.$$

- $(\Rightarrow)$ Se $(R \cap \mathcal{G}), (S \cap \mathcal{G}) \in \mathfrak{R}$, non v'è nulla da dimostrare[4]. Se invece $S = \mathcal{N}\infty$, allora necessariamente $R \in [\mathcal{N}]_r$, e dunque si ha la tesi.
- $(\Leftarrow)$ Sia $p \in S$.
  - Se $R \|_l \mathcal{N}$, e $p \in \mathcal{G}$, allora esiste una sola retta passante per p con intersezione vuota con $\mathcal{N}$, che deve dunque essere necessariamente la parallela destra per p ad $\mathcal{N}$, e dunque la tesi. D'altro canto se $p \in \mathcal{N}\infty$, si verifica che l'unica retta S per p tale che $S \cap R = \emptyset$ è $\mathcal{N}\infty$ stessa (le altre intersecano R in un punto di $\mathcal{G}$!), e quindi $S \|_l \mathcal{N}$.

[4] basta tenere conto del fatto che $R \neq (R \cap \mathcal{G}) \Rightarrow [R]_r \neq [S]_r$

– Se $R \not\parallel_l \mathcal{N}$, allora $R \cap \mathcal{N}\infty \neq \emptyset$. Si può dunque supporre $p \in S \cap \mathcal{G}$. Ora, per p passano esattamente due rette aventi intersezione vuota in $\mathcal{G}$ con R: esse sono rispettivamente $T_1 = (p \parallel_l R)$ e $T_2 = (p \parallel_r R)$. Ovviamente $[T_2]_r = [R]_r$, ma $[T_1]_r \neq [R]_r$. Allora posto

$$\forall i \in \{1,2\} : T_i' := T_i \cup [T_i]_r$$

è evidente che $R \cup T_2' = \{[R]_r\}$. Dunque, dato che

$$R \cup T_1' = \emptyset \cup ([R]_r \cap [T_1']_r) = \emptyset$$

l'unica retta per p con intersezione vuota con R è T_1 e quindi $S = T_1$, da cui segue $S \parallel_l R$.

L'unico possibile parallelismo per $(\mathfrak{P}', \mathfrak{R}')$ è dunque $\parallel_l$. Affinchè $(\mathfrak{P}', \mathfrak{R}', \parallel_l)$ sia un piano affine ora basta controllare che

$$\forall R \in \mathfrak{R}', \forall p \in \mathfrak{P}' : \exists! S \in \mathfrak{R}' : p \in S \& S \cap R = \emptyset$$

cioè, per quanto appena dimostrato.

$$\forall R \in \mathfrak{R}', \forall p \in \mathfrak{P}' : \exists! S \in \mathfrak{R}' : p \in S \& S \parallel_l R$$

Se $p \in \mathcal{G}$, l'esistenza ed unicità della parallela sinistra ci garantisce che la tesi è soddisfatta.
Supponiamo dunque $p \in \mathcal{N}\infty$.

– Se $R \parallel_l \mathcal{N}$ la dimostrazione è banale.
– Sia quindi $R \not\parallel_l \mathcal{N}$.
  Ora: il grado di p è $n+1$; d'altro canto $|R| = (n-1)+1 = n$. Esiste dunque una unica retta S passante per p ed avente intersezione vuota con R. Per quanto dimostrato sopra questa deve essere parallela sinistra ad R, e, come appena visto è unica. Segue la tesi del teorema.

$\square$

Una dimostrazione più generale di questo stesso risultato, applicabile anche nel caso infinito, ma sostanzialmente diversa può trovarsi in [**Kar73**], pag 434.

Definizione 5.4. Uno spazio di incidenza $(\mathfrak{P}, \mathfrak{R})$ si dice **stripe plane** o **piano affine poroso** se e solo se esiste un piano affine $(\mathfrak{P}', \mathfrak{R}')$ tale che

$$\exists X \in \mathfrak{R}' : \mathfrak{P} = \mathfrak{P}' \setminus R;$$

$$\mathfrak{R} := \{R \cap \mathfrak{P} : R \in \mathfrak{R}' \setminus \{X\}\}.$$

Corollario 5.3. *Sia* $(\mathcal{G}, \cdot)$ *un gruppo strettamente due transitivo, e sia* $(\mathcal{G}, \mathfrak{R}, \|_l, \|_r)$ *lo spazio di incidenza associato alla partizione* $\mathfrak{F}(\mathcal{G})$. *Allora*

$$\forall R, S \in \mathfrak{R} \setminus [\mathcal{N}] : |[R]_r \cap [S]_l| = 1$$

