LE MATEMATICHE
Vol. LIV (1999) – Fasc. II, pp. 375–397

APPLICAZIONI (h, A)-LINEARI OMOMORFISMI DI M_A-IPERGRUPPOIDI

DOMENICO FRENI

In the papers [9], [10] we introduced and studied M_λ-hypergroupoids; also, we obtained some results on the automorphism group of a G_λ-hypergroupoid. In particular, given a group G and one of its element λ, we proved that the automorphisms of the corresponding G_λ-hypergroupoid are the one-one maps $f : G \to G$ which are λ-linear, i.e. verify $f(\lambda g) = \lambda f(g)$, for every $g \in G$.

A natural generalization of the notion of λ-linearity is the notion of (h, A, B)-linearity, introduced in the present paper. Theorem 1.7 provides the existence and uniqueness of a (h, A, B)-linear map. Theorem 2.3 gives the cardinality of the group $\Lambda(G_A)$ of complete, bijective (h, A)-linear maps. In Theorem 2.7 we prove that $\Lambda(G_A)$ is a semi-direct product of $\Lambda_{Id_{<A>},T}(G_A)$ via $< \ Q \ >$, where $\Lambda_{Id_{<A>},T}(G_A)$ is the subgroup of bijective, complete $(Id_{<A>}, A)$-linear maps and Q is a suitable subset of $\Lambda(G_A)$.

The notion of M_A-hypergroupoid is defined in the last section, via group actions on sets. We also study their homomorphisms and prove that the M_A-hypergroupoid is a hypergroup or a join-space according to the set A being a stable part or a subgroup of G.

1. Applicazioni (h, A, B)-lineari. Prime proprietà..

Nell'ambito delle strutture multivoche sono numerosi gli articoli riguardanti gli omomorfismi di particolari classi d'ipergruppi come, ad esempio, gli

Entrato in Redazione il 26 Maggio 2000.

ipergruppi di tipo U a destra, i Join-Spaces e gli ipergruppi canonici, ma sono pochi i risultati sul gruppo degli automorfismi di queste strutture. In effetti, la particolare natura delle operazioni multivoche rende complesso lo studio del gruppo degli automorfismi. In questo contesto, una nozione che ha permesso di ottenere nuovi risultati è quella di applicazione λ-lineare (vedi [10]), mediante la quale si è studiato il gruppo degli automorfismi degli M_λ e dei G_λ-ipergruppoidi. Adesso, in questo paragrafo, si definiscono e si studiano le applicazioni (h, A, B)-lineari e successivamente si determina il gruppo $\Lambda(G_A)$ delle applicazioni A-lineari e il gruppo degli automorfismi di $(h, < A >)$-lineari completi di un $G_{<A>}$-Join Space.

Definizione. Siano G e G' due gruppi e A, B sottoinsiemi rispettivamente di G e G'. Un'applicazione f da G in G' si dice *(h, A, B)-lineare* se esiste un'applicazione $h : A \to B$ tale che $f(ax) = h(a)f(x)$, $\forall a \in A$, $\forall x \in G$.

L'applicazione h si chiama *l'applicazione generatrice* di f.

Le applicazioni (h, A, A)-lineari si dicono (h, A)-lineari.

Proposizione 1.1. *Sia $f : G \to G'$ un'applicazione (h, A, B)-lineare, allora:*

1) $f(a^n x) = (h(a))^n f(x), \quad \forall (n, a, x) \in Z \times A \times G.$

2) Per ogni $n \in N^*$, $(a_1, a_2, \ldots, a_n) \in A^n$, $(r_1, r_2, \ldots, r_n) \in Z^n$ e $x \in G$, si ha:

$$f(a_1^{r_1} a_2^{r_2} \ldots a_n^{r_n} x) = h(a_1)^{r_1} h(a_2)^{r_2} \ldots h(a_n)^{r_n} f(x)\,.$$

3) Esiste un omomorfismo $h^* :< A >\to< B >$ tale che $h^*(a) = h(a)$, per ogni $a \in A$. Inoltre, l'applicazione f è $(h^*, < A >, < B >)$-lineare.

Dimostrazione. 1) La dimostrazione è ovvia per $n = 0$ e $n = 1$. Supponendola vera per un intero positivo n, si ha:

$$f(a^{n+1}x) = f(a(a^n x)) = h(a)f(a^n x) = h(a)(h(a))^n f(x) = h(a)^{n+1} f(x),$$

dunque $f(a^{n+1}x) = h(a)^{n+1} f(x)$.

Inoltre, si ha

$$f(x) = f((aa^{-1})x) = f(a(a^{-1}x)) = h(a)f(a^{-1}x),$$

quindi

$$f(a^{-1}x) = (h(a))^{-1} f(x),$$

e procedendo ancora per induzione si dimostra che $f(a^{-n}x) = (h(a))^{-n} f(x)$, per ogni $n \in N$.

2) Subito da 1).

3) Sia $h^* :< A >\to< B >$ l'applicazione così definita:

$$h^*(\prod_{k=1}^{n} a_k^{r_k}) = \prod_{k=1}^{n} h(a_k)^{r_k}, \quad \forall\ n \in N - \{0\},$$

$$(a_1, a_2, \ldots, a_n) \in A^n,\ (r_1, r_2, \ldots, r_n) \in Z^n.$$

È ovvio che $h^*(\prod_{k=1}^{n} a_k^{r_k}) \in < B >$ perché $Imh \subset B$. Inoltre, se $\prod_{k=1}^{n} a_k^{r_k} = \prod_{k=1}^{m} b_k^{s_k}$, per 2), si ha

$$\prod_{k=1}^{n} h(a_k)^{r_k} f(1_G) = f(\prod_{k=1}^{n} a_k^{r_k} 1_G) = f(\prod_{k=1}^{m} b_k^{s_k} 1_G) = \prod_{k=1}^{m} h(b_k)^{s_k} f(1_G)$$

per cui $\prod_{k=1}^{n} h(a_k)^{r_k} = \prod_{k=1}^{m} h(b_k)^{s_k}$, quindi $h^*(\prod_{k=1}^{n} a_k^{r_k}) = h^*(\prod_{k=1}^{m} b_k^{s_k})$. Dunque l'applicazione h^* è ben definita. È anche facile verificare che h^* è un omomorfismo di gruppi ed inoltre è chiaro che $h^*(a) = h(a)$, per ogni $a \in A$.

Infine, per ogni $x \in G$ e per ogni $\alpha = \prod_{k=1}^{n} a_k^{r_k} \in < A >$, con $n \in N^*$, $(a_1, a_2, \ldots, a_n) \in A^n$ e $(r_1, r_2, \ldots, r_n) \in Z^n$, applicando 2), si ottiene:

$$f(\alpha x) = f(\prod_{k=1}^{n} a_k^{r_k} x) = \prod_{k=1}^{n} h(a_k)^{r_k} f(x) = h^*(\prod_{k=1}^{n} a_k^{r_k}) f(x) = h^*(\alpha) f(x),$$

perciò f è $(h^*, < A >, < B >)$-lineare.

Definizione. L'omomorfismo $h^* :< A >\to< B >$ definito nella Proposizione 1.1 3) si chiama *l'omomorfismo generatore* dell'applicazione (h, A, B)-lineare f.

Immediata conseguenza della Proposizione 1.1 è il seguente:

Corollario 1.2. *Sia $f : G \to G'$ un'applicazione (h, A, B)-lineare, allora:*

1) $f(< A > f^k(x)) \subset < B > f^{k+1}(x)$, $\forall x \in G$, $\forall k \in N$.

2) Se l'applicazione generatrice h di f è suriettiva, l'omomorfismo generatore $h^* :< A >\to< B >$ è un epimorfismo e $f(< A > f^k(x)) =< B > f^{k+1}(x)$, $\forall x \in G$, $\forall k \in N$.

Proposizione 1.3. *Se $f, g : G \to G'$ sono due applicazioni rispettivamente (h, A, B)-lineare e (k, A, B)-lineare, allora $f = g$ implica $h = k$ e $h^* = k^*$.*

Dimostrazione. Se $f = g$, allora $f(ax) = g(ax)$ e $f(x) = g(x)$, per ogni $(a, x) \in A \times G$, dunque

$$h(a)f(x) = f(ax) = g(ax) = k(a)g(x),$$

per cui $h(a) = k(a)$, per ogni $a \in A$. Quindi $h = k$ e di conseguenza anche $h^* = k^*$.

Proposizione 1.4. *Sia $f : G \to G'$ un'applicazione (h, A, B)-lineare. Si ha:*

1) Se f è iniettiva, allora h e h^* sono iniettive.

2) Se f e h sono biunivoche, allora f^{-1} è (h^{-1}, B, A)-lineare.

