Riv. Mat. Univ. Parma (2) **11** (1970), 79-96

GIOVANNI FERRERO (*)

# Stems planari e BIB-disegni. (**)

**Introduzione.**

Allo scopo di collegare varie teorie si osserva che lo studio di uno stem planare finito su un gruppo $G$ equivale allo studio della terna formata dal gruppo $G$, da un gruppo $\Phi$ di automorfismi di $G$ (tutti senza coincidenze), e da un insieme non vuoto $M$ di elementi « privilegiati » di $G$ (può essercene uno al più in ciascuna traiettoria di $\Phi$). Gli stems interi (cioè privi di divisori dello zero) sono, a meno di casi banali, gli stems planari in cui l'insieme $M$ è massimale (rispetto alla condizione sopra indicata). Queste considerazioni permettono così di discutere con una certa facilità una congettura di CLAY [6] secondo cui gli stems interi avrebbero come caratteristica un numero primo: noi mostriamo che la congettura ammette delle eccezioni.

Nella seconda parte del lavoro si utilizzano gli stems planari per costruire BIB-disegni (*Balanced Incomplete Block Designs*) di parametri $v$, $b$, $k$, $r$, $\lambda$ in cui $k = \lambda$. Il nostro procedimento (analogo in un certo senso a quello di BRUCK [5] per i BIB-disegni in cui $v = b$), tenuto conto anche di recenti ricerche di CLAY [7], sembra abbastanza adatto al calcolo automatico. Osservazioni e corollari, specie nell'ultimo paragrafo, indicano la possibilità di ulteriori sviluppi algebrici e geometrici.

Notazioni e definizioni sono introdotte all'inizio dei vari paragrafi.

## § 1. - Stems planari.

1. – Cominciamo col riproporre ed inquadrare alcune definizioni, ed a precisare la simbologia che sarà usata nel presente lavoro.

---

(*) Indirizzo: Istituto di Matematica, Università, 43100 Parma, Italia.

(**) Lavoro eseguito nell'ambito dell'attività dei Gruppi di Ricerca Matematica del Consiglio Nazionale delle Ricerche. – Ricevuto: 3-I-1970.

Uno stem (sinistro) $G$ finito (1) è *fortemente monogeno* se le corrispondenze $\varphi_a: x \to ax$ diverse dall'endomorfismo nullo formano un gruppo $\Phi$. Useremo continuamente, senza ulteriori richiami, queste notazioni, nonchè la costruzione degli stems fortemente monogeni, basata sul concetto di traiettoria principale di $\Phi$, che risulta dai nn. 5 e 6 di [12].

Si dice che due elementi $a$, $b$ di uno stem sinistro $G$ sono *equivalenti* a sinistra se per ogni $x$ di $G$ è $ax = bx$; ciò equivale a dire che le corrispondenze $\varphi_a$ e $\varphi_b$ vengono a coincidere. Per indicare questo fatto si scrive $a \equiv_s b$ (2).

Definizione $A$ (3). *Uno stem $G$ è detto planare se:*

I) *tutte le equazioni in $G$ del tipo*

$$ax = bx + c \qquad (a,\ b,\ c \in G;\ \ a \not\equiv_s b,\ \ x \text{ incognita}) \tag{1}$$

*hanno una ed una sola soluzione;*

II) *$G$ contiene almeno tre elementi due a due non equivalenti a sinistra.*

Si osserva subito che la condizione I) è vuota per gli stems i cui elementi sono tutti equivalenti a sinistra: si tratta degli stems rettangolari che abbiamo studiato in [10].

Per comprendere meglio la definizione è utile il

Lemma 1. *Se $G$ soddisfa alla condizione* I) *della Definizione $A$ e possiede un elemento non equivalente a sinistra con lo zero, allora $G$ è fortemente monogeno* (4).

Mostriamo intanto che allora $0G = 0$. Sia $a \not\equiv_s 0$ un elemento di $G$. Per la condizione I) di $A$ l'equazione (in $x$) $ax = 0x + 0$ ammette una sola soluzione. Ma tale equazione è soddisfatta tanto da 0 che da $0b$, qualunque sia $b \in G$, e pertanto $0b = 0$ e, per la genericità di $b$, è anzi $0G = 0$.

Per completare la dimostrazione mostriamo che se $b \neq 0$ divide lo zero a sinistra, il prodotto di $b$ e di un qualunque elemento di $G$ è nullo (5). Detto $c$ un elemento non nullo di $G$ tale che $bc = 0$, se non fosse $b \equiv_s 0$ (6),

---

(1) In tutto il lavoro ci riferiremo soltanto a stems finiti.

(2) Cfr. [2] e [3].

(3) Cfr. [2] e [3].

(4) Questo sembra noto, in [2] ed altrove, ma non ne abbiamo trovato enunciazioni e dimostrazioni così esplicite.

(5) Si ricordi che ci si riferisce agli stems finiti, e si tenga presente la definizione di [13] sopra riportata.

(6) Se, cioè, non valesse la tesi che ci proponiamo di dimostrare.

la $bx = 0x + 0$ avrebbe una sola soluzione, mentre — dopo quanto sopra osservato — tanto 0 che $c$ la soddisfano. L'enunciato è così dimostrato.

Ricordiamo ora che gli *stems a prodotti banali* (introdotti in [**15**]) sono quelli in cui le $\varphi_a$ diverse dall'endomorfismo nullo si riducono all'identità. Ciò posto, siamo in grado di precisare la portata della condizione II) della Definizione ***A***. Sussiste infatti il

Corollario **1.** *Gli stems che soddisfano alla condizione* I) *della Definizione* ***A*** *ed hanno due sole classi di elementi equivalenti a sinistra sono gli stems a prodotti banali.*

Ciò segue dal fatto che gli elementi di uno stem $G$ siffatto, che sono equivalenti a sinistra con lo zero, annullano a sinistra tutti gli elementi di $G$ (per la prima parte della dimostrazione del Lemma 1 ).