Dimostrazione. Se $R = S$, non c'è nulla da dimostrare. Altrimenti sia $(\mathcal{G}', \mathfrak{R}', \|_A)$ il piano affine costruito nel teorema precedente in cui si può immergere $(\mathcal{G}, \mathfrak{R})$. Ora, posti

$$R' := R \cup \{[R]_r\};$$

e

$$S' := S \cup \{[S]_r\}$$

Abbiamo che per il punto $[R]_r \in \mathcal{G}'$ deve esistere una unica parallela T' ad S', e $T' \neq \mathcal{N}\infty$. Sia $T := T' \cap \mathcal{G}$; ovviamente

$$T' \|_A S' \Rightarrow T \|_l S \Rightarrow T \in [S]_l.$$

Al contempo

$$[R]_r \in \mathcal{T}' \Rightarrow T \|_r R \Rightarrow T \in [R]_r,$$

e dunque $T \in [R]_r \cap [S]_l \neq \emptyset$.

Il fatto che T sia l'unica retta di $[R]_r \cap [S]_l$ discende dall'unicità della parallela ad S' per $[R]_r$ in $(\mathcal{G}', \mathfrak{R}', \|)$. $\square$

Teorema 5.8. *Sia* $(\mathcal{G}, \mathfrak{R})$ *la struttura di incidenza associata tramite la partizione di Frobenius ad un gruppo strettamente due transitivo e sia* $\|$ *una relazione di parallelismo su* $\mathfrak{R}$. *Allora* $\|=\|_l$ *oppure* $\|=\|_r$.

Dimostrazione. Per ogni $R \in \mathfrak{R}$ indichiamo con $[R]_{\|}$ la classe di parallelismo di $\mathfrak{R}$ rispetto $\|$.

- Poichè per ogni parallelismo:

  $$A \parallel B \Rightarrow A = B \text{ oppure } A \cap B = \emptyset$$

  necessariamente

  $$[\mathcal{N}]_{\|} \subseteq [\mathcal{N}]_l = [\mathcal{N}]_r := [\mathcal{N}],$$

  mentre l'assioma di esistenza della parallela ad una retta per un punto garantisce l'ugnuaglianza:

  $$[\mathcal{N}]_{\|} = [\mathcal{N}].$$

- Supponiamo che esista $R \in \mathfrak{R}$ tale che $[R]_{\|} \notin \{[R]_l, [R]_r\}$. Allora necessariamente $R \notin [\mathcal{N}]$.

  La caratterizzazione delle rette aventi intersezione vuota con R ci garantisce che:

  $$[R]_{\|} \subseteq ([R]_l \cup [R]_r),$$

  mentre

  $$[R]_l \cap [R]_r = \{R\}.$$

  Siano $S \in [R]_{\|} \cap [R]_l$ e $T \in [R]_{\|} \cap [R]_r$. Supponiamo $S \neq T$, e dunque $S \cap T = \emptyset$. Allora sempre per la caratterizzazione precedente è vero che:

  $$T \cap S = \emptyset \Rightarrow T \parallel_l S \text{ oppure } T \parallel_r S,$$

  cioè

  $$T \in [S]_l = [R]_l \text{ oppure } S \in [T]_r = [R]_r.$$

  Supponiamo sia vero $T \in [R]_l$. Allora deve essere $T \in [R]_l \cap [R]_r = \{R\}$, e dunque

  $$[R]_{\|} \subseteq [R]_l.$$

Da questo, per l'assioma di esistenza delle parallele discende $[R]_{||} = [R]_l$.

Nel secondo caso, con ragionamento analogo si deduce $S = R$ e dunque $[R]_{||} = [R]_r$, ovvero:

$$\forall R \in \mathfrak{R} : [R]_{||} \in \{[R]_l, [R]_r\}$$

.

- Per concludere supponiamo esistano $R, S \in \mathfrak{R} \setminus [\mathcal{N}]$ tali che $[R]_{||} = [R]_r$ e $[S]_{||} = [S]_l$. Per il corollario 5.3 si ha:

  $$[R]_{||} \cap [S]_{||} \neq \emptyset$$

  da cui, dovendo essere $\|$ di equivalenza,

  $$[R]_{||} = [S]_{||}.$$

  Sempre nel corollario 5.3 si è visto che, però $|[R]_r \cap [S]_l| = 1$, e dunque si avrebbe l'assurdo $|[R]_{||}| = 1$, impossibile in quanto $|\mathfrak{R}| \neq 1$.

  Conseguenza di ciò è che

  $$\exists R \in \mathfrak{R} \setminus [\mathcal{N}] : [R]_{||} = [R]_r \Rightarrow \| = \|_r,$$

  mentre

  $$\exists S \in \mathfrak{R} \setminus [\mathcal{N}] : [S]_{||} = [S]_l \Rightarrow \| = \|_l,$$

  che è la tesi.