Dimostrazione. 1) Se f è iniettiva e (α_1, α_2) è una coppia di elementi di $< A >$ tale che $h^*(\alpha_1) = h^*(\alpha_2)$, per la Proposizione 1.1 3), si ha

$$f(\alpha_1) = f(\alpha_1 1_G) = h^*(\alpha_1)f(1_G) = h^*(\alpha_2)f(1_G) = f(\alpha_2 1_G) = f(\alpha_2),$$

dunque $\alpha_1 = \alpha_2$ ed h^* è iniettiva. Inoltre, ancora per la Proposizione 1.1 3), l'applicazione h è la restrizione di h^* ad A, perciò anche h è iniettiva.

2) Siano f e h biunivoche. Preso $b \in B$, esiste $a \in A$ tale che $b = h(a)$, così , per ogni $y \in G'$, posto $f^{-1}(by) = x$, si ha

$$f^{-1}(by) = x \Leftrightarrow f(x) = by \Leftrightarrow b^{-1}f(x) = y \Leftrightarrow (h(a))^{-1}f(x) = y \Leftrightarrow$$

$$\Leftrightarrow f(a^{-1}x) = y \Leftrightarrow a^{-1}x = f^{-1}(y) \Leftrightarrow x = af^{-1}(y) = h^{-1}(b)f^{-1}(y),$$

quindi $f^{-1}(by) = h^{-1}(b)f^{-1}(y)$. Dunque f^{-1} è (h^{-1}, B, A)-lineare e $h^{-1} : B \to A$ è la sua applicazione generatrice.

Osservazione. La suriettività di un'applicazione (h, A, B)-lineare non comporta, in generale, la suriettività della sua applicazione generatrice. Ad esempio, considerato il gruppo $G = (R, +)$ e fissato $n \in Z - \{-1, 0, +1\}$, le due applicazioni $f : R \to R$ e $h : Z \to Z$ così definite:

$$f(x) = nx, \ \forall x \in R;$$
$$h(a) = na, \ \forall a \in Z;$$

sono tali che f è biunivoca ed h è iniettiva ma non suriettiva, inoltre

$$f(a + x) = n(a + x) = na + nx = h(a) + f(x), \ \forall a \in Z, \ x \in R.$$

Dunque f è (h, Z)-lineare biunivoca con applicazione generatrice h non suriettiva.

Definizione. Un'applicazione (h, A, B)-lineare $f : G \to G'$ si dice *completa* se la sua applicazione generatrice $h : A \to B$ è suriettiva.

Proposizione 1.5. *Siano $f : G \to G'$ e $g : G' \to G''$ due applicazioni, rispettivamente, (h, A, B)-lineare e (k, B, C)-lineare, allora $g \circ f$ è un'applicazione $(k \circ h, A, C)$-lineare e il suo omomorfismo generatore è $(k \circ h)^* = k^* \circ h^*$. Inoltre, se f e g sono complete, anche $g \circ f$ è completa.*

Dimostrazione. Per ogni $a \in A$ e $x \in G$, si ha:

$$g \circ f(ax) = g(f(ax)) = g(h(a)f(x)) = k(h(a))g(f(x)) = k \circ h(a)g \circ f(x),$$

quindi $g \circ f$ è $(k \circ h, A, C)$-lineare.

Inoltre, per ogni $\alpha = \prod_{k=1}^{n} a_k^{r_k} \in < A >$, si ha

$$k^* \circ h^*(\alpha) = k^* \circ h^*(\prod_{k=1}^{n} a_k^{r_k}) = k^*(h^*(\prod_{k=1}^{n} a_k^{r_k})) = k^*(\prod_{k=1}^{n}(h(a_k))^{r_k}) =$$

$$= \prod_{k=1}^{n}(k(h(a_k)))^{r_k} = \prod_{k=1}^{n}(k \circ h(a_k))^{r_k} = (k \circ h)^*(\prod_{k=1}^{n} a_k^{r_k}) = (k \circ h)^*(\alpha),$$

dunque $k^* \circ h^* = (k \circ h)^*$.

Infine, se f e g sono complete, allora h e k sono suriettive, per cui $k \circ h$ è suriettiva e $g \circ f$ è completa.

Proposizione 1.6. *Sia $f : G \to G'$ un'applicazione (h, A, B)-lineare completa, allora:*

1) Se f è iniettiva, la sua applicazione generatrice h è biunivoca e il suo omomorfismo generatore è un isomorfismo;

2) Se f è biunivoca, l'applicazione inversa f^{-1} è un'applicazione (h^{-1}, B, A)-lineare completa di isomorfismo generatore $(h^{-1})^* = h^{*-1}$.

Dimostrazione. 1) Segue subito dalla Proposizione 1.4 1) e dal Corollario 1.2 2).

2) Per 1) e per la Proposizione 1.4 2), f^{-1} è un'applicazione (h^{-1}, B, A)-lineare completa. Inoltre, per la Proposizione 1.5, si ha

$$(h^{-1})^* \circ h^* = (h^{-1} \circ h)^* = (Id_A)^* = Id_{<A>},$$

in quanto

$$(Id_A)^*(\alpha) = (Id_A)^*(\prod_{k=1}^{n} a_k^{r_k}) = \prod_{k=1}^{n}(Id_A(a_k))^{r_k} = \prod_{k=1}^{n} a_k^{r_k} = \alpha,$$

per ogni $\alpha = \prod_{k=1}^{n} a_k^{r_k} \in < A >$. Dunque $(h^{-1})^* = h^{*-1}$.

Teorema 1.7. (Di esistenza di un'applicazione (h, A, B)-lineare). *Siano A e B sottoinsiemi, rispettivamente, dei due gruppi G e G', e sia $h^* :< A >\to< B >$ un omomorfismo di gruppi tale che $h^*(A) \subset B$. Se $T = \{g_j\}_{j\in J}$ e T' sono due trasversali, rispettivamente, dei laterali sinistri di $< A >$ in G e di $< B >$ in G', ed f^* è un'applicazione da T in T', allora esiste una sola applicazione $(h = h^*_{|A}, A, B)$-lineare f da G in G'tale che $f(g_j) = f^*(g_j)$, per ogni $j \in J$. Inoltre, se h^* è un monomorfismo (risp. epimorfismo) ed f^* è iniettiva (risp. suriettiva), allora anche f è iniettiva (risp. suriettiva).*

Dimostrazione. Per ogni $x \in G$, esiste una sola coppia $(\alpha, g_j) \in \ < A > \times T$ tale che $x = \alpha g_j$, dunque si ponga:

$$f(x) = h^*(\alpha) f^*(g_j).$$

Si ha:

$$f(g_j) = f(1_G g_j) = h^*(1_G) f^*(g_j) = 1_{G'} f^*(g_j) = f^*(g_j), \ \forall g_j \in T.$$

Inoltre, l'applicazione f è $(h = h^*_{|A}, A, B)$-lineare. In effetti, h è un'applicazione da A in B perchè $h^*_{|A} \subset B$ e si ha:

$$f(ax) = f(a\alpha g_j) = h^*(a\alpha) f^*(g_j) = h^*(a) h^*(\alpha) f^*(g_j) =$$

$$= h^*(a) f(x) = h(a) f(x),$$

per ogni $a \in A$

Dunque $f(ax) = h(a) f(x)$, $\forall a \in A$, $x \in G$.

Se q è un'altra applicazione (h, A, B)-lineare tale che $q(g_j) = f^*(g_j)$, per ogni $g_j \in T$, allora, per la Proposizione 1.1 3), si ha:

$$q(x) = q(\alpha g_j) = h^*(\alpha) q(g_j) = h^*(\alpha) f^*(g_j) = f(\alpha g_j) = f(x).$$

per ogni $x = \alpha g_j \in G$ e $(\alpha, g_j) \in \ < A > \times T$.

Infine, sia h^* un monomorfismo e sia f^* iniettiva. Se $\{\alpha, \beta\} \subset< A >$, $\{g_i, g_j\} \subset T$, $x = \alpha g_i$ e $y = \beta g_j$, allora l'uguaglianza $f(x) = f(y)$ implica $h^*(\alpha) f^*(g_i) = h^*(\beta) f^*(g_j)$, quindi $< B > f^*(g_i) =< B > f^*(g_j)$. Del resto, essendo $\{f^*(g_i), f^*(g_j)\} \subset T'$ e T' un trasversale dei laterali sinistri di $< B >$ in G', si ha $f^*(g_i) = f^*(g_j)$, dunque $g_i = g_j$ e $h^*(\alpha) = h^*(\beta)$. Infine, si ottiene $\alpha = \beta$, perciò $x = \alpha g_i = \beta g_j = y$ ed f è iniettiva.

È anche facile dimostrare che la suriettività di h^* ed f^* comportano la suriettività di f.

Corollario 1.8. *Se $T = \{g_j\}_{j\in J}$ e T' sono due trasversali dei laterali sinistri di $< A >$ in G ed f^* è un'applicazione da T in T', allora esiste una sola applicazione (Id_A, A)-lineare f da G in G tale che $f(g_j) = f^*(g_j)$, per ogni $j \in J$. Inoltre, se f^* è biunivoca, allora anche f è biunivoca.*

Dimostrazione. Segue subito dal Teorema 1.6 prendendo $G = G'$ e $h^* = Id_{<A>}$.

