A. Barlotti (Ed.)

CIME Summer Schools

# Matroid Theory and its Applications

83

Varenna, Italy 1980

Springer

FONDAZIONE CIME ROBERTO CONTI

A. Barlotti (Ed.)

# Matroid Theory and Its Applications

Lectures given at a Summer School of the
Centro Internazionale Matematico Estivo (C.I.M.E.),
held in Varenna (Como), Italy,
August 24 - September 2, 1980

C.I.M.E. Foundation
c/o Dipartimento di Matematica “U. Dini”
Viale Morgagni n. 67/a
50134 Firenze
Italy
**cime@math.unifi.it**

ISBN 978-3-642-11109-9 e-ISBN: 978-3-642-11110-5
DOI:10.1007/978-3-642-11110-5
Springer Heidelberg Dordrecht London New York


Reprint of the 1st ed. C.I.M.E., Ed. Liguori, Napoli & Birkhäuser 1982
With kind permission of C.I.M.E.

Printed on acid-free paper

Springer.com

C O N T E N T S

CENTRO INTERNAZIONALE MATEMATICO ESTIVO

(C.I.M.E.)

# UN'INTRODUZIONE ALLA TEORIA DELLE FUNZIONI DI MÖBIUS

M. BARNABEI - A.BRINI - G.C.ROTA

# UN'INTRODUZIONE ALLA TEORIA DELLE FUNZIONI DI MÖBIUS

Marilena Barnabei
(Università di Ferrara)

Andrea Brini
(Università di Bologna)

Gian-Carlo Rota
(Massachusetts Institute of Technology)

## 1. Introduzione

Le idee principali che ci sono servite da guida e che vengono sviluppate in queste note sono le seguenti. In primo luogo si adotta pienamente la dualità tra il concetto di insieme parzialmente ordinato e quello di reticolo distributivo, idea che risale a Garrett Birkhoff e che è stata ulteriormente sviluppata da M.H. Stone, fino ad ottenere la versione definitiva nella tesi oxfordiana di Ann Priestley. Nel caso più semplice degli insiemi parzialmente ordinati finiti, questa dualità si riduce all'osservazione che ogni famiglia finita di sottoinsiemi di un insieme qualsiasi, chiusa per intersezione e unione - ma non sempre per complementazione - è funtorialmente isomorfa alla famiglia di tutti i sottoinsiemi decrescenti di un insieme parzialmente ordinato.

Questo fatto si esprime in modo naturale nell'equivalenza tra la categoria degli insiemi parzialmente ordinati finiti e la categoria dei reticoli distributivi finiti. In linea di massima, si può pensare che ogni proprietà combinatoria di insiemi parzialmente ordinati sia esprimibile in modo equivalente mediante i reticoli distributivi. In generale, l'espressione di tali proprietà in termini di reticoli distributivi è preferibile, non solo perché permette a volte generalizzazioni al caso infinito, ma soprattutto perché si inserisce più agevolmente nella problematica dell'algebra e della logica di oggi.

In secondo luogo, sviluppiamo il concetto di anello di valutazione di un reticolo distributivo, concetto che esprime in forma algebrica un processo di linearizzazione noto da tempo in analisi funzionale, cioè il passaggio da una misura su una famiglia di insiemi all'integrale sull'anello di funzioni semplici ad essa associate. Questo processo di linearizzazione ci permette di studiare le valutazioni su un reticolo distributivo come funzionali lineari sull'anello di valutazione, in analogia con lo studio della caratteristica di Eulero per le unioni finite di convessi - e più generalmente con i Quartermassintegrali di Minkowski - fatto da Hadwiger e dalla scuola di Blaschke per la geometria integrale.

Infatti, ancora sulle orme della geometria integrale, riusciamo a definire un analogo combinatorio della caratteristica di Eulero per i reticoli distributivi finiti (e quindi per gli insiemi parzialmente ordinati), come la valutazione, evidentemente unica, che prende il valore unità sugli elementi sup-irriducibili (o "coni") non zero. L'espressione di questa caratteristica di Eulero mediante la funzione di Möbius non è che un'estrema generalizzazione della nota formula di Eulero-Schläfli per i poliedri.

La teoria delle funzioni di Möbius degli insiemi parzialmente ordinati viene quindi sviluppata in base a questo legame fondamentale con la caratteristica di Eulero. Riusciamo così a ritrovare

in forma semplice e, vorremmo credere, definitiva, le identità scoperte finora per le funzioni di Möbius, nonché varie disuguaglianze profonde dovute a C. Greene, e le eleganti applicazioni geometriche dovute a T. Zaslavsky.

Nei paragrafi 3 e 4 sviluppiamo dettagliatamente la struttura algebrica dell'anello aumentato di valutazione, introdotto da uno di noi e poi studiato da L. Geissinger in tre eleganti lavori. Troviamo così che con l'uso sistematico dell'aumentazione si semplificano varie dimostrazioni. Si può affermare che, con il concetto di anello di valutazione aumentato, la classica dualità insiemistico-booleana viene linearizzata.