$\square$

3. Il caso $|\mathcal{H}| = 2$

Teorema 5.9. *Sia $n = 2k + 1$ un numero naturale dispari. Allora il gruppo diedrale*

$$D_{2n} := \left\langle a, b | a^2 = b^n = 1, b^a = b^{-1} \right\rangle$$

è un gruppo di Frobenius.

Dimostrazione. Sia $\mathcal{N} := \langle b \rangle$ il gruppo generato da b. Poichè $|D_{2n} : \mathcal{N}| = 2$, per il teorema 1.4 $\mathcal{N} \lhd \mathcal{G}$. Sia ora $x \in \mathcal{N} \setminus \{1\}$, e sia

$T = \mathrm{C}_{\mathcal{G}}(x)$. Siccome $\mathcal{N}$ è ciclico, e dunque abeliano, $\mathcal{N} = T$. La tesi è, a norma della definizione 2.1, che $T = \mathcal{N}$.

Sia $q \in \mathcal{G} \setminus \mathcal{N}$. Allora esiste $n \in \mathcal{N}$ tale che $q = an$. Supponiamo $q \in \mathrm{C}_{\mathcal{G}}(x)$:

$$q \in \mathrm{C}_{\mathcal{G}}(x) \Leftrightarrow qx = xq \Leftrightarrow (an)x = x(an) \Leftrightarrow axn = xan \Leftrightarrow$$

$$\Leftrightarrow xn = (axa)n \Leftrightarrow xn = x^{-1}n \Leftrightarrow x^2 n = n \Leftrightarrow x^2 = 1.$$

Per ipotesi $x \in \mathcal{N}$, $\mathcal{N}$ ciclico di ordine dispari, e dunque anche l'ordine di x deve essere dispari. Da $x^2 = 1$ segue allora $x = 1$, contro l'ipotesi. Segue la tesi. □

Osservazione. L'ipotesi $|\mathcal{N}|$ dispari è realmente necessaria affinchè un gruppo $\mathcal{G} = \mathcal{N}\mathcal{H}$ con $|\mathcal{H}| = 2$ sia di Frobenius, come si può facilmente verificare, ad esempio, considerando che per n pari il "nucleo" $\mathcal{N}$ *non* è un sottogruppo di Hall.

Se indichiamo con $\mathbb{Z}_m$ il gruppo ciclico di ordine m è immediato verificare alla luce del teorema precedente che per n dispari:

$$D_{2n} = \mathbb{Z}_n \rtimes \mathbb{Z}_2.$$

Da [?] e [?] si ha il seguente teorema:

Teorema 5.10. *Sia* $(\mathfrak{P}, \mathfrak{R}, \|)$ *una A-t-struttura, con* $\mathcal{G}$ *gruppo regolare di traslazioni* [5] *su* $\mathfrak{P}$. *Siano*

$$\mathrm{Aut}_{\Sigma}(\mathcal{G}, \cdot, \Sigma) := \{\theta \in \mathrm{Aut}(\mathcal{G}, \cdot, \Sigma) : \forall X \in \Sigma : \theta(X) = X\}$$

e

$$\mathfrak{D}_1(\mathfrak{P}, \mathfrak{R}, \|) := \{\theta \in \mathrm{Aut}(\mathfrak{P}, \mathfrak{R}, \|) : \theta(1) = 1\}$$

Allora sono fatti equivalenti:

1. $\mathcal{G} \lhd \mathrm{Aut}(\mathfrak{P}, \mathfrak{R}, \|)$.
2. $\mathcal{G} \lhd \mathfrak{D}(\mathfrak{P}, \mathfrak{R}, \|)$.
3. $\mathfrak{D}_1(\mathfrak{P}, \mathfrak{R}, \|) = \mathrm{Aut}_{\Sigma}(\mathcal{G}, \cdot, \Sigma)$

[5]Poichè in queste ipotesi è possibile identificare $\mathfrak{P}$ con $\mathcal{G}$ e trasformare $(\mathcal{G}, \mathfrak{R}, \|)$ in un gruppo di incidenza, è immediato vedere che $\mathcal{G}$ deve ammettere una partizione Σ.

In [**MC80**] viene verificato che, se il gruppo $\mathcal{G}$ di traslazioni non è commutativo, condizione necessaria e sufficiente affinchè possono esistere dilatazioni proprie di $(\mathfrak{P}, \mathfrak{R}, \|)$, è che:

$$\mathfrak{D}(\mathfrak{P}, \mathfrak{R}, \|) \cap \mathrm{Aut}_{\Sigma}(\mathcal{G}, \cdot, \Sigma) = \{1\},$$

da cui:

Teorema 5.11. *Sia $(\mathfrak{P}, \mathfrak{R}, \|)$ una A-t-struttura, e sia $\mathcal{G}$ un gruppo di traslazioni transitivo su $\mathfrak{P}$ e non commutativo. Allora sono equivalenti i seguenti fatti:*

1. $\mathcal{G} \lhd \mathrm{Aut}(\mathfrak{P}, \mathfrak{R}, \|)$*;*
2. *Non esistono dilatazioni proprie di* $(\mathfrak{P}, \mathfrak{R}, \|)$.

