

# RENDICONTI *del* SEMINARIO MATEMATICO *della* UNIVERSITÀ DI PADOVA

BENEDETTO SCIMEMI

## **Cappi di Bruck e loro generalizzazioni**

*Rendiconti del Seminario Matematico della Università di Padova*,  
tome 60 (1978), p. 141-149

[<http://www.numdam.org/item?id=RSMUP\\_1978\\_\\_60\\_\\_141\\_0>](http://www.numdam.org/item?id=RSMUP_1978__60__141_0)

© Rendiconti del Seminario Matematico della Università di Padova, 1978, tous droits réservés.

L'accès aux archives de la revue « Rendiconti del Seminario Matematico della Università di Padova » (<http://rendiconti.math.unipd.it/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques*  
<http://www.numdam.org/>

## Cappi di Bruck e loro generalizzazioni.

BENEDETTO SCIMEMI (\*)

Questa nota contiene due variazioni su un tema di G. Glauberman ([2]). Nella prima parte si considerano un  $p$ -gruppo finito  $G$  e un suo  $p'$ -automorfismo  $\varphi$ . Nel § 1, nell'insieme  $[\varphi, G]$  dei  $\varphi$ -commutatori si introduce una nuova operazione, che dà luogo ad un cappio su cui  $\varphi$  agisce come automorfismo privo di coincidenze. Ciò equivale a introdurre una struttura nell'insieme delle classi laterali modulo il sottogruppo  $C_G(\varphi)$ , che è quella del gruppo quoziente se il sottogruppo è normale. Nel § 2, del cappio così ottenuto si mettono in evidenza certe proprietà caratteristiche, che portano ad un teorema di « immersione speciale » (cfr. ad es. [4]) in un gruppo, tramite la rappresentazione regolare. Tutto ciò generalizza certi risultati di [2]; infatti nel § 3 si suppone  $\varphi$  involutorio (caso in cui la nilpotenza è inessenziale) e si ritrovano i cosiddetti cappi di Bruck. Nella seconda parte (§ 4) si considera un gruppo 2-divisibile sul quale, senza ricorrere ad automorfismi, si definiscono due nuove operazioni, ottenendo una struttura che ha qualche analogia con le algebre di Lie, e in cui sussiste una formula di tipo Hausdorff. In effetti, se il gruppo è nilpotente di classe  $\leq 2$ , l'analogia si precisa e (§ 5) si ritrova la corrispondenza di Lazard ([3]).

### 0. Notazione.

Per motivi che si chiariranno in seguito, ci discosteremo dalla notazione tradizionale della teoria dei gruppi, nel denotare una coniuga-

(\*) Indirizzo dell'A.: Istituto di Algebra e Geometria - Università di Padova.

zione nel gruppo  $G$  con il simbolo  $\gamma_g: z \mapsto z = gzg^{-1}$  e componendo le funzioni da destra a sinistra, cioè scrivendo, ad esempio,  $\gamma_g \gamma_h = \gamma_{gh}$ . Denoteremo con  $[h, g]$  il commutatore  $hgh^{-1}g^{-1}$  e, se  $\varphi$  è un automorfismo, porremo  $[\varphi, g] = \varphi(g)g^{-1}$ . Per un siffatto elemento  $x = [\varphi, g]$ , useremo spesso la relazione

$$\varphi^{d-1}(x)\varphi^{d-2}(x) \dots \varphi(x)x = 1 \quad (\text{dove } d \text{ è l'ordine di } \varphi)$$

che, per brevità, scriveremo anche  $\prod \varphi^j(x) = 1$ .

Se  $H$  è un sottogruppo di  $G$ , un suo « trasversale eccezionale » è un insieme  $T$  di rappresentanti (destri e sinistri) modulo  $H$ , che sia normalizzato da  $H$ .

Un coppia  $L, \circ$  è un sistema binario, con unità bilatera, in cui le equazioni  $x \circ a = b$ ,  $a \circ y = b$  hanno soluzioni uniche  $x, y \in L$  per ogni  $a, b \in L$ . Il centro  $Z(L)$  di  $L$  è l'insieme degli elementi  $z \in L$  per cui risulta

$$z \circ x = x \circ z, \quad z \circ (x \circ y) = (z \circ x) \circ y = x \circ (z \circ y)$$

per ogni  $x, y \in L$ . Allora  $L/Z(L)$  è in modo naturale un coppia, e si definisce la « nilpotenza centrale » come per i gruppi.

