Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea in Matematica

LA FUNZIONE DI MÖBIUS DI UN INSIEME PARZIALMENTE ORDINATO

Tesi di Laurea in Teoria dei Numeri

Relatore:
Chiar.mo Prof.
MARILENA BARNABEI

Presentata da:
ANTONIO SPAGNUOLO

II Sessione
Anno Accademico 2015/2016

Introduzione

Nel 1837, il matematico A.F. Möbius definì la funzione aritmetica $\mu(n)$ che vale 0 se n è divisibile per il quadrato di un numero primo, $(-1)^k$ se n è il prodotto di k primi distinti e $\mu(1) = 1$. Essa ricopre un ruolo di fondamentale importanza per quanto riguarda la distribuzione dei numeri primi, nonché per la sua duttilità nella risoluzione di diversi problemi di conteggio grazie alla formula di inversione di Möbius, che può essere pensata come un analogo formale del teorema fondamentale del calcolo integrale. Una sorprendente varietà di problemi di calcolo combinatorio si rivelano essere nient'altro che casi particolari di un problema più generale che riguarda la possibilità di invertire una somma fatta sugli elementi di un insieme parzialmente ordinato. L'obiettivo di questo elaborato è quello di illustrare come sia possibile generalizzare il concetto di funzione aritmetica estendendolo a quello di funzione di un'algebra di incidenza. Le algebre di incidenza hanno catturato l'interesse di svariati matematici a partire dagli anni '60 del secolo scorso, e si svilupparono come ambiente naturale nel quale generalizzare la formula di inversione di Möbius. La funzione di Möbius della teoria dei numeri, definita originariamente sull'insieme dei numeri interi positivi ordinato per divisibilità, può quindi essere definita su generici insiemi parzialmente ordinati.

Il primo capitolo è dedicato alla definizione dei concetti preliminari utili alla lettura della tesi. Essi si dividono essenzialmente in due parti: la prima è la teoria degli insiemi parzialmente ordinati, che costituiscono la struttura basilare su cui fondare le algebre di incidenza. La seconda invece riguarda le principali proprietà che coinvolgono i numeri interi e la divisibilità tra di essi.

Nel secondo capitolo vengono prese in esame le proprietà fondamentali delle funzioni aritmetiche. Si mostra come esse possano essere dotate della struttura di algebra sul campo dei numeri complessi e vengono enunciate le proprietà delle funzioni aritmetiche moltiplicative. Quest'ultima classe di funzione è di particolare interesse nell'ambito della teoria dei numeri.
Nel terzo capitolo vengono prima introdotte le algebre di incidenza e definite le funzioni più notevoli che ne fanno parte, poi vengono presentate le principali proprietà della funzione di Möbius di un insieme parzialmente ordinato. L'elaborato si conclude presentando tre applicazioni della formula di inversione di Möbius.

Indice

Capitolo 1

Preliminari

1.1 Insiemi Parzialmente Ordinati

Si riportano le principali nozioni che riguardano la teoria degli insiemi parzialmente ordinati. I risultati esposti possono aiutare la comprensione del terzo capitolo riguardante le algebre di incidenza; esse sono infatti strutture che presuppongono e si basano sulla nozione di insieme parzialmente ordinato.

Definizione 1.1. Sia X un insieme non vuoto; una *relazione d'ordine* su X è una relazione $\mathbf{R} \subseteq X^2$ che verifica le seguenti proprietà: per ogni $x, y, z \in X$,

- $x\mathbf{R}x$; (proprietà riflessiva)
- se $x\mathbf{R}y$ e $y\mathbf{R}x$ allora $x = y$; (proprietà antisimmetrica)
- se $x\mathbf{R}y$ e $y\mathbf{R}z$ allora $x\mathbf{R}z$ (proprietà transitiva)

In genere le relazioni d'ordine si indicano con il simbolo $\leq$, o con un simbolo analogo.