Esempio 1. In crittografia esistono molteplici sistemi di cifratura chiamati a sostituzione e trasposizione la cui sicurezza resta essenzialmente affidata alla segretezza della chiave. Un tale sistema di cifratura si può ottenere nel modo seguente:

Si supponga che il testo in chiaro da cifrare sia costituito da una sequenza di n simboli $m_0, m_1, \ldots, m_{n-1}$ e sia $n = pq$ con p e q interi entrambi maggiori di 1. Sia $H =< q >$ il solo sottogruppo di $(Z_n, +)$ di ordine p e siano T, T' due trasversali dei laterali di H in Z_n. Considerata un'applicazione biunivoca f^* da T in T' ed un automorfismo η di H (in questo caso gli automorfismi di H sono determinati dai suoi generatori perché H è ciclico), si costruisce l'applicazione biunivoca completa $f : Z_n \to Z_n$ tale che $f(x) = \eta(\alpha) + f^*(g)$, essendo (α, g) la sola coppia di elementi di $H \times T$ tale che $x = \alpha + g$.

In queste ipotesi, se m_x è uno dei simboli che costituiscono il messaggio, il suo crittogramma è m_y se e solo se $f(x) = y$.

Ovviamente $(\eta(\alpha), f^*(g))$ è la sola coppia di $H \times T'$ tale che $y = \eta(\alpha) + f^*(g)$, così, noti η ed f^*, si determinano η^{-1} e $(f^*)^{-1}$ da cui si ricava $x = \alpha + g = \eta^{-1}(\eta(\alpha)) + (f^*)^{-1}(f(g))$.

Ad esempio, nel gruppo Z_{56}, il sottogruppo $H =< 7 >$ ha ordine otto e i suoi generatori sono 7, 21, 28. Il sottogruppo $T =< 8 >$ e l'insieme $T' = \{2, 3, 5, 7, 29, 39, 41\}$ sono due trasversali dei laterali di H in Z_{56}, così, considerato l'automorfismo η determinato da 21 e l'applicazione $f^* : T \to T'$ tale che :

$$f^*(0) = 2,\ f^*(8) = 3,\ f^*(16) = 5,\ f^*(24) = 41,$$
$$f^*(32) = 7,\ f^*(40) = 29,\ f^*(48) = 39,$$

si ricava l'applicazione f (η, H)-lineare corrispondente ad η ed f^*.

La tabella seguente va letta da sinistra a destra e dall'alto verso il basso, in essa sono state riportate le immagini degli elementi di Z_{56} mediante la

permutazione f:

23	17	12	41	0	15	18	30
24	19	48	7	22	25	37	31
26	55	14	29	32	44	38	33
6	21	36	39	51	45	40	13
28	43	46	2	52	47	20	35
50	53	9	3	54	27	42	1
4	16	10	5	34	49	8	11

La permutazione f trasforma il seguente messaggio:

(1.1) LE RAGIONI DI QUESTO SECONDO ESEMPIO VERRANNO CHIARITE PIÙ AVANTI

nella sequenza:

(1.2) OSUILTEOECINDSNVEISIEIORONNCVTHEPRERAPOAANDATMAEGOIIRUIQ

e la successione di bit:

(1.3) 01010000010100100100111101010110010000010101001001000101

ha per crittogramma la sequenza

(1.4) 11010001000011000111000101010000011000100111010100000101

La scelta di Z_{56} non è stata casuale, infatti la trascrizione (o codifica) di un testo si può eseguire ricorrendo ad uno dei codici in uso, come il codice ASCII in cui le lettere sono gruppi di otto bit e il numero di bit che compongono un testo è multiplo di otto. In linguaggio ASCII si ha:

A 01000001
E 01000101
O 01001111
P 01010000
R 01010010
V 01010110

e la (1. 3) è la trascrizione della parola PROVARE.

Proposizione 1.9. *Siano G un gruppo, K un sottogruppo di G, u un elemento di K e $C_K(u)$ il centralizzante in K di u. Se $C_K(u) \neq K$, allora esistono un sottoinsieme A di K e un'applicazione $f : G \to G$ tali che $A \cap u^{-1}Au = A \cap C_K(u) = u^{-1}Au \cap C_K(u) = \emptyset$ ed f è $(h, A \cup C_K(u), u^{-1}Au \cup C_K(u))$-lineare completa con omomorfismo generatore l'automorfismo interno h^* di K determinato da u.*

Dimostrazione. Si supponga che il sottogruppo K abbia cardinalità infinita e sia

$$B = \{X \mid \emptyset \neq X \subset K,\ X \cap u^{-1}Xu = \emptyset\}.$$

B è non vuoto perchè $\{b\} \in B$, per ogni $b \in K - C_K(u)$. Inoltre, l'insieme ordinato $(B, \subseteq)$ è induttivo. Infatti, sia $C = \{X_i\}_{i \in I}$ una catena di elementi di B e si consideri l'insieme $X = \bigcup_{i \in I} X_i$. Se esiste $x \in X \cap u^{-1}Xu$, allora esistono due indici i e j di I tali che $X_i \cap u^{-1}X_j u \neq \emptyset$, e posto $r = \max\{i, j\}$, si ha $\emptyset \neq X_i \cap u^{-1}X_j u \subseteq X_r \cap u^{-1}X_r u$, impossibile. Dunque $X \in B$, cioè ogni catena di elementi di B ammette in B un maggiorante. In virtù del lemma di Zorn esiste in B un elemento massimale A. Ora, se esiste un elemento $b \in K - (A \cup u^{-1}Au \cup uAu^{-1} \cup C_K(u))$, posto $A' = \{b\} \cup A$, si ha:

$$A' \cap u^{-1}A'u = (\{b\} \cap \{u^{-1}bu\}) \cup (\{b\} \cap u^{-1}Au) \cup (A \cap \{u^{-1}bu\}) \cup (A \cap u^{-1}Au) = \emptyset,$$

impossibile per la massimalità di A in B. Pertanto, si ha

$$K = A \cup u^{-1}Au \cup uAu^{-1} \cup C_K(u),$$

da cui si ricava

$$K = < A \cup C_K(u) > = < u^{-1}Au \cup C_K(u) >,$$

con $A \cap u^{-1}Au = A \cap C_K(u) = u^{-1}Au \cap C_K(u) = \emptyset$.

Si ottiene lo stesso risultato anche nel caso in cui K ha cardinalità finita; basta prendere un sottoinsieme A di cardinalità massima tra gli insiemi della famiglia B.

Infine, se $h^* : x \mapsto u^{-1}xu$ è l'automorfismo interno di K determinato da u ed inoltre T è un trasversale dei laterali sinistri di K in G e f^* è un'applicazione da T in T, allora, per il Teorema 1.7, esiste un'applicazione $(h, A \cup C_K(u), u^{-1}Au \cup C_K(u))$-lineare con omomorfismo generatore l'automorfismo h^*. L'applicazione f è completa perché

$$h^*(A \cup C_K(u)) = h^*(A) \cup h^*(C_K(u)) = u^{-1}Au \cup C_K(u).$$

2. Il gruppo delle applicazioni (h, A)-lineari biunivoche complete.

Nel sistema di cifratura descritto nel primo paragrafo l'indice del sottogruppo H è sette e il numero dei trasversali dei laterali di H in Z_{56} è $8^7 = 2^{21}$. Le permutazioni degli elementi di un qualunque trasversale sono 7! ed esistono $7!2^{42}$ applicazioni biunivoche tra i trasversali di H in Z_{56}. Siccome H possiede tre automorfismi, si può erroneamente pensare che le possibili coppie (η, f^*), che permettono di costruire le applicazioni f, siano $7!2^{42}3$. In effetti si dimostrerà che nella scelta delle applicazioni f^* ci si può limitare a quelle aventi per dominio un prefissato trasversale, per cui le applicazioni f, come pure le possibili chiavi del sistema di cifratura, sono $7!2^{21}3$. Da notare che fissato il trasversale $T = \{0, 8, 16, 24, 32, 40, 48\}$, la chiave utilizzata nell'esempio 1 si può trascrivere nella forma (21, (2, 3, 5, 41, 7, 29, 39)).

Si osservi inoltre che per cifrare il messaggio (1.1) è possibile utilizzare applicazioni biunivoche complete costruite considerando gli altri sottogruppi propri e non banali di Z_{56}. Più in generale si può anche ipotizzare di dotare l'insieme $\{0, 1, \ldots, n-1\}$ di una struttura di gruppo che non sia isomorfo a Z_n, quindi ha senso approfondire lo studio delle applicazioni (h, A)-lineari su un generico gruppo G.

