
ATTI ACCADEMIA NAZIONALE DEI LINCEI
CLASSE SCIENZE FISICHE MATEMATICHE NATURALI

RENDICONTI

LUCJAN SZAMKOŁOWICZ

Sulla generalizzazione del concetto delle algebre A_n^3

*Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche,
Matematiche e Naturali. Rendiconti, Serie 8, Vol. 38 (1965), n.6, p. 810–814.*
Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1965_8_38_6_810_0>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

*Articolo digitalizzato nel quadro del programma
bdim (Biblioteca Digitale Italiana di Matematica)
SIMAI & UMI*

<http://www.bdim.eu/>

Algebra. — *Sulla generalizzazione del concetto delle algebre A_n^3* ^(*).
Nota di LUCJAN SZAMKOŁOWICZ, presentata^(**) dal Socio B. SEGRE.

DEFINIZIONE. — *Un'algebra A^k è una coppia ordinata $\langle A, \circ \rangle$, dove A è un insieme di elementi qualsiasi, e $\circ$ è una operazione binaria in A soddisfacente al seguente sistema compatibile di k condizioni:*

$$(W_0): \quad a[a] = a,$$

$$(W_l): \quad a^l[b] = b^s[a] \quad \text{per } l = 1, 2, \dots, k-2; \quad s \in \{1, \dots, k-2\},$$

$$(W_{k-1}): \quad a^{k-1}[b] = b,$$

dove $a^i[b] = a \circ (a \circ \dots \circ (a \circ b) \dots)$.

$i-1$ parentesi

Nel caso in cui l'insieme A sia finito: $|A| = n$, denoteremo l'algebra A^k con A_n^k (vedi [2], [3]).

Nel presente lavoro dimostreremo che un'algebra A^k è un quasigruppo, che ciascuna coppia di suoi elementi diversi genera un sottoinsieme che contiene esattamente k elementi distinti, e dimostreremo l'esistenza di sistemi compatibili di condizioni (W_i) nel caso $k = p^m$, p -primo.

1. Dimostriamo ora:

L. 1.1. Per ogni $a, b \in A$ esiste x , tale che $a[x] = b$. Infatti, abbiamo allora $a^{k-2}[a[x]] = a^{k-2}[b]$ e dunque $a^{k-1}[x] = x = a^{k-2}[b]$;

L. 2.1. Per ogni $a, b \in A$ esiste x , tale che $x[a] = b$.

Dim.: Secondo (W_1) esiste x , tale che $x[a] = a^s[x]$ e quindi $a^{k-1-s}[a^s[x]] = a^{k-1}[x] = x = a^{k-1-s}[b]$;

L. 3.1. $a[x] = a[y]$ implica $x = y$.

Dim.: Abbiamo $a^{k-2}[a[x]] = a^{k-2}[a[y]]$ e quindi $a^{k-1}[x] = a^{k-1}[y]$ e dunque, secondo (W_{k-1}) è $x = y$;

L. 4.1. $x[a] = y[a]$ implica $x = y$.

Dim.: Secondo (W_1) esiste s , tale che $x[a] = a^s[x]$ e $y[a] = a^s[y]$ e quindi $a^{k-1-s}[a^s[x]] = a^{k-1-s}[a^s[y]]$; allora $a^{k-1}[x] = a^{k-1}[y]$ e dunque, secondo (W_{k-1}) , è $x = y$.

In forza di L. 1.1-L. 4.1 abbiamo subito il:

TEOREMA 1. — *Ciascun'algebra A^k è un quasigruppo.*

Dimostriamo ora:

L. 1.2. Se $a \neq b$, allora $a^i[b] \neq a$ per $i = 1, \dots, k-1$.

(*) Lavoro eseguito nell'ambito dell'*Impresa matematica* del C.N.R. presso l'Università di Roma.

(**) Nella seduta del 17 giugno 1965.

Dim.: Abbiamo $a^{k-1-i} [a^i [b]] = a^{k-1} [b] = b$ e $a^{k-1-i} [a] = a$ e quindi, se fosse $a^i [b] = a$, sarebbe $a = b$.