Il presente materiale, con l'eccezione del paragrafo conclusivo riguardante le applicazioni della teoria delle funzioni di Möbius al problema classico dell'enumerazione delle regioni determinate da un sistema di iperpiani non in posizione generica nello spazio affine o proiettivo, è stato oggetto di alcune delle lezioni del Corso CIME tenuto a Varenna nell'agosto 1980.

La lettura di queste note non richiede particolari conoscenze preliminari, al di fuori di alcune elementari nozioni di algebra commutativa.

## 2. Reticoli distributivi ed insiemi parzialmente ordinati

Nel seguito, $L$ indicherà un reticolo distributivo finito.

Un elemento $p \in L$ si dice sup-irriducibile se $p = a \vee b$ implica $p = a$ oppure $p = b$.

L'insieme $J(L)$ degli elementi sup-irriducibili di $L$, con l'ordine indotto, è un insieme parzialmente ordinato dotato di minimo. Indicheremo con $\hat{J}(L)$ l'insieme parzialmente ordinato ottenuto da $J(L)$ togliendo il minimo.

2.1. PROPOSIZIONE Ogni elemento del reticolo distributivo L può essere espresso in uno ed in un solo modo come sup di elementi sup-irriducibili a due a due non confrontabili.

DIMOSTRAZIONE Essendo L finito, si riconosce immediatamente che ogni elemento di L si può esprimere come sup di elementi sup-irriducibili; ci limiteremo perciò a dimostrare l'unicità della rappresentazione. A questo scopo, ricordiamo che, se p è un elemento sup-irriducibile in L e $p \leq a \vee b$, allora $p \leq a$ oppure $p \leq b$. Supponiamo ora che $\{p_1, p_2, \ldots, p_n\}$ e $\{q_1, q_2, \ldots, q_k\}$ siano insiemi di elementi sup-irriducibili a due a due non confrontabili, tali che

$$p_1 \vee p_2 \vee \cdots \vee p_n = q_1 \vee q_2 \vee \cdots \vee q_k \quad .$$

Grazie all'osservazione precedente, si ottiene, ad esempio, $q_1 \leq p_1$; d'altra parte

$$p_1 = (p_1 \wedge (q_2 \vee \cdots \vee q_k)) \vee q_1$$

da cui si deduce $p_1 = q_1$. Iterando questo ragionamento, si prova la tesi. ■

Sia P un insieme parzialmente ordinato finito. Un sottoinsieme I di P si dice <u>ideale</u> se $x \leq y \in I$ implica $x \in I$.

La famiglia $\mathcal{I}(P)$ degli ideali di P, con le operazioni di unione e intersezione, risulta essere un sottoreticolo dell'algebra di Boole su P, ed è quindi un reticolo distributivo.

Un sottoinsieme F di P si dice <u>filtro</u> se $x \geq y \in F$ implica $x \in F$.

Un ideale I di P si dice <u>principale</u> se esiste $p \in P$ tale

che $I = \{x \in P;\ x \leq p\}$. Analogamente, un filtro F di P si dice principale se esiste $p \in P$ tale che $F = \{x \in P;\ x \geq p\}$.

2.2. PROPOSIZIONE Sia L un reticolo distributivo finito, sia $\hat{J}(L)$ l'insieme parzialmente ordinato dei sup-irriducibili di L privato del minimo, e sia $\mathcal{I}(\hat{J}(L))$ il reticolo degli ideali di $\hat{J}(L)$. Allora, L e $\mathcal{I}(\hat{J}(L))$ sono isomorfi.

DIMOSTRAZIONE L'applicazione

$$L \longrightarrow \mathcal{I}(\hat{J}(L))$$
$$x \longrightarrow \{y \in \hat{J}(L);\ y \leq x\}$$

è biiettiva e preserva l'ordine, quindi è un isomorfismo di reticoli. ■

2.3. PROPOSIZIONE Sia P un insieme parzialmente ordinato finito, e sia $\mathcal{I}(P)$ il reticolo distributivo degli ideali di P. Allora P e $\hat{J}(\mathcal{I}(P))$ sono isomorfi.

DIMOSTRAZIONE E' sufficiente osservare che gli elementi di $\hat{J}(\mathcal{I}(P))$ sono tutti e soli i sottoinsiemi di P della forma

$$I_p = \{x \in P;\ x \leq p\} \ ,$$

con $p \in P$. Si verifica immediatamente che l'applicazione

$$P \longrightarrow \hat{J}(\mathcal{I}(P))$$
$$p \longrightarrow I_p$$

è biiettiva e preserva l'ordine. ■

2.4. PROPOSIZIONE Sia $P$ un insieme parzialmente ordinato finito, e $P^*$ il suo duale d'ordine. Allora $\mathcal{J}(P^*)$ è il duale d'ordine di $\mathcal{J}(P)$.

