ALEF

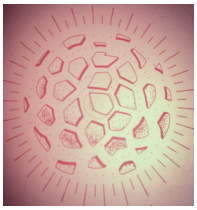
COLLANA DI LOGICA MATEMATICA, ALGEBRA E GEOMETRIA

3

Il logo richiama il *paradosso di Banach–Tarski*, per il quale, accettando l'assioma della scelta, è possibile ripartire una sfera di R^3 in un numero finito di parti e, mediante rotazioni e traslazioni, ricomporle ottenendo due sfere aventi lo stesso volume della sfera data.

ALEF

COLLANA DI LOGICA MATEMATICA, ALGEBRA E GEOMETRIA



L'essenza della Matematica è nella sua libertà

George Cantor

Áleph (א) è la prima lettera dell'alfabeto fenicio e la prima lettera dell'alfabeto ebraico. In matematica il simbolo $\aleph_0$ (*aleph–zero*) indica il numero cardinale dell'insieme dei numeri naturali ed è il più piccolo numero cardinale transfinito.

La nascita e lo sviluppo della teoria degli insiemi, a partire dalla seconda metà dell'Ottocento, fu resa possibile dall'accettazione, principalmente da parte di Cantor, del concetto di infinito attuale. Il linguaggio degli insiemi è l'alfabeto comune con cui si esprimono la Logica, l'Algebra e la Geometria e la maggior parte dei settori della Matematica.

Le tre discipline, negli ultimi due secoli, hanno avuto un considerevole e progressivo sviluppo, sia teorico che pratico, tale da costituire oggi il nucleo di base e il fondamento delle competenze nella maggior parte delle aree scientifiche. Tutto ciò ha reso necessaria la conoscenza sempre più approfondita ed estesa dei risultati ottenuti e dei metodi coinvolti nell'ambito della ricerca di queste tre materie.

ALEF ha, tra i suoi obiettivi, proprio quello di soddisfare tale esigenza di divulgazione e diffusione di dati, teorie, modelli e metodi, attraverso pubblicazioni che accolgano manuali universitari e cicli di lezioni di dottorato, monografie e atti di convegni, sia nazionali che internazionali.

Vai al contenuto multimediale

Libero Verardi

Algebre monounarie finite

Aracne editrice

www.aracneeditrice.it
info@aracneeditrice.it

www.gioacchinoonoratieditore.it
info@gioacchinoonoratieditore.it

via Vittorio Veneto, 20
00020 Canterano (RM)
(06) 45551463

ISBN 978-88-255-0861-1

I edizione: marzo 2018

Indice

Introduzione

Questo libro intende riunire risultati ottenuti da me e da alcuni collaboratori ed allievi nel corso di oltre un decennio, dal 2005 al 2016, sulle strutture (X,f) costituite da un insieme X e da una funzione f di dominio e codominio X e denominate *algebre monounarie*. Soprattutto, intende valorizzare il lavoro svolto nei vari anni da un gruppo di laureandi, i quali hanno messo a frutto le competenze algebriche, combinatorie, informatiche e statistiche apprese nei vari insegnamenti del corso di laurea in Matematica a Bologna.

Il mio interesse per questo argomento è incominciato dopo una rilettura degli assiomi di Peano: in questi ultimi si considera infatti una terna $(N,\sigma,0)$ in cui σ è appunto una funzione iniettiva da N ad N, e questa è un'algebra unaria con *elemento iniziale* 0.

Nel caso continuo le algebre unarie erano state studiate soprattutto dal punto di vista topologico. Qui invece si guardano inizialmente da un punto di vista algebrico, in particolare nel caso finito: sottoalgebre, congruenze, isomorfismi, operazioni fra algebre, rappresentazioni algebriche e geometriche mediante opportuni digrafi. Si classificano poi anche casi particolari: algebre "cicliche", semplici, connesse. Questa parte è stata sviluppata insieme alle colleghe Bianchi e Gillio e in gran parte già pubblicata. Alcuni ulteriori sviluppi sono dovuti a tre mie laureande Poni, Galbucci e Tonti.

Nel caso finito si può considerare come X l'insieme dei numeri naturali da 1 ad n e l'isomorfismo di algebre monounarie (X,f) come il coniugio delle funzioni rispetto al gruppo simmetrico S_n: il numero delle classi d'isomorfismo coincide col numero delle orbite ed è interessante contarle per classificare le algebre d'ordine n. Il computo delle orbite e della loro lunghezza è stato eseguito con approcci diversi da me e dal mio laureando Gelosi, fino all'ordine 10. Per ogni $n \leqslant 8$ è dato anche esplicitamente l'elenco delle algebre e dei loro digrafi. Il dott. Gelosi ha poi calcolato con formule sue e l'ausilio del software Mathematica anche il numero di algebre non isomorfe di ordine $n = 11$ e $n = 12$.

