SUI GRUPPI CHE AMMETTONO FUNZIONI DI STEINER (*)

di GIOVANNI FERRERO (a Parma) (**)

SOMMARIO. - *Si forniscono varie costruzioni di sistemi di Steiner aventi un gruppo di automorfismi regolare e transitivo.*

SUMMARY. - *Several constructions of Steiner systema with a regular group of automorphisms are given.*

Introduzione.

È stato notato in [4] come lo studio dei sistemi (di terne) di Steiner (1) *regolari* (dotati cioè di un gruppo N di automorfismi regolare e transitivo sui punti) sia intimamente legato allo studio delle funzioni di Steiner α definite in un gruppo additivo (2) S; in particolare è stato notato come a ciascuna di tali funzioni α sia possibile associare in modo naturale un sistema di Steiner che ammetta il cayleiano destro di S come gruppo (ovviamente regolare e transitivo) di automorfismi.

Nel presente lavoro — che fa parte di una più ampia ricerca sull'argomento — si raccolgono varie costruzioni atte a dimostrare l'esistenza di funzioni di Steiner su dati gruppi. Allo scopo useremo, nel primo capitolo, tecniche relativamente classiche, mentre il secondo capitolo sarà imperniato su una tecnica nuova — che può essere detta tecnica di ricoprimento — precisata nel Teorema 12.

(*) Pervenuto in Redazione il 5 giugno 1972.

Lavoro eseguito con contributo del C. N. R. nell'ambito del Gruppo Nazionale per le Strutture Algebriche e Geometriche e loro Applicazioni.

(**) Indirizzo dell'Autore: Istituto di Matematica dell'Università di Parma — 43100 Parma.

(1) Non necessariamente finiti.

(2) Non necessariamente abeliano.

I risultati più importanti così ottenuti sono forniti dai Teoremi 4, 6, 8, 12, 14. I relativi enunciati sono (ove occorra) preceduti dai necessari chiarimenti terminologici.

Per riferimenti di carattere generale sulla questione rimandiamo ad [8], per notizie storiche ad [1] e a [2]; occasionalmente utilizzeremo considerazioni di [3], [4], [5] senza richiamarle esplicitamente.

1. Derivazione e composizione diretta.

1. Una *funzione di Steiner* definita in un gruppo additivo S è una involuzione α di S in S che tiene fermo l'elemento neutro $O \in S$ e tale che valga la

$$(F') \qquad \alpha(-x) = \alpha(x) - x \qquad \forall x \in S.$$

Tale definizione è stata data in [4]; ivi è stato notato fra l'altro che il gruppo additivo S ammette funzioni di Steiner se e solo se il suo cayleiano destro è un gruppo di automorfismi di un sistema di Steiner (3). Un tale gruppo deve pertanto avere se finito-ordine v della forma $6k + 1$ oppure $6k + 3$. Una parziale inversione di questo fatto è fornita dal

TEOREMA 1. (PETELSON) *Un gruppo ciclico di ordine v ammette funzioni di Steiner se e solo se $v \neq 9$ è congruo ad 1 oppure a 3 modulo 6.*

In effetti in [10] si dimostra che esistono sistemi di Steiner ciclici (4) di ordine di v se e solo se v soddisfa alle condizioni del nostro enunciato (5). Grazie all'osservazione precedente richiamata da [4] possiamo tuttavia affermare che il risultato di PETELSON ed il nostro teorema 1 sono perfettamente equivalenti.

La costruzione del n. 2.1 di [1], lievemente generalizzata e riesposta dal nostro punto di vista fornisce il

(3) E precisamente di quello le cui rette sono le terne del tipo $\{a, b, \alpha(b - a) + a\}$, con a, b elementi distinti di S.

(4) Ammettenti cioè un gruppo ciclico di automorfismi regolare e transitivo sui punti.

(5) Così è riesposto in [1] un risultato di [10]. Non entriamo qui nei dettagli perchè sarà tentato altrove un recupero di vecchi lavori sull'argomento ormai buasi illeggibili (ed introvabili).

TEOREMA 2. (DOYEN). *Il gruppo additivo S sia somma diretta di un gruppo additivo G tutti i cui elementi siano dimezzabili* (6) *e di gruppo C di ordine 3. Allora S ammette funzioni di Steiner.*

Chiaramente S è, a meno di isomorfismi, il gruppo delle coppie della forma (g, a) ove $g \in G$, $a \in \{0, 1, -1\}$ appartiene a C e la somma viene calcolata termine a termine. Definiamo entro S una funzione α mediante le posizioni

$$\alpha(0, a) = (0, -a) \qquad \forall a \in C \ (7)$$

$$\alpha(x, 0) = (x/2, 1), \quad \alpha(x, 1) = (2x, 0), \quad \alpha(x, -1) = (-x, -1) \quad \forall x \neq 0$$

Grazie al fatto che tutti gli elementi di G sono dimezzabili le posizioni precedenti forniscono effettivamente una funzione. Semplici calcoli diretti mostrano che α è effettivamente una funzione di Steiner definita in S, e questo è sufficente a dimostrare il teorema.

