

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

DOMENICO BOCCIONI

Caratterizzazione di una classe di anelli generalizzati

Rendiconti del Seminario Matematico della Università di Padova,
tome 35, n° 1 (1965), p. 116-127

http://www.numdam.org/item?id=RSMUP_1965__35_1_116_0

© Rendiconti del Seminario Matematico della Università di Padova, 1965, 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/>

CARATTERIZZAZIONE DI UNA CLASSE DI ANELLI GENERALIZZATI

*Nota *) di DOMENICO BOCCIONI (a Padova) **)*

Alla base di questo lavoro sta il concetto di n -gruppo, introdotto da W. Dörnte nel 1929 ([2] ¹⁾) e poi estesamente studiato da E. L. Post ([4]), cui è dovuto l'importante « teorema del laterale » (n. 4), secondo il quale ogni n -gruppo G_n è immergibile in un certo gruppo, $C(G_n)$, (individuato da G_n a meno di isomorfismi) in modo da risultare un laterale di un certo sottogruppo normale di $C(G_n)$.

Un n -gruppo, G_n , è un insieme dotato di un'operazione n -aria associativa: $(a_1, \dots, a_n) \rightarrow f(a_1, \dots, a_n)$, nel quale ogni equazione del tipo $f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n) = a_{n+1}$ ($1 \leq i \leq n$) è univocamente risolvibile. Un 2-gruppo è quindi un ordinario gruppo.

Nella prima parte di questa nota, si considera l'insieme, $E(G_n)$, degli endomorfismi di un n -gruppo additivo commutativo G_n , e si definiscono in esso una addizione n -aria ed una moltiplicazione (binaria) nello stesso modo che è consueto per

*) Pervenuto in redazione il 23 luglio 1964.

Indirizzo dell'A.: Seminario Matematico, Università, Padova.

***) Lavoro eseguito nell'ambito dall'attività dei gruppi di ricerca matematica del C.N.R.

¹⁾ I numeri fra parentesi quadre rimandano alla bibliografia alla fine della nota.

$n = 2$, (n. 2). Rispetto a queste due operazioni, $E(G_n)$ risulta un n -gruppo additivo commutativo e un semigruppato moltiplicativo con la moltiplicazione distributiva rispetto all'addizione n -aria (teor. 1). Per $n = 2$, $E(G_n)$ si riduce al ben noto anello degli endomorfismi del gruppo commutativo G_2 .

È quindi naturale chiamare n -anello una struttura algebrica (astratta) del tipo di $E(G_n)$, come è stato fatto nel n. 1. Un 2-anello è un ordinario anello.

Nella seconda parte di questo lavoro si dimostra che per gli n -anelli sussiste un teorema (n. 7, teor. 2) perfettamente analogo al « teorema del laterale » di Post per gli n -gruppi.

In base a questo teorema, ogni n -anello A_n è immergibile in un certo anello A (il cui gruppo additivo coincide con $C(A_n^+)$, dove A_n^+ denota l' n -gruppo additivo di A_n) in modo che le operazioni dell'anello A subordinino in A_n le due omonime operazioni ivi date. Inoltre, gli elementi del dato n -anello A_n costituiscono in A un laterale di un certo ideale dell'anello A . L'anello quoziente di A per questo ideale risulta isomorfo all'anello degli interi modulo $n - 1$, e questo anello quoziente ha per elemento unità proprio A_n .

Ad esempio, se A_n è l' n -anello degli interi $\equiv 1 \pmod{n - 1}$, con addizione (n -aria) e moltiplicazione ordinarie, l'anello A è l'anello degli interi.

1. - Diremo che un insieme non vuoto, A_n , è un n -anello (n intero ≥ 2), se in esso sono ovunque definite due operazioni univoche: un'addizione n -aria,

$$(a_1, a_2, \dots, a_n) \rightarrow a_1 + a_2 + \dots + a_n \in A_n \quad (a_i \in A_n),$$

rispetto alla quale A_n è un n -gruppo commutativo ([2], [4], cfr. [1], n. 1 e 2), e una moltiplicazione (binaria) associativa, soddisfacenti alle due seguenti *proprietà distributive* (qualunque siano $a, a_i, b, b_i \in A_n$):

$$(1) \quad a(b_1 + b_2 + \dots + b_n) = (ab_1) + (ab_2) + \dots + (ab_n),$$

$$(1') \quad (a_1 + a_2 + \dots + a_n)b = (a_1b) + (a_2b) + \dots + (a_nb);$$

(nei secondi membri delle (1), (1'), le parentesi possono essere sottintese, secondo l'uso corrente, al quale ci atterremo nel seguito).