La difficoltà di contare queste funzioni e raggrupparle in classi d'isomorfismo ha portato a cercare criteri di classificazione meno stretti. Lo studio delle funzioni con "nuclei" isomorfi è stato oggetto di una mia comunicazione ad un convegno di Combinatoria Algebrica a Bologna.

Una funzione da X ad X si può fornire mediante la tabella, riducibile alla lista dei valori. Tuttavia, in certi casi servono meno dati: scelto come insieme

X l'anello Z_n delle classi di resti mod n, alcune funzioni possono essere descritte come polinomi di grado $\leqslant$ n–1. Il problema si riconduce al caso di $n = p^m$, ossia n potenza di un primo p. Questo argomento è stato sviluppato poi dalle mie allieve Accogli, Mazzoni e Tosetti. Quest'ultima, dopo aver eseguito numerose prove mediante il software Pithon, ha formulato una interessantissima congettura sull'andamento del numero di queste funzioni al variare di p e al tendere di m all'infinito.

Alcune funzioni polinomiali sono biiettive; i casi di polinomi sui campi reale, complesso e finito sono stati esaminati nella tesi della mia allieva Righetti. Nel caso di n non primo, lo studio delle funzioni polinomiali biiettive e del loro gruppo rispetto alla composizione ha dato risultati convincenti nel caso p = 2, mentre per i primi dispari non ancora.

A somiglianza del metodo di Peano per costruire le operazioni binarie in N a partire dalla funzione "successivo di", si sono cercati modi di definire operazioni binarie su algebre monounarie finite, almeno in casi particolari.

Ci sono infine altri aspetti, per i quali si dà qualche risultato:

a) le funzioni non polinomiali si possono "approssimare" in vari modi mediante funzioni polinomiali, a somiglianza del polinomio di Taylor o del polinomio interpolatore di Lagrange. Talvolta questo approccio ha portato a poter contare le funzioni polinomiali biiettive;
b) la tabella di una funzione si può convertire in una matrice d'incidenza e da questa per ogni primo p si costruisce un p–gruppo finito speciale, mediante un metodo da me usato in varie pubblicazioni. Interessante è vedere come le proprietà della funzione si traducano in proprietà del p–gruppo e viceversa;
c) un elenco di problemi legati alle algebre monounarie finite è dato in appendice, insieme con lunghe tabelle riassuntive, programmi per computer e statistiche varie.

Capitolo I

Proprietà generali delle algebre monounarie finite

Siano X un insieme non vuoto ed $f:X\to X$ un'applicazione. Se interpretiamo f come una operazione "unaria" su X, possiamo considerare la struttura algebrica (X, f), che chiameremo "algebra monounaria".

In questa prima sezione studieremo questo tipo di strutture esattamente come si procede con quelle basate su operazioni binarie[1], esaminandone sottoalgebre, congruenze, algebre quoziente, algebre semplici, ideali, omomorfismi, automorfismi. Per farlo, ci serviremo anche di una loro rappresentazione geometrica come particolari grafi orientati, mettendone in luce le proprietà topologiche e combinatorie. Si potranno così evidenziare i legami fra i due tipi di approcci, algebrico e geometrico e si potranno travasare risultati e tecniche di dimostrazione da un ambiente all'altro.

Nel seguito, soprattutto nel caso finito, chiameremo rispettivamente *ordine* ed *indice* dell'algebra (X, f) i numeri cardinali $|X|$ e $|\mathrm{Im}(f)|$. Quest'ultimo numero sarà denotato sovente con $i(f)$.

Nei disegni dei grafi orientati associati alle algebre monounarie adotteremo la seguente convenzione, per evitare quanto possibile l'uso delle frecce:

a) rappresenteremo i nodi con piccoli quadratini vuoti;
b) per i circuiti l'orientamento sarà antiorario;
c) per i rami che portano ai vertici facenti parte del circuito, l'orientamento sarà verso il circuito.

1.1. Rappresentazioni e sottoalgebre

Sia (X, f) un'algebra monounaria. Se l'insieme sostegno X è finito con n elementi, possiamo rappresentare f come di consueto con una tabella che elenchi le coppie $(x,f(x))$. Identificando X con l'insieme dei primi n numeri naturali non nulli, possiamo rappresentare f mediante la scrittura a due righe, usata di solito per le permutazioni:

1. Cfr. P.M. Cohn, *Algebra universale*, Feltrinelli, 1971.

$$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

ridotta eventualmente alla lista (f(1), ..., f(n)), se non ci sono ambiguità. Possiamo anche usare la matrice $M_f = [m_{ij}]$ d'ordine n, definita da

$$m_{ij} = \begin{cases} 1 \text{ se } f(i) = j \\ 0 \text{ altrimenti} \end{cases}$$

che è la *matrice d'incidenza* della relazione f tra X e se stesso.