L'altra classe di elementi equivalenti a sinistra deve essere costituita da non divisori dello zero a sinistra (sempre per il Lemma 1 ); poichè il prodotto di due elementi di tale classe è ancora un elemento della classe (7), se $a \not\equiv_s 0$ il relativo $\varphi_a$ deve essere un automorfismo idempotente, e dunque l'identità. Siamo dunque in presenza di uno stem a prodotti banali. Il resto è ovvio.

Teorema 1. *Lo stem $G$ è planare se, e solo se, $G$ è fortemente monogeno con prodotti non banali e se tutte le traiettorie non identiche del relativo gruppo $\Phi$ sono principali* (8).

Sia $G$ uno stem planare. Abbiamo visto che $G$ è fortemente monogeno.

Mostriamo che tutte le traiettorie non identiche del relativo $\Phi$ sono principali. Per questo si osservi che se $b \not\equiv_s 0$ (9), con le abituali notazioni richiamate all'inizio di questo numero, la (1) equivale successivamente alle

$$ax = bx + c, \qquad \varphi_a(x) = \varphi_b(x) + c, \qquad c = -\varphi_b(x) + \varphi_a(x),$$

$$\varphi_b^{-1}(c) = \varphi_b^{-1}\big(-\varphi_b(x) + \varphi_a(x)\big),$$

$$\varphi_b^{-1}(c) = -x + \varphi_b^{-1}\varphi_a(x). \tag{2}$$

Ora $\varphi_b^{-1}(c)$, al variare di $c$, percorre tutto $G$, e dunque $\varphi_b^{-1}\varphi_a$ è un automorfismo privo di coincidenze del gruppo additivo di $G$, per un lemma ormai classico (10).

---

(7) Perchè l'altra classe è costituita da divisori dello zero.

(8) Questo elementare ma fondamentale risultato verrà spesso — nel corso del lavoro — utilizzato senza esplicito richiamo.

(9) Il che, per quanto sopra osservato, equivale a dire che non divide lo zero a sinistra.

(10) Cfr. Zappa [**18**]: se $b$ è un automorfismo del gruppo *finito* $G$, la $x \to -x + b(x)$ è una suriezione (quindi una biiezione) se e solo se $b$ è privo di coincidenze non banali.

Naturalmente, al variare degli elementi $a$, $b$ nell'insieme dei non divisori dello zero di $G$ l'elemento $\varphi_b^{-1}\varphi_a$ percorre tutto il gruppo $\Phi$. Dunque, per quanto sopra asserito, tutti gli elementi non banali di tale gruppo sono automorfismi senza coincidenze; in altri termini tutte le traiettorie di $\Phi$ sono principali. Il fatto che $G$ non possa essere a prodotti banali è conseguenza immediata della condizione II) nella Definizione $\boldsymbol{A}$.

*Viceversa*, sia $G$ uno stem fortemente monogeno a traiettorie tutte principali ed a prodotti non banali. Allora la (2) ha una ed una sola soluzione ([11]), purchè ovviamente

$$\varphi_a \neq \varphi_b\,, \qquad \varphi_a \neq \varphi_0 \neq \varphi_b \qquad (\varphi_0 \text{ endomorfismo nullo}).$$

Pertanto l'equazione $ax = bx + c$, almeno nel caso che $a$, $b$ non dividano lo zero a sinistra e non siano equivalenti a sinistra, ha una ed una sola soluzione. D'altra parte, se $b$ divide lo zero a sinistra, la $ax = bx + c$ diventa $ax = c$ (perchè $G$ è fortemente monogeno) e, quando $a \not\equiv_s 0$, ha una ed una sola soluzione perchè $\varphi_a$ è un automorfismo del gruppo additivo di $G$. Un'osservazione del tutto analoga può essere fatta per il caso in cui $a$ divida lo zero a sinistra.

Dalle cose fin ora dette risulta che $G$ soddisfa alla condizione I) della Definizione $\boldsymbol{A}$. D'altra parte $G$ soddisfa anche alla II), per l'ipotesi che sia non a prodotti banali e per il Corollario 1; con questo il Teorema 1 è dimostrato.

Sussiste inoltre il

Corollario 2. *Uno stem planare $G$ è individuato dai seguenti elementi*:

I) *il suo gruppo additivo $G^+$,*

II) *un gruppo $\Phi$ di automorfismi di $G^+$, tutti senza coincidenze* ([12]);

III) *l'insieme delle sue unità sinistre* ([13]).

La dimostrazione segue facilmente dal Teorema 1 e dal Capitolo 3 di [**10**] (Corollari 9, 11).

Per comodità di linguaggio, nel seguito (e specialmente nella seconda parte) parleremo spesso di stems planari anche quando, non intervenendo effettivamente l'elemento III) di cui sopra, potremmo semplicemente parlare della coppia $< G, \Phi >$ in termini di sola teoria dei gruppi.

---

([11]) Per il lemma di Zappa sopra citato.

([12]) Salvo l'automorfismo identico e la coincidenza banale, naturalmente.

([13]) L'insieme delle unità sinistre è soggetto unicamente alle seguenti limitazioni: non deve essere vuoto e non deve contenere più di un elemento in ciascuna traiettoria di $\Phi$.

## § 2. - Stems interi.

2. – Questo paragrafo è dedicato essenzialmente alla discussione di una congettura di CLAY (14) secondo cui la caratteristica di ogni stem *intero* (privo cioè di divisori dello zero) sarebbe, salvo che in casi degeneri, un numero primo. Per questa ragione parleremo quasi sempre di stems interi anche se la maggior parte di quello che diremo è immediatamente generalizzabile agli stems planari.

Cominciamo con lo stabilire più esplicitamente la relazione tra planarità ed integrità di stems. Si osserva intanto subito che *uno stem finito intero $G$ è planare se e solo se non è a prodotti banali.* Se infatti $G$ è privo di divisori dello zero, esso è fortemente monogeno e tutti i suoi elementi stanno in traiettorie principali di $\Phi$ (15). Il resto è conseguenza immediata del Teorema 1.

