Note di Matematica, Vol. III, 229-243 (1983)

CAPPI E PERMUTAZIONI (*)

Rita CAPODAGLIO DI COCCO (**)

Summary: *The main result of this paper is a characterization of all finite loops. It is shown that every finite loop of order* n *is isomorphic to a loop in which the elements are permutations over* n-1 *objects and the operation is conveniently defined.*

INTRODUZIONE. Il presente lavoro è diviso in quattro parti. Nella prima si mostra come un qualunque insieme Ω possa essere dotato di una struttura di cappio, mediante la considerazione di opportune permutazioni su di esso.

Nella seconda parte, viceversa, si dimostra che ogni cappio finito Ω di ordine n è isomorfo a un cappio M_d i cui elementi sono permutazioni su $n-1$ elementi e in cui l'operazione è opportunamente definita. La considerazione dei cappi M_d è molto conveniente quando si vogliano determinare cappi soddisfacenti particolari proprietà. Ciò viene fatto nella terza parte, dove, dapprima si determinano le condizioni necessarie e sufficienti affinché un cappio M_d

1) contenga l'inverso di ogni suo elemento

2) sia commutativo

(*) Ricerca eseguita nell'ambito del G.N.S.A.G.A. del C.N.R.

(**) Dipartimento di Matematica Università di Bologna.

3) goda della proprietà inversa sinistra

4) goda della proprietà inversa destra

e poi si costruiscono cappi che soddisfano tali proprietà. Tutti i cappi trovati hanno ordine 6 e ciò è interessante in quanto i cappi di ordine $n < 6$ sono noti (cfr. [2]).Rileviamo inoltre che il cappio dell'esempio II possiede un'applicazione completa (secondo la terminologia di [6]) e quindi il quadrato latino che ne costituisce la tabella di moltiplicazione ha una trasversale. Ciò ha interesse in quanto è noto [6] che tutti i quasigruppi diagonali e in particolare i gruppi di ordine dispari e i quasigruppi commutativi di ordine dispari possiedono applicazioni totali, mentre il cappio in questione è di ordine pari e non è diagonale.

Infine nella quarta parte del lavoro si fa vedere che il cappio Ω individua anche un altro cappio M_s, i cui elementi coincidono con quelli di M_d, ma in cui l'operazione è definita in modo diverso. La considerazione del cappio M_s può essere utile in quanto alcune proprietà di Ω si traducono più agevolmente in proprietà di M_s piuttosto che in proprietà di M_d.

I. Sia Ω un qualunque insieme finito con n elementi ($n>2$). Senza perdere di generalità, possiamo supporre $\Omega = \{1,2,\dots,n\}$. Sia Σ il gruppo delle permutazioni su Ω. Fissato una volta per tutte un elemento x di Ω, sia Π lo stabilizzatore di x in Σ.

Definizione I. Chiamiamo insieme rappresentante di Ω in Σ un insieme $M \subset \Sigma$ tale che

1) $M \ni I$ = permutazione identica

2) M è strettamente 1-transitivo su Ω.

TEOREMA I. *Se M è un insieme rappresentante di* Ω *in* Σ *allora risulta:*

1) $|M| = n$

2) *Ogni laterale destro (sinistro) di* Π *in* Σ *contiene uno e un solo elemento di* M.

Dim. Banale.

Se M è un insieme rappresentante di Ω in Σ, sia $\phi : M \to \Omega$ l'applicazione definita da

$$\forall\, T \in M\,, \quad T \to xT\,.$$

Poiché ϕ è una biiezione, presi comunque a,b in Ω, sono univocamente determinati T e S in M tali che $a=xT$ e $b=xS$. Definiamo allora un'operazione in Ω ponendo

$$a \cdot b = xT \cdot xS = (xT)S = xTS\,.$$

TEOREMA II. *La struttura* $(\Omega,\cdot)$ *risulta un cappio.*

Dim. Poiché $I \in M$ e $xI = x$, $\forall a \in \Omega$ con $a = xT$ e $T \in M$ risulta

$$a \cdot x = xT.xI = xTI = xT = a$$
$$x.a = xI.xT = xIT = xT = a$$

e quindi x è elemento neutro.

