Riv. Mat. Univ. Parma (4) **15** (1989), 111-117

DONATO SAELI (*)

Applicazioni complete e rapporto incrementale in doppi cappi (**)

1 - Introduzione

I risultati esposti in questa nota riguardano le funzioni biiettive di una struttura algebrica con due operazioni binarie.

Sia $\boldsymbol{K}$ un campo, se f è una biiezione da $\boldsymbol{K}$ in sé, indichiamo con $C(f)$ l'insieme degli elementi $a \in \boldsymbol{K}$ tali che il *rapporto incrementale* in a

$$(\cdot) \qquad \Delta f_a(x) = (f(x) - f(a))(x - a)^{-1}$$

assuma tutti i valori di $\boldsymbol{K}^* = \boldsymbol{K} \setminus \{0\}$, al variare di x su $\boldsymbol{K} \setminus \{a\}$; cioè poniamo

$$C(f) = \{a \in \boldsymbol{K} \mid \Delta f_a \text{ sia una biiezione fra } \boldsymbol{K} \setminus \{a\} \text{ e } \boldsymbol{K}^*\}.$$

Biiezioni f da $\boldsymbol{K}$ in sé tali che $C(f) \neq \emptyset$ esistono per tutti i campi, fatta eccezione per i campi di Galois di caratteristica dispari [1].

Osserviamo che per introdurre il rapporto incrementale $(\cdot)$ in una struttura algebrica $\boldsymbol{K}(+, \cdot)$ con due operazioni binarie è sufficiente richiedere che $\boldsymbol{K}(+, \cdot)$ sia un doppio cappio, ossia che $\boldsymbol{K}(+)$ e $\boldsymbol{K}^*(\cdot)$ siano entrambi cappi.

Si può allora considerare $C(f)$ per ogni biiezione $f \in S(\boldsymbol{K})$, ove $S(\boldsymbol{K})$ indica l'insieme delle biiezioni di un doppio cappio $\boldsymbol{K}(+, \cdot)$ in sé.

In generale, un doppio cappio $\boldsymbol{K}(+, \cdot)$ ammette biiezioni f di $\boldsymbol{K}$ tali che $C(f) \neq \emptyset$; diremo pertanto *eccezionali* i doppi cappi per i quali $C(f) = \emptyset$ per ogni

---

(*) Indirizzo: Istituto di Matematica, Università, Via N. Sauro 85, I-85100, Potenza.

(**) Ricevuto: 13-III-1989.

$f \in S(\boldsymbol{K})$. In questi termini, al risultato richiamato prima si può dare la seguente formulazione

Un campo è un doppio cappio eccezionale se e solo se è un campo di Galois di caratteristica dispari.

In 2 porremo in evidenza un legame fra doppi cappi eccezionali $\boldsymbol{K}(+,\cdot)$ soddisfacenti la proprietà dell'inverso a destra e la non esistenza di applicazioni complete in $\boldsymbol{K}^*(\cdot)$ (cfr. Teorema 1), che ci permetterà di mostrare come i doppi cappi eccezionali non si riducano ai soli campi di Galois di caratteristica dispari. Ciò risulta innanzi tutto dal Teorema 2.

In 3 esamineremo i doppi cappi $\boldsymbol{K}(+,\cdot)$ soddisfacenti la prima condizione del Teorema 1 e tali che $\boldsymbol{K}^*(\cdot)$ sia un gruppo. Per doppi cappi con tali proprietà, discende dal Teorema 1, che $\boldsymbol{K}(+,\cdot)$ è eccezionale se e solo se $\boldsymbol{K}^*(\cdot)$ è privo di applicazioni complete. È stato dimostrato che i gruppi infiniti ammettono delle applicazioni complete, mentre un gruppo finito risolubile ammette delle applicazioni complete se e solo se è a sottogruppi di Sylow non ciclici. M. Hall ha formulato la congettura che ogni gruppo non risolubile ammetta delle applicazioni complete. Tale congettura è già stata provata per alcuni gruppi, quali il gruppo simmetrico S_n e quello alterno A_n ($n \geq 5$); qui la proviamo per i gruppi SL(2, 5), SL(2, 7), SL(2, 11) e SL(2, n), $n = 2^h$. L'esistenza di applicazioni complete in SL(2, 5) riveste particolare importanza perché essenziale nella dimostrazione del Teorema 3.