Il sistema di Steiner ottenuto dalla precedente funzione α è detto (8) *sistema derivato* dal gruppo G. Casi particolari della costruzione sono stati ritrovati successivamente — sempre secondo [1] — da Bose, Skolem [11], Bruck Szamkolowicz, M. Hall Jr.

Se φ è automorfismo di G la $\varphi^0 : (x, y) \longrightarrow (\varphi(x), y)$ è un automorfismo di S permutabile con la funzione α: è cioé *moltiplicatore* di α (9). Anche questo è stato in qualche modo osservato in [1].

LEMMA 3. *Se G è un gruppo (additivo) finito di ordine dispari, allora ogni suo elemento è unicamente dimezzabile.*

Per la dimostrazione basta mostrare che la $z \longrightarrow 2z$ definita in G é una biiezione di G su se stesso: grazie alla condizione di finitezza è anzi sufficiente mostrare che si tratta di una suriezione. Sia pertanto $x \in G$ un elemento di G: possiamo asserire che la sua caratteristica (10) è un numero dispari, diciamo $2k + 1$. Consideriamo ora l'elemento $y = (k+1)x$. Evidentemente $2y = (2k+2)x = x$ e

(6) Tale cioè che per ogni $x \in G$ esista uno ed un solo $y \in G$ tale che $2y = x$. In queste condizioni scriveremo nel seguito per brevità $y = x/2$, e diremo che x è dimezzabile (in modo unico).

(7) Indichiamo ancora con 0 gli elementi neutri di G e di C.

(8) Secondo [1], che si limita al caso in cui G è abeliano e finito.

(9) Nel senso di [5]; è in effetti un moltiplicatore del sistema di Steiner costruito mediante la α, se ci riferiamo soltanto a [3] e [4].

(10) Visto che il gruppo è additivo, parliamo di caratteristica di un suo elemento, anzichè di ordine.

dunque x appartiene all'immagine della $z \to 2z$. Questo basta a dimostrare l'enunciato. Di qui il

TEOREMA 4. *Il gruppo S abbia ordine dispari e possieda un fattore diretto di ordine 3. Allora S ammette funzioni di Steiner.*

È conseguenza diretta del Teorema 2 e del Lemma 3.

LEMMA 5. *Sia v un qualunque cardinale infinito. Allora esiste un gruppo di cardinalità v che ammette funzioni di Steiner* (11).

Sia Q il gruppo additivo dei razionali. Sia G la somma diretta discreta (12) di v copie di Q. Possiamo anche scrivere $G = \sum_v Q$. La cardinalità $|G|$ di G si calcola rapidamente perchè è

$$|G| = |\sum_v Q| = \sum_v |Q| = \sum_v \aleph_0 = v \cdot \aleph_0 = v \text{ (13)}.$$

La cardinalità della somma diretta S di G e di un gruppo di ordine 3 è naturalmente ancora v. D'altra parte ogni elemento di G è dimezzabile perchè somma di un numero finito di elementi dimezzabili (a due a due permutabili). Il Teorema 2 permette dunque di costruire su S (per derivazione) una funzione α di Steiner, ed il Lemma 5 è dimostrato.

Ricordando che ogni sistema di Steiner finito ha ordine congruo ad 1 oppure a 3 modulo 6 chiamiamo (14) *ordine ammissibile* per un sistema di Steiner) ogni cardinale infinito ed ogni naturale della forma $6k + 1$ o della forma $6k + 3$. Possiamo così enunciare il

TEOREMA 6. *Esiste un sistema di Steiner regolare di ogni ordine ammissibile v.*

Grazie alle considerazioni di [4] già più volte ricordate basta mostrare che per ogni ordine ammissibile v esiste un gruppo S di ordine v che ammette funzioni di Steiner.

Per il caso in cui $v = 9$ si osserva infatti che il gruppo abeliano elementare di ordine 9 ammette l'inversione $i : x \to -x$ come funzione

(11) Ricordiamo comunque da [2] che Sierpinski ha dimostrato che esistono sistemi di Steiner di qualunque cardinalità infinita v.

(12) In opposizione alla ben nota somma diretta completa. Per la terminologia ci atteniamo qui a [6].

(13) Per il primo passaggio si veda ad es. [6], pg 20.

(14) In armonia con [10].

di Steiner ([15]); se v è finito e diverso da 9 basta considerare il gruppo ciclico di ordine v e ricordare il Teorema 1; se v è infinito basta utilizzare il gruppo fornito dal Lemma 5. In ogni caso il Teorema è dunque verificato.