Si consideri in Ω l'equazione (1) $ax=b$ dove $a=xT$ con T in M. Sia $F \in M$ la permutazione (esistente e univocamente determinata) tale che $aF = b$. Se $c = xF$ si ha:

$$a.c = xT.xF = xTF = b$$

e quindi c è soluzione della (1). Viceversa sia $d = xL$ (con L in M) tale che a.d=b. Risulta a.d = xT.xL = aL = b. La permutazione L, mutando a in b, deve coincidere con F e dunque d = c, cioé l'equazione (1) ha una e una sola soluzione.

Consideriamo ora in Ω l'equazione (2) x.a = b, dove a=xT con T in M. Sia m l'elemento (univocamente determinato) tale che mT=b. Se m = xG con G in M, risulta m.a = xG.xT = xGT = b, e quindi m è soluzione della (2). Se poi è n.a = b con n = xQ e Q in M, si ha xQ.xT = xTQ = b e quindi P = Q e n = m; anche la (2) ha una e una sola soluzione. Ciò basta per affermare che Ω è un cappio.

Definizione II. Se M è un insieme rappresentante di Ω in Σ e x è un elemento fissato in Ω, allora $(\Omega,.)$ si chiama struttura associata alla coppia (M,x).

Vogliamo definire un'operazione in M. Presi T,S in M, sia xTS=a; se è a = xF per definizione poniamo T*S = F. Si vede subito che in tal modo M diviene un cappio isomorfo a Ω .

TEOREMA III. (M, *) *è un gruppo se e solo se l'operazione * coincide con l'ordinaria composizione funzionale.*

Dim. La sufficienza della condizione è ovvia. Per dimostrarne la necessità supponiamo che esistano P,Q in M tali che P*Q = F≠PQ. Ciò significa che esiste almeno un a $\in \Omega$ tale che aF = b ≠ c = aPQ. Se a = xH, è facile vedere che la permutazione H*(P*Q) = H*F muta x in c, mentre la permutazione (H*P)*Q muta x in b. Poiché in M risulta H*(P*Q) ≠ (H*P)*Q, il cappio M non è un gruppo, donde la conclusione.

D'ora in poi, senza perdere di generalità, supporremo sempre x=1.

Sia T_a la trasposizione (1,a). Poiché i laterali destri di Π in Σ sono

$$\Pi, \Pi T_2, \Pi T_3, \dots, \Pi T_n,$$

per la 2) del teorema I risulta

$$M = \{ I, H_2T_2, H_3T_3, \dots, H_nT_n \}$$

dove gli H_i $(i = 2,3,\dots,n)$ sono opportuni elementi di Π e $H_i \neq H_j$ se $i \neq j$.

Sia $M_d = \{ I, H_2, \dots, H_n\}$ in modo che $M_d \subset \Pi$.

TEOREMA IV. CNES *affinché* $M = \{I, H_2T_2, H_3T_3, \dots, H_nT_n\}$, *dove* $H_i \in \Pi$ *e* $H_i \neq H_j$ *per* $i \neq j$, *sia un insieme rappresentante di* Ω *in* Σ *è che* $M_d = \{I, H_2, H_3, \dots, H_n\}$ *soddisfi le seguenti proprietà:*

1) *ogni* H_a, *oltre all'elemento* 1, *fissa al più l'elemento* a (*per* $a = 2,3,\dots,n$).

2) $\forall a,b$ *in* Ω, $a \neq 1 \neq b$, $a \neq b \implies \exists!\, c \neq b$ *tale che* $aH_c = b$.

3) $\forall a$ *in* Ω, $a \neq 1 \implies \exists!\, c$ *tale che* $aH_c = c$ (*eventualmente con* $c = a$).

Dim. Sia M un insieme rappresentante di Ω in Σ. Poiché M è strettamente 1-transitivo su Ω, si ha

$$\forall a,b \ \ in\ \Omega\ , \ a \neq 1 \neq b \implies bH_aT_a \neq b$$

da cui se $b \neq a$, si ha $bH_a \neq b$ cioé la 1).