Talora useremo anche come insieme X l'anello $\mathbf{Z}_n$ delle classi di resti mod n, identificato con l'insieme $\{0,1\dots n-1\}$, nel quale molte funzioni possiedono rappresentazioni algebriche, che consentono l'uso di strumenti di calcolo.

Esiste anche una rappresentazione geometrica delle algebre monounarie finite, mediante digrafi di tipo particolare. Ad un'algebra monounaria finita (X, f) si può associare in modo naturale un *grafo orientato*, i cui vertici sono gli elementi di X ed in cui $x \to y \Leftrightarrow y = f(x)$. Poiché f è una funzione, allora da ogni vertice esce una ed una sola freccia. In particolare, partendo da un elemento $x_0 \in X$ ed applicando ripetutamente f, si ottiene una successione finita

$$x_0 \to x_1 = f(x_0) \to \dots \to x_{i+1} = f(x_i)$$

dove l'ultimo termine uguaglia uno dei termini x_j già incontrati. Si genera così un *circuito* comprendente $x_j, x_{j+1} \dots, x_i$, a cui è "attaccato" il *co–albero*[2] $x_0, x_1, \dots, x_j + 1$. Ogni circuito può avere più "accessi", ma non ha "uscite". Più precisamente, ad ogni nodo di un circuito possono essere attaccati dei co–alberi attraverso il loro nodo terminale.

Esempio 1.1.1. Sia data la funzione $f : \mathbf{Z}_6 \to \mathbf{Z}_6$, $f : x \mapsto x^2 - 1$. L'algebra monounaria si può rappresentare nei vari modi seguenti, algebrici e geometrici. Sono mostrate in particolare due versioni del digrafo, una dettagliata ed una astratta. Per comodità, lo zero è sostituito col 6. Si veda la Fig. 1.1.

Due vertici x, y del digrafo sono detti *connessi* se esiste una sequenza finita

$$x = x_0, x_1, \dots, x_n = y$$

di vertici, ciascuno adiacente al successivo. In tal caso, esiste al più un j tale che:

$$x = x_0 \to x_1 \to \dots \to x_j \leftarrow \dots \leftarrow x_n = y$$

2. Detto anche *albero duale*, è ottenuto da un *albero* invertendo il verso delle frecce.

dato che, altrimenti, da almeno un vertice dovrebbero uscire due frecce. Se si ha

$$x_0 \to x_1 \to \cdots \to x_n \text{ oppure } x_0 \leftarrow \ldots \leftarrow x_n$$

considereremo rispettivamente j = n e j = 0. Ciò posto, la relazione di connessione C è una relazione d'equivalenza, le cui classi sono dette *componenti connesse*. Il *rango* r(f) dell'algebra (X, f) è il numero di tali componenti del grafo Γ. Il precedente Esempio 1.1 mostra una funzione non biiettiva, il cui grafo è composto da due componenti connesse dello stesso tipo.

Come naturale, due algebre monounarie (X, f) ed (X', f') si dicono *isomorfe* se esiste $\Phi : X \xrightarrow[su]{1-1} X'$, tale che per ogni $x \in X$ si ha $\Phi(f(x)) = F'(\Phi(x))$.

In particolare, se X' = X, allora $\Phi \in S_X$ e si ha $f' = \Phi \circ f \circ \Phi^{-1}$, ossia f ed f' sono funzioni "coniugate" rispetto al gruppo simmetrico S_X. Torneremo più avanti su questo aspetto.

Dal punto di vista geometrico, sappiamo che due grafi Γ e Γ' sono detti *isomorfi* se esiste una biiezione φ tra i loro nodi, tale che per ogni coppia di nodi x, y di Γ si abbia: $x \to y \Leftrightarrow \varphi(x) \to \varphi(y)$. Ne segue subito la proposizione seguente.

Proposizione 1.1.2. Due algebre monounarie (X, f) ed (X', f') sono isomorfe se e solo se lo sono i loro digrafi Γ(X, f) e Γ(X', f').

Dimostrazione. Dato l'isomorfismo Φ fra le algebre, posto $\varphi = \Phi$ ed y = f(x), la condizione $\Phi(f(x)) = f'(\Phi(x))$ esprime proprio il fatto che $x \to y \Leftrightarrow \varphi(x) \to \varphi(y)$, perciò φ è un isomorfismo tra i due digrafi. L'affermazione inversa si dimostra analogamente.