Sia $\Lambda(G_A)$ l'insieme delle applicazioni (h, A)-lineari biunivoche complete di un gruppo G rispetto ad un suo sottoinsieme non vuoto A. È immediato verificare che l'identità Id_G è un'applicazione (Id_A, A)-lineare biunivoca completa, del resto, per le Proposizioni 1.5 e 1.6, per ogni coppia (f, g) di applicazioni (h, A)-lineari biunivoche complete, la composizione $g \circ f$ e l'inversa f^{-1} di f sono a loro volta applicazioni (h, A)-lineri biunivoche complete, perciò l'insieme $\Lambda(G_A)$ è un sottogruppo del gruppo S_G delle permutazioni di G.

Inoltre, l'insieme $\Lambda_{Id_A}(G_A)$ delle applicazioni biunivoche complete con applicazione generatrice Id_A è un sottogruppo di $\Lambda(G_A)$. Infatti per ogni coppia (g, f) di elementi di $\Lambda_{Id_A}(G_A)$, $g \circ f^{-1}$ è ancora un'applicazione (Id_A, A)-lineare. Infine, $\Lambda_{Id_A}(G_A)$ è un sottogruppo normale di $\Lambda(G_A)$, in effetti, per ogni $f \in \Lambda_{Id_A}(G_A)$ e per ogni $g \in \Lambda(G_A)$, se h è l'applicazione generatrice di g, allora $h \circ Id_A \circ h^{-1} = Id_A$, per cui $g \circ f \circ g^{-1} \in \Lambda_{Id_{<A>}}(G_A)$.

Immediata conseguenza delle Proposizioni 1.1 3) e 1.6 1) è la seguente:

Proposizione 2.1. *Sia G un gruppo e siano A, B due sottoinsiemi non vuoti di G tali che $B \subset A$ e $h^*(B) = B$, $h^*(A) = A$, per ogni automorfismo h^* di $< A >$. Se $< A >=< B >$, allora $\Lambda(G_B) = \Lambda(G_A)$.*

Nei prossimi teoremi si analizzerà la struttura del gruppo $\Lambda(G_A)$, ma prima si premette la seguente definizione:

Definizione. Se A è un sottoinsieme di G e T, T' sono due trasversali dei

laterali sinistri di $< A >$ in G e inoltre h^* e f^* sono, rispettivamente, un automorfismo di $< A >$ tale che $h^*(A) = A$ e un'applicazione biunivoca da T in T', allora l'applicazione $(h^*_{|A}, A)$-lineare biunivoca completa, corrispondente a h^* ed f^* e costruita utilizzando il Teorema 1.7, si dirà *di tipo* (h^*, f^*, T, T').

Lemma 2.2. *Siano $f, t : G \to G$ due applicazioni rispettivamente di tipo (h^*, f^*, T, T') e $(k^*, t^*, T, T")$, allora $f = t$ se e solo se $h^* = k^*$ e $f^* = t^*$.*

Dimostrazione. Per la Proposizione 1.3 , $f = t$ implica $h^* = k^*$. Inoltre, per il Teorema 1.7, $f^*(g_i) = f(g_i) = t(g_i) = t^*(g_i)$, per ogni $g_i \in T$, quindi si ha $T' = T"$ e $f^* = t^*$ perché $f^* : T \to T'$ e $t^* : T \to T"$ sono entrambe biunivoche.

Teorema 2.3. *Siano G un gruppo, A un sottoinsieme non vuoto di G, F la famiglia dei trasversali dei laterali sinistri di $< A >$ in G e $Aut_A(< A >)$ il gruppo degli automorfismi h^* di $< A >$ tali che $h^*(A) = A$. Inoltre, per ogni coppia $(h^*, T) \in Aut_A(< A >) \times F$, sia*

$$\Lambda_{h^*,T}(G_A) = \{f \in \Lambda(G_A) \mid \exists T' \in F,\ \exists f^* : T \to T',\ f \text{ sia di tipo } (h^*, f^*, T, T')\},$$

allora:

1) Fissato $T \in F$, la famiglia $\{\Lambda_{h^*,T}(G_A)\}_{h^* \in Aut_A(<A>)}$ è una partizione di $\Lambda(G_A)$.

2) Se G è finito, allora

i) $|\Lambda_{h^*,T}(G_A)| = [G :< A >]!| < A > |^{[G:<A>]}$, $\forall h^* \in Aut_A(< A >)$;

ii) $|\Lambda(G_A)| = [G :< A >]!| < A > |^{[G:<A>]} |Aut_A(< A >)|$.

Dimostrazione. 1) Per il Teorema 1.7 è ovvio che $\Lambda_{h^*,T}(G_A) \neq \emptyset$ e che

$$\bigcup_{h^* \in Aut_A(<A>)} \Lambda_{h^*,T}(G_A) \subset \Lambda(G_A).$$

Inoltre, se $f : G \to G$ è un'applicazione (h, A)-lineare biunivoca completa, per la Proposizione 1.6 1), l'omomorfismo generatore h^* è un automorfismo di $< A >$ tale che $h^*(A) = A$, perché $h^*_{|A} = h$ e h è suriettiva. Ora, posto $T = \{g_i\}_{i \in I}$, per il Corollario 1.2 2), si ha $f(< A > g_i) =< A > f(g_i)$, per ogni $i \in I$, e poichè f è biunivoca, l'insieme $T' = \{f(g_i)\}_{i \in I}$ è un trasversale dei laterali sinistri di $< A >$ in G. Pertanto, se $f^* : T \to T'$ è tale che $f^*(g_i) =$

$f(g_i)$, per ogni $i \in I$, l'applicazione (h, A)-lineare biunivoca completa di tipo (h^*, f^*, T, T'), coincide con f, per cui $f \in \Lambda_{h^*,T}(G_A)$. Dunque

$$\Lambda(G_A) \subset \bigcup_{h^* \in Aut_A(<A>)} \Lambda_{h^*,T}(G_A).$$

Infine, per il Lemma 2.2, $\Lambda_{h^*,T}(G_A) \cap \Lambda_{k^*,T}(G_A) = \emptyset$, per ogni coppia (h^*, k^*) di elementi distinti di $Aut_A(< A >)$, dunque $\{\Lambda_{h^*,T}(G_A)\}_{h^* \in Aut_A(<A>)}$ è una partizione di $\Lambda(G_A)$.

2) Si consideri un automorfismo $h^* \in Aut_A(< A >)$ e un trasversale $T \in F$.

Se $[G :< A >] = m$, allora $|F| = | < A > |^m$, inoltre, per ogni $T' \in F$, esistono $m!$ applicazioni biunivoche $f^* : T \to T'$ a cui corrispondono altrettante applicazioni biunivoche complete di tipo (h^*, f^*, T, T'). Del resto, se $T" \neq T'$, le applicazioni biunivoche da T in T' sono distinte dalle applicazioni biunivoche da T in $T"$, così, per il Lemma 2.2, anche le corrispondenti applicazioni biunivoche complete di tipo (h^*, f^*, T, T') sono distinte da quelle di tipo $(h^*, f^*, T, T")$. Dunque $|\Lambda_{h^*,T}(G_A)| = m!| < A > |^m = [G :< A >]!| < A > |^{[G:<A>]}$ e ciò prova i).

Infine, da 1) e i), si ricava

$$|\Lambda(G_A)| = [G :< A >]!| < A > |^{[G:<A>]} |Aut_A(< A >)|.$$

Corollario 2.4. *Se G è un gruppo finito ed A è un insieme di generatori di G, allora $|\Lambda(G_A)| = |G||Aut_A(G)|$.*

Corollario 2.5. *Se G è un gruppo finito ed H è un sottogruppo di G, allora:*

$$|\Lambda(G_H)| = [G : H]!|H|^{[G:H]}|Aut(H)|.$$

Immediata conseguenza del Teorema 1.7 e delle Proposizioni 1.5, 1.6 2) e 1.1 3), è il seguente:

Lemma 2.6. *Siano $f, g : G \to G$ due applicazioni rispettivamente di tipo (h^*, f^*, T, T') e $(k^*, g^*, T', T")$, allora:*

1) *f^{-1} è di tipo $(h^{*-1}, (f^*)^{-1}, T', T)$;*
2) *$g \circ f$ è di tipo $(k^* \circ h^*, g^* \circ f^*, T, T")$.*

Teorema 2.7. *Sia G un gruppo, A un sottoinsieme non vuoto di G e T un trasversale dei laterali sinistri di A in G, allora esiste un sottoinsieme Q di $\Lambda(G_A)$ tale che $\Lambda(G_A)$ sia prodotto semidiretto di $\Lambda_{Id_{<A>},T}(G_A)$ mediante $< Q >$.*

Dimostrazione. Si incominci ad osservare che se $f : G \to G$ è un'applicazione (h, A)-lineare biunivoca completa, l'applicazione generatrice h è uguale a Id_A se e solo se l'omomorfismo generatore h^* di f è $Id_{<A>}$, per cui l'insieme $\Lambda_{Id_{<A>},T}(G_A)$ coincide con il gruppo $\Lambda_{Id_A}(G_A)$ delle applicazioni (Id_A, A)-lineari biunivoche complete, dunque è un sottogruppo normale di $\Lambda(G_A)$.