Da (W_i) e da L. 1.2. risulta:

L. 2.2. Se $a \neq b$, allora $a^i [b] \neq b$ per $i = 1, \dots, k-2$.

Dimostriamo anche che:

L. 3.2. Se $a \neq b$, allora $a^i [b] \neq a^j [b]$ per $i \neq j$; $i, j = 1, \dots, k-1$.

Dim.: Se fosse $a^i [b] = a^j [b]$, $i = j + s$, $s > 0$, si avrebbe $a^{k-1-i} [a^i [b]] = a^{k-1-i} [a^j [b]]$ e quindi $a^{k-1} [b] = a^{k-1-s} [b]$, e dunque, secondo (W_{k-1}) si avrebbe $b = a^{k-1-s} [b]$, che contraddice L. 2.2.

In forza L. 1.2.-L. 3.2. abbiamo subito il:

TEOREMA 2. - *Ciascuna coppia di elementi diversi dell'algebra A^k genera un sottoinsieme che contiene almeno k elementi distinti.*

2. Sia adesso: $a^m [b] = b^j [a]$, $a^{j+1} [b] = b^s [a]$, $a [b] = b^t [a]$, $a^{t+j} [b] = b^p [a]$. Dimostriamo (ora e nel seguito sottointenderemo di effettuare la somma degli esponenti modulo $k-1$) che:

$$\text{L. 1.3.} \quad a^i [b] [a^{i+m} [b]] = \begin{cases} a, & \text{per } j+1=0, \\ b, & \text{per } s+i=0, \\ a^{s+i} [b] & \text{negli altri casi.} \end{cases}$$

Dim.: Secondo (W_m) è $a^i [b] [a^{i+m} [b]] = a^i [b] [a^m [a^i [b]]] = a^i [b] [a^i [b]^j [a]] = a^i [b]^{j+1} [a]$; se $j+1 = k-1$, abbiamo $a^i [b]^{j+1} [a] = a$, mentre se $j+1 \neq 0$, abbiamo $a^i [b]^{j+1} [a] = a^s [a^i [b]] = a^{s+i} [b]$ ($= b$ per $s+i=0$).

$$\text{L. 2.3.} \quad a^{i+m} [b] [a^i [b]] = \begin{cases} a, & \text{per } t+j=0, \\ b, & \text{per } p+i=0, \\ a^{p+i} [b] & \text{negli altri casi.} \end{cases}$$

Dim.: secondo (W_m) e (W_1) , abbiamo $a^{i+m} [b] [a^i [b]] = a^m [a^i [b]] [a^i [b]] = a^i [b]^j [a] [a^i [b]] = a^i [b]^{t+j} [a]$; se $t+j=0$, abbiamo $a^i [b]^{t+j} [a] = a$, mentre in caso contrario è $a^i [b]^{t+j} [a] = a^p [a^i [b]] = a^{p+i} [b]$ ($= b$ se $p+i=0$).

È subito visto che:

$a [a^i [b]] = a^{i+1} [b]$ ($= b$ se $i+1=0$); $a^i [b] [a] = a^t [a^i [b]] = a^{t+i} [b]$ ($= b$ se $i+t=0$); $b (a^i [b]) = b [b^q [a]] = b^{q+1} [a]$ ($= a$ se $q+1=0$ o $a^r [b]$ in caso contrario); $a^i [b] [b] = b^t [a^i [b]] = b^t [b^q [a]] = b^{t+q} [a]$ ($= a$ se $t+q=0$ o $a^r [b]$ in caso contrario).

Da qui, da L. 1.3., da L. 2.3. e dai Teoremi 1 e 2 si ha subito il:

TEOREMA 3. - *Ciascuna coppia di elementi diversi dell'algebra A^k genera un sottoinsieme che contiene esattamente k elementi distinti.*

3. Si può ora domandare: *per quali k esiste un sistema compatibile di condizioni (W_i) , e quanti sistemi siffatti esistono per un k fissato?*

Presentiamo intanto alcune condizioni che sono necessarie per la compatibilità del sistema (W_i) , ma che risultano sufficienti soltanto per $k < 7$.