Per semplicità, si considerano per lo più gruppi e cappi finiti, ma sarebbe facile generalizzare quanto segue al caso periodico (purchè, nella prima parte, si supponga la nilpotenza) perchè le argomentazioni si svolgono nell'ambito di sottogruppi finitamente generati.

**1. LEMMA.** *Se  $\varphi$  è un automorfismo di ordine  $d$  del  $p$ -gruppo finito  $G$ , e  $p$  non divide  $d$ , allora  $[\varphi, G] = \{\varphi(h)h^{-1}; h \in G\}$  è un trasversale eccezionale del sottogruppo  $C_G(\varphi) = \{f \in G, \varphi(f) = f\}$  e risulta <sup>(1)</sup>*

$$[\varphi, G] = \{x \in G; \varphi^{d-1}(x)\varphi^{d-2}(x) \dots \varphi(x)x = 1\}.$$

**DIM.** Se  $T$  è un qualunque trasversale sinistro di  $C_G(\varphi)$ , è chiaro che  $[\varphi, G] = \{\varphi(t)t^{-1}, t \in T\}$  non può avere più di  $[G: C_G(\varphi)]$  elementi. Perciò basterà provare che  $[\varphi, g] = [\varphi, h] \cdot f$ ,  $f \in C_G(\varphi)$  comporta  $f = 1$ . Se  $G$  è abeliano,  $\prod \varphi^j([\varphi, h]) \prod \varphi^j(f) = \prod \varphi^j([\varphi, g])$  dà  $f^d = 1$  e  $f = 1$ , perchè  $p$  non divide  $d$ . Se  $G$  non è abeliano si proceda per induzione sulla classe di nilpotenza, supponendo il Lemma vero su  $Z = Z(G)$  e su  $\bar{G} = G/Z$ . Allora  $[\varphi, \bar{g}] = [\varphi, \bar{h}] \bar{f}$  comporta come sopra  $\bar{f} = \bar{1}$  e

<sup>(1)</sup> Si osservi l'analogia con il teor. 90 di Hilbert.

dunque  $f \in C_G(\varphi)$ . Riapplicando  $\prod \varphi^i$  si trova  $f = 1$ . Si noti che questi stessi argomenti provano anche la parte non banale dell'altro asserto, e cioè l'inclusione

$$[\varphi, G] \supseteq \{x \in G; \prod \varphi^i(x) = 1\}.$$

Poichè per ogni  $f \in C_G(\varphi)$  risulta  $f[\varphi, g] \cdot f^{-1} = [\varphi, fgf^{-1}]$ , è chiaro che il trasversale  $[\varphi, G]$  è eccezionale.

**TEOREMA 1.** *Siano  $G$  un  $p$ -gruppo finito,  $\varphi$  un suo  $p'$ -automorfismo di ordine  $d$ , e si ponga  $L = [\varphi, G]$ ,  $F = C_G(\varphi)$ . Per ogni  $x, y \in L$  si definiscano (con il Lemma precedente) due elementi  $x \circ y \in L$ ,  $x \circ y \in F$  ponendo*

$$(1) \quad xy = (x \circ y)(x \circ y).$$

*Allora  $L, \circ$  è un cappio, centralmente nilpotente, di ordine  $p^m$ , su cui  $\varphi$  induce un automorfismo, privo di coincidenze (cioè che fissa solo l'unità); risulta per ogni  $z \in L$*

$$(2) \quad \varphi^{d-1}(x) \circ (\varphi^{d-2}(x) \circ (\dots \circ (\varphi(x) \circ (x \circ z)) \dots)) = z,$$

$$(3) \quad x \circ (y \circ z) = (x \circ y) \circ (x \circ y)z,$$

*e la coniugazione  $\gamma_{(x \circ y)}: z \mapsto (x \circ y)z(x \circ y)^{-1}$  induce su  $L, \circ$  un automorfismo che commuta con  $\varphi$ .*