2. Una semplice (e praticamente classica) tecnica per costruire funzione di Steiner è fornita dal

TEOREMA 7. *Sia* $\{G_i\}$ $(i \in I)$ *un sistema di gruppi, ciascuno dei quali ammetta una funzione di Steiner* α_i. *Allora la somma diretta (e anche quella completa) dei gruppi* G_i *ammette funzioni di Steiner.*

Per evitare di discutere in dettaglio le notazioni ci limitiamo ad indicare la dimostrazione per il caso in cui $I = \{1, 2\}$. Allora il generico elemento di $S = G_1 + G_2$ ([16]) può essere scritto come $g = (g_1, g_2)$, con $g_1 \in G_1$ e $g_2 \in G_2$. Basta porre $\alpha(g_1, g_2) = (\alpha_1(g_1), \alpha_2(g_2))$ per avere la funzione di Steiner richiesta, come subito si verifica.

Le funzioni ottenute attraverso il Teorema 7 verranno dette ottenute per *composizione diretta* dalle α_i.

Siano v un cardinale infinito e G un gruppo finito ammettente la funzione di Steiner α. È chiaro che possiamo formare la somma diretta discreta S di v copie di G, ed in essa definire per composizione diretta una funzione di Steiner usufruendo del Teorema 7. Come nella dimostrazione del Lemma 5 si vede che la cardinalità di S è ancora v, e questo fornisce un'altra dimostrazione di tale Lemma. La ridondanza è tuttavia soltanto apparente perchè i gruppi e le funzioni di Steiner così ottenuti sono del tutto diversi da quelli ottenuti nella dimostrazione originaria del Lemma 5. Anche più avanti ci capiterà di usare enunciati simili per mettere in evidenza costruzioni essenzialmente diverse ([17]).

La composizione diretta permette (sia pure passando attraverso il Teorema 1) di costruire con una certa facilità funzioni di Steiner su molti gruppi abeliani finiti. Richiamiamo anzitutto a tale scopo il concetto di *invariante* di un gruppo abeliano finito ([18]).

Se A è un p-gruppo abeliano finito esso può essere scritto essenzialmente in un solo modo come somma diretta di gruppi ciclici.

([15]) E in definitiva fornisce un particolarissimo sistema fine. Cfr. [5].

([16]) Ove il segno « + » indica la somma diretta.

([17]) Perchè una costruzione eventualmente complicata non può essere tutta inserita in un enunciato.

([18]) Secondo [7], pg. 41.

Gli ordini di tali gruppi prendono il nome di invarianti di A. Un generico gruppo abeliano finito S è somma diretta dei suoi sottogruppi di Sylow: chiamiamo invarianti di S gli invarianti dei suoi sottogruppi di Sylow [19].

Introduciamo ora notazioni atte ad alleggerire l'enunciato del prossimo teorema.

Sia S un gruppo abeliano finito di ordine dispari. Siano $p_1, p_2, \ldots, p_n$ i divisori primi del suo ordine che sono congrui a 5 modulo 6. Indichiamo con a_i $(i = 1, 2, \ldots, n)$ il numero degli invarianti di S che sono potenze di p_i e sono ancora congrui a 5 modulo 6 [20].

Non è restrittivo supporre che sia $a_1 \leqq a_3 \leqq \ldots \leqq a_n$ perchè possiamo sempre, ove occorra, permutare in modo qualunque gli indici dei p_i.

Indichiamo con b il numero degli invarianti di S che sono eguali a 9; indichiamo con c il numero degli invarianti di S che sono multipli proprii di 9.

Indichiamo ancora con d il numero degli invarianti di S che sono congrui ad 1 modulo 6. Poniamo inoltre

$$r = \Sigma_i\, (-1)^{n-i} a_i\,; \quad a = \Sigma_i\, a_i\,.$$

Possiamo ora enunciare il

TEOREMA 8. *Sia S un gruppo abeliano di ordine dispari* [21]. *Valgano le condizioni*

$$r \leqq b + c\,; \quad b \leqq (a + r)/2 + d \text{ [22]}.$$

Allora S ammette funzioni di Steiner.

Osserviamo intanto che la tesi è senz'altro verificata quando uno degli invarianti di S è uguale a 3 (per il Teorema 4). Possiamo pertanto per semplicità supporre che gli invarianti di S siano precisamente quelli (in numero di $a + b + c + d$) cui abbiamo fatto riferimento poco sopra.

[19] Così un gruppo di invarianti 9, 9, 5, 5 è la somma diretta di due gruppi ciclici di ordine 9 e di due gruppi di ordine 5.

[20] Si tratta, ovviamente, degli invarianti di S che sono potenze di p_i *con esponente dispari.*

[21] Da [4] risulta che nessun gruppo contenente elementi di caratteristica 2 può possedere funzioni di Steiner.

[22] Dalle posizioni iniziali risulta subito che $a + r$ è un numero pari.

Premettiamo che *è possibile scrivere S come somma diretta* di $(a - r)/2 + d$ gruppi ciclici avente ordine congruo ad 1 modulo 6, di b gruppi ciclici di ordine 9, di c 3-gruppi ciclici aventi ordine propriamente multiplo di 9 e di un residuo di r p_n-gruppi ciclici aventi ordine congruo a 5 modulo 6.