Definizione 1.2. Un *insieme parzialmente ordinato* è una coppia $(X, \leq)$, dove X è un insieme non vuoto e $\leq$ è una relazione d'ordine su X. L'insieme X è detto sostegno dell'insieme parzialmente ordinato.

Esempio 1.1.
La relazione $|$ sull'insieme $\mathbb{N}$ dei numeri naturali, definita come segue: per

ogni $a, b \in \mathbb{N}$: $a \mid b \Leftrightarrow$ esiste $c \in \mathbb{N}$ tale che $a \cdot c = b$, è una relazione d'ordine su $\mathbb{N}$ detta *ordinamento per divisibilità*.

Esempio 1.2. Sia U un insieme; la relazione $\subseteq$ di inclusione tra sottoinsiemi di U è una relazione d'ordine su $\mathcal{P}(U)$. L'insieme parzialmente ordinato $(\mathcal{P}(U), \subseteq)$ viene detto *algebra di Boole dei sottoinsiemi di U* e denotato con il simbolo $\mathcal{B}(U)$.

Esempio 1.3. Sia A un insieme non vuoto, e $P(A)$ l'insieme delle partizioni di A. Definiamo in $P(A)$ una relazione $\leq_P$ nel modo seguente: per ogni $\pi, \sigma \in P(A)$,
$\pi \leq_P \sigma \Leftrightarrow$ per ogni blocco X di π esiste un blocco Y di σ tale che $X \subseteq Y$. La relazione $\leq_P$ così definita, che viene detta *raffinamento*, è una relazione d'ordine.

Definizione 1.3. Sia $\leq$ una relazione d'ordine su un dato insieme X; due elementi $x, y \in X$ si dicono *confrontabili* (secondo la relazione $\leq$) se risulta: $x \leq y$ oppure $y \leq x$. Due elementi di X che non siano confrontabili si dicono *inconfrontabili*.

Definizione 1.4. Una relazione d'ordine su un insieme X tale che due qualunque elementi di X siano sempre confrontabili si dice *ordine lineare*. In questo caso la coppia $(X, \leq)$ si dice *insieme totalmente ordinato* o *linearmente ordinato*, oppure *catena*.

Esempio 1.4. Gli ordinamenti usuali (detti *ordinamenti naturali*) degli insiemi $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sono tutti ordini lineari.

Esempio 1.5. La relazione $\mid$ sull'insieme $\mathbb{N}$ dei numeri naturali definita dell'esempio precedente non è un ordine lineare; poiché dati due numeri naturali non è detto che uno dei due divida l'altro. Ad esempio 7 e 15 non sono confrontabili secondo la relazione $\mid$.

Definizione 1.5. Sia $(X, \leq)$ un insieme parzialmente ordinato, e sia Y un sottoinsieme non vuoto di X, la restrizione a Y della relazione $\leq$ viene detta *ordine indotto* da $\leq$ su Y; l'insieme parzialmente ordinato $(Y, \leq)$ viene anche detto *sottoordine* di $(X; \leq)$.

Definizione 1.6. Sia $(X, \leq)$ un insieme parzialmente ordinato, e siano x,y$\in$ X tali che $x \leq y$. Si dice *intervallo* in X di *estremi* x ed y l'insieme parzialmente ordinato il cui sostegno è il seguente sottoinsieme di X: [x;y] $= \{z \in X | x \leq z \leq y\}$, e l'ordine è quello indotto.

Definizione 1.7. Un insieme parzialmente ordinato $(X, \leq)$ si dice *localmente finito* se ogni intervallo di X è finito.

Definizione 1.8. Una *catena* di un insieme parzialmente ordinato $(X, \leq)$ è un sottoinsieme C di X che, con l'ordine indotto, risulti linearmente ordinato. Se C è una catena finita, si dice lunghezza di C il numero $|C|$-1.