2 - Applicazioni complete e doppi cappi eccezionali

Def. 1. Un cappio $\boldsymbol{K}(+)$ ha la *proprietà dell'inverso a destra*, se per ogni $a \in \boldsymbol{K}$, vi è $c \in \boldsymbol{K}$ tale che $(x+a)+c = x$, per ogni $x \in \boldsymbol{K}$ ([2], p. 111).

Def. 2. Una biiezione ϑ di un quasigruppo $Q(\cdot)$ si dice *applicazione completa*, se l'applicazione $\eta : x \rightarrowtail x \cdot \vartheta(x)$ risulta essere ancora una biiezione di Q ([3], § 1.4).

Teorema 1. *Se $\boldsymbol{K}(+,\cdot)$ è un doppio cappio soddisfacente le condizioni:*

(1) *$\boldsymbol{K}(+)$ è un cappio con la proprietà dell'inverso a destra*
(2) *esiste una biiezione f di $\boldsymbol{K}$ tale che $C(f) \neq \emptyset$*

allora valgono le seguenti condizioni equivalenti:

(3) *esiste una biiezione* g *di* K *tale che* $0 \in C(g)$
(4) $K^*(\cdot)$ *ammette delle applicazioni complete.*

Dim. Cominciamo col provare la (3). Sia $a \in C(f)$, posto $g(x) = f(x+a) - f(a)$ e $y = x - a$, è ovvio che $g(0) = 0$ e dalla (1) segue immediatamente che $g \in S(K)$; inoltre

$$g(y)\,y^{-1} = g(x-a)(x-a)^{-1} = (f((x-a)+a) - f(a))(x-a)^{-1}$$

$$= (f(x) - f(a))(x-a)^{-1} = \Delta f_a(x)$$

assume tutti i valori non nulli di K al variare di x su $K \setminus \{a\}$, cioè al variare di y su K^*. Riguardo all'equivalenza fra le (3) e (4), posto $\delta : x \rightarrowtail x^{-1}$, basta osservare che $g(x)\,x^{-1}$ è una biiezione di K^* se e solo se δg^{-1} è una applicazione completa di K^*.

Teorema 2. *Se* $K(+, \cdot)$ *è un doppio cappio soddisfacente le condizioni*: (1), (5) $|K| = 4k+3$ *e* (6) $K^*(\cdot)$ *contiene un sottocappio di ordine* $2k+1$, *allora* $C(f) = \emptyset$ *per ogni biiezione* f *di* K.

Dim. Per il Teorema 1.4.1 di [3], se un quasigruppo di ordine m ammette delle applicazioni complete, allora la sua tavola di Cayley è dotata di trasversali, in altri termini dalla tavola è possibile estrarre m celle, una per ciascuna riga e colonna di modo che mai due celle contengono uno stesso elemento. L'asserto segue pertanto dal Teorema 1, tenendo conto di un risultato dovuto a H. B. Mann [6] (cfr. [3], p. 32) secondo cui un quasigruppo di ordine $m = 4n+2$ contenente un sottoquasigruppo di ordine $2n+1$ è privo di trasversali.

3 - Applicazioni complete di SL(2, q)

In questo numero mostreremo che SL(2, q) ammette delle applicazioni complete per q pari ($q = 2^h$) e anche per $q = 5$, 7 e 11.

Proposizione 1. SL(2, q), $q = 2^h$, $h \geq 2$, *ammette delle applicazioni complete.*

Dim. Premettiamo alcune proprietà di SL(2, q), $q=2^h$, $h\geq 2$; per le definizioni e proprietà fondamentali di tale gruppo si rimanda a [5] (§ 8).