Ricordando ancora il Corollario 2 ed il Teorema 13 di [10], si ha immediatamente:

Osservazione 1. *Gli stems interi sono:*

I) *gli stems i cui elementi non nulli sono tutti unità sinistre* (16),

II) *gli stems planari in cui ogni traiettoria principale di $\Phi$ contiene una unità sinistra* (17).

Resta così chiarito il significato di molti risultati di [2] e [3], ove si parla di stems planari interi, e precisata la relazione tra quasicorpi associativi e stems planari (18).

Grazie al Corollario 2 ed al noto teorema di THOMPSON (19), secondo cui un gruppo avente un automorfismo senza coincidenze e di ordine primo è un gruppo nilpotente, possiamo mostrare che *lo studio degli stems interi* (20) *può in un certo*

---

(14) Cfr. [6]. Infatti, se solo volessimo fornire un controesempio a tale congettura, ci basterebbe usare gli stems che incontreremo al successivo Corollario 5. Noi vogliamo tuttavia approfondire la questione ed invitare alle ulteriori ricerche che sorgono spontanee dalle nostre osservazioni.

(15) Si ricordino le considerazioni di [11] (n. 3) e [12].

(16) Cioè gli stems interi a prodotti banali.

(17) In cui cioè l'insieme delle unità sinistre è massimale rispetto alle condizioni precisate nella precedente annotazione (13).

(18) Cfr.: [9], n. 3.4; [12], osservazione 13.

(19) Cfr. J. THOMPSON, *Finite groups with fixed-point-free automorphisms of prime order*; Proc. Math. Acad. Sci. U.S.A. **45** (1959), 578-581.

(20) E quello degli stems planari.

*senso essere ricondotto allo studio degli stems interi a gruppo additivo primario, o anche allo studio degli automorfismi senza coincidenze di gruppi primari.*

Se infatti $G$ è uno stem intero, esso risulta (dal punto di vista additivo) somma diretta di stems interi a gruppo additivo primario.

Inoltre:

Osservazione 1. Siano $G$, $G'$ due gruppi, e siano $A$, $A'$ gruppi di automorfismi di $G$ e $G'$, rispettivamente. Supponiamo inoltre che $A$, $A'$ siano entrambi formati da automorfismi senza coincidenze. Sia $b$ un isomorfismo da $A$ ad $A'$. Per ogni $a \in A$ si consideri la corrispondenza che associa al generico elemento $< g, g' >$ del prodotto diretto gruppale $G \times G'$, l'elemento $< a(g), b(a)(g') >$; tale corrispondenza è un automorfismo senza coincidenze di $G \times G'$.

La dimostrazione è un semplice esercizio, e può essere omessa.

3. – Per sfruttare la precedente Osservazione notiamo intanto che, se $C$ è un gruppo ciclico, i suoi automorfismi sono tutte e sole le trasformazioni che mandano il generico $c$ di $C$ nell'elemento $kc$, ove $k$ sia primo con l'ordine $n$ di $C$ (e può essere scelto positivo e minore di $n$).

Diamo inoltre il

Teorema 2. *Sia $C$ un gruppo ciclico di ordine $p^b$ ($p$ primo); sia $\varphi$ un automorfismo di $C$, e supponiamo che $\varphi$ e tutte le sue potenze non identiche siano prive di coincidenze. Sia $k$ un numero tale che $\varphi$ mandi il generico elemento $c$ di $C$ nell'elemento $kc$, e sia $a$ l'ordine di $\varphi$. Allora $a$ è il minimo degli interi positivi $x$ tali che $k^x - 1$ sia un multiplo di $p$, ed anzi $k^a - 1$ è un multiplo di $p^b$* ([21]).

Ricordiamo anzitutto un risultato di Ahmad [1] secondo cui il numero delle coincidenze della $c \to kc$ è il massimo comun divisore di $k-1$ e dell'ordine di $C$. Si ha dunque che, se $\varphi: c \to kc$ è privo di coincidenze insieme con le sue potenze

$$\varphi^i: c \to k^i c \qquad (i = 1, 2, \ldots, a-1),$$

allora i numeri $k-1$, $k^2-1$, ..., $k^{a-1}-1$ sono primi con $p$. Invece, dal momento che $\varphi^a$ è l'identità, accade che $k^a - 1$ è un multiplo di $p^b$, ed il Teorema è dimostrato.

---

([21]) Qualche calcolo eseguito con una calcolatrice elettronica da tavolo ci induce a pensare che le circostanze studiate nel Teorema 2 si verifichino abbastanza di rado.

Nel seguito servirà sopratutto il

Teorema 3. *Consideriamo un numero primo $p$ ed una sua potenza $p^b$. Supponiamo che esista un intero positivo $k$ tale che il minimo dei numeri della forma $k^x - 1$ che sia un multiplo di $p$ sia addirittura un multiplo di $p^b$. Indichiamo con $k^a - 1$ tale minimo. Allora esiste uno stem intero $G$, avente gruppo additivo ciclico di ordine $p^b$, il cui relativo $\Phi$ è ciclico di ordine $a$.*

In queste condizioni infatti $k$ è primo con $p$, e dunque la corrispondenza che manda ogni elemento del gruppo $C$ (ciclico di ordine $p^b$) nel suo $k$-uplo è un automorfismo di $C$. Per il già citato risultato di AHMAD tale corrispondenza (insieme con le sue potenze degli ordini 2, 3, ..., $a-1$) è priva di coincidenze. Invece la sua potenza di ordine $a$ coincide ovviamente con l'identità. Pertanto il gruppo ciclico costituito da tali potenze possiede traiettorie, tutte principali, in numero di $(p^b-1)/a$. Seguendo [12] possiamo perciò costruire $a^{(p^b-1)/a}$ stems interi aventi $C$ come gruppo additivo, ed il Teorema è dimostrato.

Abbiamo ora la possibilità di discutere in modo relativamente completo la congettura di CLAY [6], secondo cui uno stem intero a prodotti non banali avrebbe come caratteristica un numero primo. Osserviamo che ci sono automorfismi di ordine 5 privi di coincidenze nei seguenti gruppi:

I) nel gruppo ciclico di ordine 31 (si tratta della corrispondenza che manda ogni elemento nel suo doppio),

II) nel gruppo ciclico di ordine $11^2$ (si tratta della corrispondenza che manda ogni elemento nel suo triplo) ([22]),

III) in gruppi non abeliani di ordine $11^4$ ([23]).

