Federico Bartolozzi

Immersione di un reticolo distributivo finito nel reticolo degli interi rispetto alla divisione.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **21** (1966), n.2, p. 178–185.
Zanichelli
<http://www.bdim.eu/item?id=BUMI_1966_3_21_2_178_0>

Immersione di un reticolo distributivo finito nel reticolo degli interi rispetto alla divisione

FEDERICO BARTOLOZZI (a Palermo)

Sunto. - *Si dimostra, per via elementare, che ogni reticolo distributivo finito è isomorfo a un subreticolo del reticolo formato dagli interi positivi quando come «unione» e «intersezione» di due interi positivi si assumono rispettivamente il loro minimo comune multiplo ed il loro massimo comun divisore.*

1. - Il teorema di rappresentazione qui ottenuto per i reticoli distributivi finiti è deducibile da un teorema di rappresentazione noto, essendo un corollario del Teorema 6 del volume di G. BIRKHOFF ([1], p. 140) il quale asserisce che: «Ogni reticolo distributivo finito è isomorfo a un subreticolo del prodotto diretto di n copie di $\underline{2}$».

Abbiamo tuttavia ritenuto non del tutto superfluo pubblicare questa nota, per due motivi. In primo luogo, la dimostrazione da noi data, essendo di carattere affatto elementare, può avere qualche interesse didattico. In secondo luogo, la nostra dimostrazione, che ha carattere costruttivo, dice qualcosa di più di quanto è noto, giacché fa vedere come a rappresentare i reticoli distributivi finiti sia sufficiente una certa classe di subreticoli del reticolo degli interi rispetto alla divisione (subreticoli che si potrebbero chiamare «regolari» in analogia col teorema di CAYLEY per la rappresentazione dei gruppi finiti, per il quale è sufficiente appunto considerare i sottogruppi regolari dei gruppi simmetrici finiti).

2. - Nell'insieme, N, dei numeri interi positivi, la relazione

$$a/b \qquad (a \text{ divide } b)$$

definisce in N un ordinamento parziale; anzi, dati due interi (positivi [1]), x e y, esistono un loro minimo comune maggiorante ed un loro massimo comune minorante rispetto alla relazione d'ordine « / » che sono, precisamente, il loro minimo comune multiplo (m.c.m.) ed il loro massimo comune divisore (M.C.D.).

[1] Quest'aggettivo sarà d'ora in poi sottointeso.

Pertanto, a norma di un teorema generale (v. Lombardo Radice L. [2]) alla relazione d'ordine « / » definita in N è associata una struttura di reticolo di N, ottenuta ponendo

$$x \cup y = \text{m.c.m. } (x,\ y) = [x,\ y]$$

$$x \cap y = \text{M.C.D. } (x,\ y) = (x,\ y).$$

Il reticolo così definito, che chiameremo « reticolo degli interi rispetto alla divisione », e che denoteremo con il simbolo N_d, è distributivo.

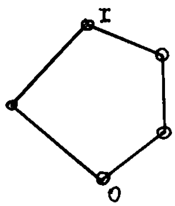
L'asserzione può essere facilmente provata verificando la validità di una delle leggi distributive:

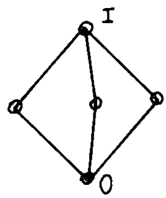
$$D_1)\quad x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$$

$$D_2)\quad x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$$

quali che siano x, y, z in N (v. Lombardo Radice L. [2]).

Nel seguito, però, ci avvarremo di una diversa definizione di reticolo distributivo ([2]): un reticolo è distributivo se e solo se non possiede subreticoli aventi uno dei due seguenti diagrammi:

(a) 

; (b) 

Poichè ogni subreticolo di un reticolo distributivo è, a sua volta, distributivo, avremo in particolare che: *i subreticoli finiti di* N_d *sono distributivi.*

È possibile invertire questa proposizione nel senso del teorema che passiamo ad enunciare ed a dimostrare.

3. – Teorema: *Assegnato comunque un reticolo distributivo finito,* R_d, *esiste sempre* (*almeno*) *un subreticolo,* R'_d, *di* N_d *isomorfo a* R_d.