Un 2-anello è quindi un ordinario anello.

L' n -gruppo commutativo costituito dagli elementi di un n -anello e dalla sua addizione n -aria verrà detto *n -gruppo additivo* dell' n -anello. Il semigruppato costituito dagli elementi di un n -anello e dalla sua moltiplicazione verrà detto il *semigruppato moltiplicativo* dell' n -anello.

Gli elementi di un anello A costituiscono evidentemente un n -anello (per ogni dato n) rispetto alla consueta addizione di n elementi di A ed alla moltiplicazione di A (cfr. [1], n. 2). In questo senso alluderemo ad A come ad un n -anello.

Esistono n -anelli, con $n > 2$, che non si possono ottenere da anelli (aventi i loro stessi elementi) nel modo detto nel precedente capoverso. Uno di questi è, ad esempio, l' n -anello costituito dagli interi che sono congrui ad 1 modulo $n - 1$, con addizione (di n addendi) e moltiplicazione ordinarie. È noto infatti ([2], p. 5) che l' n -gruppo additivo di questo n -anello non si può ottenere da un gruppo (additivo) avente i suoi stessi elementi, considerando la consueta addizione di n elementi del gruppo.

Per un *sotto- n -anello* di un n -anello A_n , intenderemo un sottinsieme non vuoto di A_n che sia contemporaneamente un sotto- n -gruppo dell' n -gruppo additivo ([1], n. 2) e un sotto-semigruppato del semigruppato moltiplicativo di A_n . Parlando di un sotto- n -anello di un anello, penseremo naturalmente quest'ultimo come n -anello (nel senso sopra chiarito).

2. - Un omomorfismo di un n -gruppo G_n in sè stesso (cfr [1], n. 1) si dirà un *endomorfismo* di G_n . L'insieme degli endomorfismi di G_n verrà denotato con

$$E(G_n).$$

Un endomorfismo di un n -gruppo additivo G_n è dunque una

applicazione, $\omega : a \rightarrow a\omega$ di G_n in G_n tale che

$$(2) \quad (a_1 + \dots + a_n)\omega = a_1\omega + \dots + a_n\omega,$$

qualunque siano $a_1, \dots, a_n \in G_n$. Si noti che $E(G_n)$ non è vuoto, poichè contiene l'applicazione identica.

TEOREMA 1: *Supponiamo che un n -gruppo additivo G_n sia commutativo, e definiamo, nell'insieme $E(G_n)$ dei suoi endomorfismi, un'addizione n -aria ed una moltiplicazione (binaria) mediante le seguenti posizioni ($a \in G_n$, $\omega_i \in E(G_n)$):*

$$(3) \quad a(\omega_1 + \dots + \omega_n) = a\omega_1 + \dots + a\omega_n,$$

$$(4) \quad a(\omega_1\omega_2) = (a\omega_1)\omega_2.$$

Allora, rispetto a queste due operazioni, $E(G_n)$ è un n -anello.

Per $n = 2$ questo teor. 1 è ben noto, riducendosi ad un classico risultato sugli endomorfismi di un gruppo commutativo.

Dimostrazione per $n > 2$: È perfettamente analoga a quella del caso $n = 2$ (cfr., ad es., [3], p. 79), tranne in un punto, sul quale soltanto ci soffermeremo.

Anzitutto si verifica facilmente (ricordando le proprietà associativa e commutativa generalizzate di G_n — cfr. [1], n. 1 —) che $E(G_n)$ è chiuso rispetto alle due operazioni in discorso, cioè che da $\omega_1, \dots, \omega_n \in E(G_n)$ segue $\omega_1 + \dots + \omega_n, \omega_1\omega_2 \in E(G_n)$, che l'addizione n -aria definita dalla (3) è associativa ([1], (1)) e commutativa, e che valgono le due proprietà distributive (1) e (1'), la moltiplicazione definita dalla (4) essendo notoriamente associativa.