Per vederlo pensiamo anzitutto di aver decomposto S in somma diretta di gruppi ciclici i cui ordini siano gli invarianti di S. Grazie al fatto che $a_1 \leqq a_2$ ([23]) possiamo associare a ciascuno dei p_1-fattori ([24]) avente ordine congruo a 5 modulo 6 un p_2-fattore (anch'esso avente ordine congruo a 5 modulo 6). Possiamo anzi farlo in modo che a p_1-fattori distinti corrispondono p_2-fattori distinti. La somma di ciascun p_1-fattore col p_2-fattore ad esso associato risulta essere un gruppo ciclico ([25]); il suo ordine è congruo ad 1 modulo 6 ([26]). Possiamo così aggiungere a_1 fattori ciclici aventi ordine congruo ad 1 modulo 6 ai d fattori di tale tipo che già erano presenti nella decomposizione iniziale ([27]).

A ciascuno degli $a_2 - a_1$ p_2-fattore aventi ordine congruo a 5 modulo 6 non utilizzati nel ragionamento precedente ([28]) possiamo come sopra associare un p_3-fattore (visto che $a_2 - a_1 \leqq a_2 \leqq a_3$). Ragionando al solito modo ci possiamo procurare così $a_2 - a_1$ ulteriori fattori ciclici aventi ordine congruo ad 1 modulo 6: ricordando il passaggio precedente avremo in tutto $a_1 + (a_2 - a_1) = a_2$ fattori di tale tipo, mentre rimarranno a disposizione $a_3 - (a_2 - a_1) = a_3 - a_2 + a_1$ p_3-fattori. Continuando a ragione allo stesso modo ([29]) si ottengono, dopo $n - 1$ passi, $(a - r)/2$ fattori di S ciclici con ordine congruo ad uno modulo 6, mentre rimangono «a disposizione» r p_n-fattori con ordine congruo a 5 modulo 6. Aggiungendo ai fattori costruiti quelli che non sono intervenuti nel ragionamento si dimostra la richiesta premessa.

([23]) Continuiamo ad usare le notazioni introdotte prima dell'enunciato.

([24]) Chiamiamo p^i-fattore ogni fattore diretto che sia un p_i-gruppo.

([25]) Perchè somma diretta di gruppi ciclici aventi ordini primi fra loro.

([26]) Perchè ha ordine eguale (modulo 6) a $5.5 = 25 = 1$.

([27]) È evidente che più tardi applicheremo il Teorema 1 a tali fattori.

([28]) Che non sono cioè stati associati ad alcun p_1-fattore.

([29]) Crediamo sia inutile usare più esplicitamente il principio di induzione: Osserviamo soltanto che al passaggio successivo ci saremo procurati $a_2 + (a_3 - a_2 + a_1) = a_3 + a_1$ gruppi ciclici aventi ordine del tipo $6k + 1$, conservando a disposizione $a_4 - (a_3 - a_2 + a_1) = a_4 - a_3 + a_2 - a_1$ p_4-fattori di ordine congruo a 5 modulo 6.

Ora *la dimostrazione del Teorema* 8 può essere completata *esaminando separatamente* il caso in cui $r \leqq b$ e quello in cui

$$b \leqq r (\leqq b + c).$$

Supponiamo dapprima che sia $r \leqq b$. Possiamo allora associare a ciascuno degli r p_n-fattori residui della decomposizione precedente uno dei b fattori di ordine 9 ([30]). La somma diretta dei fattori così associati risulta essere un gruppo ciclico avente ordine congruo a 3 modulo 6 ([31]). Ora, grazie alla seconda delle condizioni che fanno parte dell'ipotesi, possiamo vedere che $b - r \leqq (a - r)/2 + d$. Pertanto possiamo, come al solito, associare ognuno dei residui fattori di ordine 9 ad un fattore ciclico di ordine congruo ad uno modulo 6 (e dunque primo con 9). Formando la somma diretta dei fattori così associati si trovano così $b - r$ fattori ciclici con ordine congruo a 3 modulo 6 ma diverso da 9. In definitiva S risulta scritto come somma diretta di $(a + r)/2 + d - b$ fattori ciclici di ordine congruo ad 1 modulo 6, e di $b + c$ gruppi ciclici di ordine congruo a 3 modulo 6 ma diverso da 9. Per il Teorema 1 ciascuno di tali fattori ammette funzioni di Steiner, e dunque, per il Teorema 7, anche il gruppo S di partenza ammette una funzione di Steiner, e la tesi del Teorema è in questo caso verificata.

Veniamo ora al caso in cui $b \leqq r$. In tale condizione possiamo associare ad ognuno dei b fattori di ordine 9 uno degli r p_n-fattori ciclici residui ([32]). Come al solito per somma diretta dei fattori associati otteniamo b fattori ciclici aventi ordine congruo a 3 modulo 6 ma diverso di 9. Rimangono $r - b$ p_n-fattori ciascuno dei quali potrà essere associato a qualcuno dei c 3-fattori che non hanno ordine 9 ([33]). Come nel caso precedente si ottiene così una decomposizione di S in un certo numero di fattori diretti ciclici ciascuno dei quali ammette funzioni di Steiner in base al Teorema 1. Basta ricordare ancora il Teorema 7 per avere la verifica della nostra tesi anche nel presente caso.