Siano ora m, d tali che $0 \leqslant m \leqslant \infty$, $1 \leqslant d \leqslant \infty$. Nel seguito denoteremo con $C_{m,d}$ le algebre monounarie isomorfe alle seguenti:

x	f(x)
1	6
2	3
3	2
4	3
5	6
6	5

$$\Rightarrow M_f = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \Rightarrow f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 3 & 6 & 5 \end{pmatrix}$$

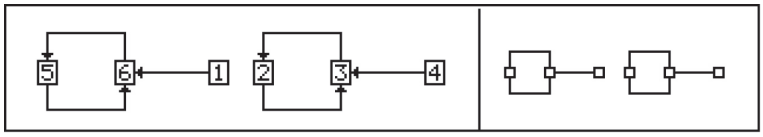


Figura 1.1. Rappresentazioni tabulari, algebriche e grafiche di una funzione.

a) tipo $C_{\infty,\infty}$: (Z, σ), dove $\sigma(x) = x+1$. La σ è biiettiva;
b) tipo $C_{0,\infty}$: $(\mathbf{N}, \sigma)$, dove $\mathbf{N}$ è l'insieme dei numeri naturali e $\sigma(x) = x+1$. In questo caso, σ è iniettiva, $\mathrm{Im}(\sigma) = \mathbf{N}\setminus\{0\}$;
c) tipo $C_{m,d}$: $0 \leqslant m \leqslant \infty$, $1 \leqslant d \leqslant \infty$: $\left(\left\{x \in \mathbf{Z} \mid -m \leqslant x \leqslant d-1\right\}\psi\right)$ dove:

$$\psi(x) = \begin{cases} x+1 \text{ se } x < d-1 \\ 0 \text{ se } x = d-1. \end{cases}$$

Circa queste ultime, se $m = 0$, le algebre di tipo $C_{0,d}$ saranno dette *cicli*: in tal caso, ψ è una permutazione ciclica di lunghezza d, ed il suo digrafo è un circuito. Se $m > 0$, allora 0 è l'unico elemento con due preimmagini. Sul sottoinsieme $\{0, \ldots, d-1\}$ l'applicazione ψ agisce come un ciclo di lunghezza d. In particolare, se $d = 1$ allora 0 è un *punto unito* per ψ. Si osservi che se $0 < m < \infty$ allora $\mathrm{Im}(\psi) = \{-m+1, \ldots, d-1\}$, mentre se $m = \infty$, ψ è suriettiva.

Nota. Le algebre $C_{m,\infty}$ del tipo $\left(\left\{x \in \mathbf{Z} \mid -m \leqslant x\right\}, \psi\right)$, dove $\sigma(x) = x+1$, sono tutte isomorfe a $C_{0,\infty}$.

Sottoalgebre. Una *sottoalgebra* $(Y, f_{|Y})$ di (X, f) ha come sostegno un sottoinsieme Y *chiuso* rispetto ad f, ossia tale che per ogni $y \in Y$ si ha $f(y) \in Y$; l'operazione è la restrizione ad Y dell'applicazione f. Denoteremo nel seguito con f anche le restrizioni di f ai sottoinsiemi chiusi.

Esempio 1.1.3.

a) Per ogni algebra (X, f), $\varnothing$, X ed $\mathrm{Im}(f)$ sono sottoalgebre. Come sempre, le prime due sono dette rispettivamente sottoalgebra *banale* ed *impropria*;
b) ogni componente connessa di un'algebra (X, f) è una sottoalgebra;
c) le algebre di tipo $C_{0,d}$, ossia i cicli di lunghezza $d \geqslant 1$, non hanno sottoalgebre proprie, e sono dette algebre *minimali*.

Nota. Ogni sottoalgebra dell'algebra $C_{0,\infty}$, che contenga lo zero è impropria: questo è quanto affermato dal principio d'induzione di Peano.

È immediato verificare che l'unione e l'intersezione di una famiglia qualunque di sottoalgebre è una sottoalgebra. Pertanto, il reticolo delle sottoalgebre, che denoteremo con $\zeta(X, f)$ $(= (\zeta(X, f), \subseteq))$, è un sottoreticolo completo del reticolo $(\wp(X), \subseteq)$ dei sottoinsiemi di X. In particolare, è

distributivo, per cui, se X è finito, le catene massimali che congiungono la sottoalgebra banale con l'impropria hanno tutte la stessa lunghezza[3].

Per ogni $x \in X$, la minima sottoalgebra che contiene x sarà denotata con $\langle x \rangle$, e sarà detta sottoalgebra 1–*generata*. Posto $x_0 = x$ e, per induzione, $x_{n+1} = f(x_n)$ per ogni $n \geqslant 0$, si ha subito:

$$\langle x \rangle = \left\{ x_n | n \in \mathbf{N} \right\}$$

In particolare, ogni sottoalgebra Y sarà unione di sottoalgebre 1−generate, in quanto se Y è una sottoalgebra ed $x \in Y$ allora per ogni $n \in \mathbf{N}$ si ha $x_n = f^n(x) \in Y$.