**DIM.** Proviamo anzitutto che ogni automorfismo  $\beta$  del gruppo  $G$  che lasci  $F$  ed  $L$  invarianti induce un automorfismo di  $L, \circ$ . Infatti per ogni  $x, y \in L$  risulta  $\beta(x), \beta(y) \in L$ ,

$$\begin{aligned} \beta(x \circ y)\beta(x \circ y) &= \beta((x \circ y)(x \circ y)) = \beta(xy) = \beta(x)\beta(y) = \\ &= (\beta(x) \circ \beta(y))(\beta(x) \circ \beta(y)) \end{aligned}$$

e dunque  $\beta(x \circ y) = \beta(x) \circ \beta(y)$  per l'unicità della decomposizione nel Lemma. In particolare, sono automorfismi di  $L, \circ$  le restrizioni ad  $L$  delle coniugazioni  $\gamma_f$  ( $f \in F$ ) e di  $\varphi$ . Quest'ultima è anzi priva di coincidenze (perchè  $L \cap F = 1$ ) e commuta con ogni  $\gamma_f$ . Quanto alla (3), scriviamo, per ogni  $x, y, z \in L$

$$\begin{aligned} xyz &= x(yz) = x(y \circ z)(y \circ z) = (x \circ (y \circ z))(x \circ (y \circ z))(y \circ z) = \\ &= (xy)z = (x \circ y)(x \circ y)z = (x \circ y)(x \circ y)z(x \circ y) = \\ &= ((x \circ y) \circ (x \circ y)z)((x \circ y) \circ (x \circ y)z)(x \circ y) \end{aligned}$$

Come sopra, la (3) si deduce con il Lemma, per unicità. Osserviamo che se  $x, y \in L$  e anche  $xy \in L$ , allora  $x \circ y = xy$ ,  $x \circ y = 1$ . Ciò vale, ad esempio, per gli elementi centrali. Se dunque  $z \in L \cap Z(G)$ , per ogni  $x, y \in L$  è  $(x \circ y)z = z$ ,  $z \circ x = 1$ , e dunque

$$\begin{aligned} x \circ z &= xz = zx = z \circ x, \\ x \circ (y \circ z) &= (x \circ y) \circ (x \circ y)z = (x \circ y) \circ z = \\ &= z \circ (x \circ y) = (z \circ x) \circ (z \circ x)y = (z \circ x) \circ y. \end{aligned}$$

In particolare,  $x \circ 1 = x = 1 \circ x$ , e dunque 1 è unità bilatera per  $L, \circ$ .

Più generalmente, se  $x_1, x_2, \dots, x_r \in L$  e risulta  $x_1 x_2 \dots x_r \in L$ , applicando più volte la (3) si ottiene

$$x_1 x_2 \dots x_r = x_1 \circ (x_2 \circ (\dots (x_{r-1} \circ x_r) \dots)).$$

Poichè per ogni  $x, z \in L$  risulta  $z = \prod \varphi^j(x) \cdot z$ , ne segue l'identità (2).

Per provare che  $L, \circ$  è un cappio, basterà provare la cancellazione; ci limitiamo a quella sinistra, perchè l'altra si prova analogamente. Siano  $x, y, y' \in L$ ,  $x \circ y = x \circ y'$ . Procediamo per induzione sulla classe di nilpotenza di  $G$ , perchè il caso abeliano è ovvio. Allora il risultato vale su  $\bar{G} = G/Z$  e dunque  $y' = ya$  per qualche  $a \in Z$ ; scriviamo  $a = zz'$  con  $z \in L \cap Z$ ,  $z' \in F \cap Z$ . Allora  $yz = y \circ z \in L$  e dunque  $z' = 1$  e, come sopra,  $x \circ y = x \circ y' = x \circ yz = x \circ (y \circ z) = (x \circ y) \circ z = (x \circ y)z$  e infine  $1 = z = a$ ,  $y = y'$ , come si voleva.

Dunque  $L, \circ$  è un cappio. Poichè, come risulta dalle precedenti relazioni, il suo centro contiene  $L \cap Z(G)$ , si prova subito, ancora per induzione, che il cappio è centralmente nilpotente, di classe non superiore a quella del gruppo  $G$ .