È stato verificato da Seier in [?] e da Andrè in [**And61**] che le condizioni seguenti sono sufficienti affichè $\mathcal{G} \lhd \mathrm{Aut}(\mathfrak{P}, \mathfrak{R}, \|)$:

1. $\mathcal{G}$ abeliano,
2. $\mathcal{G} = \mathcal{T}(\mathfrak{P}, \mathfrak{R}, \|)$, ovvero $\mathcal{G}$ coincidente con l'insieme di tutte le traslazioni di $(\mathfrak{P}, \mathfrak{R}, \|)$.

La condizione $\mathcal{G} = \mathcal{T}(\mathfrak{P}, \mathfrak{R}, \|)$ in particolare è sicuramente vera nei seguenti casi (si veda [**And61**], [**MC80**]):

- Tutte le rette hanno cardinalità finita[6]
- Ogni traslazione è centrale;
- $(\mathfrak{P}, \mathfrak{R}, \|)$ è un piano affine.

Da quanto appena visto discende che lavorando su spazi cinematici finiti derivati da gruppi non commutativi, non è certamente possibile trovare dilatazioni proprie.

Vogliamo ora provare il seguente teorema originale, da cui segue in modo indipendente che, nel caso $|\mathcal{H}| = 2$, non possono esistere dilatazioni che non siano traslazioni. Tale risultato consente inoltre di individuare un'altra condizione sufficiente per avere $\mathcal{G} = \mathcal{T}(\mathfrak{P}, \mathfrak{R}, \|)$:

[6] Tale condizione è soddisfatta in particolare quando $\mathcal{G}$ è finito

Teorema 5.12. *Sia* $(\mathfrak{P}, \mathfrak{R}, \|)$ *una A-struttura, non necessariamente finita. Supponiamo che esista* $H \in \mathfrak{R}$ *tale che, chiamata* $[H]$ *la sua classe di parallelismo:*

$$\forall R \in \mathfrak{R} \setminus [H] : |R| = 2.$$

Sia poi σ *una dilatazione. Allora*

$$\mathrm{Fix}(\sigma) \neq \emptyset \Rightarrow \sigma = 1.$$

Dimostrazione. Supponiamo $x \in \mathrm{Fix}(\sigma)$, e siano $Q = (x \parallel H)$. Poniamo

$$\mathfrak{R}(x) := \{R \in \mathfrak{R} : x \in R\}.$$

Poichè x è fissato:

$$\forall R \in \mathfrak{R}(x) : \sigma(R) = (\sigma(x) \parallel R) = (x \parallel R) = R.$$

Consideriamo in particolare le rette di $\mathfrak{R}(x) \setminus [H]$. Tutte queste rette sono della forma

$$R = \{x, z\} \text{ con } z \in \mathfrak{P} \setminus Q.$$

Allora:

$$\{x, z\} = R = \sigma(R) = \{\sigma(x), \sigma(z)\} = \{x, \sigma(z)\},$$

da cui si deduce, tenuto conto della esistenza della retta per due punti,

$$\forall z \in \mathfrak{P} \setminus Q : \sigma(z) = z,$$

Sia ora $y \in Q$. Fissiamo uno $z \in \mathfrak{P} \setminus Q \subseteq \mathrm{Fix}(\sigma)$, e sia $T = \{y, z\} \in \mathfrak{R}$. Poichè z è fissato si può ragionare come sopra e dedurre che:

$$\forall y \in Q : \sigma(y) = y,$$

da cui la tesi $\mathfrak{P} = \mathrm{Fix}(\sigma)$, ovvero $\sigma = 1$. □

Osservazione. La tesi del teorema precedente può essere riformulata dicendo che il gruppo $\mathfrak{D}(\mathfrak{P}, \mathfrak{R}, \|)$ delle dilatazioni di $(\mathfrak{P}, \mathfrak{R}, \|)$ deve essere *semiregolare* sui punti, cioè constare di sole traslazioni.

Da questo segue che se $(\mathfrak{P}, \mathfrak{R}, \|)$ è una A-t-struttura, e quindi esiste un gruppo $\mathcal{G}$ regolare su $\mathfrak{P}$, allora $\mathcal{G} = \mathfrak{D}(\mathfrak{P}, \mathfrak{R}, \|)$

4. Partizioni lineari

Il teorema 3.11 limita i tipi di gruppo finito che possono ammettere partizione, ma non asserisce nulla riguardo il modo in cui queste partizioni possano essere costruite.