Dim. – Osserviamo dapprima che, essendo R_d finito:

i) R_d possiede un minimo assoluto, o, ed un massimo assoluto I rispettivamente intersezione e unione di tutti gli elementi di R_d);

([2]) Equivalente alla precedente, v. [2].

ii) R_d ha dimensione finita, n, cioè $n-1$ è il numero dei tratti di ogni catena avente per estremi I e o (per il teorema di JORDAN, valido in un reticolo che sia soltanto semimodulare, in R_d le catene limitate complete aventi gli stessi estremi hanno la medesima lunghezza (v. [2])),

iii) gli elementi di R_d possono essere suddivisi in n classi, a seconda della loro dimensione relativa sopra lo o, ponendo in una stessa classe gli elementi che hanno una medesima dimensione i sopra 0 ($i=0, 1, 2, \dots, n-1$).

Chiameremo *elementi di livello i* gli elementi aventi dimensione i sopra 0; gli elementi di livello 1 (cioè gli elementi che coprono 0) si chiamano, con notazione ordinaria, *atomi*.

Ciò premesso, un subreticolo R'_d di N_d isomorfo a R_d, sarà da noi ottenuto in modo costruttivo.

Anzitutto. facciamo corrispondere a o il numero 1, agli atomi $A_1, A_2, \dots, A_h$ i primi h numeri primi: $p_1=2$, $p_2=3, \dots, p_h$.

Passiamo alla rappresentazione degli elementi di livello due di R_d. A questo scopo osserviamo che per un elemento qualsiasi B di livello due si possono presentare solo due casi: o B copre un solo atomo A, o B copre due atomi A_h e A_k. Infatti, B non può coprire tre (o più) atomi, altrimenti R_d conterebbe un subreticolo del tipo escluso (b). Nel primo caso facciamo corrispondere a B il prodotto di p_i, atomo di N_d immagine di A, per il numero primo immediatamente successivo a quelli già utilizzati per rappresentare gli atomi di R_d; nel secondo caso, facciamo corrispondere a B l'unione, $p_h p_k$, dei due atomi di N_d corrispondenti ai due atomi A_h e A_k di R_d.

In tal modo, abbiamo costruito una rappresentazione T_2, fino al livello 2, di R_d in N_d, avendo assegnato le immagini in N_d degli elementi di R_d di livello 0, 1, 2.

È subito visto che T_2 è un isomorfismo di R_d in N_d sino al livello due, più precisamente: a) la immagine della intersezione di due elementi di R_d di livello ≤ 2 è la intersezione delle loro immagini in N_d: b) se l'unione di due elementi di livello ≤ 1 di R_d è ancora un elemento di livello ≤ 2 di R_d, l'immagine in N_d della unione è l'unione delle immagini; c) la rappresentazione T_2 conserva la relazione di copertura, cioè $T_2(B)$ copre $T_2(A)$ in N_d se e solo se B copre A in R_d; d) le immagini di elementi di R_d sono numeri « liberi da quadrato ».

Procediamo ora per induzione, supponendo assegnata una rappresentazione T_i di R_d in N_d sino al livello i, tale che $T_i(A) = T_{i-1}(A)$ se A è di livello $< i$.

Supponiamo inoltre che T_i sia un isomorfismo sino al livello i di R_d in N_d per cui valgono le proprietà $a)$ ... $d)$ quando in esse si sostituisca il numero i al numero 2 (e allora $i - 1$ a 1). Per estendere la rappresentazione T_i al livello $i + 1$, dobbiamo assegnare le immagini, in N_d, degli elementi di livello $i + 1$ di R_d.

Premettiamo una osservazione.

Sia L_{i+1} un elemento di livello $i + 1$ di R_d che copre i tre elementi distinti $L_{i,1}$, $L_{i,2}$, $L_{i,3}$ di livello i di R_d; le intersezioni due a due di detti tre elementi devono allora essere tre elementi distinti di livello $i - 1$:

$L_{i-1,3} = L_{i,1} \cap L_{i,2}$; $L_{i-1,2} = L_{i,1} \cap L_{i,3}$; $L_{i-1,1} = L_{i,2} \cap L_{i,3}$.

Infatti, l'intersezione, ad es., di $L_{i,1}$ e $L_{i,2}$ deve essere coperta dai due elementi stessi perchè essi sono coperti dalla loro unione L_{i+1} ([3]); pertanto, detta intersezione deve essere un elemento di livello $i - 1$.