([30]) Sempre facendo in modo che a fattori diversi siano associati fattori diversi.

([31]) Perchè somma diretta di gruppi ciclici aventi ordine primo tra loro e perchè $5.3 = 15 = 3$ modulo 6.

([32]) Secondo la decomposizione che costituisce la prima parte della dimostrazione del presente teorema.

([33]) Grazie al fatto che $r \leqq b + c$, come richiesto nell'enunciato del teorema.

Tra i gruppi che non soddisfano le ipotesi del teorema S troviamo fra l'altro i p gruppi abeliani elementari di ordine p^{2k} ([34]) ove p sia congruo a 5 modulo 6) e le somme dirette di gruppi ciclici di ordine 9.

Per discutere inoltre i moltiplicatori delle funzioni di Steiner ottenute bisognerebbe aver studiato i moltiplicatori delle funzioni fornite solo indirettamente dal Teorema 1. Qui ci limitiamo ad una semplice osservazione, a carattere indicativo. *Se S è somma diretta di gruppi ciclici aventi ordine della forma $2^x - 1$, allora S ammette una funzione di Steiner α i cui moltiplicatori numerici sono tutte e sole le potenze di* 2. Per vederlo è sufficiente, scomposto S in somma diretta di gruppi ciclici di ordine del tipo $2^x - 1$, introdurre in ciascuno di essi una funzione di Steiner come indicato nel capitolo 2 di [5], a partire da campi finiti opportuni.

Applicando il Teorema 7 si ottiene una funzione di Steiner α definita su tutto S. Il fatto che tutte le funzioni iniziali ammettono tutte e sole le potenze di 2 come moltiplicatori numerici ([35]) permette di dimostrare rapidamente in modo ovvio la stessa cosa con riferimento alla funzione α stessa.

2. Partizioni e ricoprimenti.

3. La banale osservazione che una traiettoria di un gruppo di Steiner Σ_α definito nel gruppo additivo S ([36]) è sempre contenuta nel gruppo generato da due suoi (opportuni) elementi ([37]) suggerisce subito una *tecnica di incollamento* per costruire funzione di Steiner su un gruppo a partire da funzioni di Steiner definite su suoi sottogruppi.

OSSERVAZIONE 9. *Il gruppo additivo S ammetta un ricoprimento $\{G_i\}$ $(i \in I)$ formato da suoi sottogruppi. In ciascun G_i sia definita una funzione Steiner α_i. Supponiamo che $(\forall\, i, j \in I)$ le restrizioni di α_i ed α_j al gruppo $G_i \cap G_j$ coincidano. Allora l'unione α delle α_i è una funzione di Steiner definita su tutto S.*

([34]) Quelli di ordine p^{2k+1} non hanno qui alcun interesse visto che hanno ordine congruo a 5 modulo 6, e dunque non possono ammettere funzioni di Steiner. Per $p^{2k} = 6k + 1$ cfr. [8], pag. 233, che fornisce la possibilità di migliorare il nostro enunciato; ritorneremo altrove sull'argomento.

([35]) Si tenga presente in particolare il n. 7 di [5].

([36]) Per questa terminologia — qui del resto non essenziale- — si veda [5].

([37]) E più precisamente la traiettoria rappresentata dal generico $x \in S$ è contenuta nel gruppo additivo generato da x e da $\alpha(x)$.

Intanto la condizione relativa alle restrizioni implica che l'unione α delle α_i è una funzione. Che poi α sia involutoria e soddisfi alla (F') discende immediatamente dal fatto che ciascuna delle α_i gode di tale proprietà. È poi evidente che $\alpha(0) = 0$, e l'enunciato è dimostrato.

Un risultato che ([38]) sarà tra poco superato — almeno dal punto di vista esistenziale — ma non privo di interesse perchè permette di costuire funzioni di Steiner in modo piuttosto esplicito è il

COROLLARIO 10. *Il gruppo S ammetta una partizione π ([39]). Per ogni elemento G_i di π sia data una funzione di Steiner α_i. Allora l'unione α di tali funzioni di Steiner è una funzione definita su tutto S.*

È conseguenza immediata della precedente Osservazione 9. Da esso si deduce subito per esempio che ogni gruppo avente esponente ([40]) primo p congruo ad 1 modulo 6 oppure avente esponente 3 ammette funzioni di Steiner.

Particolarmente interessante appare il caso in cui S *ha esponente primo di Mersenne* (cioè della forma $p = 2^n - 1$): allora possiamo usare il Corollario 10 usando le funzioni di Steiner considerate nel secondo capitolo di [5]. Più precisamente possiamo definire in ciascuno dei sottogruppi G_i di S aventi ordine p una funzione di Steiner α_i che ammette come moltiplicatori tutte e sole le funzioni del tipo $x \to 2^t x$ ([41]). Riunendo le α_i otteniamo una funzione di Steiner α. I moltiplicatori numerici (di Hall) di α sono certamente moltiplicatori numerici di tutte le α_i, perchè un moltiplicatore di Hall tiene fermi tutti i sottogruppi del gruppo in cui opera ([42]). Pertanto i moltiplicatori numerici da α saranno tutti potenze di 2. Ma se 2^t è un tale molitplicatore deve essere $(\forall\, a, b \in S)$ $2^t(a + b) = 2^t a + 2^t b$.