Inoltre, per ogni x, si ha $|\langle x \rangle \setminus \mathrm{Im}(f)| \leqslant 1$. Vediamo la loro struttura.

Proposizione 1.1.4. Siano dati l'algebra monounaria (X, f) ed $x \in X$. Allora sono possibili per $\langle x \rangle$ i due casi seguenti:

a) se $\langle x \rangle$ è infinito, è di tipo $C_{0,\infty}$;
b) se $\langle x \rangle$ è finito, è di tipo $C_{m,d}$, con m, d finiti.

Dimostrazione. Se per ogni n, $m \geqslant 0$, $m \neq n$, si ha $x_m \neq x_n$, allora $\langle x \rangle$ è infinito ed $f : \langle x \rangle \to \langle x \rangle \setminus \{x\}$ è biettiva. Se poi Y è una sottoalgebra di $\langle x \rangle$ contenente x, allora contiene anche ogni $x_n = f_n(x)$ e quindi coincide con $\langle x \rangle$. Siamo cioè nel caso *a*).

Se invece esistono n, m, con $m < n$ tali che $x_m = x_n$, se m è il minimo indice di un elemento che si ripete ed $n = m+d$ è il minimo indice che fornisce $x_n = x_m$, si ha $\langle x \rangle = \{x_i \mid 0 \leqslant i \leqslant m + d - 1\}$, quindi $|\langle x \rangle| = m + d$.

Se $m > 0$, il solo elemento con due preimmagini in $\langle x \rangle$ è $x_m = f(x_{m-1}) = f(x_{m+d-1})$, ed f agisce come un ciclo di lunghezza d su $\{x_i \mid m \leqslant i \leqslant m + d - 1\}$. Se $m = 0$, $f_{|\langle x \rangle|}$ è quindi un ciclo di lunghezza d, e siamo nel caso *b*).

Corollario 1.1.5.

a) Le sole algebre minimali sono i cicli, di tipo $C_{0,d}$;
b) gli *atomi* del reticolo $\zeta(X, f)$, ossia i suoi elementi minimali, sono i cicli, di tipo $C_{0,d}$.

Fra le sottoalgebre 1–generate, o meglio fra i cicli, ci sono quelle del tipo $C_{0,1}$ ossia i singoletti $\{x\}$ in cui x è un elemento *unito* per f. Poniamo:

$$Fix(X, f) = \{x \in X | f(x) = x\}.$$

3. Cfr. G. Szasz, *Introduction to Lattice Theory*, ACAD Press 1963.

Quest'ultimo sottoinsieme è una sottoalgebra di (X, f) inclusa in Im(f). Inoltre, $(\varphi(\mathrm{Fix}(X, f)), \subseteq)$ è un sottoreticolo di $(\zeta(X, f), \subseteq)$.

Caratterizziamo ora alcune algebre in base alla struttura del reticolo delle sottoalgebre. Vediamo per primo il seguente problema: per quali f può accadere che $\zeta(X, f)$ sia un'algebra di Boole? Questo problema ha senso anche per i gruppi, ed è risolto dal teorema di Ore[4]. Nel nostro caso si ha:

Teorema 1.1.6.

a) Se $\zeta(X, f)$ è un'algebra di Boole allora f è biiettiva;
b) se f è biiettiva di periodo finito nel gruppo simmetrico su X, allora $\zeta(X, f)$ è un'algebra di Boole.

Dimostrazione. Innanzitutto, $\zeta(X, f)$ è un'algebra di Boole se e solo se ogni sottoalgebra è complementata da una sottoalgebra, e poiché le operazioni reticolari sono l'unione e l'intersezione "insiemistiche", ciò significa che se Y è una sottoalgebra, anche $Y' = X \setminus Y$ deve esserlo. Ciò posto:

a) se $\zeta(X, f)$ è un'algebra di Boole, poiché Im(f) è una sottoalgebra, anche (Im(f))' è una sottoalgebra, e ciò è possibile solo se è vuoto. Dunque, f è suriettiva. Inoltre, per ogni $x \in X$, $\langle x \rangle$ è una sottoalgebra, per cui anche $\langle x \rangle'$ lo è. Essendo f suriettiva esiste $y \in X$ tale che $f(y) = x$. Se $y \notin \langle x \rangle$, allora $y \in \langle x \rangle'$, per cui $x = f(y) \in \langle x \rangle'$, assurdo. Ne segue $y \in \langle x \rangle$, quindi esiste $m \in \mathbf{N}$, tale che $y = x_m$. Ma allora $\langle x \rangle$ è una sottoalgebra con al più m elementi, ossia finita, quindi su di essa la f, che è suriettiva, è anche iniettiva. Se dunque $x = f(y) = f(y')$ allora y, $y' \in \langle x \rangle$, ed allora $y = y'$. Di qui segue f biiettiva;
b) supponiamo f biiettiva di periodo m. Siano Y una sottoalgebra e Y' il suo complemento. Sia infine $x \in Y'$ tale che $y = f(x) \notin Y'$: ma allora $y \in Y$, quindi per ogni $n \in \mathbf{N}$ si ha $f^n(y) \in Y$. Posto $y_{m-1} = f^{m-1}(y)$, si ha $y_{m-1} \in Y$ e $f(y_{m-1}) = f^m(y) = y = f(x)$. Per la iniettività di f segue però $y_{m-1} = x$, che apparterrebbe così ad Y, assurdo. Dunque, $y \in Y'$ e Y' è una sottostruttura a sua volta.

Corollario 1.1.7. Sia X un insieme finito e sia $f: X \to X$. Allora f è una permutazione di X se e solo se $\zeta(X, f)$ è un'algebra di Boole.

Osservazione. Nell'algebra $(\mathbf{Z}, \sigma)$ in cui si ha $\sigma: \mathbf{Z} \to \mathbf{Z}$, $\sigma(x) = x + 1$, σ ha periodo infinito e le sottoalgebre di $(\mathbf{Z}, \sigma)$ sono solo quelle cicliche. Pertanto, pur essendo σ biiettiva, $\zeta(\mathbf{Z}, \sigma)$ non è un'algebra di Boole.

4. Cfr. R. Schmidt, *Subgroup Lattices of Groups*, de Gruyter, 1994, p. 12.

Un altro tipo di reticoli distributivi notevoli sono le catene. Per i gruppi è ben noto che il reticolo dei sottogruppi è una catena se e solo se G è un p–gruppo ciclico oppure è un p-gruppo di Prüfer[5]. Nel nostro caso si ha:

Teorema 1.1.8. Se $\zeta(X, f)$ è totalmente ordinato, allora (X, f) è uno dei tipi seguenti:

a) se f non è suriettiva, (X, f) è "ciclica", ossia di tipo $C_{0,\infty}$ o $C_{m,d}$, $m > 0$;
b) se f è suriettiva, allora (X, f) è di tipo $C_{0,d}$, $C_{\infty,\infty}$, oppure $C_{\infty,n}$.

Dimostrazione. Per ogni x, y si deve avere $\langle x \rangle \subseteq \langle y \rangle$ o viceversa. Inoltre, $\mathrm{Im}(f) \subseteq \langle x \rangle$ o viceversa. Vediamo vari casi:

a) supponiamo esista $x \notin \mathrm{Im}(f)$: allora $\mathrm{Im}(f) \subseteq \langle x \rangle$, il che implica $\mathrm{Im}(f) = \langle x \rangle \setminus \{x\}$. Ogni altro elemento $y \in X$ deve appartenere ad $\mathrm{Im}(f)$, quindi ad $\langle x \rangle$, altrimenti $\zeta(X, f)$ non sarebbe una catena. Ne segue $X = \langle x \rangle$, cioè (X, f) è "ciclica" generata da x;
b) sia f suriettiva. Poniamo $x \approx y$ se $\langle y \rangle = \langle x \rangle$. Questa è una relazione d'equivalenza in X e, dalla proposizione 1.1.5, segue che due elementi distinti x ed y sono in relazione se e solo se $\langle x \rangle$ è un ciclo. In caso contrario, x è in relazione solo con se stesso. Distinguiamo ora due casi:
   1) nessun $\langle x \rangle$ è un ciclo di lunghezza > 1. Allora ogni $\langle x \rangle$ è del tipo $C_{0,\infty}$. Per ogni $x, y \in X$ poniamo:

$$x \geqslant y \Leftrightarrow \langle y \rangle \subseteq \langle x \rangle$$

   Questa è una relazione d'ordine in X, ed è totale. Inoltre, ogni x ha un successivo, f(x), ed essendo f suriettiva, è il successivo di almeno un elemento, ma, come si prova subito, di uno solo, ossia f è anche iniettiva. Ne segue che $(X, \leqslant)$ è una catena senza minimo e massimo, quindi isomorfa a $(Z, \leqslant)$ e (X, f) è isomorfo a $C_{\infty,\infty}$;
   2) ci sia almeno un ciclo, sia $\langle y \rangle$, di lunghezza $d = n+1$, che è quindi, nel nostro caso, necessariamente contenuto in ogni altra sottoalgebra non vuota. Allora, ogni x non equivalente ad y genera una sottoalgebra ciclica di tipo $C_{m,d}$. Fra gli elementi non equivalenti ad y possiamo definire allora una relazione d'ordine come nel caso 1) ed ottenere un ordine totale discreto dotato di massimo, y, ma non di minimo. La struttura è quindi quella del tipo $C_{\infty,d}$.