Definizione 1.9. Sia $(X, \leq)$ un insieme parzialmente ordinato, e siano $x, y \in X$ tali che $x < y$. Si dice che x *è coperto da* y (oppure che y copre x) se risulta [x;y] $= \{x, y\}$, cioè se l'intervallo di estremi x ed y si riduce alla catena formata dai due punti x ed y.

Esempio 1.6. Nell'insieme parzialmente ordinato $(\mathbb{N}, \leq)$, dove $\leq$ è l'ordinamento naturale, x è coperto da y se e solo se y è il successivo di x.

Esempio 1.7. Nell'insieme parzialmente ordinato $(\mathbb{Q}, \leq)$, dove $\leq$ è l'ordinamento naturale, la relazione di copertura è la relazione vuota.

Esempio 1.8. Nell'insieme parzialmente ordinato $(\mathbb{N}, |)$, il numero x è coperto dal numero y se e solo se esiste un numero primo p tale che $y = x \cdot p$.

Definizione 1.10. Sia $(X, \leq)$ un insieme parzialmente ordinato; consideriamo il grafo orientato della relazione di copertura associata alla relazione d'ordine $\leq$. Tracciamo tale grafico in modo che tutte le volte che l'elemento x è coperto dall'elemento y, il punto corrispondente ad x si trovi più in basso di quello corrispondente ad y. Il grafo disegnato con queste convenzioni prende il nome di *diagramma di Hasse della relazione d'ordine* $\leq$.

Definizione 1.11. Sia $(X, \leq)$ un insieme parzialmente ordinato. Una *linearizzazione* della relazione d'ordine $\leq$ è una relazione d'ordine $\leq'$ su X tale che:

(i) $(X, \leq')$ sia una catena.

(ii) per ogni $a, b \in X$ si ha: $a \leq b \Rightarrow a \leq' b$

Riportiamo il seguente teorema poiché di fondamentale importanza nella teoria degli ordini, ma che nel corso della trattazione avrà un valore puramente strumentale. La dimostrazione, che è possibile trovare in [2], verrà quindi omessa.

Teorema 1.1.1 (Szpilrajn)**.** *Per ogni insieme parzialmente ordinato* $(X, \leq)$ *esiste una linearizzazione della relazione d'ordine* $\leq$*.*

Definizione 1.12. Sia $(X, \leq)$ un insieme parzialmente ordinato; un elemento x di X si dice *minimale* se: per ogni $y \in X$, $y \leq x \Rightarrow y = x$.
Dualmente, un elemento x di X si dice *massimale* se: per ogni $y \in X$, $x \leq y \Rightarrow y = x$.
Se poi X possiede esattamente un elemento minimale, esso si dice *minimo* di X, e si indica solitamente con il simbolo 0. Se X possiede esattamente un elemento massimale, esso si dice *massimo* di X, e viene solitamente indicato con il simbolo 1.

Esempio 1.9. Sia U un insieme; l'algebra di Boole $\mathcal{B}(U)$ dei sottoinsiemi di U ha come minimo l'insieme vuoto e come massimo l'insieme U.

Esempio 1.10. Sia A un insieme non vuoto. L'insieme parzialmente ordinato $P(A)$ delle partizioni di A ha come elemento minimo la partizione discreta e come massimo la partizione banale.

Definizione 1.13. Siano $(X, \leq_X)$ e $(Y, \leq_Y)$ due insiemi parzialmente ordinati. L'insieme parzialmente ordinato $Z = (X \times Y, \leq_Z)$ con la relazione d'ordine definita da $(x_1, y_1) \leq_Z (x_2, y_2)$ se e solo se $x_1 \leq_X x_2$ e $y_1 \leq_Y y_2$ si dice *prodotto diretto* degli insiemi parzialmente ordinati X e Y.

Definizione 1.14. Siano $(X, \leq)$ e $(Y, \leq)$ due insiemi parzialmente ordinati. Una funzione $f : X \longmapsto Y$ si dice *morfismo d'ordine* se verifica la seguente condizione:
per ogni $x, y \in X$, $x \leq y \Rightarrow f(x) \leq f(y)$.