([38]) Come del resto la precedente Osservazione 9.

([39]) Ricordiamo che una partizione del gruppo S è un insieme di suoi sottogruppi non ridotti al solo zero tale che ogni elemento non nullo di S appartenga ad uno ed un solo elemento della partizione. Cfr. per es. [9].

([40]) Nonostante la notazione addiva diciamo ancora gruppo di esponente n ogni gruppo S tale che $nx = 0\ \forall\, x \in S$. Si potrebbe anche parlare di caratteristica.

([41]) Per già citato n. 7 di [5]; per ragioni di brevità non riteniamo opportuno dilungarci in richiami più espliciti.

([42]) Anche qui rimandiamo senz'altro a [3] e [5] per questo tipo di terminologia.

Allora (per un noto risultato di Baer già usato nel n. 2 di [3]) il gruppo S risulta somma diretta di un gruppo abeliano, un 2-gruppo ed un $(2^t - 1)$-gruppo ([43]). Ma S per ipotesi è un p-gruppo, con $p = 2^n - 1$ e dunque se 2^t non è un moltiplicatore numerico banale S si riduce ad un gruppo abeliano ([44]). Ne segue che *la funzione α sopra costruita ammette moltiplicatori numerici non banali se e solo se S è abeliano.* Se anzi S è abeliano i moltiplicatori numerici di α sono tutte e sole le potenze di 2 ([45]).

In generale tuttavia α possiede moltiplicatori non banali. Ad esempio pel caso $p = 3$ (studiato in [5] perchè fornisce i sistemi fini) ogni automorfismo di S risulta essere un moltiplicatore dell'unica funzione α che può essere costruita come poco sopra.

Anche il caso $p = 7$ presenta particolare interesse perchè in esso (come per i sistemi fini) tutte le traiettorie di Σ_a hanno lo stesso ordine e ciascuna di esse — unita con lo zero di S — fornisce un sottogruppo di S. La situazione è tuttavia qui più complessa perchè le funzioni di Steiner definite su un gruppo ciclico di ordine 7 sono due ([46]). Approfondiremo altrove il caso.

COROLLARIO 11. *Sia S un gruppo. Sia $p = 3$ o $p = 6k + 1$ un divisore primo del suo ordine. Se il sottogruppo (di Hughes) H_p di S ([47]) ammette una funzione di Steiner, allora S stesso ammette funzioni di Steiner.*

Se $H_p = S$ la cosa è banale. Altrimenti si osserva che H_p, insieme con i sottogruppi di ordine p di S che non sono contenuti in H_p, fornisce una partizione di S. L'enunciato segue ora subito dal Corollario 10 e dal Teorema 1.

Si osservi che per il caso dei p-gruppi finiti questa è l'unica possibile applicazione diretta del Corollario 10. Infatti, per il lemma di [9] un p-gruppo finito ammette una partizione non banale se e

([43]) Ricordiamo che un n-gruppo è un gruppo le caratteristiche dei cui elementi sono tutte prime con tutti i numeri primi con n.

([44]) Perchè un $2^t - 1$-gruppo S è un p-gruppo non identico solo se $2^t - 1$ è un multiplo di p; in queste condizioni la $x \to 2^t x$ coincide con l'identità e 2^t è un moltiplicatore numerico banale perchè $(\forall x \in S)$ è $(2^t - 1)x = 0$.

([45]) Naturalmente questo non esclude che funzioni di Steiner definite su S ma diverse dalla α possano ammettere moltiplicatori di Hall.

([46]) Scrivendole come sostituzioni sugli interi modulo 7 sono infatti: $\alpha_1 = (15)(23)(46)$ e $\alpha_2 = (13)(26)(45)$. Gli automorfismi del gruppo che non sono moltiplicatori (per entrambe) le scambiano fra loro.

([47]) Il sottogruppo cioè di S generato dai suoi elementi che non hanno ordine p. Cfr. per es. [12].

solo se non ha ordine di p e non è generato dai suoi elementi di caratteristica diversa da p.

4. Vediamo ora di migliorare l'Osservazione 9 allo scopo di ottenere risultati esistenziali più incisivi.

TEOREMA 12. *Sia S un gruppo additivo. Sia $R = \{G_i\}$ $(i \in I)$ un ricoprimento di S costituito da suoi sottogruppi* (48). *Supponiamo che ogni G_i ammetta una funzione di Steiner α^i. Supponiamo inoltre che per ogni sottoinsieme J di I ed ogni $j \in J$ sia $\alpha_j \left(\bigcap_{k \in J} G_k\right) = \bigcap_{k \in J} G_k$. Allora S ammette funzioni di Steiner che tengono fermi tutti gli elementi di R.*

Non è restrittivo supporre ancora che i $G_i \in R$ siano distinti, che cioè $G_i = G_j$ implichi $(\forall\, i, j \in I)$ che sia $i = j$ (49).