(a) *I 2-sottogruppi di Sylow di* SL(2, q) *sono abeliani elementari.*

Infatti, $\Sigma=\{\begin{pmatrix}1 & s\\ 0 & 1\end{pmatrix},\ s\in GF(q)\}$ è un 2-gruppo abeliano elementare di ordine q. Poiché l'ordine di SL(2, q) è $(q-1)q(q+1)$, ne segue che Σ è un 2-sottogruppo di Sylow.

(b) *Se* Σ_1 *e* Σ_2 *sono due 2-sottogruppi di Sylow di* SL(2, q), allora $\Sigma_1\cap\Sigma_2=\{I\}$.

Per mostrare ciò notiamo che $\Sigma'=\{\begin{pmatrix}1 & 0\\ t & 1\end{pmatrix},\ t\in \mathrm{GF}(q)\}$ è pure un 2-sottogruppo di Sylow di SL(2, q) inoltre $\Sigma\cap\Sigma'=\{I\}$. D'altra parte presi comunque due 2-sottogruppi di Sylow distinti Σ_1 e Σ_2 di SL(2, q), esiste $\gamma\in$ SL(2, q) tale che $\gamma^{-1}\Sigma_1\gamma=\Sigma$ e $\gamma^{-1}\Sigma_2\gamma=\Sigma'$, in quanto la rappresentazione naturale di SL(2, q), q pari, è un gruppo di permutazioni doppiamente transitivo sull'insieme dei suoi 2-sottogruppi di Sylow.

Siamo ora in grado di costruire una applicazione completa ϑ di SL(2, q). Se Σ è un 2-sottogruppo di Sylow, ammette applicazioni complete, perché risolubile e non ciclico. Per ciascun 2-sottogruppo di Sylow Σ_i, $i=1,\ldots,q+1$, consideriamo una applicazione completa ϑ_1, tale che $\vartheta_i(I)=I$, e poniamo

$$\vartheta(x)=\begin{cases}\vartheta_i(x) & \text{se } x\in\Sigma_i\\ x & \text{altrimenti.}\end{cases}$$

Evidentemente ϑ è biietiva, per provare che è completa rimane da vedere che $x\cdot\vartheta(x)=y\cdot\vartheta(y)$ implica $x=y$. A tal fine notiamo che un sottogruppo ciclico proprio di SL(2, q) ha ordine 2 oppure un divisore di $q+1$ o $q-1$. Occorre distinguere i seguenti casi:

(1) $x,\ y\in\Sigma_i$ (2) $x\in\Sigma_i,\ y\in\Sigma_j\ (i\neq j)$
(3) $x\in\Sigma_i,\ y\notin\cup\Sigma_i$ (4) $x,\ y\notin\cup\Sigma_i$.

Caso (1). Per $x\neq y$ si ha: $x\cdot\vartheta(x)=x\cdot\vartheta_i(x)\neq y\cdot\vartheta_i(y)=y\cdot\vartheta(y)$, essendo ϑ_i completa.

Caso (2). È chiaro che $x \cdot \vartheta(x) = x \cdot \vartheta_i(x) \in \Sigma_i$, analogamente $y \cdot \vartheta(y) \in \Sigma_j$; poiché $\Sigma_i \cap \Sigma_j = \{I\}$, segue che $x \cdot \vartheta_i(x) = I$. Avendo posto $\vartheta_i(I) = I$, abbiamo anche $I \cdot \vartheta_i(I) = I$ ed essendo ϑ_i una applicazione completa di Σ_i, risulta $x = I$. Similmente si mostra $y = I$.

Caso (3). Se $x \in \Sigma_i$, $x \neq I$, si ha $x \cdot \vartheta(x) \in \Sigma_i$ e quindi $x \cdot \vartheta(x)$ ha ordine 2. Se $y \notin \cup \Sigma_i$ e $y \neq I$, il gruppo generato da y ha ordine dispari, in particolare y^2 ha ordine dispari. Pertanto $x \cdot \vartheta(x) \neq y^2 = y \cdot \vartheta(y)$.