**2. TEOREMA 2.** *Sia  $L, \circ$  un cappio, centralmente nilpotente, di ordine  $p^m$ , dotato di un  $p'$ -automorfismo  $\varphi$ , di ordine  $d$ , che soddisfa per ogni  $x, z \in L$  la relazione*

$$(2) \quad \varphi^{d-1}(x) \circ (\varphi^{d-2}(x) \circ \dots \circ (\varphi(x) \circ (x \circ z)) \dots) = z.$$

*Per ogni  $x, y, z \in L$  si definisca l'elemento  $(x \circ y)z \in L$  con la posizione*

$$(3) \quad x \circ (y \circ z) = (x \circ y) \circ (x \circ y)z.$$

Si supponga che ogni funzione  $\gamma_{(x \circ y)}: z \mapsto (x \circ y)z$  sia un automorfismo del coppia, che commuta con  $\varphi$ . Allora esistono un  $p$ -gruppo finito  $\mathfrak{S}$  e un suo automorfismo  $\Phi$  tali che il coppia definito con il Teor. 1 su  $[\Phi, \mathfrak{S}]$  è isomorfo ad  $L$ , e le azioni di  $\varphi$  e  $\gamma_{(x \circ y)}$  su  $L$  corrispondono a quelle indotte su  $[\Phi, \mathfrak{S}]$  da  $\Phi$  e da coniugazioni nel gruppo  $\mathfrak{S}$ .

DIM. Poichè  $L, \circ$  è un coppia, le moltiplicazioni sinistre

$$A = \{\lambda_x: z \mapsto x \circ z; x, z \in L\}$$

sono permutazioni di  $L$ . Poichè  $L$  è centralmente nilpotente di ordine  $p^m$ , il suo gruppo delle moltiplicazioni è un  $p$ -gruppo ([1], pag. 98) e tale è pure il sottogruppo  $\mathfrak{S} = \langle A \rangle$ , generato da  $A$  nel gruppo delle permutazioni di  $L$ . Allora gli elementi  $\gamma_{(x \circ y)} = \lambda_{x \circ y}^{-1} \lambda_x \lambda_y$  generano un sottogruppo di  $\mathfrak{S}$ , sia

$$\Gamma = \langle \gamma_{(x \circ y)}: z \mapsto (x \circ y)z; x, y, z \in L \rangle.$$

Proviamo che  $A$  è un trasversale eccezionale di  $\Gamma$  in  $\mathfrak{S}$ . Poichè ogni  $\alpha \in \Gamma$  è un automorfismo di  $L, \circ$ , risulta  $\alpha \lambda_x \alpha^{-1} = \lambda_{\alpha(x)}$  per ogni  $x \in L$ , e dunque  $\Gamma$  normalizza  $A$ . Se anche  $y \in L$ ,  $\beta \in \Gamma$  risulta

$$\lambda_x \alpha \lambda_y \beta = \lambda_x \lambda_{\alpha(x)} \alpha \beta = \lambda_{x \circ \alpha(x)} \gamma_{(x \circ \alpha(x))} \alpha \beta \in A \Gamma.$$

Ne segue che  $A \Gamma$  è un sottogruppo, e dunque coincide con  $\mathfrak{S} = \langle A \rangle$ . Infine da  $\lambda_x \alpha = \lambda_y \beta$  segue

$$x = \lambda_x(\alpha(1)) = \lambda_y(\beta(1)) = y, \quad \text{e} \quad \lambda_x = \lambda_y.$$

Consideriamo ora la coniugazione indotta da  $\varphi$  nel gruppo delle permutazioni di  $L$ ; poichè  $\varphi$  è un automorfismo di  $L, \circ$  risulta per ogni  $x \in L$ ,  $\varphi \lambda_x \varphi^{-1} = \lambda_{\varphi(x)}$ ; poichè  $\varphi$  commuta con  $\gamma_{(x \circ y)}$ , è  $\varphi \alpha \varphi^{-1} = \alpha$  per ogni  $\alpha \in \Gamma$ . Allora tale coniugazione induce su  $\mathfrak{S}$  l'automorfismo

$$\Phi: \lambda_x \alpha \mapsto \lambda_{\varphi(x)} \alpha,$$

che ha l'ordine di  $\varphi$ . Applichiamo il Teor. 1 alla coppia  $\mathfrak{S}, \Phi$ . Se  $\lambda_x = \Phi(\lambda_x)$ , la (2) fornisce  $(\lambda_x)^d = 1$  e dunque  $\lambda_x = 1$ , cioè  $x$  è l'unità del coppia. Così  $\varphi$  è privo di coincidenze su  $L$ , e perciò  $C_{\mathfrak{S}}(\Phi) = \Gamma$ . Proviamo che risulta  $[\Phi, \mathfrak{S}] = A$ ; anzi, basterà l'inclusione  $\supseteq$ , poichè

si tratta di trasversali di un medesimo sottogruppo. Ora l'identità (2) si riscrive

$$\prod \Phi^j(\lambda_x) = \prod \lambda_{\varphi^j(x)} = 1$$

e dunque, per il Lemma,  $\lambda_x \in [\Phi, \mathfrak{S}]$ , come si voleva.