Per ogni $\eta \in Aut_A(< A >)$, sia q_η l'applicazione biunivoca completa di tipo (η, Id_T, T, T). Si ponga $Q = \{q_\eta\}_{\eta \in Aut_A(<A>)}$. Fissato $\eta \in Aut_A(< A >)$, per ogni $\delta \in \Lambda_{\eta,T}(G_A)$, esiste un trasversale T' dei laterali sinistri di $< A >$ in G e un'applicazione biunivoca $\delta^* : T \to T'$ tale che δ sia di tipo (η, δ^*, T, T'). Sia $f_\delta : G \to G$ l'applicazione biunivoca completa di tipo $(Id_{<A>}, \delta^*, T, T')$. Ovviamente $f_\delta \in \Lambda_{Id_{<A>},T}(G_A)$, inoltre, per ogni $x = \alpha g_j \in G$, con $\alpha \in < A >$ e $g_j \in T$, si ha:

$$f_\delta \circ q_\eta(x) = f_\delta(q_\eta(\alpha g_j)) = f_\delta(\eta(\alpha) Id_T(g_j)) = f_\delta(\eta(\alpha) g_j) =$$

$$= \eta(\alpha)\delta^*(g_j) = \delta(\alpha g_j) = \delta(x),$$

quindi $\delta = f_\delta \circ q_\eta \in (\Lambda_{Id_{<A>},T}(G_A)) \circ < q_\eta >$.

Dunque,

$$\Lambda_{\eta,T}(G_A) \subset (\Lambda_{Id_{<A>},T}(G_A)) \circ < q_\eta > \subset (\Lambda_{Id_{<A>},T}(G_A)) \circ < Q >,$$

per ogni $\eta \in Aut_A(< A >)$. Pertanto, per il Teorema 2.3 1), si ha

$$\Lambda(G_A) = (\Lambda_{Id_{<A>},T}(G_A)) \circ < Q > .$$

Del resto, per ogni $f \in < Q >$, esistono $n \in N^*$, $(\eta_1, \eta_2, \ldots, \eta_n) \in Q^n$ e $(r_1, r_2, \ldots, r_n) \in Z^n$ tali che $f = q_{\eta_1}^{r_1} \circ q_{\eta_2}^{r_2} \circ \ldots \circ q_{\eta_n}^{r_n}$, così, per il Lemma 2.6, l'applicazione f è di tipo

$$(\eta_1^{r_1} \circ \eta_2^{r_2} \circ \ldots \circ \eta_n^{r_n}, (Id_T)^{r_1} \circ (Id_T)^{r_2} \circ \ldots \circ (Id_T)^{r_n}, T, T),$$

cioè di tipo $(\eta_1^{r_1} \circ \eta_2^{r_2} \circ \ldots \circ \eta_n^{r_n}, Id_T, T, T)$. Ora, se $f \in \Lambda_{Id_{<A>},T}(G_A) \cap < Q >$, allora $\eta_1^{r_1} \circ \eta_2^{r_2} \circ \ldots \circ \eta_n^{r_n} = Id_{<A>}$ e di conseguenza f è di tipo $(Id_{<A>}, Id_T, T, T)$, cioè $f = Id_G$. Pertanto $< Q >$ è un complemento di $\Lambda_{Id_{<A>},T}(G_A)$ in $\Lambda(G_A)$, perciò $\Lambda(G_A)$ è prodotto semidiretto di $\Lambda_{Id_{<A>},T}(G_A)$ mediante $< Q >$.

Corollario 2.8. *Sia G un gruppo ed A un sottoinsieme di generatori di G tale che $Aut_A(G) = \{Id_G\}$, allora $\Lambda(G_A) \cong G$.*

Dimostrazione. Essendo $< A >= G$ e $Aut_A(G) = \{Id_G\}$, per il Teorema 2.7, si ha

$$\Lambda(G_A) = \Lambda_{\{Id_G\},\{1_G\}}(G_A)$$

(si prenda $Q = \{Id_G\}$ e $T = \{1_G\}$).

Per il Teorema 1.7, per ogni $x \in G$, esiste una sola applicazione biunivoca completa $f : G \to G$ che ha per omomorfismo generatore Id_G e tale che $f(1_G) = f^*(1_G) = x$, essendo f^* la sola applicazione possibile da $\{1_G\}$ in $\{x\}$. Dunque l'applicazione $\psi : \Lambda(G_A) \to G$ tale che $\psi(f) = f(1_G)$ è biunivoca. Infine, se f e g sono due elementi di $\Lambda(G_A)$, rispettivamente, di tipo $(Id_G, f^*, \{1_G\}, \{x\})$ e $(Id_G, g^*, \{1_G\}, \{y\})$, allora

$$\psi(g \circ f) = g \circ f(1_G) = g(f(1_G)) = g(f(1_G)1_G) =$$

$$= Id_G(f(1_G))g^*(1_G) = f(1_G)g(1_G) = \psi(f)\psi(g).$$

Quindi $\Lambda(G_A) \cong G$.

Corollario 2.9. *Sia G è un gruppo ciclico ed A è un sottoinsieme di G che contiene un solo generatore λ di G, allora $\Lambda(G_A) \cong G$.*

Dimostrazione. Sia E_G l'insieme dei generatori di G. Se $A \cap E_G = \{\lambda\}$ e η è un automorfismo di G tale che $\eta(A) = A$, allora

$$\eta(A \cap E_G) = \eta(A) \cap \eta(E_G) = A \cap E_G,$$

per cui $\eta(\lambda) = \lambda$ e $\eta = Id_G$. Dunque $Aut_A(< A >) = Aut_A(G) = \{Id_G\}$ e $\Lambda(G_A) \cong G$ (Corollario 2.8).

Osservazione. Se G è un gruppo, il prodotto cartesiano $Aut(G) \times G$ è un gruppo rispetto all'operazione: $(h^*, x)(k^*, y) = (h^* \circ k^*, h^*(y)x)$, $\forall\{(h^*, x), (k^*, y)\} \subset Aut(G) \times G$. Tale gruppo si chiama prodotto semi-diretto di G mediante il gruppo $Aut(G)$ relativamente all'omomorfismo $\varphi = Id_{Aut(G)}$. Si indica con $Aut(G) \times_\varphi G$.

Teorema 2.10. *Sia G un gruppo ed A un sottoinsieme di generatori di G. Se $Aut_A(G) = Aut(G)$, allora $\Lambda(G_A) \cong Aut(G) \times_\varphi G$.*

Dimostrazione. I trasversali di $< A >$ in G sono i singleton $\{x\}$ degli elementi di G, perché $< A >= G$. Posto $T = \{1_G\}$, per ogni automorfismo h^* di G e per ogni $x \in G$, esiste una sola applicazione biunivoca completa $f_{h^*,x} : G \to G$ tale che $f_{h^*,x}(1_G) = x$. L'applicazione $f_{h^*,x}$ è di tipo $(h^*, f^*, T, \{x\})$, essendo $f^* : T \to \{x\}$ la sola applicazione possibile da $T = \{1_G\}$ in $\{x\}$.

Dunque è ben definita l'applicazione $\psi : Aut(G) \times_\varphi G \to \Lambda(G_A)$ tale che:

$$\psi(h^*, x) = f_{h^*,x}, \quad \forall (h^*, x) \in Aut(G) \times G.$$

Per il Teorema 2.3 1), ψ è suriettiva. Inoltre, per il Lemma 2.2, se $f_{h^*,x} = f_{k^*,y}$, allora $h^* = k^*$ e $x = f_{h^*,x}(1_G) = f_{k^*,y}(1_G) = y$, per cui $(h^*, x) = (k^*, y)$, quindi ψ è anche iniettiva. Infine,

$$f_{h^*,x} \circ f_{k^*,y}(1_G) = f_{h^*,x}(f_{k^*,y}(1_G)) = f_{h^*,x}(y) =$$
$$= f_{h^*,x}(y1_G) = h^*(y) f_{h^*,x}(1_G) = h^*(y)x,$$

e per la Proposizione 1.5, si ha $f_{h^*,x} \circ f_{k^*,y} = f_{h^* \circ k^*, h^*(y)x}$. Dunque

$$\psi((h^*, x)(k^*, y)) = \psi(h^* \circ k^*, h^*(y)x) =$$
$$= f_{h^* \circ k^*, h^*(y)x} = f_{h^*,x} \circ f_{k^*,y} = \psi((h^*, x)) \circ \psi((k^*, y)),$$

così $\Lambda(G_A) \cong Aut(G) \times_\varphi G$.