Tenendo conto di ciò e dell'Osservazione 2, *possiamo costruire stems interi con gruppo additivo primario o no, abeliano o no, che contraddicono alla congettura di Clay*.

Lasciamo al Lettore i dettagli tecnici, che ormai si riducono ad applicazioni della costruzione di [12].

4. – La congettura di CLAY è tuttavia valida se ci si riferisce a stems interi che soddisfano qualche ulteriore condizione.

Definizione ***B***. *Uno stem $G$ sarà detto $\boldsymbol{Z}$-distributivo se per tutti gli $n \in \boldsymbol{Z}$ ([24]) e qualunque siano $z$, $x \in G$ è*

$$(nz)x = n(zx) .$$

([22]) È stata individuata per mezzo del Teorema 3. Cfr. la precedente annotazione ([21]).

([23]) Cfr. [8], pag. 90.

([24]) Cioè per tutti gli $n$ interi relativi.

Osserviamo subito che *se $G$ è $\boldsymbol{Z}$-distributivo* si ha $0G = 0$ inoltre i sottostems della forma $zG$ hanno gruppo additivo abeliano, e *la caratteristica di ciascun elemento di $zG$ divide quella di $z$.*

Infatti, poichè $0x = (n0)x = n(0x)$ [25], si ha che per ogni $n$ di $z$ è $(n-1).\ 0x = 0$, e dunque $0x = 0$ per ogni $x$ di $G$.

D'altra parte, osservato che la corrispondenza che manda ogni $x$ in $(nz)x = n(zx)$ conserva la somma, si ha subito che $nz(x+y) = nzx + nzy = n(zx + zy)$; in particolare, ponendo $n = 2$ si ha che $zx + zx + zy + zy = zx + zy + zx + zy$, da cui $zx + zy = zy + zx$, e dunque $zG$ è abeliano rispetto alla somma.

Se poi è $cz = 0 (c \in \boldsymbol{Z})$ è anche $c(zx) = (cz)x = 0x = 0$ per quanto visto precedentemente, e la caratteristica di $zx$ divide quella di $z$.

È facile completare le precedenti osservazioni con il

Teorema 4. *Se $G$ è $\boldsymbol{Z}$-distributivo ed intero il suo gruppo additivo è abeliano elementare; le traiettorie del relativo $\Phi$ sono unione di gruppi additivi disgiunti.*

Intanto allora, per ogni $z \neq 0$, si ha $G = zG$, e la caratteristica di ogni elemento di $G$ divide quella di $z$. Pertanto tutti gli elementi di $G$ hanno la stessa caratteristica, che deve essere un numero primo [26].

Sia inoltre $e$ una unità sinistra di $G$ (certamente esistente per l'Osservazione 1) e sia $x$ un elemento della traiettoria $T$. Anche gli elementi del tipo $(ke)x$, $(k \in \boldsymbol{N})$, cioè gli elementi $k(ex) = kx$ appartengono a $T$. Pertanto $T$ contiene tutto il gruppo ciclico additivo generato da $x$. Ricordando la prima parte del Teorema, il resto è ovvio [27].

Naturalmente gli stems $\boldsymbol{Z}$-distributivi sono già piuttosto vicini agli anelli. Per esempio si ha il

Teorema 5. *Se $G$ è $\boldsymbol{Z}$-distributivo ed il suo ordine è multiplo di $p$ (numero primo), allora $G$ possiede un sottoanello di ordine $p$* [28].

Osserviamo intanto che un qualunque sottostem di $G$ è a sua volta $\boldsymbol{Z}$-distributivo. Se $G$ non avesse sottostems di ordine $p$, per il teorema 1 di [**11**],

---

[25] Si noti che continuiamo ad indicare con 0 l'elemento neutro del gruppo additivo di $G$, non intervenendo mai nelle nostre considerazioni il numero zero.

[26] Si confronti con la classica dimostrazione relativa ai domini di integrità.

[27] Si osservi anche che $T$, contenendo una unità sinistra, contiene il sottogruppo additivo generato da tale unità: esso risulta un sottocampo di $G$, essendo un anello di ordine primo che non è uno 0-anello, come si vede immediatamente con facili calcoli.

[28] Cfr. [**10**], [**11**].

conterrebbe un sottostems $p$-singolare e $Z$-distributivo. Sottostems siffatti non esistono, perchè uno di questi, contenendo una unità sinistra (cfr. [11], corollario 10) conterrebbe un sottocampo di ordine $p$, contro l'ipotesi di $p$-singolarità. Pertanto il nostro $G$ contiene un sottostem di ordine $p$: questo, essendo $Z$-distributivo, non può non essere un anello, come si vede dalla annotazione ([27]).

## § 3. - Blocchi.

5. – Generalizziamo ora il concetto di laterale con la seguente

Definizione $C$. *Dato uno stem $G$, diciamo blocco individuato dalla coppia $< a, b >$ $(a \neq 0)$ l'insieme degli elementi $x$ di $G$ che si possono scrivere nella forma $x = ya + b$ $(y \in G)$. Lo indicheremo con la scrittura $Ga + b$.*

È subito visto che se $G$ è planare e $k-1$ è l'ordine del relativo $\Phi$, $Ga + b$ *contiene $b$ ed altri $k-1$ elementi distinti.* La prima osservazione discende dal fatto che $b = 0a + b$; per la seconda osserviamo che al variare di $y$ sui non divisori dello zero a sinistra gli elementi $ya$ sono tutti e soli gli elementi equivalenti ad $a$ rispetto a $\Phi$, il numero appunto di $k-1$, perchè tutte le traiettorie di $\Phi$ sono principali (Teorema 1).

Apriamo ora una parentesi per comprendere il significato geometrico delle condizioni suesposte: diamo pertanto tre esempi che, senza essere particolarmente significativi in questo contesto, possono dar luogo per analogia ad ulteriori ricerche.