Applichiamo il Teor. 1 e definiamo il coppia  $A, \circ$  ponendo, per ogni  $\lambda_x, \lambda_y \in A$ ,

$$\lambda_x \lambda_y = (\lambda_x \circ \lambda_y)(\lambda_x \circ \lambda_y) \quad \text{dove} \quad \lambda_x \circ \lambda_y \in A, \quad \lambda_x \circ \lambda_y \in I.$$

Confrontando con la (3), nella forma  $\lambda_x \lambda_y = \lambda_{x \circ y} \gamma_{(x \circ y)}$  si trova, per l'unicità,  $\lambda_x \circ \lambda_y = \lambda_{x \circ y}$ .

Si conclude che  $\lambda: x \mapsto \lambda_x$  è un isomorfismo di coppia, in cui, come si è visto,  $\varphi(x)$  corrisponde a  $\Phi(\lambda_x)$  e  $\lambda_{(x \circ y)_x}$  corrisponde a  $\gamma_{(x \circ y)} \lambda_y \gamma_{(x \circ y)}^{-1}$ .

**3.** Nel caso che  $\varphi$  sia involutorio ( $d = 2$ ), il Lemma e il Teor. 1 si possono dimostrare senza far uso della nilpotenza, riferiti a un qualunque gruppo  $G$  di ordine dispari, o più semplicemente 2-divisibile, cioè tale che la funzione  $x \mapsto x^2$  sia una permutazione di  $G$ . In effetti, nel lemma risulta  $[\varphi, G] = \{x \in G; \varphi(x) = x^{-1}\}$  e la fattorizzazione (ben nota, nel caso finito) si ottiene subito scrivendo  $g = [\varphi, [\varphi, g]^{\frac{1}{2}}] \cdot f = (g \cdot \varphi(g^{-1}))^{\frac{1}{2}} \cdot f$ . Allora nel Teor. 1 risulta

$$x \circ y = (xy \cdot \varphi(xy)^{-1})^{\frac{1}{2}} = (xy^2 x)^{\frac{1}{2}}$$

e l'automorfismo  $\varphi$  è l'inversione:  $(x \circ y)^{-1} = x^{-1} \circ y^{-1}$ . Come si è già osservato in [4],  $L, \circ$  è isomorfo al coppia  $L(\frac{1}{2})$  di Bruck, studiato in [2]. Quanto al Teor. 2, l'ipotesi di nilpotenza si può sostituire con quella, assai più debole, che oltre al coppia  $L$  sia 2-divisibile anche il gruppo  $\mathfrak{S}$  generato dalle moltiplicazioni sinistre. Infatti l'equazione (2) per  $d = 2$  fornisce  $\varphi(x) \circ (x \circ z) = z$ , in particolare  $\varphi(x) \circ x = 1 = x \circ \varphi(x)$ , e dunque  $\varphi(x)$  è inverso bilatero di  $x$ , sia  $x^{-1}$ . Allora la (2), il fatto che  $\varphi$  è automorfismo e permuta con  $\gamma_{x \circ y}$  sono le identità

$$x^{-1} \circ (x \circ z) = z, \quad (x \circ y)^{-1} = x^{-1} \circ y^{-1},$$

$$(x \circ y)^{-1} \circ (x \circ (y \circ z)) = (x \circ y) \circ (x^{-1} \circ (y^{-1} \circ z))$$

e danno

$$\lambda_{x^{-1}} = \lambda_x^{-1}, \quad \lambda_{(x \circ y)^{-1}} \lambda_x \lambda_y = \lambda_{x \circ y} \lambda_{x^{-1}} \lambda_{y^{-1}}$$

e infine (poichè si è supposto  $\mathfrak{G}$  2-divisibile)  $\lambda_{x \circ y} = (\lambda_x \lambda_y^2 \lambda_x)^{\frac{1}{2}}$ . Il resto della dimostrazione procede senza far uso della nilpotenza, perchè  $[\Phi, \mathfrak{G}] = A$  è conseguenza, ancora, della 2-divisibilità di  $\mathfrak{G}$ . Si perviene all'isomorfismo tra  $L$  e  $A$ , e dunque si tratta di cappi di Bruck. Si noti che dalle relazioni precedenti segue anche  $\lambda_{x \circ x} = \lambda_x^2$ , e la  $\lambda_{x \circ y}^2 = \lambda_x \lambda_y^2 \lambda_x$  fornisce (scrivendo  $y$  al posto di  $y \circ y$ ) l'identità « duale di Bol »:  $x \circ (y \circ (x \circ z)) = (x \circ (y \circ x)) \circ z$ , che in [2] è uno dei punti di partenza per la caratterizzazione dei cappi di Bruck. Si vede quindi come i Teoremi 1 e 2 generalizzino e siano suggeriti dai Teor. 1 e 2 di Glauberman.