Proposizione 2.11. *Se G è un gruppo ciclico finito generato da λ ed A è un sottoinsieme di generatori di G tale che $Aut_A(G) = \{Id_G\}$, allora $\Lambda(G_A) = \Lambda(G_\lambda)$.*

Dimostrazione. Per il Teorema 3.6 di [10] e il Corollario 2.8, si ha $\Lambda(G_A) \cong G \cong \Lambda(G_\lambda)$, quindi $|\Lambda(G_A)| = |\Lambda(G_\lambda)|$. Inoltre, se g è un'applicazione (h, A)-lineare biunivoca completa, l'omomorfismo generatore h^* di g è un automorfismo di $< A >= G$ tale che $h^*(A) = h(A) = A$, perciò $h^* = Id_G$ perché $Aut_A(G) = \{Id_G\}$. Ora, per ogni $a \in A$, esiste $m \in Z$ tale che $a = \lambda^m$, sicchè, per ogni $f \in \Lambda(G_\lambda)$ e $x \in G$, si ha:

$$f(ax) = f(\lambda^m x) = \lambda^m f(x) = af(x) = Id_G(a) f(x),$$

pertanto $f \in \Lambda(G_A)$ e dunque $\Lambda(G_\lambda) \subset \Lambda(G_A)$.

Vedremo adesso come i precedenti teoremi permettono di determinare, ad esempio, i gruppi $\Lambda((Z_6)_A)$ per tutti i sottoinsiemi non vuoti A di Z_6.

Esempio 2. Le parti non vuote A di Z_6 si possono classificare in modo da distinguere i seguenti cinque casi:

1) A è un singleton.

2) A contiene un solo generatore di Z_6 oppure A è uno dei seguenti dodici insiemi: $\{2,3\}$, $\{3,4\}$, $\{0,2,3\}$, $\{0,3,4\}$, $\{1,2,5\}$, $\{1,4,5\}$, $\{0,1,2,5\}$, $\{0,1,4,5\}$, $\{1,2,3,5\}$ $\{1,3,4,5\}$, $\{0,1,2,3,5\}$, $\{0,1,3,4,5\}$.

3) A è uno dei seguenti dieci insiemi: $\{1,5\}$ $\{0,1,5\}$, $\{1,3,5\}$, $\{2,3,4\}$, $\{0,1,3,5\}$, $\{0,2,3,4\}$, $\{1,2,4,5\}$, $\{0,1,2,4,5\}$, $\{1,2,3,4,5\}$, Z_6.

4) $A \in \{\{0,2\},\{0,3\},\{0,4\}\}$.

5) $A \in \{\{2,4\},\{0,2,4\}\}$.

Caso 1. Se A è il singleton $\{\lambda\}$, allora le applicazioni A-lineari biunivoche complete sono le applicazioni biunivoche λ-lineari di Z_6, così, dall'Esempio 8 di [10], si ricava:

$$\Lambda((Z_6)_{\{0\}}) \cong S_6.$$

$$\Lambda((Z_6)_{\{1\}}) \cong \Lambda((Z_6)_{\{5\}}) \cong Z_6.$$

$$\Lambda((Z_6)_{\{4\}}) \cong \Lambda((Z_6)_{\{2\}}).$$

Le tre permutazioni di Z_6 : $t = (0,1)(2,3)(4,5)$, $p = (1,3,5)$ e $q = (0,2,4)$ appartengono a $\Lambda((Z_6)_{\{2\}})$ e sono tali che $< p,q > \triangleleft \Lambda((Z_6)_{\{2\}})$, $< p,q > \cap < t >= \{Id_{Z_6}\}$ e $\Lambda((Z_6)_{\{2\}}) =< t >< p,q >$, cioè $\Lambda((Z_6)_{\{2\}})$ è prodotto semidiretto di $< p,q >$ mediante $< t >$. Inoltre $< p,q > \cong Z_3^2$ e $< t > \cong Z_2$.

$\Lambda((Z_6)_{\{3\}}) =< \alpha > N$, dove α è il ciclo: $\alpha = (0,1,2,3,4,5)$ ed N è un sottogruppo normale di $\Lambda((Z_6)_{\{3\}})$ tale che $< \alpha > \cap N = \{Id_{Z_6}\}$. Inoltre $< \alpha > \cong Z_6$ e $N \cong Z_2^3$.

Caso 2. Se A contiene un solo generatore oppure A è uno dei dodici insiemi considerati, allora, applicando il Corollario 2.9 o il Corollario 2.8, si ha $\Lambda((Z_6)_A) \cong Z_6$.

Caso 3. Gli automorfismi di Z_6 sono le due applicazioni: Id_{Z_6} e $h^* = (1,5)(2,4)$. È immediato verificare che in questo caso i nove insiemi soddisfano le ipotesi del Teorema 2.10, per cui $\Lambda((Z_6)_A) \cong Aut(Z_6) \times_\varphi Z_6$.

Caso 4. Sono verificate le ipotesi della Proposizione 2.1, quindi $\Lambda((Z_6)_{\{0,2\}}) \cong \Lambda((Z_6)_{\{2\}}) \cong \Lambda((Z_6)_{\{4\}}) \cong \Lambda((Z_6)_{\{0,4\}})$ e $\Lambda((Z_6)_{\{0,3\}}) \cong \Lambda((Z_6)_{\{3\}})$.

Caso 5. I due insiemi $B = \{2,4\}$ e $A = \{0,2,4\}$ verificano le ipotesi della Proposizione 2.1, perciò $\Lambda((Z_6)_{\{0,2,4\}}) \cong \Lambda((Z_6)_{\{2,4\}})$.

Il sottogruppo $< B >= \{0, 2, 4\}$ ha due soli automorfismi: $Id_{<B>}$ e il ciclo $\eta = (2, 4)$; entrambi fissano il sottoinsieme B. Posto $T = \{0, 1\}$, per il Teorema 2.3, si ha $\Lambda((Z_6)_B) = \Lambda_{Id_{<B>},T}((Z_6)_B) \bigcup \Lambda_{\eta,T}((Z_6)_B)$ e $|\Lambda((Z_6)_B)| = 2!3^2 2 = 2^2 3^2$.

Considerando i nove trasversali: $T_1 = T = \{0, 1\}$, $T_2 = \{0, 3\}$, $T_3 = \{0, 5\}$, $T_4 = \{1, 2\}$, $T_5 = \{2, 3\}$, $T_6 = \{2, 5\}$, $T_7 = \{1, 4\}$, $T_8 = \{3, 4\}$, $T_9 = \{4, 5\}$, si costruiscono 18 applicazioni biunivoche $f^* : T \to T_k$.

L'equazione $f(\alpha + g_j) = h^*(\alpha) + f^*(g_j)$, $\forall(\alpha, g_j) \in < B > \times T$ (vedi dimostrazione Teorema 1.7) porge:

$$\begin{cases} f(0) = f^*(0); \\ f(1) = f^*(1); \\ f(2) = 2 + f^*(0); \\ f(3) = 2 + f^*(1); \\ f(4) = 4 + f^*(0); \\ f(5) = 4 + f^*(1). \end{cases} \qquad \text{se } h^* = Id_{<B>}$$

$$\begin{cases} f(0) = f^*(0); \\ f(1) = f^*(1); \\ f(2) = 4 + f^*(0); \\ f(3) = 4 + f^*(1); \\ f(4) = 2 + f^*(0); \\ f(5) = 2 + f^*(1). \end{cases} \qquad \text{se } h^* = \eta$$

da cui, al variare di f^*, si ottengono le applicazioni biunivoche complete rispettivamente di $\Lambda_{Id_{<B>},T}((Z_6)_B)$ e $\Lambda_{\eta,T}((Z_6)_B)$.

L'insieme $X = \{\eta\}$ genera $Aut_B(< B >)$ e l'applicazione biunivoca completa di tipo (η, Id_T, T, T) corrispondente a η e Id_T è la permutazione $q_\eta = (2, 4)(3, 5)$. Per il Teorema 2.7, $\Lambda(G_B)$ è prodotto semidiretto di $\Lambda_{Id_{<B>},T}((Z_6)_B)$ mediante $< q_\eta >$. Si osservi che $< q_\eta > \cong Z_2$ perchè $|q_\eta| = 2$.

La permutazione $c = (0, 2, 4)(1, 3, 5)$ appartiene ad

$$N = \Lambda_{Id_{<B>},T}((Z_6)_B)$$

e ha ordine $|c| = 3$. È facile verificare che il sottogruppo $< c >$ è il centro $Z(N)$ di N.

Le due permutazioni: $a = (0, 1)(2, 3)(4, 5)$, $b = (1, 3, 5)$ appartengono a N e hanno ordine: $|a| = 2$, $|b| = 3$. Ovviamente $< b > \cap < c >= \{Id_{Z_6}\}$, dunque $< b, c > =< b >< c > \cong Z_3^2$ e $[N :< b, c >] = 2$, per cui il sottogruppo $< b, c > =< b >< c >$ è normale in N. Infine, siccome $a \notin < b, c >$, si ha $| < a >< b, c > | = 3^2 2 = |N|$, quindi

$N = < a >< b, c >$, cioè N è prodotto semidiretto di $< b, c >$ mediante $< a >$.