DIMOSTRAZIONE Osserviamo che $\mathcal{J}(P^*)$ è il reticolo dei filtri di $P$. Poiché l'insieme complementare di un ideale è un filtro e viceversa, l'applicazione

$$\begin{aligned} \mathcal{J}(P) &\longrightarrow \mathcal{J}(P^*) \\ I &\longrightarrow P-I \end{aligned}$$

risulta un antiisomorfismo di reticoli. ■

Siano $L_1, L_2$ reticoli finiti. Un'applicazione

$$\alpha : L_1 \longrightarrow L_2$$

si dirà u-z morfismo di reticoli se è un morfismo reticolare e fa corrispondere il massimo di $L_1$ al massimo di $L_2$ e il minimo di $L_1$ al minimo di $L_2$.

2.5. TEOREMA La categoria dei reticoli distributivi finiti con gli u-z morfismi è funtorialmente equivalente alla categoria degli insiemi parzialmente ordinati finiti con i morfismi d'ordine.

DIMOSTRAZIONE Siano $P_1, P_2$ due insiemi parzialmente ordinati finiti, e sia

$$\alpha : P_1 \longrightarrow P_2$$

un morfismo d'ordine. Siano $\mathcal{J}(P_1)$ e $\mathcal{J}(P_2)$ i reticoli degli

ideali di $P_1$ e $P_2$, rispettivamente. Definiamo un'applicazione

$$\alpha' : \mathcal{I}(P_2) \longrightarrow \mathcal{I}(P_1)$$

ponendo

$$\alpha'(I) = \left\{x \in P_1;\ \alpha(x) \in I\right\}$$

dove $I \in \mathcal{I}(P_2)$; $\alpha'$ risulta evidentemente un u-z morfismo di reticoli.

Viceversa, siano $L_1, L_2$ reticoli distributivi finiti, e sia

$$\beta : L_1 \longrightarrow L_2$$

un u-z morfismo; definiamo un'applicazione

$$\beta' : \hat{J}(L_2) \longrightarrow \hat{J}(L_1)$$

ponendo

$$\beta'(p) = \min \left\{x \in \hat{J}(L_1);\ \beta(x) = p\right\} \quad ,$$

dove $p \in \hat{J}(L_2)$ .

La definizione di $\beta'$ è ben posta, in quanto, se $x, y \in \hat{J}(L_1)$ sono tali che $\beta(x) = p = \beta(y)$ e sono minimali rispetto a tale condizione, allora $\beta(x \wedge y) = p$ ; sia $x \wedge y = p_1 \vee p_2 \vee \ldots \vee p_n$ , con $p_i$ sup-irriducibile per ogni $i$ . Poiché $p$ è a sua volta sup-irriducibile, deve esistere un indice $j$ tale che $\beta(p_j) = p$; dato che $x,y$ sono minimali, si ha necessariamente $x = p_j = y$ .

Si verifica poi immediatamente che $\beta'$ è un morfismo d'ordine.

Utilizzando le costruzioni precedenti si completa la dimostrazione. ■

## 3. Coni di valutazione

Sia $A$ un anello, e sia $\varepsilon$ una aumentazione per $A$, cioè un morfismo di anelli da $A$ all'anello $\mathbb{Z}$ degli interi.

Definiamo ora una nuova operazione su $A$, che chiameremo moltiplicazione di Geissinger, e indicheremo con $*$, ponendo

$$a * b = \varepsilon(a)\, b + a\, \varepsilon(b) - ab$$

per ogni $a, b \in A$.

3.1. PROPOSIZIONE $(A, +, *)$ è un anello; inoltre, $(A, +, *)$ è commutativo se e solo se $A$ è commutativo.

DIMOSTRAZIONE Per ogni $a, b, c \in A$ si ha:

i) $a * (b * c) = a * (\varepsilon(b)c + b\varepsilon(c) - bc) =$

$= \varepsilon(a)\varepsilon(b)\, c + \varepsilon(a)\, b\, \varepsilon(c) - \varepsilon(a)\, bc + a\, \varepsilon(b)\, \varepsilon(c) +$

$+ a\varepsilon(b)\, \varepsilon(c) - a\, \varepsilon(b)\, \varepsilon(c) - a\, \varepsilon(b)\, c - ab\, \varepsilon(c) + abc$ .