Consideriamo un comune piano cartesiano $\pi$, di origine $O$. I punti di $\pi$ possono notoriamente essere visti come elementi di uno spazio vettoriale, ed in particolare di un gruppo additivo $G$. Dato un gruppo $\Phi$ di automorfismi privi di coincidenze di $G$ possiamo costruire stems planari colla tecnica di [12], e quindi costruire blocchi secondo la definizione $C$.

Esempio I. Se $\Phi$ è il gruppo delle omotetie aventi centro in $O$, i blocchi dello stem così ottenuto sono le ordinarie rette di $\pi$.

Esempio II. Se $\Phi$ è il gruppo delle omotetie dirette aventi centro in $O$, i blocchi che si ottengono sono le semirette di $\pi$.

Esempio III. Se $\Phi$ è il gruppo delle rotazioni attorno ad $O$, i blocchi sono le varietà impure costituite dalle circonferenze di $\pi$ insieme con i relativi centri.

6. – Esaminiamo ora i vari modi di scrivere un blocco. Cominciamo con il

Lemma 2. *Se i blocchi* $Ga + b$ *e* $Ga' + b'$ *dello stem planare coincidono, allora si verifica una delle circostanze sottoindicate:* $b = b'$ *ed* $a$, $a'$ *sono equivalenti rispetto a* $\Phi$; *oppure la differenza di due qualunque elementi non nulli di* $Ga$ *è un elemento di* $G(-a)$.

È chiaro intanto che, se $b = b'$, $a$ ed $a'$ devono essere equivalenti rispetto a $\Phi$.

Supponiamo che invece sia $b \neq b'$.

Per l'osservazione che segue immediatamente la Definizione **C** esiste allora un $g \in G$ tale che $b = ga' + b'$, e allora $b - b' = ga'$. Analogamente si vede che esiste un $g' \in G$ tale che $b' - b = g'a$. Se ne deduce che $b - b'$ appartiene contemporaneamente a $Ga'$ ed a $G(-a)$, e dunque $Ga' = G(-a)$ ed $a'$, $-a$ sono equivalenti rispetto a $\Phi$.

Possiamo scrivere $Ga + b = G(-a) + b'$ ed aggiungere che esiste un $\varphi \in \Phi$ tale che $b' = \varphi(a) + b$, e dunque $Ga + b = G(-a) + \varphi(a) + b$. Pertanto si ha che $Ga = G(-a) + \varphi(a)$. Ora ricordando che $\varphi^{-1}$ permuta soltanto tra loro gli elementi degli insiemi $Ga$, $G(-a)$, e trasforma $\varphi(a)$ in $a$, operando sui due membri dell'ultima eguaglianza trovata con $\varphi^{-1}$, si ottiene che $Ga = G(-a) + a$.

Naturalmente le considerazioni ora svolte valgono per tutti gli $a \neq 0$ di $Ga$. Se ne deduce che la differenza di due qualunque elementi non nulli di $Ga$ è un elemento di $G(-a)$, il che conclude la dimostrazione.

Corollario 3. *Sia* $G$ *uno stem planare che non contenga quasicorpi; si suppenga che il relativo gruppo* $\Phi$ *abbia ordine pari. Allora i blocchi* $Ga + b$ *e* $Ga' + b'$ *coincidono se e solo se* $b = b'$ *ed* $a$, $a'$ *sono equivalenti rispetto a* $\Phi$.

Se $\Phi$ infatti ha ordine pari, esso possiede un elemento di ordine due che manda ogni elemento di $G$ nel suo opposto ([29]), quindi, per ogni $a \in G$, $a$ e $-a$ sono equivalenti rispetto a $\Phi$ e dunque $Ga = G(-a)$. Se pertanto la differenza di due elementi di $Ga$ è un elemento di $G(-a)$, allora $Ga = G(-a)$ è un gruppo additivo, e anzi un quasicorpo.

Ora dal Lemma 2 si ha che se $Ga + b = Ga' + b'$ senza che sia $b = b'$, allora si verifica proprio la detta circostanza. Tale caso è escluso dall'ipotesi che $G$ non contenga quasicorpi (neppure improprii), ed il Corollario è dimostrato.

## § 4. - Disegni.

7. – I BIB-disegni sono strutture combinatorie che generalizzano i piani grafici, e recentemente sono stati oggetto di rinnovato interesse anche in vista

([29]) Cfr. [16]; si noti inoltre che allora il gruppo additivo di $G$ deve essere abeliano.

delle applicazioni alla statistica, alla ricerca operativa ed alla teoria dei codici [30].

Ricordiamone anzitutto la definizione:

Un BIB-*disegno* (*Balanced Incomplete Block Design*) è un insieme di $v$ oggetti (che diremo punti od elementi, ma che spesso vengono detti varietà) e di $b$ suoi sottoinsiemi distinti [31] detti blocchi, tali che:

I) ogni blocco contenga esattamente $k$ oggetti;

II) ogni oggetto appartenga esattamente ad $r$ blocchi;

III) ogni coppia non ordinata di oggetti distinti sia contenuta esattamente in $\lambda$ blocchi.

Si dimostra facilmente che tra i parametri $v$, $b$, $k$, $r$, $\lambda$ di un BIB-disegno intercorrono le *relazioni fondamentali* [32]

$$bk = vr, \qquad r(k-1) = \lambda(v-1) .$$

Trovare condizioni necessarie e sufficienti perchè numeri dati siano parametri di un BIB-disegno è un problema ancora aperto.

Vogliamo qui indicare una tecnica per costruire BIB-disegni in cui $k = \lambda$. Introduciamo per brevità la

Definizione ***D***. *Chiamiamo stem fondamentale uno stem planare $G$ soddisfacente le seguenti condizioni*:

I) *il relativo gruppo $\Phi$ è di ordine pari,*

II) *$G$ non contiene quasicorpi* [33].