Il gruppo $\Lambda((Z_6)_B)$ ammette la seguente serie di composizione:

$$\{Id_{Z_6}\} \triangleleft < c > \triangleleft < b, c > \triangleleft N \triangleleft \Lambda((Z_6)_B).$$

Esempio 3. Il gruppo $(Z, +)$ ha due soli automorfismi: Id_Z e l'applicazione $\eta : Z \to Z$ tale che $\eta(n) = -n$, per ogni $n \in Z$.

Se A è un insieme di generatori di Z, si distinguono i due casi.

1) $\exists X \subset A$ tale che $A = X \cup (-X)$;

2) $A \neq X \cup (-X)$, $\forall X \in P(A)$.

Nel primo caso si ha $Aut_A(Z) = Aut(Z)$. Applicando il Teorema 2.10, si ottiene $\Lambda(Z_A) \cong Aut(Z) \times_\varphi Z$.

Nel secondo caso si ricava $Aut_A(Z) = \{Id_Z\}$, da cui, per il Corollario 2.8, si ha $\Lambda(Z_A) \cong Z$.

Se A non genera Z, si distinguono i casi:

3) $A = \{0\}$.

4) $\{0\} \neq < A > \neq Z$.

Se $A = \{0\}$, il gruppo $\Lambda(Z_A)$ coincide col gruppo S_Z delle permutazioni di Z, in effetti $f(0+x) = f(x) = 0 + f(x)$, per ogni $x \in Z$ e per ogni applicazione biunivoca $f : Z \to Z$.

Se $\{0\} \neq < A > \neq Z$, allora esiste un intero $n > 1$ tale che $< A > = nZ$. Inoltre, si ha: $Aut_A(nZ) = Aut(Z)$ oppure $Aut_A(nZ) = \{Id_Z\}$, perché $nZ \cong Z$. Pertanto, considerato il trasversale $T = \{0, 1, 2, \ldots, n-1\}$, si ottiene:

i) $\Lambda(Z_A) = \Lambda_{Id_{nZ},T}(Z_A) \circ < q_{\eta'} >$ se $Aut_A(nZ) = Aut(Z)$;

ii) $\Lambda(Z_A) = \Lambda_{Id_{nZ},T}$ se $Aut_A(nZ) = \{Id_Z\}$.

Si osservi che η' è l'automorfismo di nZ tale che $\eta'(nx) = -nx$, per ogni $x \in Z$, e $q_{\eta'}$ è l'applicazione biunivoca completa di tipo (η', Id_T, T, T). Ovviamente $< q_{\eta'} > \cong Z_2$.

3. M_A-ipergruppoidi. Una generalizzazione della nozione di applicazione (h, A, B)-lineare.

Negli articoli [9] e [10] sono state studiate le principali proprietà di un M_λ-ipergruppoide: Assegnato un gruppo G che opera a sinistra su un insieme M mediante l'azione $\varphi : (x, a) \mapsto xa$ e fissato un elemento $\lambda \in G$, si definisce su M l'iperprodotto:

$$a \bullet b = b \bullet a = \{\lambda a, \lambda b\}, \quad \forall (a, b) \in M^2. \tag{3.1}$$

L'insieme M munito dell'iperprodotto $\bullet$ è un H_V-gruppo, cioè soddisfa le due proprietá:

$$\forall (a, b, c) \in M^3, \quad (a \bullet b) \bullet c \cap a \bullet (b \bullet c) \neq \emptyset; \tag{3.2}$$

$$\forall a \in M, \quad a \bullet M = M \bullet a = M. \tag{3.3}$$

$(M, \bullet)$ si chiama M_λ-ipergruppoide e con abuso di notazione si utilizza il simbolo M_λ per indicare non solo il sostegno M, ma anche lo stesso H_V-gruppo.

La definizione di M_λ-ipergruppoide ammette in modo del tutto naturale la seguente generalizzazione: Considerato un sottoinsieme non vuoto A di G, si definisce su M il seguente iperprodotto:

$$x \bullet y = y \bullet x = Ax \cup Ay, \quad \forall (x, y) \in M^2, \tag{3.4}$$

essendo $Az = \{az \mid a \in A\}$, per ogni $z \in M$.

L'ipergruppoide $(M, \bullet)$ soddisfa le due proprietà (3.2) e (3.3). In effetti, per ogni terna (x, y, z) di elementi di M, si ha $(x \bullet y) \bullet z = (AA)x \cup (AA)y \cup Az$ e $x \bullet (y \bullet z) = Ax \cup (AA)y \cup (AA)z$, quindi $(AA)y \subset (x \bullet y) \bullet z \cap x \bullet (y \bullet z)$. Inoltre, preso $a \in A$, si ha:

$$y = (aa^{-1})y = a(a^{-1}y) \in A(a^{-1}y) \subset Ax \cup A(a^{-1}y) = \\ = x \bullet (a^{-1}y) \in x \bullet M = M \bullet x$$

dunque $M = x \bullet M = M \bullet x$.

$(M, \bullet)$ si chiama M_A-ipergruppoide e si utilizza il simbolo M_A per indicare oltre al sostegno M anche lo stesso ipergruppoide.

Proposizione 3.1. *Se A è un sottoinsieme non vuoto di G tale che $AA = A$, allora M_A è un ipergruppo. Se in particolare A è un sottogruppo di G, allora M_A è un Join Space (vedi* [13]*).*

Dimostrazione. Se $AA = A$, per ogni terna (x, y, z) di elementi di M, si ha

$$(x \bullet y) \bullet z = (AA)x \cup (AA)y \cup Az = Ax \cup Ay \cup Az = \\ = Ax \cup (AA)y \cup (AAz) = x \bullet (y \bullet z),$$

dunque M_A è un ipergruppo commutativo.

Adesso, sia A un sottogruppo di G. Per ogni coppia (x, y) di elementi di M_A, si ha

$$x/y = \{m \in M \mid x \in m \bullet y\} = \{m \in M \mid x \in Am \cup Ay\},$$

per cui $m \in x/y \Leftrightarrow x \in Am$ oppure $x \in Ay$. Pertanto, se $x \in Ay$, allora $x/y = M$. Mentre, se $x \notin Ay$, allora

$$m \in x/y \Leftrightarrow x \in Am \Leftrightarrow m \in A^{-1}x \Leftrightarrow m \in Ax,$$

per cui $x/y = Ax$.

Infine, per ogni quadrupla (x, y, z, w) di elementi di M, se $x \in Ay$ oppure $z \in Aw$, allora $Ax = Ay$ oppure $Az = Aw$ e inoltre $x/y = M$ oppure $z/w = M$, per cui $x/y \cap z/w \neq \emptyset \neq x \bullet w \cap y \bullet z$. Mentre, se $x \notin Ay$ e $z \notin Aw$, allora $x/y = Ax$ e $z/w = Az$, quindi, supponendo che $x/y \cap z/w \neq \emptyset$, si ha $Ax \cap Az \neq \emptyset$, da cui $Ax = Az$, perciò $x \bullet w \cap y \bullet z \neq \emptyset$. Pertanto, in ogni caso,

$$x/y \cap z/w \neq \emptyset \Rightarrow x \bullet w \cap y \bullet z \neq \emptyset,$$

sicchè M_A è un Join Space.

Nell'articolo [10] si è analizzato il gruppo degli automorfismi di un M_λ-ipergruppoide e si è dimostrato che gli automorfismi di M_λ sono le applicazioni biunivoche $f : M_\lambda \to M_\lambda$ λ-lineari, cioè tali che $f(\lambda a) = \lambda f(a)$, per ogni $a \in M_\lambda$. Adesso, più in generale, si ha la seguente:

Proposizione 3.2. *Siano G e G' due gruppi che operano a sinistra rispettivamente su gli insiemi M e M'. Se A e B sono sottoinsiemi rispettivamente di G e G', allora un'applicazione f da M_A in M'_B è un omomorfismo se e solo se $f(Ax) \subset Bf(x)$, per ogni $x \in M$.*

Dimostrazione. Se $f : M_A \to M'_B$ è un omomorfismo, allora

$$f(Ax) = f(x \bullet x) \subset f(x) \bullet f(x) = Bf(x), \quad \forall x \in M.$$

Viceversa, se $f(Ax) \subset Bf(x)$, per ogni $x \in M_A$, allora

$$f(x \bullet y) = f(Ax \cup Ay) = f(Ax) \cup f(Ay) \subset Bf(x) \cup Bf(y) = f(x) \bullet f(y),$$

dunque f è un omomorfismo.

Definizione. Siano G e G' due gruppi che operano a sinistra su gli insiemi M e M'. Considerati due sottoinsiemi non vuoti A, B rispettivamente di G e G' e una famiglia $\{h_i\}_{i\in I}$ di applicazioni da A in B, un'applicazione $f : M \to M'$ si dice $(\{h_i\}_{i\in I}, A, B)$-*lineare* se per ogni coppia $(a, x) \in A \times M$ esiste $i \in I$ tale che $f(ax) = h_i(a)f(x)$.