È subito visto che:

$$(C\ 1): \quad (W_i): a^i [b] = b^j [a] \quad \text{implica} \quad (W_j): a^j [b] = b^i [a].$$

Dimostriamo che:

$$(C\ 2): \quad (W_i): a^i [b] = b^j [a] \quad \text{implica} \quad a^{i+j} [b] \neq b^{j+i} [a].$$

Dim.: Sia $a \neq b$ e poniamo $a^i [b] = c$. Se fosse $a^{i+j} [b] = b^{j+i} [a]$, sarebbe $a^i [c] = b^j [c]$, è dunque per la (W_i) sarebbe $a^i [b] = b^j [a]$ e perciò sarebbe $c^s [a] = c^s [b]$, e quindi $a = b$.

$$(C\ 3): \quad (W_i): a^i [b] = b^{i+2} [a] \quad \text{implica} \quad a^{i+1} [b] \neq b^{i+1} [a].$$

Dim.: Sia $a \neq b$ e poniamo $ba = c$. Se fosse $a^{i+1} [b] = b^{i+1} [a]$ sarebbe:

$$(1) \quad a^{i+1} [b] = b^{i+1} [a] = b^i [c] = [c]^{i+2} [b] = c [c^{i+1} [b]],$$

$$(2) \quad a^i [b] = b^{i+2} [a] = b^{i+1} [c] = c^{i+1} [b];$$

d'altronde, in forza della (2), è:

$$(3) \quad a^{i+1} [b] = a [a^i [b]] = a [c^{i+1} [b]]$$

e, secondo la (1) e la (3) risulta:

$$a [c^{i+1} [b]] = c [c^{i+1} [b]]$$

e quindi, in base al Teorema 1, sarebbe $a = c$.

$$(C\ 4): \quad W_i: a^i [b] = b^{i+3} [a] \quad \text{implica} \quad a^{i+1} [b] \neq b^{i+2} [a].$$

Dim.: Sia $a \neq b$ e $ab = c$. Se fosse $a^{i+1} [b] = b^{i+2} [a]$, sarebbe:

$$(1') \quad b^{i+1} [a] = a^{i+2} [b] = a^{i+1} [c] = c^{i+2} [a] = c [c^{i+1} [a]],$$

$$(2') \quad b^i [a] = a^{i+3} [b] = a^{i+2} [c] = c^{i+1} [a],$$

d'altra parte, in forza della (2'), è:

$$(3') \quad b^{i+1} [a] = b [b^i [a]] = b [c^{i+1} [a]],$$

e, secondo la (1') e la (3') risulta:

$$b [c^{i+1} [a]] = c [c^{i+1} [a]],$$

e quindi, in base al Teorema 1, sarebbe $a = c$.

4. Usufruendo delle condizioni (C 1)–(C 4), è facile dimostrare che:

a) Esiste al più un sistema compatibile di condizioni per le algebre A^3 e A^4 (vedi [2]);

b) esistono al più due sistemi compatibili di condizioni per l'algebra A^5 :

$$A^{5'}: (W_0): a[a] = a, (W_1): a[b] = [a], (W_2): a^2[b] = b^3[a], (W_4): a^4[b] = b;$$

$$A^{5''}: (W_0): a[a] = a, (W_1): a[b] = b^2[a], (W_3): a^3[b] = b^3[a], (W_4): a^4[b] = b;$$

c) non esiste alcun sistema compatibile di condizioni per l'algebra A^6 .

Si dimostra facilmente la *compatibilità* delle assiomatiche $A^3, A^4, A^5, A^{5''}$ usufruendo dei seguenti modelli:

Sia γ_q un campo di Galois d'ordine q (con $q = p^m$, ove p è un numero primo e h e un intero positivo).

Prendiamo un *elemento primitivo* di questo campo, cioè un elemento $b \neq 0$, tale che risulta $b^s \neq 1$ per ciascun $s \neq q - 1$. Introduciamo ora l'operazione $\circ$ sugli elementi di γ_q definita nel modo seguente: $x \circ y = (1 - b)x + by$. Abbiamo evidentemente: (1): $x^i[y] = (1 - b^i)x + b^i y \neq y$, per $i \neq q - 1$, e $x^{q-1}[y] = y$. È anche $x \circ x = x$. Mettendo in (1) $b^j = 1 - b^i$, si ottiene $x^i[y] = y^j[x]$. Si ha così un modello per le algebre A^k nel caso $k = q = p^m$.