Fino al termine del lavoro indicheremo con $v$ *l'ordine* ( il numero cioè degli elementi) *dello stem fondamentale $G$*, e con $k-1$ *l'ordine del relativo $\Phi$.*

Lemma 3. *Se $G$ è uno stem fondamentale, i suoi blocchi sono in numero di $b = v(v-1)/(k-1)$. Ogni suo elemento appartiene a $r = k(v-1)/(k-1)$ blocchi.*

---

[30] Si vedano [4], [13], o i Volumi [9], [14], [17] che li presentano da diversi punti di vista.

[31] Spesso non si chiede che i blocchi siano distinti; si vedano [9] e [14] per precisazioni.

[32] Cfr., per esempio, [14], pag. 101.

[33] L'esistenza di stems siffatti risulta, per esempio, dalla dimostrazione del successivo Corollario 5.

La prima parte del Lemma è conseguenza del Corollario 3: le scritture del tipo $Ga + b$ $(a \neq 0)$ sono in numero di $v(v-1)$, ma esse dànno luogo, $k-1$ a $k-1$, allo stesso blocco.

Per la seconda parte basta contare i blocchi che passano per l'elemento $x \in G$. Se $x \in Ga + b$ esiste un $g \in G$ tale che $x - b = ga$. Fissato un qualunque $b \neq x$ in $G$ (e lo possiamo fissare in $v-1$ modi), esiste una ed una sola traiettoria di $\Phi$ passante per $x - b \neq 0$ e quindi, a meno dell'equivalenza rispetto a $\Phi$, uno ed un solo $a$ tale che $x \in Ga + b$. Si ottengono pertanto $v-1$ blocchi passanti per $x$.

Invece i blocchi per $x$ della forma $Ga + x$ sono tanti quanti le traiettorie non identiche di $\Phi$, e dunque sono $(v-1)/(k-1)$ per la planarità di $G$. Per il Corollario 3 i blocchi fin qui considerati sono due a due distinti, e la dimostrazione può essere conclusa con semplici passaggi aritmetici.

Per semplificare le dimostrazioni successive e comprendere meglio la portata di quello che stiamo facendo, introduciamo due osservazioni gruppali, del resto abbastanza semplici.

Lemma 4. *Siano $G$ un gruppo additivo e $\Phi$ un suo gruppo di automorfismi tutti senza coincidenze. Sia fissata una coppia ordinata $< \varphi, \bar{\varphi} >$ di elementi distinti di $\Phi$. Allora ogni elemento non nullo di $G$ può essere scritto, in uno ed un sol modo, nella forma*

$$z = \varphi(a) - \bar{\varphi}(a) \qquad (a \in G) . \tag{3}$$

È infatti chiaro che la (3) equivale alla

$$\varphi^{-1}(z) = a - \varphi^{-1}\bar{\varphi}(a) . \tag{4}$$

Ora, per le ipotesi fatte, $\varphi^{-1}\bar{\varphi} \in \Phi$ è un automorfismo di $G$ privo di coincidenze (non banali). Per il già ricordato lemma di Zappa [34] la (4) ammette, come equazione in $a$, una ed una sola soluzione, ed il Lemma è dimostrato.

Corollario 4. *Sia $G$ un gruppo additivo e sia $\Phi$ un suo gruppo di automorfismi tutti senza coincidenze. Supponiamo che ogni elemento non nullo $z$ di $G$, che possa essere scritto come differenza di due elementi di una data traiettoria $T$ di $\Phi$, ammetta esattamente $d$ scritture del tipo indicato. Si consideri la funzione* [35] *$g_z(< \varphi, \bar{\varphi} >)$ che manda ogni coppia $< \varphi, \bar{\varphi} >$ di elementi distinti di $\Phi$ nella tra-*

---

[34] Cfr. l'annotazione [10].

[35] Che si tratti di una funzione e non di una semplice corrispondenza è assicurato dal Lemma 4.

*iettoria rappresentata dall'elemento (unico) a soddisfacente la* (3). *Allora ogni traiettoria proviene da* $d(k-1)$ *coppie distinte.*

Sia infatti $z \in G$ differenza di due (dunque di $d$) elementi della traiettoria $T$. Vuol dire che esistono $d$ coppie $< a_i , b_i >$ $(i = 1, 2, ..., d)$ tali che $z = a_i - b_i$. Consideriamo i $k-1$ elementi $c_j$ $(j = 1, 2, ..., k-1)$ di $T$. Poichè gli elementi $a$, $b$ appartengono a $T$, per ogni $c$ esistono $d$ coppie $< \varphi_{i,j} , \bar{\varphi}_{i,j} >$ tali che sia

$$\varphi_{i,j}(c_j) = a_i , \qquad \bar{\varphi}_{i,j}(c_j) = b_i . \tag{5}$$

Ciascuna di tali coppie è formata ovviamente da elementi distinti. Possiamo dunque scrivere le $d(k-1)$ eguaglianze analoghe alla (3):

$$z = \varphi_{i,j}(c_j) - \bar{\varphi}_{i,j}(c_j) . \tag{6}$$

Ora, le coppie $< \varphi_{i,j} , \bar{\varphi}_{i,j} >$ così individuate sono distinte perchè se $< \varphi_{i,j} , \bar{\varphi}_{i,j} > = < \varphi_{i',j'} , \bar{\varphi}_{i',j'} >$ allora $j = j'$, per la (6) ed il Lemma 4. Di qui e dalle (5) (sempre per la planarità di $G$) $i = i'$, donde l'asserto. È chiaro d'altronde che, se $g_z(< \varphi, \bar{\varphi} >) \in T$, la coppia $< \varphi, \bar{\varphi} >$ è una delle coppie sopra considerate, e con questo il Corollario 4 è dimostrato.

La situazione prospettata dal Corollario 4 (e vale la pena di osservarlo esplicitamente) è analoga a quella in cui si mette BRUCK [36] per costruire BIB-disegni (in cui $v = b$) [37], secondo la seguente definizione:

Un insieme $D$ di elementi di un gruppo $G$ è un *insieme differenza* (*difference set*) se ogni elemento non nullo di $G$ può essere scritto esattamente in $\lambda$ modi come differenza di elementi di $D$.