4. È noto che la struttura del cappio  $G(\frac{1}{2})$  definito sul gruppo  $G$  (con le operazioni « isomorfe »  $x^{\frac{1}{2}} y x^{\frac{1}{2}}$  ovvero  $(xy^2 x)^{\frac{1}{2}}$ ) non riproduce fedelmente quella del gruppo  $G$ , nel senso che due gruppi non isomorfi possono dar luogo a cappi isomorfi. Tuttavia, con il punto di vista da noi adottato, su ogni gruppo 2-divisibile, accanto all'operazione  $\circ$  di cappio nasce in modo naturale un'altra operazione  $\circ$ , definita ponendo, per ogni  $x, y \in G$

$$x \circ y = (x \circ y)^{-1} x y = (x y^2 x)^{-\frac{1}{2}} x y.$$

Ci proponiamo di esaminare alcune proprietà della struttura  $G, \circ, \circ$  e di provare che da essa la moltiplicazione gruppale è « ricostruibile ».

**TEOREMA 3.** *Sul gruppo 2-divisibile  $G$ , si definiscano due operazioni  $\circ, \circ$  ponendo per ogni  $x, y \in G$*

$$x \circ y = (x y^2 x)^{\frac{1}{2}}, \quad x \circ y = (x \circ y)^{-\frac{1}{2}} x y.$$

*Allora valgono le identità:*

$$(1) \quad x^{-1} \circ y^{-1} = (x \circ y)^{-1},$$

$$(2) \quad x^{-1} \circ y^{-1} = x \circ y,$$

$$(3) \quad y \circ x = (v \circ x)(x \circ y),$$

$$(4) \quad y \circ x = (x \circ y)^{-1},$$

$$(5) \quad (x \circ y)^{-1} \circ (x \circ (y \circ z)) = (x \circ v)z,$$

$$(6) \quad (x \circ y)((y \circ x) \circ z) = (x \circ (y \circ z))(y \circ z),$$

$$(7) \quad x y = ((x \circ y)^{\frac{1}{2}} \circ (x \circ v)^{\frac{1}{2}}(y \circ x)^{\frac{1}{2}})^2.$$

*L'operazione di gruppo si esprime mediante le nuove operazioni. In particolare, due gruppi  $G_1, G_2$  sono isomorfi se e solo se sono isomorfe le strutture  $G_1, \circ, \circ$  e  $G_2, \circ, \circ$ .*

**DIM.** Tutte le identità si possono verificare con il calcolo effettivo, ma è più significativo operare come segue. Si consideri un gruppo libero con 3 generatori, sia  $E = \langle x, y, z \rangle$ , lo si immerga in un gruppo 2-divisibile minimale (come in [5]), sia  $E^*$ , e sia  $\varphi$  l'automorfismo di  $E^*$  individuato dalle posizioni  $\varphi(x) = x^{-1}$ ,  $\varphi(y) = y^{-1}$ ,  $\varphi(z) = z^{-1}$ . Si applichi il Lemma, decomponendo opportune « parole » in  $x, y, z$  e si usi l'unicità, come nella dimostrazione del Teor. 1. La sostituzione in  $G$  (cioè un opportuno omomorfismo  $E^* \rightarrow G$ ) trasforma le varie espressioni di un medesimo elemento di  $E^*$  in altrettante identità in  $G$ ; ad esempio, le (3), (4) e (5), (6) si ottengono applicando il procedimento indicato agli elementi  $xy = (y^{-1}x^{-1})^{-1}$  e rispett.  $(xy)z = x(yz)$ . Poichè sappiamo che  $G, \circ$  è un coppia in cui le potenze hanno lo stesso significato che nel gruppo, il secondo membro della (7), diventa — mediante la (7) — un'espressione di tipo polinomiale in  $x, y$  che fa uso delle sole operazioni  $\circ, \circ$ . Ad esempio, se  $|G| = 2n - 1$ , allora risulta

$$(x \circ y)^{\frac{1}{2}} z = (x \circ y)^n z = \underbrace{(x \circ y)^{-1} \circ \left( x \circ \left( y \circ \dots \left( (x \circ y)^{-1} \circ (x \circ (y \circ z)) \right) \dots \right) \right)}_{n \text{ volte}}.$$