I tre elementi $L_{i,j}$ ($j = 1, 2, 3$) non possono poi coprire un medesimo elemento di livello $i - 1$, loro comune intersezione, perchè, in tal caso, si avrebbe in R_d un subreticolo del tipo escluso (b).

Passiamo alle immagini $L'_{i,j} = T_i(L_{i,j})$ in N_d.

Per ipotesi induttiva, T_i è un isomorfirmo sino al livello i, e si ha quindi:

$$L'_{i-1,3} = (L'_{i,1},\ L'_{i,2}) = d_3;\ L'_{i-1,2} = (L'_{i,1},\ L'_{i,3}) = d_2;$$
$$L'_{i-1,1} = (L'_{i,2},\ L'_{i,3}) = d_1$$

ed inoltre

$$L'_{i,1} = [d_2,\ d_3];\ L'_{i,2} = [d_1,\ d_3];\ L'_{i,3} = [d_1,\ d_2].$$

Poniamo allora:

$$L'_{i+1} = [L'_{i,1},\ L'_{i,2}]\ (^4).$$

La posizione fatta non dipende, come facilmente si può verificare, dalla particolare scelta degli elementi $L'_{i,j}$ ($j = 1, 2, 3$) di N_d coperti da L'_{i+1}; infatti, L'_{i+1} è divisibile per d_1 e d_2, divisori

([3]) Si ricordi che un reticolo distributivo è, in particolare, sottomodulare (v. [2]).

([4]) Osserviamo che L'_{i+1} è di livello $i + 1$ in N_d, perchè, attesa la sopramodularità di N_d, deve coprire $L'_{i,1}$ e $L'_{i,2}$.

rispettivamente di $L'_{i,2}$ e $L'_{i,1}$, perciò L'_{i+1} è divisibile anche per $L'_{i,3} = [d_1, d_2]$ ([5]); anzi, L'_{i+1}, di livello $i+1$, copre $L'_{i,3}$, di livello i, e quindi necessariamente:

$$L'_{i+1} = [L'_{i,1}, L'_{i,2}] = [L'_{i,1}, L'_{i,3}] = [L'_{i,2}, L_{i,3}].$$

L'osservazione ora fatta rende legittima la seguente estensione T_{i+1} della rappresentazione T_i sino al livello $i+1$:

I) a un elemento L_{i+1} di livello $i+1$ di R_d che copre due o più elementi di R_d di livello i, si faccia corrispondere il m.c.m. delle immagini di due qualunque, $L_{i,j}$. $L_{i,k}$, degli elementi di livello i da esso coperti;

II) a un elemento L_{i+1} di livello $i+1$ di R_d, che copre un solo elemento L_i di livello i, si faccia corrispondere il prodotto del numero L'_i, immagine di L_i in T_i, per il più piccolo dei numeri primi che non compaiono come fattori nelle immagini di elementi di R_d precedentemente assegnate.

T_{i+1} *soddisfa le proprietà* c) *e* d).

La d) è senz'altro evidente.

Quanto alla c), osserviamo che, nel caso II), L'_{i+1} copre l'unico elemento L'_i di livello i in esso contenuto, perchè si ottiene da L'_i moltiplicandolo per un numero primo; nel caso I), perchè $L'_{i,1}$ e $L'_{i,2}$ coprono, per l'ipotesi induttiva, la loro intersezione, quindi $L'_{i+1} = [L'_{i,1}, L'_{i,2}]$ copre $L'_{i,1}$ e $L'_{i,2}$ e così gli eventuali altri elementi di livello i in esso contenuti.

T_{i+1} *soddisfa la proprietà* b). Infatti, se A_i e B_i sono elementi distinti di livello i in R_d e $A_i \cup B_i$ è di livello $i+1$, allora $(A_i \cup B_i)'$ in N_d è di livello $i+1$ e copre A'_i e B'_i, essendo, per I), il m.c.m. $(A'_i . B'_i)$.

È allora $(A_i \cup B_i)' = A'_i \cup B'_i$.