Eccoci all'ultimo lemma:

Lemma 5. *Sia $G$ uno stem fondamentale. Allora due suoi elementi distinti appartengono esattamente a $k$ blocchi.*

Siano $x$, $y$ due elementi di $G$, e sia $x \neq y$. Tra i blocchi che contengono tanto $x$ che $y$ ci possono essere:

i) blocchi della forma $Ga + x$ (per un opportuno $a \in G$),

ii) blocchi della forma $Ga + y$,

iii) blocchi della forma $Ga + b$ (con $x \neq b \neq y$).

---

[36] Cfr. [5] o [14], pp. 122-166. Vedasi anche [2] e [3].

[37] Anche la nostra tecnica, sarà già stato notato, è analoga a quella di BRUCK; ci metteremo comunque in una situazione più generale di quella del presente Corollario.

Cominciamo dai blocchi della forma i). Se il blocco $Ga + x$ contiene $y$, ciò significa che esiste un $\varphi \in \Phi$ tale che $y = \varphi(a) + x$, dunque in questo caso $y - x \in Ga$ è equivalente ad $a$ [38]. È chiaro che, a meno dell'equivalenza rispetto a $\Phi$, esiste uno ed un solo $a_1$ tale che $y - x \in Ga_1$ o, che è lo stesso, tale che $Ga_1 + x$ contenga $y$. Esiste dunque uno ed un solo blocco della forma i) che contiene tanto $x$ che $y$.

Scambiando tra loro $x$ ed $y$ nel ragionamento precedente si trova che esiste uno ed un solo blocco $Ga_2 + y$, della forma cioè ii), cui appartengano tanto $x$ che $y$. Ricordando il Corollario 3 si ha subito che i due blocchi sopra individuati sono effettivamente distinti.

Veniamo ora ai *blocchi della forma* iii). Sia $Ga + b$ $(x \neq b \neq y)$ uno di essi. Tale blocco contiene $x$, $y$ se e solo se esistono $\varphi$, $\bar{\varphi} \in \Phi$ tali che

$$x = \varphi(a) + b, \qquad y = \bar{\varphi}(a) + b . \tag{7}$$

Dalle (7) si deduce che

$$x - y = \varphi(a) - \bar{\varphi}(a) . \tag{8}$$

Osserviamo subito che per ogni coppia $<\varphi, \bar{\varphi}>$ $(\varphi, \bar{\varphi} \in \Phi;\ \varphi \neq \bar{\varphi})$ esiste uno ed un solo $a$ di $G$ che soddisfa la (8) [39], e dunque uno ed un solo $b$ che soddisfa la prima delle (7). Verificato che tale $b$ soddisfa anche la seconda delle (7), sapremo che il blocco $Ga + b$ è effettivamente uno dei blocchi cercati. Ricordando che $G$ è commutativo [40] e che ci siamo messi nel caso in cui vale la (8), si ha infatti successivamente

$$\bar{\varphi}(a) + b = \bar{\varphi}(a) + x - \varphi(a) =$$

$$= (\bar{\varphi}(a) - \varphi(a)) + x = (y - x) + x = y .$$

Pertanto possiamo dire che ad ognuna delle $(k-1)(k-2)$ coppie $<\varphi, \bar{\varphi}>$ $(\varphi \neq \bar{\varphi})$ corrisponde una ed una sola coppia $<a, b>$ che soddisfa alle (7).

Tali coppie, per il Corollario 3, dànno luogo, esattamente $k-1$ a $k-1$, allo stesso blocco, e pertanto i blocchi di tipo iii) contenenti $x$, $y$ sono in numero

---

[38] Non potendo essere nullo, visto che per ipotesi $x$ ed $y$ sono distinti.

[39] Cfr. Lemma 4.

[40] Contenendo $\Phi$ un automorfismo privo di coincidenze di ordine 2: cfr. [16].

di $k-2$. Ancora per il Corollario 3 questi blocchi risultano distinti dai due blocchi di tipo i) ed ii) che abbiamo in precedenza individuato; con questo il Lemma è dimostrato.

8. – Molti dei risultati precedenti si raccolgono nel conclusivo

Teorema 6. *Sia $G$ uno stem fondamentale. I suoi elementi, insieme con i suoi blocchi, formano un* BIB-*disegno in cui il numero dei blocchi che contiene una data coppia di elementi distinti è uguale al numero di punti di ciascun blocco* (41).

Ciò è conseguenza immediata della definizione di BIB-disegno, dei Lemmi 3, 5 e del fatto che ogni blocco contiene $k$ elementi, già osservato subito dopo la Definizione ***C***.

Poichè il presente lavoro, ripetiamo, ha soprattutto lo scopo di collegare diverse teorie e di indicare ulteriori possibilità di ricerca, riteniamo utile fare le seguenti osservazioni.

Osservazione 3. La relativa abbondanza di condizioni che abbiamo introdotto nella Definizione di stem fondamentale è giustificata dal fatto che solo tre dei cinque parametri di un BIB-disegno sono indipendenti (42), e che quindi, se volevamo che i blocchi formassero un BIB-disegno, dovevamo fare in modo che valessero le tesi dei Lemmi 3, 5. Si noti anche che le relazioni fondamentali cui sopra alludevamo risultano identicamente soddisfatte per ogni sistema di parametri per cui valgano le eguaglianze della annotazione (41). Si potrebbe vedere se costruzioni analoghe possono dar luogo a BIB-disegni (cfr. [4]).

Osservazione 4. Non ci risulta che siano comunemente noti molti BIB-disegni in cui $k = \lambda$ (come nei nostri) all'infuori dei piani di MOBIUS (43). In essi, tra l'altro, esiste un intero $n$ tale che $v = n^2 + 1$, $k = n + 1$ (44). Per-

---

(41) Colle notazioni abituali (richiamate al principio del paragrafo) i parametri (diversi da $v$ e da $k$) del nostro BIB-disegno risultano essere

$$b = v(v-1)/(k-1), \qquad r = k(v-1)/(k-1), \qquad \lambda = k.$$

Si noti che $(v-1)/(k-1)$ non è altro che il numero delle traiettorie principali di $\Phi$.