Di particolare interesse è il seguente concetto:

Definizione 5.5. Sia $\mathcal{G}$ un gruppo; una partizione $\pi(\mathcal{G})$ si dice **lineare** se esiste un insieme non vuoto $\epsilon(\mathcal{G})$ di sottogruppi di $\mathcal{G}$ tali che

1. Ogni elemento di $\epsilon(\mathcal{G})$ è unione di almeno due differenti[7] elementi di $\pi(\mathcal{G})$;
2. Ogni due componenti di $\pi(\mathcal{G})$ sono contenute esattamente in un elemento di $\epsilon(\mathcal{G})$.
3. $\mathcal{G} \notin \epsilon(\mathcal{G})$.

Osservazione. Se $(\mathcal{G}, +)$ è un gruppo con partizione $\pi(\mathcal{G})$ è sempre possibile, per il teorema 4.8 associarvi uno spazio di incidenza $(\mathcal{G}, \mathfrak{R})$ ponendo

$$\mathfrak{R} := \{g + X : g \in \mathcal{G}, X \in \pi(\mathcal{G})\}.$$

Supponiamo $\pi(\mathcal{G})$ sia una partizione lineare, e sia $\epsilon(\mathcal{G})$ la famiglia ad essa associata. Chiamiamo $\mathfrak{E}$ l'insieme:

$$\mathfrak{E} := \{g + Y : g \in \mathcal{G}, Y \in \epsilon(\mathcal{G})\}.$$

È possibile considerare $\mathfrak{E}$ come l'insieme dei "piani" di $(\mathcal{G}, \mathfrak{R})$.

Infatti se $E \in \epsilon(\mathcal{G})$, allora

$$\pi(E) := \{P \in \pi(\mathcal{G}) : P \subseteq E\}$$

è una partizione per E, e dunque, posto

$$\mathfrak{R}(E) := \{R \in \mathfrak{R} : R \subseteq E\},$$

$(E, \mathfrak{R}(E))$ è risulta ancora essere uno spazio di incidenza, sottospazio proprio di $(\mathcal{G}, \mathfrak{R})$. Se poi $F = f + E \in \mathfrak{E} \setminus \epsilon(\mathcal{G})$, si verifica rapidamente

[7] dovendo essere ogni $X \in \epsilon(\mathcal{G})$ un gruppo in effetti sono sempre necessarie almeno tre componenti distinte di $\pi(\mathcal{G})$ per costituirlo.

che

$$\mathfrak{R}(F) = f + \mathfrak{R}(E) = \{f + R : R \in \mathfrak{R}(E)\},$$

da cui si deduce che anche $(F, \mathfrak{R}(F))$ deve essere uno spazio di incidenza.

Inoltre gli elementi di $\mathfrak{E}$ sono tutti individuati da coppie di rette *incidenti*[8], e dunque rappresentano una buona la nozione di "piano[9]".

Schulz ha provato il seguente teorema:

Teorema 5.13. *Sia $\mathcal{G}$ un gruppo finito non abeliano. Se $\mathcal{G}$ ammette una partizione lineare, allora esso è di Frobenius.*

La dimostrazione, che può essere trovata in [**Sch86**], si basa sul teorema 3.11 e consiste nel mostrare che supposto $\mathcal{G}$ non abeliano, esso non può appartenere a nessuna classe di gruppi con partizione diversa da quella dei gruppi di Frobenius.

È importante notare che questo risultato *non* asserisce che un gruppo di Frobenius ammette necessariamente una partizione lineare, ma semplicemente fornisce una condizione necessaria.

In effetti la partizione di Frobenius $\mathfrak{F}(\mathcal{G})$ non è mai lineare. Se esistesse un $\epsilon(\mathcal{G})$ con le proprietà richieste, allora

$$\exists : X \in \epsilon(\mathcal{G}) : \mathcal{N} \cup \mathcal{H} \subseteq X.$$

Ma

$$\mathcal{G} = \mathcal{N}\mathcal{H} = \langle \mathcal{N} \cup \mathcal{H} \rangle = \langle X \rangle = X \in \epsilon\mathcal{G},$$

contro la proprietà 3 della definizione.

Vogliamo ora presentare un esempio di gruppo di Frobenius con partizione lineare.

---

[8]le rette di $\pi(\mathcal{G})$ passano tutte per 1 !