Neppure è restrittivo supporre che *l'intersezione degli elementi di un qualunque sottoinsieme di R sia ancora un elemento di R.*

Se non è così possiamo infatti sostituire R con l'insieme R^0 delle intersezioni degli elementi di R (50). Sia poi il I^0 l'insieme dei sottoinsiemi non vuoti di I. Chiaramente ciascun elemento di R^0 potrà essere scritto come $G_J = \bigcap_{k \in J} G_k$ $(J \in I^0)$. A ciascun G_J possiamo associare una funzione α_J ottenuta restringendo a G_J una (arbitraria) delle α_k, per $k \in J$, (51). Grazie alla condizione sulle intersezioni che compare nell'enunciato del Teorema α_J risulta una funzione di G_J su G_J, ed è immediato vedere che si tratta ancora di una funzione di Steiner. Scegliendo un opportuno sottoinsieme J^0 di I^0 in modo da evitare le ripetizioni (come abbiamo accennato poco sopra) si ottiene un ricoprimento $R^0 = \{G_J\}$ $(J \in J^0)$ che soddisfa ancora alle ipotesi del teorema ma in cui ogni intersezione di elementi di R^0 appartiene ancora ad R^0 ed in cui gruppi aventi indice distinto sono distinti. *Ritorniamo ora alle notazioni dell'enunciato supponendo che condizioni predette siano soddisfatte.*

È chiaro che ora R risulta parzialmente ordinato per inclusione, è anzi un $\cap$-semireticolo completo (52). Possiamo trasportare ad I la

(48) Ogni elemento di S appartenga cioè ad uno almeno dei G_i.

(49) Basta, all'occorrenza, pensare di sostituire I con un opportuno sottoinsieme in modo da « scartare le ripetizioni ».

(50) Ricordando che, in base ad abituali convenzioni, $\bigcap_{k \in J} G_k$ coincide con G_i se $J = \{i\}$.

(51) Nel caso più generale questo passaggio richiede l'assioma di Zermelo.

(52) Nel senso che ogni suo sottoinsieme ammette un massimo minorante; qui addirittura l'intersezione dei suoi elementi.

relativa struttura d'ordine dicendo che ($\forall\, i, j \in I$) è $i \leqq j$ se e solo se $G_i \subseteq G_j$. Per ogni $x \in S$ ora l'insieme degli elementi di R che contengono x ammette un minimo elemento $G_{i(x)}$: *a questo modo risulta ben definita una funzione* $x \longrightarrow i(x)$ da S ad I. Per le posizioni fatte sarà chiaramente $x \in G_i$ se e solo se $i(x) \leqq i$.

Di qui e dal fatto che gli elementi di R sono sottogruppi di S si ottiene subito che è $i(x) = i(-x)$, $\forall\, x \in S$.

Mostriamo che è anche $i(x) = i(\alpha_{i(x)}(x))$. Intanto $\alpha_{i(x)}(x) \in G_{i(x)}$, perchè $x \in G_{i(x)}$ e $\alpha_{i(x)}$ tiene fermo $G_{i(x)}$. Se ne deduce — utilizzando una delle precedenti osservazioni — che è $i(\alpha_{i(x)}(x)) \leqq i(x)$. D'altra parte ora ha senso considerare l'elemento $\alpha_{i(x)}(\alpha_{i(x)}(x))$, che è eguale ad x perchè per ipotesi $\alpha_{i(x)}$ è involutoria. Ma — per l'ultima delle ipotesi del teorema — $\alpha_{i(x)}$ tiene fermo $G_{i(\alpha_{i(x)}(x))}$ che è contenuto in $G_{i(x)}$ [53] (e appartiene ad R) e dunque $x = \alpha_{i(x)}(\alpha_{i(x)}(x)) \in G_{i(\alpha_{i(x)}(x))}$. Ne segue che $i(x) \leqq i(\alpha_{i(x)}(x))$ e in definitiva che $i(x) = i(\alpha_{i(x)}(x))$.

Poniamo ora, $\forall\, x \in S$

$$\alpha(x) = \alpha_{i(x)}(x):$$

abbiamo così definito una funzione α da S ad S.

Mostriamo che la funzione α *è una funzione di Steiner.*

È intanto ovvio che $\alpha(0) = \alpha_{i(0)}(0) = 0$ perchè tutte le α_i — in quanto funzioni di Steiner — tengono fermo lo zero di S. Inoltre, $\forall\, x \in S$ è

$$\alpha(\alpha(x)) = \alpha(\alpha_{i(x)}(x)) = \alpha_{i(\alpha_{i(x)}(x))}(\alpha_{i(x)}(x)) = \alpha_{i(x)}(\alpha_{i(x)}(x)) = x$$

tosto che si ricordi che $i(\alpha_{i(x)}(x)) = i(x)$ e che $\alpha_{i(x)}$ è involutoria. Per verificare che α soddisfa anche alla (F') basta notare che

$\alpha(-x) = \alpha_{i(-x)}(-x) = \alpha_{i(x)}(-x) = \alpha_{i(x)}(x) - x = \alpha(x) - x$, come risulta ricordando che è $i(-x) = i(x)$ e che $\alpha_{i(x)}$ — in quanto funzione di Steiner — soddisfa alla $\alpha_{i(x)}(-x) = \alpha_{i(x)}(x) - x$, $\forall\, x \in S$.