Inoltre se $a,b \in \Omega$ con $a \neq 1 \neq b$ e $a \neq b$, $\exists!\, c$ tale che $aH_cT_c = b$. Se fosse $aH_c = c$ si avrebbe l'assurdo $aH_cT_c = 1 = b \neq 1$. E' dunque $aH_c \neq c$ e quindi $aH_cT_c = aH_c = b$.

Se infine $a\neq 1$, $\exists!\ c$ tale che $aH_cT_c = 1$ e questo comporta la 3).

Avendo dimostrato la necessità delle condizioni, passiamo alla sufficienza.

L'insieme M_d soddisfi le 1),2),3). Basta dimostrare che M è strettamente 1-transitivo su Ω. Siano a,b in Ω. Se $a = b$, l'unico elemento di M che muta a in b è I. Sia allora $a\neq b$ e anche $a\neq 1\neq b$. Per la 2) $\exists!\ c \neq b$ tale che $aH_c = b$ e quindi l'elemento H_cT_c di M muta a in b, mentre evidentemente, se $aP = b$ con P in M, è $P = H_cT_c$. Se invece $a = 1 \neq b$, l'unica permutazione di M che muta a in b è H_bT_b. Se infine $a \neq 1 = b$, l'unica permutazione di M che muta a in b è H_cT_c, dove c è l'elemento univocamente individuale in base alla 3), per il quale $aH_c = c$.

COROLLARIO. *Se* $aH_a \neq a$, *allora esiste un'unica coppia* b,c *tale che* $b \neq c$, $b \neq a \neq c$ *e* $aH_b = aH_c$.

Dim. Per la 3) del teorema precedente $\exists!\ c\neq a$ tale che $aH_c=c$; per la 2) dello stesso teorema $\exists!\ b \neq c$ tale che $aH_b = c$, da cui l'asserto.

Introduciamo adesso in M_d un'operazione ponendo per definizione:

$$H_a * H_b = I \qquad , \quad \text{se} \quad aH_b = b$$

$$H_a * H_b = H_c \qquad \text{con } c = aH_b \quad \text{se} \quad aH_b \neq b.$$

Si verifica senza difficoltà che, così strutturato, M_d è un cappio isomorfo a M e quindi a Ω.

Notiamo che l'operazione $*$ introdotta in M_d coincide sostanzialmente con quella considerata da Baer in [3].

II. Sia ora $(\Omega,.)$ un cappio finito di ordine n. Senza perdere di generalità, supporremo che gli elementi di Ω siano i numeri naturali $1,2,\dots,n$ e che 1 sia l'elemento neutro.

In armonia con [1] e [3], per ogni a in Ω, chiamiamo traslazione destra di coefficiente a la permutazione R_a tale che

$$\forall x \in \Omega \ , \quad xR_a = x.a.$$

Sia $M = \{R_a, a \in \Omega\}$. In M definiamo un'operazione $*$, ponendo

$$R_a * R_b = R_{ab}$$

essendo ovviamente R_{ab} la permutazione tale che

$$\forall x \in \Omega, xR_{ab}=x.(a.b).$$

TEOREMA V. $(M.*)$ *è un cappio isomorfo a* $(\Omega,.)$.

Dim. Basta osservare che l'applicazione $\psi : \Omega \to M$, definita da $a \to R_a$ è un isomorfismo.

Detto Σ il gruppo delle permutazioni sull'insieme sostegno di Ω e ricordando la definizione I, si ha il

TEOREMA VI. M *è un insieme rappresentante di* Ω *in* Σ.

Dim. Evidentemente $I = R_1$. Inoltre, se $a,b \in \Omega$, $\exists !$ c tale che $a.c = b$, e quindi R_c è l'unica permutazione di M che muti a in b.

Analogamente $\forall a$ in Ω, si chiama traslazione sinistra di coefficiente a la permutazione L_a definita da

$$\forall x \in \Omega \ , \ xL_a = a.x.$$

In $N = \{L_a, a \in \Omega\}$ definiamo un'operazione $*$ ponendo

$$L_a * L_b = L_{ab}$$

essendo ovviamente L_{ab} la permutazione tale che

$$\forall x \in \Omega\ ,\ xL_{ab} = (a.b).x.$$

E' immediato verificare che, così strutturato, anche N è un cappio isomorfo a Ω.