[9]osserviamo inoltre che in uno spazio vettoriale tutti i piani passanti per l'unità sono sottogruppi

Teorema 5.14. *Sia* $(V,+)$ *uno spazio vettoriale di dimensione* n *su* $\mathrm{GF}(p)$. *Sia* $\forall v \in V$*:*

$$\tau_v : \begin{cases} V \to V \\ x \to v + x \end{cases}$$

Poniamo $T = \{\tau_v : v \in V\}$, *e sia* $\Lambda \leq \mathrm{GF}(p,n)$ *un gruppo di automorfismi di* V *privo di punti fissi. Allora* $\mathcal{G} = T \rtimes \Lambda$ *è un gruppo di Frobenius.*

Dimostrazione. Si tratta di una conseguenza immediata del teorema 2.13 □

Il teorema precedente ci consente di costruire gruppi di Frobenius il cui nucleo T ammette una partizione $\mathfrak{N}(T)$ non banale, costituita dall'immagine in T di tutte le rette vettoriali[10] di V.

Teorema 5.15. *Sia* V *uno spazio vettoriale di dimensione* $n > 0$, *finita su* $\mathrm{GF}(p)$, *con* $p > 2$. *Allora, posto* $T = \tau(V)$, $T \rtimes \mathrm{GF}(p)^\star$ *è un gruppo di Frobenius. Inoltre*

$$\forall \mathcal{N} \in \mathfrak{N}(T) : \mathcal{G} = \mathcal{N} \rtimes \mathrm{GF}(p)^\star \text{ è un gruppo di Frobenius.}$$

Dimostrazione.

- Poichè possiamo identificare $\mathrm{GF}(p)^\star$ con il gruppo Π delle matrici scalari di $\mathrm{GL}(p,n)$, abbiamo:

  $$\mathrm{GF}(p)^\star \simeq \Pi \leq \mathrm{GL}(p,n).$$

  Tenuto conto del fatto che:

  $$\forall \lambda \in \mathrm{GF}(p)^\star, \forall x \in V : \lambda x = x \Leftrightarrow \lambda = 1,$$

  abbiamo che $\mathrm{GF}(p)^\star$ agisce in modo privo di punti fissi su V e dunque anche su T.

  La prima parte della tesi è dunque conseguenza dal teorema precedente.

[10]in uno spazio vettoriale su di un campo $\mathbb{K}$ tutte le rette passano per 1 e sono sottogruppi isomorfi a $(\mathbb{K},+)$. Evidentemente la loro intersezione è ridotta al solo $\{1\}$.

- Per ogni $\mathcal{N} \in \mathfrak{N}(T)$, $\mathrm{GF}(p)^\star$ agisce su $\mathcal{N}$. Infatti, chiamato τ l'isomorfismo del teorema precedente fra V e T:

$$\mathcal{N} \in \mathfrak{N}(T) \Rightarrow \exists v \in V : \mathcal{N} = \tau(GF(p)v) \Rightarrow$$

$$\Rightarrow \forall \lambda \in \mathrm{GF}(p) : \lambda\mathcal{N} = \lambda\tau(\mathrm{GF}(p)v) = \tau(\lambda\,\mathrm{GF}(p)v) =$$

$$= \tau(\mathrm{GF}(p)v) = \mathcal{N}.$$

- Sia $\mathcal{N} \in \mathfrak{N}(T)$, $\tau_n \in \mathcal{N} \setminus \{\tau_0\}$, $q \in \mathcal{G} \setminus \mathcal{N}$. Allora $q = \tau_s\lambda$ con $s \in V$ e $\lambda \in \mathrm{GF}(p)^\star$. Ora

$$\tau_n q = q\tau_n \Leftrightarrow \tau_n\tau_s\lambda = \tau_s\lambda\tau_n \Leftrightarrow \tau_n\lambda = \lambda\tau_n.$$

D'altro canto:

$$\lambda n = n\lambda \Leftrightarrow \forall v \in V : \lambda\tau_n(v) = \tau_n\lambda(v) \Leftrightarrow$$

$$\Leftrightarrow \forall v \in V : \lambda n + \lambda v = \lambda(n+v) = n + \lambda v = \tau_n\lambda(v) \Leftrightarrow$$

$$\Leftrightarrow n = \lambda n \Leftrightarrow \lambda = 1,$$

contro l'ipotesi. Segue che $\mathrm{C}_{\tau_n} \leq \mathcal{N}$, da cui la tesi.