Caso (4). Supponiamo $x \cdot \vartheta(x) = y \cdot \vartheta(y)$, si ha allora $x^2 = y^2$. Posto $0(x) = 2k + 1$, abbiamo:

$$I = x^{2k+1} = (x^2)^k \cdot x = (x \cdot \vartheta(x))^k \cdot x = (y \cdot \vartheta(y))^k \cdot x = (y^2)^k \cdot x.$$

Ne segue che $x = y^{-2k}$, quindi $x \in \langle y \rangle$ e in particolare $xy = yx$. Da $x^2 = y^2$ segue ora $(xy^{-1})^2 = I$, ma $xy^{-1} \in \langle y \rangle$ e l'ordine di $\langle y \rangle$ è dispari; pertanto deve essere $xy^{-1} = I$ cioè $x = y$.

Proposizione 2. SL(2, q), $q = 5$, 7, 11 *ammette delle applicazioni complete.*

Dim. Faremo uso dei seguenti risultati dovuti a Hall e Paige [4]:

(c) Un gruppo finito risolubile, i cui 2-sottogruppi di Sylow non sono ciclici, ammette delle applicazioni complete.

(d) Un gruppo d'ordine dispari ammette sempre delle applicazioni complete.

(e) Sia G un gruppo fattorizzabile in senso stretto, cioè $G = A \cdot B$, dove A e B sono sottogruppi di G con $A \cap B = \{1\}$. Se A e B ammettono entrambi delle applicazioni complete, allora ne ammette anche G.

Sia $q = 5$, come è noto, SL(2, 5) ammette un sottogruppo $\Gamma \cong$ SL(2, 3), cosicché SL(2, 5) è il prodotto di Γ e un sottogruppo Δ di ordine 5. In altri termini SL(2, 5) ammette una fattorizzazione in senso stretto, con fattori isomorfi a SL(2, 3) e C_5, rispettivamente. SL(2, 3) è un gruppo risolubile di ordine 24 con 2-sottogruppi di Sylow isomorfi al gruppo dei quaternioni. Per (c) SL(2, 3)

ammette delle applicazioni complete; poiché, per (d), anche C_5 ne ammette, l'asserto segue da (e). Per i due casi rimanenti si procede in modo analogo, tenendo conto che è $\mathrm{SL}(2, q) = \Gamma \cdot \Delta$, con $\Gamma \cong \mathrm{GL}(2, 3)$, $\Delta \cong C_7$, per $q = 7$ e $\Gamma \cong \mathrm{SL}(2, 5)$, $\Delta \cong C_{11}$, per $q = 11$ ([8], p. 411).

4 - Sul gruppo moltiplicativo di un quasicorpo associativo finito

Teorema 3. *Un quasicorpo associativo $N(+, \cdot)$ è un doppio cappio eccezionale se e solo se è finito e il gruppo $N^*(\cdot)$ è a 2-sottogruppi di Sylow ciclici.*

Dim. Faremo uso ancora di (c) e dei due risultati seguenti sulle applicazioni complete di un gruppo [5], [8]:

(f) Se un gruppo finito G ha un 2-sottogruppo di Sylow ciclico, allora non ammette applicazioni complete.

(g) Sia G un gruppo e H un suo sottogruppo normale. Se H e G/H ammettono entrambi delle applicazioni complete, allora ne ammette anche G.

Sia $N(+, \cdot)$ un quasicorpo associativo di ordine q dispari, in base al Teorema 1, basta provare che $N^*(\cdot)$ è a 2-sottogruppi di Sylow ciclici se e solo se è privo di applicazioni complete. Secondo la classificazione di Zassenhaus [9], N è *regolare* (uno dei quasicorpi di Dickson) oppure è uno dei sette quasicorpi detti *irregolari*. È noto inoltre (Zassenhaus [9]) che se N è regolare oppure è uno dei primi quattro quasicorpi irregolari allora $N^*(\cdot)$ è risolubile. Per tali quasicorpi associativi l'asserto segue da (c) e (f). Se N è uno degli ultimi tre dei sette quasicorpi irregolari, il gruppo moltiplicativo N^* è isomorfo a $\mathrm{SL}(2, 5) \otimes C$, con C isomorfo rispettivamente a $\{1\}$, C_7, C_{29}; perciò la Proposizione 2 e (g) implicano che N^* ammetta in questi casi, delle applicazioni complete.