L'espressione così ottenuta è una funzione simmetrica in $a, b, c$, quindi

$$a * (b * c) = (a * b) * c \quad .$$

ii) $a * (b + c) = \varepsilon(a)(b + c) + a\,(\varepsilon(b) + \varepsilon(c)) - a\,(b + c) =$

$= \varepsilon(a)\, b + \varepsilon(a)\, c + a\varepsilon(b) + a\varepsilon(c) - ab - ac$ ;

$(a * b) + (a * c) = \varepsilon(a)\, b + a\, \varepsilon(b) - ab + \varepsilon(a)\, c + a\, \varepsilon(c) - ac$ .

Analogamente si dimostra l'altra legge distributiva.

L'ultima affermazione dell'enunciato segue direttamente dalla definizione dell'operazione $*$. ∎

3.2. COROLLARIO L'aumentazione $\varepsilon$ di $A$ è un'aumentazione per l'anello $(A, +, *)$. Inoltre, la moltiplicazione di Geissinger di $(A, +, *)$ è la moltiplicazione di $A$. ∎

Sia $A$ un anello con aumentazione $\varepsilon$. Un elemento $z \in A$ si dirà integrale se risulta:

i) $\varepsilon(z) = 1$

ii) $\varepsilon(a)z = az$ per ogni $a \in A$.

3.3. PROPOSIZIONE Sia $z$ un integrale di $A$; allora, $z$ è l'elemento neutro dell'operazione $*$. Viceversa, se $A$ possiede elemento neutro moltiplicativo $\nu$, questo è un integrale per $(A, +, *)$. In particolare l'integrale, se esiste, è unico. ∎

Un semianello $S(+, \cdot)$ sarà nel seguito una struttura dotata di due operazioni tali che

i) $S(+)$ ed $S(\cdot)$ siano semigruppi;

ii) in $S(+)$ valga la legge di cancellazione;

iii) $a(b+c) = ab + ac$
$(a+b)c = ac + bc$
per ogni $a, b, c \in S$.

Un'aumentazione di $S$ sarà un'applicazione

$$\varepsilon: S \longrightarrow \mathbb{N}$$

che risulti un morfismo di semianelli.

Un cono di valutazione è un semianello commutativo unitario $S$ con una aumentazione $\varepsilon$, dotato di integrale, e tale che sia definita in $S$ un'operazione $*$ che soddisfi l'identità:

$$a * b + ab = a\,\varepsilon(b) + \varepsilon(a)b$$

per ogni $a, b \in S$.

Osserviamo che, nelle precedenti ipotesi, la struttura $(S,+,*)$ risulta anch'essa un cono di valutazione.

Siano $S_1, S_2$ coni di valutazione; un'applicazione

$$\varphi : S_1 \longrightarrow S_2$$

si dirà morfismo di coni di valutazione se $\varphi$ è un morfismo di semianelli, ed inoltre:

i) $\varphi(a * b) = \varphi(a) * \varphi(b)$ ;

ii) $\varepsilon(\varphi(a)) = \varepsilon(a)$

per ogni $a, b \in S_1$.

3.4. PROPOSIZIONE (Principio di inclusione-esclusione)
Sia $S$ un cono di valutazione, e siano $a_1, a_2, \ldots, a_n \in S$.
Allora:

$$a_1 * a_2 * \ldots * a_n + \sum_{i<j} \varepsilon(a_i)\varepsilon(a_j) a_1 \ldots \hat{a}_i \ldots \hat{a}_j \ldots a_n +$$

$$+ \sum_{i<j<h<k} \varepsilon(a_i)\varepsilon(a_j)\varepsilon(a_h)\varepsilon(a_k) a_1 \ldots \hat{a}_i \ldots \hat{a}_j \ldots \hat{a}_h \ldots \hat{a}_k \ldots$$

$$\ldots a_n + \ldots = \sum_i \varepsilon(a_i)\, a_1 \ldots \hat{a}_i \ldots a_n +$$

$$+ \sum_{i<j<k} \varepsilon(a_i)\varepsilon(a_j)\varepsilon(a_k)\ a_1 \dots \hat{a}_i \dots \hat{a}_j \dots \hat{a}_k \dots a_n + \dots$$

DIMOSTRAZIONE Segue per induzione su $n$. ∎

Sia $L$ un reticolo distributivo finito.

Consideriamo il semigruppo abeliano libero su $L$ e definiamo su questo semigruppo una struttura di semianello ponendo

$$x \cdot y = x \wedge y$$

se $x,y \in L$, ed estendendo il prodotto così definito per linearità. Tale semianello sarà indicato con $\mathbb{N}[L,\wedge]$.

Consideriamo ora le congruenze

$$(*) \qquad x \vee y + x \wedge y = x + y$$

per $x,y \in L$.

Osserviamo che le congruenze $(*)$ sono compatibili con la struttura di semianello, in quanto, per ogni $a \in L$ e per ogni $x,y \in L$:

$$a(x \vee y + x \wedge y) = (a \wedge x) \vee (a \wedge y) + (a \wedge x) \wedge (a \wedge y)$$

e

$$a(x + y) = (a \wedge x) + (a \wedge y) \ .$$

Quindi, è ben definito il semianello quoziente di $\mathbb{N}[L,\wedge]$ rispetto alle congruenze $(*)$. Tale semianello si indicherà con $V(L)$.