Sia A la tabella di moltiplicazione di Ω. Usando la terminologia di [8] pag. 131, notiamo che la permutazione R_a ha come denominatore la colonna a-ma di A, mentre la permutazione L_b ha come denominatore la riga b-ma di A.

TEOREMA VII. *Il cappio* $(\Omega,.)$ *coincide con la struttura associata alla coppia* (M,1).

*Dim.*Con i simboli del paragrafo I, consideriamo l'applicazione ϕ: $M \to \Omega$ individuata dalla posizione

$$\forall\ G \in M,\ G \to 1G \quad .$$

In questo caso si ha $M = \{R_a,\ a \in \Omega\}$, sicché

$$R_a \to 1R_a = 1.a = a,$$

cioé $\phi = \psi^{-1}$ dove ψ è l'isomorfismo considerato nella dimostrazione del teorema V. Da ciò la conclusione.

COROLLARIO. *Mediante il procedimento descritto nel paragrafo I si ottengono tutti i possibili cappi finiti.*

Sia Π lo stabilizzatore dell'elemento $1 \in \Omega$ in Σ .

TEOREMA VIII. *Ogni cappio finito* Ω *di ordine* n *è isomorfo a un cap-*

pio M_d *che gode delle seguenti proprietà:*

1) *gli elementi* $H_1, H_2, \ldots, H_n$ *di* M_d *sono anche elementi di* Π.

2) $H_1 = I$ = *identità di* Σ .

3) *Ogni permutazione* H_a *fissa al più l'elemento* a $(a=2,3,\ldots,n)$

4) *se* $a \neq 1 \neq b$ e $a \neq b$, *allora* $\exists! \; c \neq b$ *tale che* $aH_c = b$.

5) *se* $a \neq 1$, *allora* $\exists!$ c *tale che* $aH_c = c$

6) *l'operazione* * *in* M_d *è definita dalla posizione*

$$H_a * H_b = I \quad \textit{se} \quad aH_b = b$$

$$H_a * H_b = H_c, \; \textit{dove} \; c = aH_b \quad \textit{se} \quad aH_b \neq b.$$

Dim. In base al teorema V e VII, Ω risulta isomorfo a un cappio M il cui insieme sostegno è un insieme rappresentante di Ω in Σ . Per il teorema IV, allora Ω risulta isomorfo a un cappio M_d soddisfacente le 1),...,6).

III. Per quanto visto nei paragrafi precedenti, lo studio dei cappi finiti può limitarsi a quello dei cappi M_d soddisfacenti le 1), 2),3),4),5),6) che compaiono nell'enunciato del teorema VIII. Vogliamo ora vedere sotto quali condizioni un cappio M_d gode di particolari proprietà.

1. *Esistenza dell'inverso.*

Secondo la terminologia usuale, diremo che un elemento H_a di M_d ammette inverso se, per tale elemento, l'inverso destro coincide con l'inverso sinistro. L'inverso di H_a nel cappio M_d sarà indicato con il simbolo H_a^i per distinguerlo da H_a^{-1} (l'inverso di H_a nel gruppo Σ).

TEOREMA IX. *L'elemento* H_a *di* M_d *ammette inverso se e solo se è* *verificata una delle condizioni seguenti*

i) $aH_a = a$ *e in tal caso* $H_a^i = H_a$

ii) *posto* $b = aH_a^{-1} \neq a$, *risulta* $aH_b = b$; *in tal caso si ha* $H_a^i = H_b$.

Dim. Se è $aH_a = a$, per definizione si ha $H_a * H_a = I$, sicché $H_a^i = H_a$. Se $aH_a \neq a$, sia $b = aH_a^{-1}$. Risulta allora

$$H_a * H_b = I \iff aH_b = b$$

$$H_b * H_a = I \iff bH_a = a$$

da cui la condizione voluta.

ESEMPIO I. Il cappio (20) di [2] ha 5 elementi ciascuno dotato di inverso in quanto è verificata la i).

ESEMPIO II. Cappio di 6 elementi ciascuno dotato di inverso in quanto è verificata la ii).