Abbiamo (vedi [1]):

TEOREMA 4. - Per $k = q = p^m$ (p -primo) esiste almeno un sistema compatibile di condizioni per A^k .

Nel caso di A^3 , si ha $b = 2, x \circ y = 2(x + y)$; nel caso di A^4 , b è un qualsiasi elemento diverso da 0 e 1; nel caso di $A^{5'}$, $b = 3, x \circ y = 3(x + y)$ e per $A^{5''}$ si ha $b = 2, x \circ y = 4x + 2y$.

È facile anche verificare che esistono esattamente due sistemi compatibili di condizioni per le algebre A^7, A^8, A^9 :

$$A^{7'}: (W_0): a[a] = a, (W_1): a[b] = b^5[a], (W_2): a^2[b] = b^2[a], (W_3): a^3[b] = b^4[a], (W_6): a^6[b] = b;$$

$$A^{7''}: (W_0): a[a] = a, (W_1): a[b] = b^5[a], (W_2): a^2[b] = b^3[a], (W_4): a^4[b] = b^4[a], (W_6): a^6[b] = b;$$

$$A^{8'}: (W_0): a[a] = a, (W_1): a[b] = b^3[a], (W_2): a^2[b] = b^6[a], (W_4): a^4[b] = b^5[a], (W_7): a^7[b] = b;$$

$$A^{8''}: (W_0): a[a] = a, (W_1): a[b] = b^5[a], (W_2): a^2[b] = b^3[a], (W_4): a^4[b] = b^6[a], (W_7): a^7[b] = b;$$

$$A^{9'}: W_0: a[a] = a, (W_1): a[b] = b^2[a], (W_3): a^3[b] = b^6[a], (W_4): a^4[b] = b^4[a], (W_5): a^5[b] = b^7[a], (W_8): a^8[b] = b;$$

$$A^{9''}: W_0: a[a] = a, (W_1): a[b] = b^3[a], (W_2): a^2[b] = b^5[a], (W_4): a^4[b] = b^4[a], (W_6): a^6[b] = b^7[a], (W_8): a^8[b] = b.$$

Usufruento del campo di Galois d'ordine 11, si vede che esistono almeno quattro sistemi compatibili di condizioni per A^{11} (esistono quattro elementi primitivi: 2, 6, 7, 8).

È interessante sapere per quali k, n esistano le algebre A_n^k , perché l'esistenza di un'algebra siffatta implica l'esistenza di un sistema di Steiner $\sigma(2, k, n)$. È subito visto che non vale il viceversa (non appena sia $k > 3$).

BIBLIOGRAFIA.

- [1] B. SEGRE, *Lectures on modern geometry*, Roma (1961).
- [2] L. SZAMKOŁOWICZ, *On the problem of existence of finite regular planes*, « Colloquium Math. », 9, (2), 245–250 (1962).
- [3] L. SZAMKOŁOWICZ, *Alcuni problemi della teoria dei sistemi di Steiner*, « Rendiconti di matematica e delle sue applicazioni » (in corso di stampa).

RÉSUMÉ. — Nous appelons algèbre A^k une paire ordonnée $\langle A, \circ \rangle$, où A est un ensemble et $\circ$ est une opération binaire satisfaisant aux conditions:

$$\begin{aligned} (W_0): & \quad a[a] = a \\ (W_l): & \quad a^l[b] = b^s[a], \quad l = 1, 2, \dots, k-2; \quad s \in \{1, 2, \dots, k-2\}, \\ (W_{k-1}): & \quad a^{k-1}[b] = b, \end{aligned}$$

où $a^i[b] = a \circ (a \circ \dots \circ (a \circ b) \dots)$.

$i-1$ parenthèses

Toute algèbre A^k est un quasigroupe et chaque paire d'éléments différents $a, b \in A$ engendre un ensemble à k éléments.

Pour trouver la solution du problème d'existence d'un système non-contradictoire des conditions (W_i) , on présente ici certaines modèles pour les algèbres A^k (seulement pour tout k de la forme p^n , p -nombre premier), et exemples des tous systèmes des conditions pour $k < 11$.