Diremo elementi <u>puri</u> di $V(L)$ quelli che sono immagine di elementi di $L$ nell'immersione canonica $L \to V(L)$.

Definiamo ora un'applicazione:

$$\varepsilon : V(L) \to \mathbb{N}$$

nel modo seguente:

i) $\varepsilon(x) = 1$ se $x$ è puro;

ii) $\varepsilon(\sum_i x_i) = \sum_i \varepsilon(x_i)$ con $x_i$ puro per ogni $i$.

$\varepsilon$ risulta perciò un'aumentazione per $V(L)$.

Si ha poi immediatamente che il massimo $u$ del reticolo corrisponde all'unità del semianello, e che il minimo $z$ del reticolo corrisponde all'integrale del semianello, cioè $\varepsilon(z) = 1$ e $z \cdot x = \varepsilon(x)z$ per ogni $x \in V(L)$.

Definiamo ora un'operazione su $V(L)$, che indicheremo con $*$, nel modo seguente:

$$x * y = x \vee y \qquad \text{se } x,y \text{ sono puri}$$

$$(\sum_i x_i) * (\sum_j y_j) = \sum_{i,j} (x_i \vee y_j) \quad ,$$

dove $x_i, y_j$ sono puri per ogni $i,j$.

Questa definizione non dipende dalla rappresentazione mediante elementi puri che è stata scelta, poiché, se $a,b,c$ sono puri, si ha

$$a \vee (b \vee c + b \wedge c) = a \vee (b + c) \quad .$$

3.5. PROPOSIZIONE Se $f,g \in V(L)$ si ha:

$$f * g + fg = f\,\varepsilon(g) + \varepsilon(f)g \quad .$$

DIMOSTRAZIONE Siano $f = \sum_i x_i$, $g = \sum_j y_j$, $x_i, y_j$ puri. Allo-

ra

$$f * g + fg = \sum_{i,j} (x_i \vee y_j) + \sum_{i,j} (x_i \wedge y_j) = \sum_{i,j} (x_i + y_j) =$$

$$= \varepsilon(g) \sum_i x_i + \varepsilon(f) \sum_j y_j \quad . \blacksquare$$

Di conseguenza, $V(L)$ risulta un cono di valutazione.

Diremo <u>cono ridotto</u> del reticolo distributivo $L$ il semianello $V_o(L)$ quoziente del cono di valutazione $V(L)$ rispetto al semiideale generato dall'integrale $z$:

$$V_o(L) = V(L)/\langle z \rangle \quad .$$

3.6. PROPOSIZIONE Sia $P$ un insieme parzialmente ordinato finito, e $\mathcal{J}(P)$ il reticolo distributivo degli ideali d'ordine di $P$.
Una funzione

$$f : P \to \mathbb{N}$$

è decrescente se e solo se esistono $x_1, x_2, \ldots, x_n \in \mathcal{J}(P)$ e $c_1, \ldots, c_n \in \mathbb{N}$ tali che

$$f = \sum_{i=1}^{n} c_i I_{x_i}$$

dove $I_{x_i}$ è la funzione caratteristica dell'ideale $x_i$.

DIMOSTRAZIONE Sia $f : P \to \mathbb{N}$ decrescente. Dato che $P$ è finito, $f$ assume un numero finito di valori non nulli; siano $v_1 < v_2 < \ldots < v_n$ questi valori. Poniamo

$$A_o = \{p \in P;\ f(p) > 0\}$$

$$A_i = \{p \in P;\ f(p) > v_i\} \qquad i = 1, \ldots, n-1 \ .$$

Ciascuno degli insiemi $A_o, A_1, \ldots, A_{n-1}$ è un ideale d'ordine di $P$. La funzione

$$f_1 = f - v_1 I_{A_o}$$

è anch'essa decrescente, ed inoltre

$$f_1(p) = \begin{cases} f(p) - v_1 & \text{se } p \in \bigcup_{i=1}^{n-1} A_i \\ 0 & \text{altrimenti} \end{cases}$$

Per induzione si ha allora

$$f = v_1 I_{A_o} + (v_2 - v_1) I_{A_1} + \ldots + (v_{n-1} - v_{n-2}) I_{A_{n-1}} \ .$$

Dato che ciascun $A_i$ è un elemento di $\mathcal{J}(P)$, l'affermazione è vera.