Inoltre α *tiene fermi tutti i* $G_i \in R$. Infatti se $x \in G_i$ è ovviamente $\alpha(x) = \alpha_{i(x)}(x) \in G_{i(x)} \subseteq G_i$ perchè allora $i(x) \leqq i$.

Con questo il Teorema 12 è dimostrato. Per fornire una prima facile applicazione premettiamo il

[53] Infatti $G_{i(\alpha_{i(x)}(x))}$ è intersezione degli elementi di R che lo contengono, ed uno di questi è $G_{i(x)}$, per quanto sopra osservato.

LEMMA 13. *Il gruppo ciclico S abbia ordine privo di quadrati. I fattori primi del suo ordine diversi da tre siano tutti congrui ad uno modulo 6. Allora S ammette una funzione di Steiner che tiene fermi tutti i suoi sottogruppi.*

Chiaramente S è somma diretta dei suoi sottogruppi di Sylow: questi hanno ordine primo e per ciascuno di essi valgono le ipotesi del Teorema 1. Ciascuno di questi ammette pertanto una funzione di Steiner. Componendo tali funzioni giusta il Teorema 7 si ottiene una funzione di Steiner α. Essa evidentemente tiene fermi tutti i sottogruppi della decomposizione iniziale. Ma i sottogruppi di S sono tutti somma di un certo numero di suoi sottogruppi di Sylow, e chiaramente ciascuno di essi risulta tenuto fermo dalla funzione α.

TEOREMA 14. *Sia S un n-gruppo* ([54]), *ove n sia prodotto di numeri della forma $6k+1$ ed eventualmente di 3. Supponiamo che le caratteristiche dei suoi elementi siano tutte prive di quadrati. Allora S ammette una funzione di Steiner α che tiene fermi tutti i suoi sottogruppi.*

Chiaramente i sottogruppi ciclici G_i di S formano un suo ricoprimento. Possiamo associare a ciascun G_i una funzione di Steiner α_i in esso definita che tenga fermi tutti i suoi sottogruppi (Lemma 13). Pertanto il ricoprimento $R = \{G_i\}$ con le funzioni α_i soddisfa alle ipotesi del Teorema 12. Da tale Teorema si deduce che S possiede una funzione di Steiner α che tiene fermi tutti i suoi sottogruppi ciclici (cioè gli elementi di R): una tale funzione non può che tenere fermi tutti i sottogruppi di S, e il Teorema è dimostrato.

Naturalmente esistono molti gruppi che soddisfano contemporaneamente alle ipotesi del Teorema 8 ed a quelle del Teorema 14, ma è facile convincersi che applicando tali teoremi ad uno di questi gruppi si ottengono in generale funzioni di Steiner essenzialmente diverse. Anche questo discorso sarà ripreso altrove.

([54]) Non necessariamente finito, nè abeliano.

BIBLIOGRAFIA

[1] J. DOYEN, *Sur la structure de certaines systèmes triples de Steiner*, Math. Zeit. **111** (1969), 289-300.

[2] J. DOYEN, *Sur la croissance du nombre de systèmes triples de Steiner non isomorphes*, J. Comb. **8** (1970), 424-441.

[3] G. FERRERO, *Sul concetto di moltiplicatore nel senso di Hall*, Riv. Mat. Univ. Parma, **12** (1972), in corso di stampa.

[4] G. FERRERO e A. SUPPA, *Sistemi, annelloidi e funzioni di Steiner*, Atti Sem. Mat. Fis. Univ. Modena, **20** (1971), 1-9.

[5] G. FERRERO, *Gruppi di Steiner e sistemi fini*, «Le Matematiche», Catania, in corso di stampa.

[6] L. FUCHS, *Abelian groups*, P. H. Hungarian Acad. Sci., Budapest, 1958.

[7] M. HALL Jr. *The theory of groups*, The MacMillan C. New York, 1959.

[8] M. HALL. Jr. *Combinatorial theory*, Blaisdell P. C. Waltham, Mass. 1967.

[9] O. K. KEGEL, *Nicht-einfache Partitionen endicher Gruppen*, Ark. Math. (1961), 170-175.

[10] R. PETELSON, *Eine lösung der beiden Hefftersehen Differenzprobleme*, Comp. Math. **6** (1939), 251-257.

[11] TH. SKOLEM, *Some remarks on the triple systems of Steiner*, Math. Scand. **6** (1958), 237-280.

[12] G. ZAPPA, *Contributo allo studio del problema di Hughes sui gruppi*, Ann. Mat. Pura e Appl. (4), **58**, 211-220.