$H_2 = (2,4,5,3,6)$, $H_3 = (2,5,4,6)$, $H_4 = (2,6,3,5,4)$, $H_5 = (2,3)(4,5,6)$, $H_6 = (2,6,5)(3,4)$. Notiamo che la permutazione $(3,4,6)$ applicata agli indici degli elementi H_i $(i=1,2,\dots,6)$ dà luogo a una applicazione completa (cfr. [6] pag. 28). Pertanto la tabella di moltiplicazione di questo cappio è un quadrato latino che possiede una trasversale.

2. *Commutatività.*

Chiaramente il cappio M_d risulta commutativo se e solo se

$$\forall a,b \quad \text{in } \Omega \Longrightarrow aH_b = bH_a .$$

ESEMPIO III. Cappio commutativo con 6 elementi

$H_2 = (3,4,5,6)$, $H_3 = (2,4,3,6,5)$, $H_4 = (2,5,3,4,6)$, $H_5 = (2,6,5,4,3$, $H_6 = (2,3,5,6,4)$.

3. *Forme deboli della proprietà associativa.*

TEOREMA X. *Nel cappio* M_d *è verificata la proprietà (associativa) inversa sinistra*

$$H_a^i * (H_a * H_b) = H_b \qquad (\textit{con } aH_b \neq b)$$

se e solo se vale una delle condizioni seguenti:

i) $aH_a = a$, *e, posto* $c = aH_b$, *risulta* $aH_c = b$

ii) $aH_a \neq a$, *e, posto* $c = aH_b$, *risulta* $aH_a^{-1}H_c = b$.

Dim. Se $aH_a = a$, per il teorema IX è $H_a^{-1} = H_a$. Pertanto si ha

$$H_a^i * (H_a * H_b) = H_b \iff H_a * H_c = H_b \iff aH_c = b$$

cioé la condizione i).

Se invece $aH_a \neq a$, sempre per il teorema IX, si ha $H_a^i = H_d$ con $d = aH_a^{-1}$, sicché

$$H_a^i * (H_a * H_b) = H_b \iff H_d * H_c = H_b \iff dH_c = b$$

cioé la ii).

ESEMPIO IV. Cappio di 6 elementi che gode della proprietà inversa sinistra, ma non della destra

$H_2 = (2,3,4,5,6)$, $H_3 = (2,5,4,6)$, $H_4 = (2,6,5,4,3)$, $H_5 = (2,4,5)(3,6)$, $H_6 = (2,6,4)(3,5)$.

TEOREMA XI. *Nel cappio* M_d *è verificata la proprietà (associativa) inversa destra*

$$(H_a * H_b) * H_b^i = H_a$$

se e solo se vale una delle condizioni seguenti:

i) $bH_b = b$ *e* $aH_b^2 = a$ *(questo caso è possibile solo se* n *è pari)*

ii) $bH_b \neq b$ *e* $H_b^i = H_b^{-1}$.

Dim. Sia $bH_b = b$. Allora $H_b^i = H_b$, e, posto $c = aH_b$, risulta

$$(H_a * H_b) * H_b^i = H_a \iff H_c * H_b = H_a \iff aH_b^2 = a$$

cioé la i).

Se invece $bH_b \neq b$, si ha, sempre ponendo $c = aH_b$,

$$(H_a * H_b) * H_b^i = H_a \iff H_c * H_b^i = H_a \iff aH_bH_b^i = a$$

cioé la ii).

ESEMPIO V. Cappi di 6 elementi che godono della proprietà inversa destra ma non della sinistra. Imponendo la i) si trova il cappio $H_2 = (3,4)(5,6)$, $H_3 = (2,5)(4,6)$, $H_4 = (2,6)(3,5)$, $H_5 = (2,4)(3,6)$, $H_6 = (2,3)(4,5)$.

Imponendo invece la ii) si ha

$H_2 = (2,3,4,5,6)$, $H_3 = (2,5)(4,6)$, $H_4 = (2,6,3,5,4)$, $H_5=(2,4,5,3,6)$, $H_6 = (2,6,5,4,3)$.