Ciò fatto (e questo è il punto a cui alludevamo), rimane soltanto da verificare (cfr. [1], n. 2, 2° capov.) che è risolubile in $E(G_n)$ l'equazione nell'incognita ξ_1 :

$$(5) \quad \xi_1 + \omega_2 + \dots + \omega_n = \omega \quad (\omega_i, \omega \in E(G_n)).$$

Infatti, se esiste in $E(G_n)$ una soluzione ω_1 della (5), di conseguenza (v. (3)) $a\omega_1$ è la soluzione nell' n -gruppo G_n dell'equa-

zione:

$$(6) \quad x_1 + a\omega_2 + \dots + a\omega_n = a\omega \quad (a \in G_n).$$

Data l'equazione (5), definiamo allora un'applicazione, $\omega_1 : a \rightarrow a\omega_1$, di G_n in G_n , ponendo $a\omega_1$ uguale all'unica soluzione in G_n dell'equazione (6), di modo che per definizione risulta

$$(7) \quad a\omega_1 + a\omega_2 + \dots + a\omega_n = a\omega \quad \text{per ogni } a \in G_n.$$

La (7) dice già (v. (3)) che l'applicazione ω_1 così definita risolve la (5), onde resta solo da dimostrare che $\omega_1 \in E(G_n)$, ossia che vale la (2) con ω_1 in luogo di ω . E invero, se $a_1, \dots, a_n \in G_n$, per la definizione (7) si ha:

$$(8) \quad (a_1 + \dots + a_n)\omega_1 + (a_1 + \dots + a_n)\omega_2 + \dots + (a_1 + \dots + a_n)\omega_n = \\ = (a_1 + \dots + a_n)\omega,$$

$$(9) \quad a_i\omega_1 + a_i\omega_2 + \dots + a_i\omega_n = a_i\omega \quad (i = 1, \dots, n).$$

Sommando allora (nell' n -gruppo commutativo G_n) membro a membro le (9), si ha, per la (2), poichè $\omega_2, \dots, \omega_n, \omega \in E(G_n)$:

$$(10) \quad (a_1\omega_1 + \dots + a_n\omega_1) + (a_1 + \dots + a_n)\omega_2 + \dots \\ + (a_1 + \dots + a_n)\omega_n = (a_1 + \dots + a_n)\omega.$$

Le (8), (10) dicono che i due elementi di G_n :

$$(a_1 + \dots + a_n)\omega_1, \quad a_1\omega_1 + \dots + a_n\omega_1$$

risolvono la medesima equazione nell' n -gruppo G_n , dunque sono eguali (per l'unicità della soluzione), cioè appunto vale la (2) con ω_1 in luogo di ω . Ed il teorema 1 è dimostrato.

Il teorema 1 (oltre a fornire un mezzo per la costruzione di n -anelli a partire da n -gruppi commutativi) mostra che la nozione di n -anello, introdotta nel n. 1, si presenta spontaneamente nella teoria degli n -gruppi, nello stesso modo in cui la nozione di anello si presenta in teoria dei gruppi.

Sia dunque A_n un n -anello qualsiasi, e denotiamo con A_n^+ l' n -gruppo additivo di A_n , (quindi i due insiemi A_n e A_n^+ coincidono — n. 1 —). Per il « teorema del laterale » di Post, esiste un gruppo (additivo), $C(A_n^+)$, circoscritto all' n -gruppo A_n^+ nel senso chiarito nel n. 2 di [1]. Questo gruppo $C(A_n^+)$ è individuato da A_n^+ a meno di isomorfismi, ed è commutativo (v., ad es., [5], Satz 9), perchè è commutativo l' n -gruppo A_n^+ . Poniamo

$$A^+ = C(A_n^+),$$

e ricordiamo che ogni elemento di questo gruppo commutativo A^+ è una somma finita di elementi (di A_n^+ ossia) di A_n :

$$(14) \quad x \in A^+ \quad \text{se e solo se} \quad x = a_1 + \dots + a_r \quad (a_i \in A_n).$$