(42) Devono infatti valere le relazioni fondamentali ricordate insieme alla Definizione di BIB-disegno.

(43) Cfr. per la definizione, ad esempio, [9] (Cap. 6).

(44) Cfr. [9], pag. 262.

tanto i nostri BIB-disegni possono essere piani di MÖBIUS solo se l'ordine di $\Phi$ coincide con il numero delle sue traiettorie, come si vede immediatamente dalla annotazione (41).

Osservazione 5. Il Teorema 6 può essere ampiamente sfruttato per generalizzare la teoria di BRUCK (45); rende inoltre importante la determinazione degli stems fondamentali. Ci limitiamo, a titolo indicativo, a due osservazioni praticamente immediate, ma che invitano ad ulteriori sviluppi.

Corollario 5. *Se $v$ è un numero primo con* 6, *esiste un* BIB-*disegno di parametri* $v$, $b = v(v-1)/2$, $r = 3(v-1)/2$, $\lambda = k = 3$ (46).

Sia infatti $G$ un gruppo abeliano additivo di ordine $v$ (primo con 6), e $\Phi$ contenga soltanto l'identità e l'automorfismo che manda ogni elemento nel suo opposto. La costruzione di [12] dà luogo a stems fondamentali perchè un quasicorpo contenuto in uno degli stems così costruiti avrebbe ordine 3, il che è escluso dal teorema di LAGRANGE. Di qui, usando il nostro Teorema 6 si ottengono proprio BIB-disegni con i parametri indicati nell'enunciato. Come è stato osservato in [3], se $G$ è ciclico di ordine 5 si ottiene un piano di MÖBIUS.

Concludiamo il lavoro con un'altra osservazione di natura vagamente *geometrica.*

Ogni blocco $Ga + b$ individua in modo unico (Corollario 3) il suo elemento $b$ che, se vogliamo, possiamo chiamare elemento improprio del blocco (47). Se chiamiamo paralleli due blocchi aventi lo stesso elemento improprio si ha che ogni punto $x$ di $G$ appartiene ad uno ed un solo blocco parallelo ad un blocco dato $Ga + b$ *salvo che* il punto $x$ sia il punto improprio $b$ del blocco dato (48). In questo caso i blocchi per $x = b$ paralleli a $Ga + b$ sono in numero di $(v-1)/(k-1)$. È chiaro che di qui, specie tenendo presente il trattato [9], si potrebbe sviluppare facilmente una intera teoria, ma non siamo sicuri che sia molto importante farlo effettivamente.

---

(45) Cfr. [5].

(46) È un caso particolare del teorema di HANANI (cfr.: [14], pp. 236, 243; [9], p. 110) secondo cui le condizioni fondamentali per l'esistenza di un BIB-disegno di dati parametri sono anche sufficienti quando $k = 3$.

(47) Ogni elemento di $G$ risulta punto improprio di qualche blocco.

(48) Si veda la prima parte della dimostrazione del Lemma 5.

## References.


[1] S. AHMAD, *Cycle structure of automorphisms of finite cyclic groups*, J. Comb. Theory **6** (1969), 370-374.

[2] M. ANSHEL and J. CLAY, *Planar algebraic systems: some geometric interpretazions*, J. Algebra, **10** (1968); 166-173.

[3] M. ANSHEL and J. CLAY, *Planarity in algebric system*, Bull. Amer. Math. Soc. **74** (1968), 746-748.

[4] A. BARLOTTI, *Procedimenti geometrici per la costruzione di* PBIB-*disegni*, Period. Mat. (Bologna) (4) **46** (1968), 59-68.

[5] R. H. BRUCK, *Difference sets in a finite group*, Trans. Amer. Math. Soc. **78** (1955), 464-481.

[6] J. CLAY, *A note on integral domains that are not right distributive*, Elem. Math. (Basel) **24** (1969), 40-41.

[7] J. CLAY, *Research in near-rings using a digital computer*, Mathematica (Budapest) **19** (1968), 221-227.

[8] G. CORSI, *Automorfismi senza coincidenze dei gruppi non abeliani di ordine* $p^3$ *o* $p^4$. Matematiche (Catania) **15** (1960), 79-91.

[9] P. DEMBOWSKI, *Finite Geometries*, Springer-Verlag, Berlin 1968.

[10] G. FERRERO, *Sui problemi «tipo Sylow» relativi ai quasi-anelli finiti*, Atti Accad. Sci. Torino, Cl. Sci. Fis. Mat. Natur. **100** (1965-66), 645-657.

[11] G. FERRERO, *Struttura degli «stems» p-singolari*, Riv. Mat. Univ. Parma (2) **7** (1966), 243-254.

[12] G. FERRERO, *Classificazione e costruzione degli stems p-singolari*, Istituto Lombardo, Accad. Sci. Lett. Rend. A **102** (1968), 597-613.

[13] M. HALL (jr.), *Block designs*, Applied Combinatorial Mathematics, J. Wiley & Sons, 1964.

[14] M. HALL (jr.), *Combinatorial Theory*, Blaisdell P. C., 1967.

[15] J. MALONE, *Near-rings with trivial multiplications*, Amer. Math. Monthly **74** (1967), 1111-1112.

[16] B. NEUMANN, *On the commutativity of addition*, J. London Math. Soc. **15** (1940), 203-208.

[17] B. SEGRE, *Istituzioni di Geometria Superiore*, Vol. III, Istituto Matematico «G. Castelnuovo», Roma 1965.

[18] G. ZAPPA, *Sugli automorfismi uniformi nei gruppi di Hirsch*, Ricerche Mat. (Napoli) **7** (1958), 3-13.

## Summary.

*In this paper,*

1. *relationships are described, between finite planar near-rings, near integral domains and groups with a group of fixed-point-free automorphisms;*

2. *the conjecture is disproved, that the caracteristic of a near integral domain needs be a prime integer;*

3. *planar near-ring are used to construct balanced incomplete block design with parameters $v$, $b$, $k$, $r$, $\lambda$ for the case $k = \lambda$;*

4. *possible further developments are suggested, of a geometrical as well of an algebraic nature.*


* * *