Viceversa, è ovvio che ogni $I_A$, con $A \in \mathcal{J}(P)$, è una funzione decrescente su $P$. ■

Da questo risultato si deduce il seguente teorema di struttura:

3.7. TEOREMA Per ogni reticolo distributivo finito $L$, il cono ridotto $V_o(L)$ è isomorfo al semianello delle funzioni decrescenti sull'ordine parziale $\hat{J}(L)$, a valori in $\mathbb{N}$. ■

## 4. Anello di valutazione di un reticolo distributivo

Sia L un reticolo distributivo finito ed M un semigruppo abeliano, nel quale valga la legge di cancellazione. Una valutazione su L è una funzione

$$f : L \longrightarrow M$$

tale che

$$f(a \vee b) + f(a \wedge b) = f(a) + f(b)$$

per ogni a,b nel reticolo.

Se poi $f : L \to M$ è una valutazione che associa al minimo z di L l'elemento neutro del semigruppo M, f si dice misura.

Sia A un anello unitario; una valutazione $f : L \to A$ si dice moltiplicativa se, per ogni $x, y \in L$, risulta

$$f(x \wedge y) = f(x)\, f(y) \quad .$$

4.1. PROPOSIZIONE L'immersione canonica

$$i : L \to V(L)$$

del reticolo distributivo L nel suo cono di valutazione è la valutazione universale su L, cioè, per ogni semigruppo M e per ogni valutazione

$$f : L \to M \quad ,$$

esiste un morfismo di semigruppi

$$\varphi : V(L) \to M$$

tale che

$$f = \varphi \circ i \quad .$$

DIMOSTRAZIONE Definiamo $\varphi: V(L) \to M$ nel modo seguente:

1) $\varphi(x) = f(i^{-1}(x))$ se $x$ è puro;

2) se $x = \sum_k a_k$ , con $a_k$ puro per ogni $k$ ,

poniamo

$$\varphi(x) = \sum_k f(i^{-1}(a_k)) \quad .$$

Dato che $f$ è una valutazione, questa definizione non dipende dalla rappresentazione di $x$ mediante elementi puri. ■

4.2. PROPOSIZIONE Un morfismo di reticoli distributivi finiti

$$\varphi: L_1 \to L_2$$

induce un (unico) morfismo di coni di valutazione

$$\varphi': V(L_1) \to V(L_2)$$

tale che

$$\varphi' \circ i_1 = i_2 \circ \varphi \ ,$$

dove $i_1, i_2$ sono le immersioni di $L_1$ in $V(L_1)$ e di $L_2$ in $V(L_2)$ , rispettivamente.

DIMOSTRAZIONE E' sufficiente osservare che, prolungando per linearità la $\varphi$ a $\mathbb{N}[L, \wedge]$ , si ottiene una funzione che rispetta

le congruenze

$$a \vee b + a \wedge b = a + b$$

e che quindi è ben definita su $V(L)$. ■

4.3. PROPOSIZIONE Siano $L_1$, $L_2$ reticoli distributivi, e sia

$$\varphi' : V(L_1) \to V(L_2)$$

un morfismo di coni di valutazione. Allora esiste un unico morfismo di reticoli

$$\varphi: L_1 \longrightarrow L_2$$

tale che

$$\varphi' \circ i_1 = i_2 \circ \varphi ,$$

dove $i_1, i_2$ denotano le immersioni naturali di $L_1$ in $V(L_1)$ e di $L_2$ in $V(L_2)$, rispettivamente.

DIMOSTRAZIONE E` ovvio che gli elementi puri di $V(L_1)$ e $V(L_2)$ sono tutti e soli gli elementi di aumentazione 1. E' quindi sufficiente provare che $\varphi'$ muta elementi puri in elementi puri. Ma, se $x \in V(L_1)$, ed $x$ è puro, si ha

$$x \cdot x = x$$

che implica

$$\varphi'(x)\ \varphi'(x) = \varphi'(x)$$

da cui:

$$\varepsilon(\varphi(x))^2 = \varepsilon(\varphi(x))$$

quindi

$$\varepsilon(\varphi(x)) = 1 \quad .\blacksquare$$

Sia L un reticolo distributivo finito; consideriamo il gruppo abeliano libero su L. Tale gruppo si può dotare di una struttura di $\mathbb{Z}$-algebra mediante l'operazione di prodotto indotta dall'inf $\wedge$ del reticolo. Questa algebra si dice <u>algebra di semigruppo</u> di L, e si indica con $\mathbb{Z}[L,\wedge]$. Sia I(L) l'ideale di $\mathbb{Z}[L,\wedge]$ generato dagli elementi del tipo

$$a \vee b + a \wedge b - a - b$$

con $a,b \in L$. L'anello quoziente

$$W(L) = \mathbb{Z}[L,\wedge] / I(L)$$

si dirà <u>anello di valutazione</u> di L. Gli elementi di W(L) immagine degli elementi di L si diranno elementi puri.