A_n^+ è un sotto- n -gruppo di A^+ , quindi l'addizione (generalizzata) di $k(n-1) + 1$ elementi dell' n -anello A_n ($k = 0, 1, 2, \dots$) è subordinata dalla consueta addizione di altrettanti elementi del gruppo A^+ (cioè il simbolo (11) rappresenta lo stesso elemento di A_n sia se interpretato come somma in A_n , sia come somma in A^+). Sappiamo che $(n-1)A_n$ (cioè l'insieme degli elementi di A^+ che sono somme di $n-1$ elementi di A_n) è un sottogruppo di A^+ , e che la decomposizione del gruppo (additivo) commutativo A^+ nei laterali del suo sottogruppo $(n-1)A_n$ è la seguente:

$$(15) \quad A^+ = A_n \cup 2A_n \cup \dots \cup (n-2)A_n \cup (n-1)A_n,$$

dalla quale si vede che il gruppo quoziente $A^+/(n-1)A_n$ è ciclico di ordine $(n-1)$ con elemento generatore A_n . Gli elementi di A_n costituiscono dunque un laterale di $(n-1)A_n$ in A^+ (di qui il nome di « teorema del laterale »). Sappiamo infine che, se $a_1, \dots, a_r \in A_n$ e se q è un intero, nel gruppo A^+ risulta

$$(16) \quad a_1 + \dots + a_r \in qA_n \quad \text{se e solo se} \quad r \equiv q \pmod{n-1}.$$

5. — Cerchiamo ora di definire nell'insieme degli elementi del gruppo (additivo) commutativo A^+ (v. n. preced.) una mol-

tiplicazione in modo che A^+ diventi il gruppo additivo di un anello A , e inoltre in modo (che A_n risulti un sotto- n -anello di questo anello A , cioè in modo) da subordinare in A_n la moltiplicazione ivi esistente.

Se una tale moltiplicazione esiste, essa è unica, perchè (A essendo un anello) essa deve soddisfare alla (13) del n. 3, con $a_i, b_j \in A_n$, le somme eseguite in A^+ ed r, s qualsiasi, e quindi rimane univocamente determinata (v. 2° membro della (13)) dalla moltiplicazione di A_n (si ricordi la (14)).

Assumiamo allora la (13) (ossia l'unica possibile, in relazione al nostro problema) come definizione di una moltiplicazione nel gruppo additivo commutativo A^+ (cioè nell'insieme dei suoi elementi). Cioè, in base alla (14), assumiamo come prodotto dei due elementi

$$(17) \quad x = a_1 + a_2 + \dots + a_r, \quad y = b_1 + b_2 + \dots + b_s, \\ (a_i, b_j \in A_n)$$

di A^+ (r ed s essendo qualsiasi) la somma degli rs prodotti $a_i b_j$ (calcolati nell' n -anello A_n):

$$(17') \quad xy = \sum a_i b_j.$$

Questa definizione (17), (17') ha senso ($a_i, b_j \in A_n$, quindi $\sum a_i b_j \in A^+$), ma non è affatto chiaro a priori che il prodotto xy sia indipendente dalla particolare rappresentazione (17) dei due elementi x, y di A^+ come somme di elementi di A_n . Dimosteremo ora che questa indipendenza effettivamente sussiste, cioè che vale il

LEMMA: *Nel gruppo (additivo) commutativo A^+ , circoscritto ([1], n. 2) all' n -gruppo additivo dell' n -anello A_n , dalle seguenti due eguaglianze:*

$$(18) \quad a_1 + \dots + a_r = c_1 + \dots + c_u,$$

$$(19) \quad b_1 + \dots + b_s = d_1 + \dots + d_v,$$

con $a_i, b_j, c_k, d_k \in A_n$ ed r, s, u, v numeri naturali qualsiasi, di-

scende la seguente altra:

$$(20) \quad a_1 b_1 + \dots + a_1 b_s + \dots + a_r b_1 + \dots + a_r b_s = \\ = c_1 d_1 + \dots + c_1 d_v + \dots + c_u d_1 + \dots + c_u d_v .$$

questi prodotti $a_i b_j$, $c_k d_l$ essendo naturalmente calcolati nell' n -anello A_n .