Si conclude che due strutture  $G_1, \circ, \circ$  e  $G_2, \circ, \circ$  sono isomorfe (con ovvio significato del termine) soltanto se lo sono i gruppi  $G_1, G_2$  da cui provengono. Questo risponde affermativamente ad un quesito posto in [5].

**5.** Per mezzo della (7), tutte le identità precedenti si possono esprimere senza far uso della moltiplicazione di gruppo, ottenendo così una caratterizzazione intrinseca della struttura  $G, \circ, \circ$ . Ci proponiamo di farlo per esteso in altra occasione, limitandoci qui ad un caso particolare, che ripropone un fatto noto (cfr. [3]), che ha in parte motivato l'intero problema.

**COROLLARIO.** *Sia  $G$  un gruppo 2-divisibile, nilpotente di classe  $c \leq 2$ . Per ogni  $x, y \in G$  si ponga*

$$x + y = xy[y, x]^{\frac{1}{2}}, \quad \llbracket x, y \rrbracket = [x, y].$$

Allora  $G, +, \llbracket, \rrbracket$  è un anello di Lie, 2-divisibile, nilpotente di classe  $c$ , da cui la moltiplicazione di gruppo si ricostruisce con la formula (di Hausdorff)

$$xy = x + y + \frac{1}{2} \llbracket x, y \rrbracket.$$

DIM. Poichè  $G$  è di classe  $\leq 2$ , ogni commutatore  $[x, y]$  è centrale, e perciò risulta  $[x^{-1}, y^{-1}] = [x, y]$ ,  ${}^{[x, y]}z = z$  per ogni  $x, y, z \in G$ . Si applichi il Teor. 3 e si verifichi:

$$x + y = x \circ y; \quad \llbracket x, y \rrbracket = (x \circ y)^2.$$

Allora il coppia  $G, +$  è commutativo (per la (3)) e associativo (per la (5)), e quindi è un gruppo abeliano 2-divisibile. La (4) è l'antisimmetria del crochet. Quanto alla bilinearità, la (6) si può scrivere

$$\frac{1}{2} \llbracket x, y \rrbracket + \frac{1}{2} \llbracket x + y, z \rrbracket = \frac{1}{2} \llbracket x, y + z \rrbracket + \frac{1}{2} \llbracket y, z \rrbracket$$

da cui, permutando ciclicamente  $x, y, z$  e opportunamente combinando si ottiene appunto  $\llbracket x + y, z \rrbracket = \llbracket x, z \rrbracket + \llbracket y, z \rrbracket$ . Infine la relazione di Jacobi è banalmente soddisfatta, perchè

$$\llbracket [x, y], z \rrbracket = 1 \quad \text{implica} \quad \llbracket \llbracket x, y \rrbracket, z \rrbracket = 0.$$

Così  $G, +, \llbracket, \rrbracket$  è un anello di Lie, di classe  $c$ , e la (7) si legge appunto  $xy = x + y + \frac{1}{2} \llbracket x, y \rrbracket$ , che è la formula di Hausdorff in classe  $\leq 2$ .

## BIBLIOGRAFIA

- [1] R. BRUCK, *A survey of binary systems*, Ergebnisse der Math., Springer, Berlin, 1958.
- [2] G. GLAUBERMAN, *On loops of odd order*, J. Algebra, **1** (1964), pp. 374-396.
- [3] M. LAZARD, *Sur le groupes nilpotents et les anneaux de Lie*, Ann. E.N.S., **71** (1954), pp. 101-190.
- [4] D. A. ROBINSON, *A special embedding of Bol loops in groups*, Acta Math. Ac. Sci. Hung., **30** (1977), pp. 95-103.
- [5] B. SCIMEMI, *Homogeneous verbal functions on groups*, Rend. Sem. Mat. Univ. Padova, **49** (1973), pp. 299-321.

Manoscritto pervenuto in redazione il 24 gennaio 1979.