Se poi A e B sono elementi distinti di livello $\leq i$ in R_d e $A \cup B$ è di livello $i+1$, esisteranno ([6]) (almeno) due elementi $A_i \geq A$, $B_i \geq B$ di livello i coperti da $A \cup B$ tali che $A \cup B = A_i \cup B_i$.

In N_d avremo allora, al livello $i+1$, $(A \cup B)' = (A_i \cup B_i)' = = A'_i \cup B'_i$; infatti $(A_i \cup B_i)'$ copre sia A'_i che B'_i, quindi a $(A_i \cup B_i)'$ associamo, per I), il m.c.m. (A'_i, B'_i).

([5]) gioca in questa asserzione il fatto che d_1 e d_2 sono elementi distinti di livello $i-1$ contenuti in $L'_{i,3}$.

Basterà far vedere quindi che

$$A' \cup B' = A'_i \cup B'_i .$$

Ora, si ha in N_d: $A'_i \cup B'_i = (A \cup A_i)' \cup (B \cup B_i)' = (A' \cup A'_i) \cup \cup (B' \cup B'_i) = (A' \cup B') \cup (A'_i \cup B'_i)$, cioè: $A' \cup B' \leq A'_i \cup B'_i$ quindi $A'_i \cup B'_i = k(A' \cup B')$ con k opportuno intero.

Attualmente è $k = 1$, altrimenti $A' \cup B'$ sarebbe un divisore proprio di $A'_i \cup B'_i$, cioè $A' \cup B'$ sarebbe di livello $< i+1$, quindi, per l'ipotesi induttiva, $A' \cup B' = (A \cup B)'$ e $(A \cup B)'$ sarebbe di livello $< i+1$, il che è in contrasto coll'osservazione prima fatta, e cioè che, in virtù della I), il livello di $(A \cup B)' = (A_i \cup B_i)'$ è $i+1$.

La proprietà b) è cosi dimostrata.

Resta da verificare la proprietà a).

A questo scopo basterà considerare due elementi distinti A_{i+1}, B_{i+1} di livello $i+1$ di R_d e verificare che la immagine $(A_{i+1} \cap B_{i+1})'$ in N_d della loro intersezione in R_d é il M.C.D. (A'_{i+1}, B'_{i+1}).

Se $A_{i+1} \cap B_{i+1}$ è di livello i in R_d, l'elemento $(A_{i+1} \cap B_{i+1})'$ di N_d è anch'esso di livello i in N_d; essendo poi $(A_{i+1} \cap B_{i+1})'$ coperto tanto da A'_{i+1} che da B'_{i+1}, l'elemento $(A_{i+1} \cap B_{i+1})'$ è necessariamente il M.C.D. (A'_{i+1}, B'_{i+1}).

Se poi $A_{i+1} \cap B_{i+1}$ è di livello $< i$ in R_d, esisteranno (almeno) due elementi distinti A_i, B_i di livello i, coperti rispettivamente da A_{i+1}, B_{i+1}, tali che $A_{i+1} \cap B_{i+1} = A_i \cap B_i$. Per l'ipotesi induttiva si ha:

$$(1) \qquad (A_{i+1} \cap B_{i+1})' = (A_i \cap B_i)' = A'_i \cap B'_i .$$

Se, in R_d, A_{i+1} e B_{i+1} coprono soltanto gli elementi A_i e B_i, è $A'_{i+1} = p_1 A'_i$, $B'_{i+1} = q_1 B'_i$ (p_1, q_1 numeri primi distinti), quindi M.C.D. $(A'_{i+1}, B'_{i+1}) =$ M.C.D. (A'_i, B'_i) e:

$$(A_{i+1} \cap B_{i+1})' = (A'_i \cap B'_i) = A'_{i+1} \cap B'_{i+1} .$$

Può però avvenire che A_{i+1}, B_{i+1}, in R_d, coprano più elementi di livello i (oltre com'è ovvio, ad A_i e B_i, per i quali, in N_d, vale sempre la (1)).

Siano, per fissare le idee, $\bar{A}_i \neq A_i$ e $\bar{B}_i \neq B_i$ due altri elementi di livello i coperti da A_{i+1} e B_{i+1} rispettivamente.

Allora, in N_d, poichè A'_{i+1} deve coprire $A'_i . A'_{i+1}$ differisce da A'_i solamente per un fattore primo q_i che entra nella rappresentazione di $\bar{A}'_i$.