Osserviamo che il gruppo moltiplicativo di ciascuno dei sette quasicorpi associativi finiti irregolari è a 2-sottogruppi di Sylow generalizzati dei quaternioni. Ciò non è sempre vero nel caso dei quasicorpi associativi regolari, ad esempio, il gruppo moltiplicativo del quasicorpo associativo *eccezionale* $N(2, 3)$ è isomorfo al gruppo dei quaternioni; d'altra parte i 2-sottogruppi di Sylow del gruppo moltiplicativo del quasicorpo associativo (proprio) $N(3, 7)$ sono ciclici.

Bibliografia

[1] A. BICHARA and G. KORCHMAROS, *Note on* $(q+2)$*-sets in a Galois plane of order* q, Ann. Discrete Math. 14 (1982), 117-122.

[2] R. H. BRUCK, *A survey of binary systems*, Springer-Verlag, 1971.

[3] J. DÉNES and A. D. KEEDWELL, *Latin squares and their applications*, Akadémia Kiadó, Budapest, 1974.

[4] M. HALL and L. J. PAIGE, *Complete mappings of finite groups*, Pacific J. Math. 5 (1955), 541-549.

[5] B. HUPPERT, *Endliche Gruppen* (I), Springer-Verlag, 1967.

[6] H. B. MANN, *On orthogonal latin squares*, Bull. Amer. Math. Soc. 50 (1944), 249-257.

[7] L. J. PAIGE, *Complete mappings of finite groups*, Pacific J. Math. 1 (1951), 111-116.

[8] M. SUZUKI, *Group theory* (I), Springer-Verlag, 1982.

[9] H. ZASSENHAUS: $[\bullet]_1$ *Über endliche Fastkörper*, Abh. Math. Sem. Univ. Hamburg 11 (1934), 187-220; $[\bullet]_2$ *On Frobenius groups* (I), Resultate Math. 8 (1985), 132-145.

Summary

For a one to one mapping f *of a double-loop* $\boldsymbol{K}(+,\cdot)$ *onto itself, let* $C(f)$ *denote the set of all elements* $a \in \boldsymbol{K}$ *such that the «difference ratio in* a*»* $(\cdot)$ *takes up all non zero values in* $\boldsymbol{K}$ *when* x *ranges over* $\boldsymbol{K} \setminus \{a\}$. *In most cases a double-loop* $\boldsymbol{K}(+,\cdot)$ *admits a bijective mapping* f *such that* $C(f) \neq \emptyset$. *We shall call «exceptional» each double-loop* $\boldsymbol{K}(+,\cdot)$ *for which* $C(f) = \emptyset$ *holds for every* $f \in D(\boldsymbol{K})$. *All finite fields of characteristic* $p > 2$ *are exceptional* [1]. *There is a strong link between the fact that the double-loop* $\boldsymbol{K}(+,\cdot)$ *is exceptional and the non existence of complete mappings in* $\boldsymbol{K}^*(\cdot)$. *Groups admitting complete mappings have been studied by several authors. M. Hall and L. J. Paige proved that all infinite groups have complete mappings and that a finite solvable group has a complete mapping if and only if its Sylow 2-subgroups are non-cyclic. We prove here that* SL$(2, n)$ *admits complete mappings for* $n = 2^h$ *and* $n = 5, 7, 11$. *Results on complete mappings allow us to determine all nearfields which are exceptional double-loops. They are characterized by the property that they are finite and the Sylow 2-subgroups of their multiplicative group* $\boldsymbol{K}^*(\cdot)$ *are cyclic.*

***