4.4. PROPOSIZIONE Sia L un reticolo distributivo finito, e sia M un gruppo abeliano. Per ogni valutazione

$$f : L \to M$$

esiste un morfismo di gruppi

$$\varphi : W(L) \to M$$

tale che

$$f = \varphi \circ i$$

dove $i$ è l'immersione canonica di $L$ in $W(L)$.

DIMOSTRAZIONE Analoga a quella della Proposizione 4.1. ■

Analogamente a quanto fatto per il cono di valutazione $V(L)$, definiamo l'<u>aumentazione</u>

$$\varepsilon : W(L) \to \mathbb{Z}$$

nel modo seguente:

i) $\varepsilon(x) = 1$ se $x$ è puro;

ii) $\varepsilon(\sum_i x_i) = \sum_i \varepsilon(x_i)$ se $x_i$ è puro per ogni $i$.

Dal momento che $W(L)$ è un anello con aumentazione, si può definire in esso la moltiplicazione di Geissinger $*$ :

$$a * b = a\,\varepsilon(b) + \varepsilon(a)b - ab$$

per ogni $a,b \in W(L)$. Ovviamente, se $a,b$ sono puri, risulta

$$a * b = a \vee b$$

e, se $a = \sum_i x_i$ , $b = \sum_j y_j$ , dove $x_i, y_j$ sono puri, si ha:

$$a * b = \sum_{i,j} (x_i \vee y_j) \ .$$

4.5. PROPOSIZIONE L'immersione canonica

$$j : V(L) \to W(L)$$

è un morfismo di coni di valutazione. ■

Osserviamo che la costruzione di $W(L)$ può essere ripetuta utilizzando l'operazione sup di $L$ in luogo dell'operazione inf; si ottiene così un anello $W^{*}(L)$, che gode evidentemente delle stesse proprietà di $W(L)$. Più precisamente:

4.6. PROPOSIZIONE L'applicazione

$$\tau : W(L) \longrightarrow W^{*}(L)$$

tale che

$$\tau(x) = u + z - x$$

è un isomorfismo involutorio di anelli.

DIMOSTRAZIONE E' sufficiente osservare che

$$\tau(x \wedge y) = z + u - (x \wedge y) = z + u + x \vee y - x - y =$$

$$= (z + u - x) \vee (z + u - y) = \tau(x) \vee \tau(y) \quad .$$

4.7. PROPOSIZIONE Gli elementi di $W(L)$ che corrispondono agli elementi sup-irriducibili di $L$ costituiscono una base per $W(L)$.

DIMOSTRAZIONE

i) gli elementi sup-irriducibili di $L$ sono ovviamente linearmente indipendenti in $W(L)$;

ii) sia $x \in L$, non sup-irriducibile, e sia

$$x = p_1 \vee p_2 \vee \dots \vee p_n$$

con $p_1, \dots, p_n$ sup-irriducibili e non confrontabili; grazie

al principio di inclusione-esclusione, in $W(L)$ , si ha:

$$x = p_1 + p_2 + \ldots + p_n - p_1 \wedge p_2 - p_1 \wedge p_3 - \ldots + p_1 \wedge p_2 \wedge p_3 + \ldots \quad ;$$

ciascuno degli addendi al secondo membro è strettamente minore di $x$ ; ripetendo il procedimento per ogni addendo che non sia sup-irriducibile, dato che il reticolo $L$ è finito, otteniamo

$$x = q_1 + q_2 + \ldots + q_k$$

con $q_1, \ldots, q_k$ sup-irriducibili;

iii) dato che gli elementi puri generano $W(L)$, l'affermazione è vera. ■

4.8. PROPOSIZIONE Sia $L$ un reticolo distributivo finito. Ogni valutazione su $L$ è determinata dai suoi valori su $J(L)$ , e questi valori possono essere assegnati arbitrariamente.

DIMOSTRAZIONE Segue dal fatto che $J(L)$ è una base per $W(L)$ , e che ogni valutazione $f : L \to A$ si può esprimere nella forma $\varphi \circ i$ , dove $\varphi : W(L) \to A$ è un morfismo di gruppi.

4.9. COROLLARIO Se $J(L)$ è un inf-semireticolo, allora $J(L)$ è un inf-sottosemireticolo di $L$ , e $W(L)$ è l'algebra di semigruppo di $(J(L), \wedge)$.

DIMOSTRAZIONE Indichiamo con $\wedge$ l'operazione di inf in $L$ , con $\overset{\wedge}{J}$ l'operazione di inf in $J(L)$ . Siano $p, q \in J(L)$ ; supponiamo che

$$p \overset{\wedge}{J} q < p \wedge q = t \quad .$$

D'altra parte si avrà

$$t = a_1 \vee a_2 \vee \ldots \vee a_n$$

con $a_1, a_2, \ldots, a_n \in J(L)$ ; questo implica

$$p \underset{J}{\wedge} q < a_i$$

per qualche $i$ , il che è assurdo. Di conseguenza

$$p \underset{J}{\wedge} q = p \wedge q \quad .$$

La seconda affermazione segue dal fatto che gli elementi di $J(L)$ costituiscono una base per $W(L)$ .■

4.10. TEOREMA Sia $L$ un reticolo distributivo finito; $L$ si può immergere in un'algebra di Boole finita, $B(L)$ , di rango $|\hat{J}(L)|$ .