□

Teorema 5.16. *Sia V uno spazio vettoriale di dimensione $n > 1$ su $\mathrm{GF}(p)$, con $p > 3$, $T = \tau(V)$, e $\mathcal{G} = T \rtimes \mathrm{GF}(p)^\star$. Allora $\mathcal{G}$ ammette una partizione lineare.*

Dimostrazione. Sia $\mathfrak{N}(T)$ l'insieme di tutte le rette vettoriali di T, e sia

$$\mathfrak{F}'(\mathcal{G}) = (\mathfrak{F}(\mathcal{G}) \setminus \{T\}) \cup \mathfrak{N}(T).$$

È immediato verificare che $\mathfrak{F}'(\mathcal{G})$ è una partizione normale di $\mathcal{G}$. Sia ora

$$\epsilon(\mathcal{G}) := \{\langle(\mathrm{GF}(p)^\star)^t, F\rangle : t \in \mathcal{T}, F \in \mathfrak{N}(T)\} \cup \mathfrak{N}(T).$$

Verifichiamo l'esistenza di un elemento di $\epsilon(\mathcal{G})$ passante per due rette di $\mathfrak{F}'(\mathcal{G})$:

- se $H, K \subseteq T$, allora $\langle H, K\rangle$ è un piano vettoriale, da cui, passando allo spazio affine associato la tesi.
- se $H \subseteq T$, $K \in \mathfrak{F}(\mathcal{G})$, allora $|\mathcal{K}| > 2$ e $\exists t \in T : \mathcal{K} = (\mathrm{GF}(p)^\star)^t$ Ora:

  $$W = \langle H, \mathrm{GF}(p)^\star\rangle = H \rtimes \mathrm{GF}(p)^\star,$$

  è per il teorema precedente un gruppo di Frobenius, cui per il teorema 5.2 è associato come spazio cinematico un piano di scambio. Osserviamo che essendo T abeliano, il coniugio per elementi del nucleo è una rotazione attorno la retta T, ovvero T risulta fissata punto per punto. Inoltre esso è un automorfismo di $\mathcal{G}$, e quindi un isomorfismo fra i suoi sottogruppi. Allora

  $$H, K = (\mathrm{GF}(p)^\star)^t \subseteq \langle H, \mathrm{GF}(p)^\star\rangle^t = W^t \in \epsilon(G)$$

- Se $H, K \in \mathfrak{F}(\mathcal{G})$, $H \neq K$, allora esistono $m, n \in T$ tali che $K = \mathrm{GF}(p)^m$, $H = \mathrm{GF}(p)^n$. Sia $t = m - n$, e sia $\mathcal{N}$ l'unica retta di T tale che $1, t \in \mathcal{N}$, e sia

  $$W := \mathcal{N} \rtimes \mathrm{GF}(p)^\star.$$

  Ovviamente:

  $$H = \mathrm{GF}(p)^n \subseteq W^n;$$

  d'altro canto anche:

  $$K = \mathrm{GF}(p)^m = \mathrm{GF}(p)^(m - n + n) \subseteq W^n$$

  Dunque W^n è il gruppo di Frobenius cercato.

L'unicità della partizione contenente due rette segue immediatamente dall'essere i gruppi di Frobenius piani di scambio.

A questo punto che $\epsilon(\mathcal{G})$ soddisfi le proprietà della definizione 5.5 è di verifica immediata.

□

È possibile generalizzare il teorema precedente nel seguente modo:

Teorema 5.17. *Sia $\mathcal{G} = \mathcal{N} \rtimes \mathcal{H}$ un gruppo di Frobenius con $|\mathcal{H}| >$ 2.*

Se il nucleo $\mathcal{N}$ ammette una partizione lineare non banale $\mathfrak{N}(\mathcal{N})$, tale che:

$$\forall X \in \mathfrak{N}(\mathcal{N}) : X \lhd \mathcal{G},$$

allora

$$\mathfrak{F}'(\mathcal{G}) := (\mathfrak{F}(\mathcal{G}) \setminus \{\mathcal{N}\}) \cup \mathfrak{N}(\mathcal{N})$$

è una partizione lineare di $\mathcal{G}$.

Dimostrazione. Osserviamo che affinchè $\mathcal{N}$ ammetta una partizione non banale, esso deve essere un p-gruppo, e dunque, per il teorema [**Sch86**], abeliano.

Sia η la famiglia associata alla partizione lineare $\mathfrak{N}(\mathcal{N})$, e poniamo:

$$\theta := \{(T \rtimes \mathcal{H})^t : T \in \mathfrak{N}(\mathcal{G}), t \in \mathcal{N}\}$$

Sia inoltre:

$$\epsilon(\mathcal{G}) := \eta \cup \theta.$$

Gli elementi di θ sono tutti gruppi di Frobenius, e dunque piani di scambio. Inoltre essi intersecano $\mathcal{N}$ in esattamente una retta di $\mathfrak{N}(\mathcal{G})$.