([6]) ciò perchè una catena completa di estremi A e $A \cap B$ deve avere come dimensione la differenza tra il livello di A e quello di $A \cup B$.

Analogamente. B'_{i+1} differisce da B'_i solamente per un fattore primo q_j che entra nella rappresentazione di $\overline{B'}_i$.

Osserviamo che q_i, distinto da ciascun fattore (primo) che entra nella rappresentazione di A'_i, è in particolare distinto da ciascun fattore (primo) che entra in (A'_i, B'_i); analogamente, q_j, distinto da ciascun fattore (primo) che entra nella rappresentazione di B'_i, è in particolare diverso da ciascun fattore (primo) che compare in (A'_i, B'_i). Dimostriamo ora che $q_i \neq q_j$; dopo di che sarà dimostrato che $(A'_{i+1}, B'_{i+1}) = (A'_i, B'_i)$.

Due casi possono presentarsi in R_d:

o $\overline{A}_i \cap \overline{B}_i = A_i \cap B_i$;

o $\overline{A}_i \cap \overline{B}_i$ contenuto (in particolare coperto) in $A_i \cap B_i$.

Il primo caso si presenta non appena $\overline{A}_i$ è collegato a qualche elemento della catena che, contenendo A_i, congiunge A_{i+1} con $A_i \cap B_i$ e $\overline{B}_i$ è collegato a qualche elemento della catena che, contenendo B_i, congiunge B_{i+1} con $A_i \cap B_i$.

Il secondo caso si presenterà, sfruttando essenzialmente la sottomodularità di R_d [7], se uno almeno dei due elementi $\overline{A}_i$ e $\overline{B}_i$ non è collegato a qualche elemento della catena che, contenendo A_i, congiunge A_{i+1} con $A_i \cap B_i$ o che, contenendo B_i, congiunge B_{i+1} con $A_i \cap B_i$. In N_d sarà allora:

$$(2) \qquad \begin{aligned} &\text{o } (\overline{A'}_i, \overline{B'}_i) = (A'_i, B'_i) \\ &\text{o } (\overline{A'}_i, \overline{B'}_i) \text{ divisore di } (A'_i, B'_i). \end{aligned}$$

Se fosse $q_i = q_j$, in $(\overline{A'}_i, \overline{B'}_i)$ dovrebbe comparire q_i, e per la (2), q_i comparirebbe in (A'_i, B'_i), il che, per quanto prima osservato, è da escludere.

La rappresentazione così costruita sino al livello $i+1$ è quindi un isomorfismo sino al livello $i+1$; cioè: è sempre possibile, con le regole I), II), ampliare un isomorfismo di R_d in N_d fino al livello i in un isomorfismo di R_d in N_d sino al livello $i+1$.

Poichè R_d è un reticolo distributivo finito, quindi di dimensione finita, dopo un numero finito di passi si sarà costruito un subreticolo R'_d di N_d isomorfo a R_d. Il teorema su dimostrato può essere formulato diversamente e forse in modo più espressivo:

Il reticolo distributivo N_d degli interi rispetto alla divisione è un reticolo universale per la classe dei subreticoli distributivi finiti, intendendosi con ciò che ogni possibile reticolo distributivo

[7] Poichè nella nostra ipotesi $A_{i+1} = \overline{A}_i \cup (A_i \cap B_i)$ e A_{i+1} copre $\overline{A}_i$, la intersezione di $\overline{A}_i$ e $A_i \cap B_i$ deve essere coperta da $A_i \cap B_i$.

R_d ha tra i suoi modelli subreticoli, tra loro isomorfi, di N_d; la nostra costruzione permette anzi di realizzare ogni reticolo distributivo finito astratto mediante un determinato tipo di subreticolo di N_d.

BIBLIOGRAFIA

[1] G. BIRKHOFF, *Lattice Theory*, American Math Soc. Coll. Publ. XXV, 1948 (Revised Edition).

[2] L LOMBARDO RADICE, *Istituzioni di Algebra astratta*, Feltrinelli 1965

[3] G. ZAPPA, *Reticoli e geometrie finite*, Liguori Napoli.

Pervenuta alla Segreteria dell' U.M I.
il 21 luglio 1965