6. — Infatti, i due membri della (18) (risp. (19)) appartengono ad un medesimo laterale, pA_n (risp. qA_n), fra quelli che figurano a 2° membro della (15), quindi (v. (16)):

$$(21) \quad r \equiv p \pmod{n-1}, \quad u \equiv p \pmod{n-1},$$

$$(22) \quad s \equiv q \pmod{n-1}, \quad v \equiv q \pmod{n-1},$$

dove

$$(23) \quad 1 \leq p \leq n-1, \quad 1 \leq q \leq n-1 .$$

Dalle (21), (22) risulta rispettivamente

$$(24) \quad r + (n-p) \equiv 1 \pmod{n-1}, \\ u + (n-p) \equiv 1 \pmod{n-1},$$

$$(25) \quad s + (n-q) \equiv 1 \pmod{n-1}, \\ v + (n-q) \equiv 1 \pmod{n-1} .$$

Se m è un qualsiasi numero naturale, useremo nel seguito (per comodità espositiva) la prima di queste due scritte:

$$[m]a, \quad \underbrace{a + \dots + a}_m$$

come sostituta della seconda.

Sia a un qualsiasi elemento di A_n . Sommando (in A^+) ad ambo i membri della (18) l'elemento $(n - p)a$ e ad ambo i membri della (19) $(n - q)a$, otteniamo due nuove eguaglianze che possiamo scrivere (proprietà associativa generalizzata in A^+):

$$(26) \quad a_1 + \dots + a_r + [n - p]a = c_1 + \dots + c_u + [n - p]a,$$

$$(27) \quad b_1 + \dots + b_s + [n - q]a = d_1 + \dots + d_v + [n - q]a.$$

Per le (24), (25), il numero degli addendi è tale che si possono interpretare queste (26), (27) come eguaglianze valide nell' n -anello A_n (cfr. n. 4). Moltiplicandole in A_n , si ha in A_n l'eguaglianza

$$(28) \quad (a_1 + \dots + a_r + [n - p]a)(b_1 + \dots + b_s + [n - q]a) = \\ = (c_1 + \dots + c_u + [n - p]a)(d_1 + \dots + d_v + [n - q]a).$$

Operando ancora in A_n , poichè delle (26), (27) si trae

$$(a_1 + \dots + a_r + [n - p]a)a = (c_1 + \dots + c_u + [n - p]a)a, \\ a(b_1 + \dots + b_s + [n - q]a) = a(d_1 + \dots + d_v + [n - q]a),$$

da queste, per le (12), (12'), si ottiene

$$(29) \quad a_1a + \dots + a_ra + [n - p]a^2 = c_1a + \dots + c_ua + [n - p]a^2,$$

$$(30) \quad ab_1 + \dots + ab_s + [n - q]a^2 = ad_1 + \dots + ad_v + [n - q]a^2.$$

Le (29), (30) valgono pure nel gruppo A^+ (cfr. n. 4), quindi (semplificando) in A^+ risulta:

$$(31) \quad a_1a + \dots + a_ra = c_1a + \dots + c_ua,$$

$$(32) \quad ab_1 + \dots + ab_s = ad_1 + \dots + ad_v.$$

Ritorniamo allora alla (28), e (ricordate le (24), (25)) eseguiamo in A_n i due prodotti che in essa figurano secondo la proprietà distributiva generalizzata (13), (13'). Otteniamo così

l'eguaglianza di due somme (i cui addendi sono prodotti di elementi di A_n , quindi sono elementi di A_n), eguaglianza che è valida anche in A^+ (cfr. n. 4), e che in A^+ si può scrivere nel modo seguente:

$$\begin{aligned} & (a_1b_1 + \dots + a_1b_s + \dots + a_rb_1 + \dots + a_rb_s) + \\ & + (n - q)(a_1a + \dots + a_ra) + (n - p)(ab_1 + \dots + ab_s) + \\ & + ((n - p)(n - q))a^2 = \\ & = (c_1d_1 + \dots + c_1d_v + \dots + c_ud_1 + \dots + c_ud_v) + \\ & + (n - q)(c_1a + \dots + c_ua) + (n - p)(ad_1 + \dots + ad_v) + \\ & + ((n - p)(n - q))a^2. \end{aligned}$$

Da quest'ultima eguaglianza, in virtù delle (31) e (32), risulta appunto (semplificando) l'eguaglianza (20). Quindi il lemma è dimostrato.