Tenuto conto che il coniugio per $t \in \mathcal{N}$ fissa $\mathcal{N}$ elemento per elemento abbiamo che

$$\forall T \in \mathfrak{N}(\mathcal{G}); \forall H \in \mathfrak{F}(\mathcal{G}) \setminus \{\mathcal{N}\} : \exists V \in \theta : T, H \subseteq V.$$

Se poi $H, K \in \mathfrak{F}(\mathcal{G}) \setminus \{\mathcal{N}\}$, allora sia H che K sono complementi di $\mathcal{N}$ in $\mathcal{G}$, e dunque risultano coniugati. Sia $n \in \mathcal{N}$ tale che:

$$\exists n \in \mathcal{N} \setminus \{1\} : H = K^n,$$

e sia $F \in \mathfrak{N}(\mathcal{N})$ l'unico sottogruppo della partizione tale che $n \in F$. Se consideriamo il prodotto interno $\pi = FH \in \theta$, si vede subito che $H, K \subseteq \pi$ come desiderato. L'unicità di π si verifica come nel teorema precedente.

A questo punto è facile dimostrare che le condizioni postulate dalla definizione di partizione lineare sono tutte soddisfatte.

$\square$

Bibliografia

[And61] J. André. Über parallelstrukturen: Teil i: Grundbegriffe. *Math. Z.*, 76:85–102, 1961.

[Art57] Emil Artin. *Geometric Algebra.* Interscience Publishers, 1957.

[Bae52] Reinhold Baer. *Linear Algebra and Projective Geometry.* Academic Press, New York, 1952.

[Gor80] Daniel Gorenstein. *Finite Groups.* Chelsea Publishing Company, New York, 2 edition, 1980.

[JL93] Gordon James and Martin Liebeck. *Rapresentations and characters of groups.* Cambridge university press, Cambridge, UK, 1993.

[Kar73] Helmut Karzel. Kinematic spaces. *Symposia Mathematica*, 11:413–439, 1973.

[KK80] H. Karzel and H.-J. Kroll. Zur inzidenzstruktur kinematischer räume und absoluter ebenen. *Beitr. Geom. und Alg. der TU Müenchen*, 6:42–61, 1980.

[KKS73] Helmut Karzel, H.-J. Kroll, and K. Sörensen. Invariante gruppenpartitionen und doppleräume. *J. reine angew. Math.*, 262:153–157, 1973.

[KSW73] Helmut Karzel, Kay Sörensen, and Dirk Windelberg. *Einführung in die Geometrie.* Vandenhoeck & Ruprecht, Göttingen, 1973.

[Lün80] Heinz Lüneburg. *Translation Planes.* Springer-Verlag, Berlin, 1980.

[Mar77] Mario Marchi. S-spazi e loro problematica. Conferenza tenuta presso l'istituto Matematico della Università di Roma, Aprile 1977.

[MC80] Mario Marchi and C. Perelli Cippo. Su di una particolare classe di s-spazi. Rendiconti del Seminario Matematico di Brescia, Università Cattolica del Sacro Cuore, dipartimento di Matematica, 1980.

[Pia87] Silvia Pianta. On automorphisms for some fibred incidence groups. *Journal of Geometry*, 30, 1987.

[Rob82] Derek J.S. Robinson. *A Course in the Theory of Groups.* Springer-Verlag, New York, 1982.

[Rot95] Joseph J. Rotman. *An Introduction to the Theory of Groups.* Springer Verlag, New York, 4 edition, 1995.

[Sch86] Ralph-Hardo Schulz. On a conjecture of herzer concerning linear partitions. *Journal of Geometry*, 26, 1986.

[Sch94] Roland Schmidt. *Subgroup Lattices of Groups.* Walter de Gruyter, Berlin, 1994.

[Sco64] W. R. Scott. *Group Theory.* Prentice-Hall, Englewood Cliffs, N.J., 1964.

[Suz60] Michio Suzuki. A new type of simple groups of finite order. *Proc. Nat. Acad. Sci. U.S.A.*, 46:868–870, 1960.

[Suz61] Michio Suzuki. On a finite group with a partition. *Arch. Math.*, 12:241–254, 1961.

[Suz62] Michio Suzuki. On a class of doubly transitive groups. *Annals of Mathematics*, 75(1):105–145, 1962.

[Tei86] Luc Teirlinck. Combinatorial properties of planar spaces and embeddability. *Journal of combinatorial theory*, 43:291–302, 1986.

[Tho59] J.G. Thompson. Finite groups with fixed-point-free authomorphisms of prime order. *Proc. Nat. Acad. Sci. U.S.A.*, 45:578–581, 1959.

[Wie64] Helmut Wielandt. *Finite Permutation Groups.* Academic Press, New York, 1964.

[Zap69] Guido Zappa. Partizioni ed s-partizioni dei gruppi finiti. *Symposia Mathematica*, 1:85–94, 1969.

Indice