IV. Riprendendo la notazioni del paragrafo I, sia M un insieme rappresentante di Ω in Σ. Poiché i laterali sinistri di Π in Σ sono

$$\Pi,\ T_2\Pi.,T_3\Pi....,T_n\Pi$$

risulta

$$M = \{I,T_2K_2,T_3K_3,...,T_nK_n\}$$

dove i K_i $(i = 2,3,...,n)$ sono opportuni elementi di Π e $K_i \neq K_j$ se $i \neq j$.

Sia $M_s = \{I,K_2,K_3,...,K_n\}$ in modo che $M_s \subset \Pi$.

TEOREMA XII. *Condizione necessaria e sufficiente affinché* $M = \{I,T_2K_2,T_3K_3,...,T_nK_n\}$, *dove* $K_i \in \Pi$ *e* $K_i \neq K_j$ *se* $i \neq j$, *sia un insieme rappresentante di* Ω *in* Σ , *è che* $M_s = \{I,K_2,K_3,...,K_n\}$. *soddisfi le proprietà:*

1) *ogni* K_a, *oltre all'elemento* 1, *fissa al più l'elemento* a $(a=2,3,...,n)$

2) *se* $a \neq 1 \neq b$ *e* $a \neq b \Longrightarrow \exists!$ *tale che* $aK_c = b$

3) *se* $b \neq 1 \Longrightarrow \exists!\ c$ *tale che* $cK_c = b$ (*eventualmente* $c=b$).

Dim. Analoga a quella del teorema IV.

TEOREMA XIII. *Gli insiemi* M_d *e* M_s *hanno gli stessi elementi, differendo solo per l'ordine degli stessi.*

Dim. Se $P \in M$, esistono a,b in Ω tali che $P=H_aT_a=T_bK_b$. Risulta pertanto

$$bP = 1 \Longleftrightarrow b = 1P^{-1} = 1T_aH_a^{-1} = aH_a^{-1} \Longleftrightarrow bH_a = a$$

$$a = 1P \iff a = 1T_bK_b = bK_b \iff bK_b = a$$

Da ciò si deduce esplicitamente la corrispondenza biunivoca tra M_d e M_s che si stabilisce chiamando corrispondenti H_a in M_d e K_b in M_s se risulta $H_aT_a = T_bK_b$. Precisamente noto a, in base alla 3) del teorema XII b è individuato dalla $bK_b = a$, mentre noto b, in base alla 3) del teorema V a è individuato dalla $bH_a = a$.

Vogliamo mostrare ora che se $H_aT_a = T_bK_b$ è addirittura $H_a = K_b$.

Infatti $\forall c \in \Omega$ si ha

$$cK_b = cT_bH_aT_a = \begin{cases} cH_a & \text{se } c \neq 1,b \quad (\text{essendo } cH_a \neq a) \\ 1 & \text{se } c = 1 \\ a & \text{se } c = b \end{cases}$$

quindi in ogni caso si ha $cH_a = cK_b$ cioè $H_a = K_b$.

BIBLIOGRAFIA

[1] A.A.ALBERT: "*Quasigroups I*", Trans.Amer.Math.Soc. 54 (1943) 507-519.

[2] A.A.ALBERT: "*Quasigroups II*", Trans. Amer. Math. Soc. 55(1944) 401-419.

[3] R.BAER: "*Nets and groups I*", Trans. Amer. Math. Soc. 46 (1939) 110-141.

[4] R.H.BRUCK: "*Some results in the theory of quasigroups*", Trans. Amer. Math. Soc. 55 (1944) 19-52.

[5] A.CAYLEY: "*On the theory of groups*", Amer. J. Math. 11 (1889) 139-157.

[6] J.DENES-A.D.KEEDWELL: "*Latin squares and their applications*". English Univ. P.L. 1974.

[7] E.SCHÖNHARDT: "*Ueber lateinisches Quadrate und Unionen*". J.Reine Angew. Math. 163 (1930) 183-229.

[8] G.SCORZA DRAGONI: "*Elementi di Analisi Matematica*" , Vol. I (Algebra) CEDAM 1961.

Lavoro pervenuto alla Redazione il 16 Maggio 1983
ed accettato per la pubblicazione il 10 Aprile 1984
su parere favorevole di M. Biliotti e G. Tallini