7. - In base al lemma ora dimostrato, le (17), (17') definiscono effettivamente una moltiplicazione in A^+ , la quale evidentemente subordina in A_n la moltiplicazione ivi esistente. Diciamo allora A il sistema algebrico i cui elementi sono quelli di A^+ , la cui addizione (binaria) è quella del gruppo commutativo A^+ , e la cui moltiplicazione è quella ora definita. Si verifica immediatamente che questa moltiplicazione è associativa e distributiva (sia a sinistra che a destra) rispetto all'addizione. Quindi A è un anello.

Dunque il problema enunciato all'inizio del n. 5 ammette una e (2° capov. del n. 5) una sola soluzione.

Consideriamo adesso (v. (15), n. 4) il sottogruppo $(n - 1)A_n$ di A^+ . I prodotti

$$(a_1 + \dots + a_r)(b_1 + \dots + b_{n-1}), \quad (b_1 + \dots + b_{n-1})(a_1 + \dots + a_r)$$

di un elemento $a_1 + \dots + a_r$ di A per un elemento $b_1 + \dots + b_{n-1}$ di $(n - 1)A_n$ constano di $r(n - 1)$ addendi, dunque ((16)) sono elementi di $(n - 1)A_n$, il quale è dunque un ideale (bilatero) dell'anello A .

Se \bar{q} denota la classe degli interi $\equiv q \pmod{n-1}$, è chiaro (n. 4) che la corrispondenza

$$qA_n \rightarrow \bar{q} \quad (q = 1, 2, \dots, n-1)$$

è un isomorfismo dell'anello quoziente $A/(n-1)A_n$ sull'anello, $I/(n-1)$, degli interi modulo $n-1$. Dunque

$$A/(n-1)A_n \cong I/(n-1).$$

In particolare A_n (i cui elementi costituiscono un laterale dell'ideale $(n-1)A_n$ in A) è l'identità dell'anello $A/(n-1)A_n$. Abbiamo così dimostrato il seguente

TEOREMA 2: (Teorema del laterale per gli n -anelli): *Se A_n è un qualsiasi n -anello (n. 1), nel gruppo additivo A^+ , circoscritto ([1], n. 2) all' n -gruppo additivo A_n^+ di A_n , è possibile definire una ed una sola moltiplicazione in modo che A^+ diventi il gruppo additivo di un anello A e che A_n risulti un sotto- n -anello di questo anello A (n. 1).*

$(n-1)A_n$ (cioè l'insieme degli elementi di A che sono somme di $n-1$ elementi di A_n) è un ideale dell'anello A , e l'anello quoziente $A/(n-1)A_n$ è isomorfo all'anello $I/(n-1)$ degli interi modulo $n-1$.

Gli elementi del dato n -anello A_n costituiscono, nell'anello A , un laterale dell'ideale $(n-1)A_n$, e precisamente A_n è l'elemento unità dell'anello quoziente $A/(n-1)A_n$.

BIBLIOGRAFIA

- [1] BOCCIONI, D.: *Simmetrizzazione di una operazione n -aria*, Rend. Sem. Mat. Univ. Padova, vol. 35.
- [2] DÖRNTE, W.: *Untersuchungen über einen verallgemeinerten Gruppenbegriff*, Math. Zeitschrift, vol. 29 (1929), pp. 1-19.
- [3] JACOBSON, N.: *Lectures in abstract algebra, vol. I*, Van Nostrand (1951).
- [4] POST, E. L.: *Polyadic groups*, Trans Amer. Math. Soc., vol. 48 (1940), pp. 208-350.
- [5] TVERMOES, H.: *Über eine Verallgemeinerung des Gruppenbegriffs*, Math. Scandinavica, vol. 1 (1953), pp. 18-30.