5. Cfr. R. Schmidt, *Subgroup Lattices of Groups*, de Gruyter, 1994, p. 16.

1.2. Congruenze, omomorfismi, automorfismi

Congruenze. Una *congruenza* $\sim$ in (X, f) è una relazione d'equivalenza tale che, per ogni x, x' *in* X, se $x \sim x'$ allora $f(x) \sim f(x')$. Chiaramente, nell'insieme quoziente $X/\sim$ è possibile definire l'operazione monounaria quoziente $f_\sim$ definita da $f_\sim([x]) = [f(x)]$.

Diremo poi che una partizione di X è una congruenza se la relazione d'equivalenza ad essa associata lo è.

Un *ideale* di una congruenza $\sim$ di (X, f) è una classe d'equivalenza che sia anche una sottoalgebra.

Lemma 1.2.1. Sono equivalenti per una classe I della congruenza $\sim$ di (X, f):

a) I è un ideale di $\sim$;
b) $f_\sim(I)=I$;
c) I contiene una sottoalgebra H non vuota di (X, f).

Dimostrazione. Che *a*) e *b*) siano equivalenti e che *a*) implichi *c*) segue per definizione di ideale e di operazione quoziente. Proviamo che *c*) implica *b*). Sia $h \in H$, allora $[h] = I$ e $f(h) \in H \subseteq I$ quindi $f_\sim(I) = [f(h)] = I$.

La serie di esempi seguenti serve come lemma per il Teorema 1.2.3. Per le nozioni sui gruppi di permutazioni si veda per esempio[6].

Esempio 1.2.2.

a) Esempi ovvi di congruenze sono l'identità (o *congruenza discreta*) e il prodotto cartesiano $X \times X$ (o *congruenza banale*). Un ideale della congruenza discreta è un elemento unito per f;
b) poniamo $x \sim_f x'$ se $f(x) = f(x')$. Chiaramente, questa relazione, detta *nucleo* di f, è una congruenza per f. Su questa relazione torneremo più avanti;
c) la partizione $\{\mathrm{Im}(f), X \setminus \mathrm{Im}(f)\}$ è una congruenza. Più in generale, per ogni partizione $\mathbb{B}$ di $X \setminus \mathrm{Im}(f)$, la partizione $\mathbb{B} \cup \{\mathrm{Im}(f)\}$ è una congruenza. Infatti, se x ed x' stanno nello stesso blocco, anche f(x) ed f(x') stanno nello stesso blocco Im(f). Si noti che Im(f) è un ideale di tutte le congruenze di cui è una classe;
d) una partizione $\mathbb{B}$ di X costituita da sottoalgebre è una congruenza: se x, y appartengono ad un blocco $\mathbb{B}$, che è una sottoalgebra, anche

6. W.R. Scott, *Group theory*, Prentice–Hall, 1964.

f(x) e f(y) appartengono a $\mathbb{B}$. Dunque, la partizione produce una congruenza. In tal caso, $f_\sim$ è l'identità;

e) sia f biiettiva. Allora il sottogruppo ciclico G di S_X generato da f determina in X una partizione in G-orbite. Ossia poniamo $x \approx_f y$ se esiste $n \in \mathbf{Z}$ tale che $y = f^n(x)$. Ognuna di queste G-orbite è una sottoalgebra, per cui $\approx_f$ è una congruenza;

f) sia f biiettiva tale che il gruppo G da essa generato sia transitivo su X. Sia B un sistema di blocchi per G su X, allora B è una congruenza per f. Infatti, per ogni $B \in B$ e per ogni $x, x' \in B$ si ha che esiste $B' \in B$ tale che f(x) ed $f(x') \in B'$. Inversamente, ogni congruenza determina un sistema di blocchi per G, costituito dalle classi d'equivalenza;

g) esistono congruenze prive di ideali. Sia infatti f = (1 2 3 4 5 6) il ciclo agente su X = {1, 2, 3, 4, 5, 6}. Sia $\mathfrak{R}$ definita dalla partizione {{1,4}, {2,5}, {3,6}}. Allora $\mathfrak{R}$ è una congruenza, ma nessuna sua classe è una sottoalgebra.

Una struttura algebrica si dice *semplice* se le sole congruenze sono quelle ovvie.