Se per ogni coppia (i, j) di elementi di I si ha $h_i = h_j$, le applicazioni $(\{h_i\}_{i\in I}, A, B)$-lineari si dicono (h, A, B)-lineari.

Osservazione. Se G opera su M ed A è un sottoinsieme non vuoto di G, la relazione $\sim_A$ tale che $x \sim_A y \Leftrightarrow Ax = Ay$ è una relazione di equivalenza su M. Inoltre, se G opera liberamente su M e $T = \{x_i\}_{i\in I}$ è un trasversale delle classi di equivalenza modulo $\sim_A$, allora, per ogni elemento $x \in M$, esiste una sola coppia (a, x_i) di elementi di $A \times T$ tale che $x = ax_i$. Per cui, se G' è un altro gruppo che opera su un insieme M' e B è un sottoinsieme non vuoto di G', per ogni famiglia di applicazioni $\{h_i : A \to B\}_{i\in I}$ e per ogni applicazione $f^* : T \to M'$, è ben definita la funzione $f : M \to M'$ tale che

$$f(x) = h_i(a)f^*(x_i), \quad \forall x = ax_i \in M, a \in A, x_i \in T. \tag{3.5}$$

Proposizione 3.3. *Siano G e G' due gruppi che operano liberamente a sinistra su gli insiemi M e M' e siano H e K sottogruppi rispettivamente di G e G'. Se $T = \{x_i\}_{i\in I}$ è un trasversale delle classi di equivalenza modulo $\sim_H$, un'applicazione $f : M_H \to M'_K$ è un omomorfismo se, e solo se, esistono una famiglia $F_T = \{h_i\}_{i\in I}$ di applicazioni da H in K e un'applicazione $f^* : T \to M'$ tali che $f(x) = h_i(a)f^*(x_i)$, per ogni $x = ax_i \in M$, $a \in H$, $x_i \in T$.*

Dimostrazione. Se $f : M_H \to M_K$ è un omomorfismo, per la Proposizione 3.2, $f(Hx_i) \subset Kf(x_i)$, per ogni $x_i \in T$. Inoltre, per ipotesi, G' opera liberamente su M', per cui, fissato $x_i \in T$, per ogni elemento $a \in H$ esiste un solo elemento $b \in K$ tale che $f(ax_i) = bf(x_i)$, quindi è ben definita l'applicazione $h_i : H \to K$ tale che $h_i(a) = b \Leftrightarrow f(ax_i) = bf(x_i)$. Al variare di x_i in T si ottiene una famiglia $\{h_i\}_{i\in I}$ di applicazioni da H in K. Indicata con f^* la restrizione di f al trasversale T, si ha

$$f(x) = h_i(a)f(x_i) = h_i(a)f^*(x_i), \quad \forall x = ax_i \in M,\ a \in H,\ x_i \in T.$$

Viceversa, l'applicazione $f : M_H \to M'_K$ è tale che $f(x) = h_i(a)f^*(x_i)$, per ogni $x = ax_i \in M$, $a \in H$, $x_i \in T$. Dunque, se $x = ax_i$, si ha $Hx = Hx_i$, per cui

$$f(Hx) = f(Hx_i) = h_i(H)f^*(x_i) \subset Kf^*(x_i) = Kh_i(a)f^*(x_i) = Kf(x),$$

quindi f è un omomorfismo (Proposizione 3.2).

Corollario 3.4. *Siano G e G' due gruppi che operano liberamente a sinistra su gli insiemi M e M' e siano H e K sottogruppi rispettivamente di G e G'. Se $T = \{x_i\}_{i\in I}$ ed $F_T = \{h_i\}_{i\in I}$ sono rispettivamente un trasversale delle classi di equivalenza modulo $\sim_H$ e una famiglia di omomorfismi da H in K, allora, per ogni applicazione f^* da T in M', la funzione $f : M_H \to M'_K$ definita come in* $(3, 5)$ *è un omomorfismo* $(\{h_i\}_{i\in I}, H, K)$*-lineare.*

Dimostrazione. Per la Proposizione 3.3, l'applicazione $f : M_H \to M'_K$ è un omomorfismo, inoltre, per ogni $x \in M$, esiste una sola coppia $(b, x_i) \in H \times T$ tale che $x = bx_i$, per cui

$$f(ax) = f((ab)x_i) = h_i(ab)f^*(x_i) = \\ = h_i(a)h_i(b)f^*(x_i) = h_i(a)f(x), \quad \forall a \in M.$$

Osservazione. L'azione di un gruppo G in sé, determinata dalla stessa operazione di G, è libera. Se A e B sono sottoinsiemi rispettivamente dei gruppi G e G', le applicazioni (h, A, B)-lineari costruite nel Teorema 1.7 sono degli omomorfismi $(h^*, < A >, < B >)$-lineari dei due Join-Space $G_{<A>}$ e $G'_{<B>}$. Inoltre, il gruppo $\Lambda(G_A)$ è il gruppo degli automorfismi $(h, < A >)$-lineari completi del Join-Space $G_{<A>}$.

BIBLIOGRAFIA

[1] M. De Salvo - D. Freni - G. Lo Faro, *On the hypergroups with four proper pairs and two or three non scalar elements,* Rend. Circolo Matematico di Palermo, 46 (2) (1997), pp. 29–51.

[2] M. De Salvo - D. Freni - G. Lo Faro, *On the hypergroups with four proper pairs and three or four non scalar elements,* Analele Stiintifice Ale Universitatii Al. I Cuza Iasi (Romania), 43 (1) (1997), pp. 103–132.

[3] D. Freni, *Structure des hypergroupes quotients et des hypergroupes de type U, application à la théorie de la dimension et à l'Homologie non abelienne,* These de Doctorat, Univ. de Clermont Ferrand II, (1985).

[4] D. Freni, *Sur les hypergroupes cambistes,* Rendiconti Istituto Lombardo, 119 (1985), pp. 175–186.

[5] D. Freni, *Sur la théorie de la dimension dans les hypergroupes,* Acta Univ. Carolinae, Math. et Physica, 27 (2) (1986), pp. 67–80.

[6] D. Freni, *Une note sur le coeur d'un hypergroupe et sur la clôture transitive β^* de β,* Riv. Mat. Pura e Applicata Univ. Udine, 8 (1991), pp. 153–156.

[7] D. Freni, *On a strongly regular relation in hypergroupoids,* P.U.M.A. Budapest Ser. A, 3 (1992), pp. 191–198.

[8] D. Freni-Y. Sureau, *Hypergroupe de type U et homologie de Complexes,* Algebra Universalis, 35 (1996), pp. 34–62.

[9] D. Freni, *Contributo alle iperstrutture matroidali,* Le Matematiche, 52 (1997), pp. 271–295.

[10] D. Freni, *M_λ-ipergruppoidi matroidali, applicazioni λ-lineari e automorfismi di M_λ-ipergruppoidi,* Le Matematiche, 53 (1998), pp. 133–154.

[11] M. Gutan - D. Freni - Y. Sureau, *Sur le groupe des scalaires d'un hypergroupe,* Atti del convegno "New frontiers in hyperstructures and related algebras" di Monteroduni, Hadronic Press, U.S.A., (1996), pp. 103–124.

[12] J. Mittas, *Hypergroupes canoniques,* Mathematica Balkanica, 2 (1972), pp. 165–179.

[13] W. Prenowitz - J. Jantosciak, *Geometries and Join Spaces,* Journal fur die reine und angewandte Mathematik, 257 (1972).

[14] M. Scafati Tallini, *Matroidal hypervector spaces,* Journal of Geometry, 42, pp. 132–140.

[15] A. Sgarro, *Crittografia,* Muzzio Editore, (1993).

[16] S. Spartalis - T. Vougiouklis, *The fundamental relations on H_V-rings,* Rivista di Matematica Pura e Applicata, 13 (1993).

[17] G. Tallini, *Geometric hyperquasigroups and line spaces,* Acta Univ. Carolinae Math Phys., 25–1 (1984), pp. 69–73.

[18] G. Tallini, *On Steiner hypergroups and linear codes,* Atti Convegno su Ipergruppi e altre strutture multivoche e loro applicazioni, Univ. Udine, (1985), pp. 87–91.

[19] G. Tallini, *Dimensione negli ipergruppi,* Atti Univ. Cattolica di Milano, Sci. Mat., 11 (1994), pp. 367–390.

[20] T. Vougiouklis, *The fundamental relations on H_V-rings. The general hyperfield,* Proc. Fourth Int. Cong. on Algebraic Hyperstr. and Appl., World Scientific, (1991), pp. 203–211.

Dipartimento di Matematica e Informatica,
Università degli studi di Udine,
Via delle Scienze 206 Località Rizzi,
33100 Udine (Italy)
email: freni@dimi.uniud.it