DIMOSTRAZIONE E' sufficiente osservare che, per il Teorema 2.5, $L$ è isomorfo a un sottoreticolo dell'algebra di Boole generata dagli elementi di $\hat{J}(L)$ .■

4.11. PROPOSIZIONE Sia $L$ un reticolo distributivo finito, e $B(L)$ l'algebra di Boole generata da $\hat{J}(L)$ ; allora $W(L)$ e $W(B(L))$ sono isomorfi.

DIMOSTRAZIONE Segue dal fatto che

$$|J(L)| = |J(B(L))|$$

e quindi i due anelli di valutazione sono generati dallo stesso numero di elementi.■

## 5. La funzione di Möbius

Sia $L$ un reticolo distributivo finito, e sia $J(L)$ l'insieme parzialmente ordinato degli elementi sup-irriducibili di $L$. Per ogni $p \in \hat{J}(L)$, l'insieme

$$\{x \in L;\ x < p\}$$

ha un massimo, che indicheremo con $\partial p$. Osserviamo inoltre che, se $p_1, p_2, \ldots, p_n$ sono gli elementi sup-irriducibili di $L$ tali che $p_i < p$ per ogni $i$, allora

$$\partial p = p_1 \vee p_2 \vee \cdots \vee p_n \ .$$

Nell'anello di valutazione $W(L)$, definiamo

$$e_p = p - \partial p \ .$$

Poniamo inoltre

$$e_z = z \ .$$

5.1. PROPOSIZIONE L'insieme

$$\{e_p;\ p \in J(L)\}$$

è una base di idempotenti ortogonali per $W(L)$. Inoltre, per ogni $x \in L$, risulta

$$x = \sum_{p \leq x} e_p \ .$$

DIMOSTRAZIONE Innanzi tutto osserviamo che, per ogni $p \in J(L)$, si ha:

$$e_p \cdot e_p = (p - \partial p)^2 = p \wedge p + \partial p \wedge \partial p - 2\, p \wedge \partial p = p - \partial p = e_p \ ,$$

e, per ogni $p, q \in J(L)$ , $p \neq q$ , risulta

$$p \wedge q = \partial p \wedge \partial q \ ,$$

da cui

$$e_p \cdot e_q = (p - \partial p)(q - \partial q) = p \wedge q + \partial p \wedge \partial q - \partial p \wedge q - p \wedge \partial q = 0 \ .$$

Inoltre, per ogni $x \in L$ , risulta

$$x = \sum_{p \leq x} e_p \ ;$$

infatti, supponiamo vera l'affermazione per ogni $y \in L$ , $y < x$; se $x$ non è sup-irriducibile, avremo $x = a \vee b$; se

$$a = \sum_{p \leq a} e_p \ , \qquad b = \sum_{q \leq b} e_q \ ;$$

allora

$$a \wedge b = \Big(\sum_{p \leq a} e_p\Big)\Big(\sum_{q \leq b} e_q\Big) = \sum_{p \leq a \wedge b} e_p$$

poiché gli $e_p$ sono idempotenti ortogonali; quindi

$$x = a + b - a \wedge b = \sum_{p \leq x} e_p \ .$$

Se invece $x$ è sup-irriducibile, si ha:

$$x = e_x + \partial x \quad ,$$

dal momento che $\partial x < x$ , la tesi è vera. ■

Dato che gli elementi di $J(L)$ sono una base per $W(L)$ , sarà in particolare

$$e_p = \sum_{\substack{q \leq p \\ q \in J(L)}} \mu(q,p)\, q$$

per ogni $p \in J(L)$ . I coefficienti $\mu(q,p)$ sono evidentemente numeri interi. Per convenzione, poniamo

$$\mu(q,p) = 0 \qquad \text{se} \quad q \not\leq p \quad .$$

Abbiamo quindi:

5.2. PROPOSIZIONE Per ogni $x \in L$ si ha

$$x = \sum_{\substack{p,q \in J(L) \\ q \leq x}} \mu(p,q)\, p \quad .$$

DIMOSTRAZIONE Segue dalla Proposizione precedente e dalla definizione di $\mu(p,q)$ . ■

5.3. PROPOSIZIONE Per ogni $a,b \in J(L)$ si ha:

$$\sum_{a \leq x \leq b} \mu(x,b) = \begin{cases} 0 & \text{se} \quad a \neq b \\ 1 & \text{se} \quad a = b \end{cases} \quad .$$