Teorema 1.2.3. Un'algebra monounaria (X, f) è semplice se e solo se è di tipo $C_{0,p}$, con p primo.

Dimostrazione. Sia (X, f) semplice. Allora, per *b*) e *c*), f deve essere biiettiva. Il sottogruppo ciclico G generato da f per *e*) deve agire transitivamente su X e per *f*) deve essere primitivo. Ne segue che lo stabilizzatore di ogni $x \in X$ deve essere massimale[7], ossia deve avere indice primo p e coincidere con il sottogruppo generato da f^p. Ma essendo G abeliano, lo stabilizzatore è lo stesso per tutti gli elementi di X, quindi $f^p = id$. Ne segue che f è un ciclo di lunghezza p.

Inversamente, se (X, f) è di tipo $C_{0,p}$ con p primo, allora f agisce primitivamente su X. Ma allora, per *f*), (X, f) è semplice.

Corollario 1.2.4. Sia (X, f) un'algebra monounaria e sia $\mathfrak{R}$ una congruenza massimale, allora $X/\mathfrak{R}$ ha un numero primo di elementi.

Proposizione 1.2.5. Sia (X, f) un'algebra monounaria, siano H una sottoalgebra ed $\mathfrak{R}$ una congruenza. Allora:

a) la partizione $\mathfrak{R}_{|H}$ indotta in H dalla sua intersezione con le classi di $\mathfrak{R}$ è una congruenza in $(H, f_{|H})$;

7. Cfr. W.R. Scott, *Group theory*, Prentice–Hall 1964.

b) sia $\bar{H} = \{x \in X \mid \exists h \in H, h\mathfrak{R}x\}$ la *chiusura di H rispetto ad* $\mathfrak{R}$. Allora $\bar{H}$ è una sottoalgebra unione di classi di congruenza di $\mathfrak{R}$;
c) se $\mathfrak{R}$ è massimale in X allora $\mathfrak{R}_{|H}$ o è massimale in H, con lo stesso numero di classi, o coincide con $H \times H$ (cioè H è una classe di $\mathfrak{R}$).

Dimostrazione.

a) Siano $x, x' \in H$ tali che $x \mathfrak{R} x'$: allora $f(x) \mathfrak{R} f(x')$, ed inoltre, f(x) e f(x') appartengono ad H. Ne segue $f_{|H}(x) \mathfrak{R}_{|H} f_{|H}(x')$, quindi la restrizione ad H di $\mathfrak{R}$ è una congruenza in $(H, f_{|H})$;
b) sia $x \in \bar{H}$, per cui esiste $h \in H$ tale che $h \mathfrak{R} x$. Allora $f(h) \mathfrak{R} f(x)$, essendo $\mathfrak{R}$ una congruenza. Dunque, essendo $f(h) \in \bar{H}$ perché H è una sottoalgebra, allora $f(x) \in \bar{H}$. Dunque, $\bar{H}$ è una sottoalgebra. Inoltre, se $x \mathfrak{R} x'$, allora per la proprietà transitiva di $\mathfrak{R}$ si ha anche $h \mathfrak{R} x'$, quindi anche $x' \in \bar{H}$;
c) se $\bar{H}$ non coincide con H o con X allora, insieme con le classi di $\mathfrak{R}$ che esso non contiene forma una congruenza in X, maggiore di $\mathfrak{R}$, che di conseguenza non è massimale. Pertanto, se $\mathfrak{R}$ è massimale, allora o $\bar{H}$ è una sua classe, oppure $\bar{H} = X$, ma in questo caso, tutte le classi di $\mathfrak{R}$ devono avere intersezione non vuota con H.

Lemma 1.2.6. Siano (X, f) un'algebra monounaria, $\mathfrak{R}$ una congruenza ed H una sottoalgebra unione di classi di $\mathfrak{R}$. Allora la relazione $\mathfrak{R}^*_H$ definita da:

$$x \mathfrak{R}^*_H y \Leftrightarrow \begin{cases} x, y \in H \\ \text{oppure} \\ x, y \notin H, x \mathfrak{R} y \end{cases}$$

è una congruenza di cui H è un ideale.
Dimostrazione. Certamente $\mathfrak{R}^*_H$ è una relazione d'equivalenza di cui H è un blocco. La verifica che è una congruenza è immediata.

Corollario 1.2.7.

a) Ogni sottoalgebra di (X, f) è un ideale rispetto a qualche congruenza;
b) ogni sottoalgebra massimale è un ideale rispetto ad una congruenza massimale.

Dimostrazione.

a) Sia H una sottoalgebra e I la congruenza discreta. Allora applicando il lemma 1.2.6 segue che H è ideale rispetto alla congruenza I^*_H;