Definizione 1.15. Siano $(X;\leq)$ e $(Y;\leq)$ due insiemi parzialmente ordinati. Una funzione $f : X \longmapsto Y$ si dice *ismorfismo d'ordine* se:

(a) f è biettiva

(b) f è un morfismo d'ordine

(b) f^{-1} è un morfismo d'ordine

Definizione 1.16. Due insiemi parzialmente ordinati $(X, \leq)$ e $(Y, \leq)$ si dicono *isomorfi* se esiste un isomorfismo d'ordine $f : X \longmapsto Y$.

Definizione 1.17. Sia $(X, \leq)$ un insieme parzialmente ordinato. Un *ideale* di X è un suo sottoinsieme I tale che: $x \in I, y \leq x \Rightarrow y \in I$. La nozione duale di ideale è quella di *filtro*. Un filtro di X è un suo sottoinsieme F tale che: $x \in F, x \leq y \Rightarrow y \in F$.

1.2 I numeri interi e la loro fattorizzazione

Diamo alcune essenziali proprietà che coinvolgono i numeri interi, la divisibilità tra di essi e la loro scomposizione in fattori primi; esse posso risultare utili alla comprensione del capitolo successivo.
Le proposizioni che sono riportate in questa sezione non saranno corredate con le relative dimostrazioni, che è comunque possibile trovare in [5].
Indichiamo con $\mathbb{Z} = \{0, -1, 1, -2, 2 - 3, 3, \cdots\}$ l'insieme di tutti i numeri interi. Per una possibile costruzione formale di $\mathbb{Z}$ si veda [1].

Definizione 1.18. Sia n un numero intero. Diremo che d *divide* n se esiste $c \in \mathbb{Z}$ tale che $n = dc$. In tal caso scriveremo $d|n$.

Definizione 1.19. Se $d|n$ allora $\frac{n}{d}$ è detto *divisore coniugato* di d.

Teorema 1.2.1. *La relazione di divisibilità gode delle seguenti proprietà:*

(a) $n|n$ *(riflessiva)*

(b) $d|n$ *e* $n|m$ *implica* $d|m$ *(transitiva)*

(c) $1|n$ *(*1 *divide ogni intero)*

(d) $n|0$ *(ogni intero divide 0)*

(e) $d|n$ *e* $n|d$ *implica* $|d| = |n|$.

Definizione 1.20. Se d divide due interi a e b, allora diremo che d è un *divisore comune* di a e b.

Osservazione 1. Ogni coppia di numeri interi a e b possiede un divisore comune d; basta prendere $d = 1$.

Proposizione 1.2.2. *Dati due numeri interi* a *e* b*, esiste un loro divisore comune della forma*

$$d = ax + by,$$

Dove x *ed* y *sono interi. Inoltre ogni altro divisore comune di* a *e* b *divide* d.

Proposizione 1.2.3. *Dati due interi* a *e* b*, esiste uno ed un solo intero* d *con le seguenti proprietà:*

(a) $d \geq 0$

(b) $d|a$ *e* $d|b$

(c) $d'|a$ *e* $d'|b$ *implica* $d'|d$.

Definizione 1.21. Quell'unico numero intero d definito nella proposizione precedente è detto *massimo comune divisore* di a e b, e si denota con (a, b).

Definizione 1.22. Due numeri interi a e b si dicono *primi tra loro (o relativamente primi)* se $(a, b) = 1$.

Proposizione 1.2.4. *Il massimo comune divisore gode delle seguenti proprietà:*

(a) $(a, b) = (b, a)$

(b) $(a, (b, c)) = ((a, b), c)$

(c) $(ac, bc) = |c|(a, b)$

(d) $(a, 1) = 1$ *e* $(a, 0) = |a|$.

Definizione 1.23. Sia n un numero intero. Diremo che n è *primo* se:

(i) $n > 1$

(ii) gli unici suoi divisori sono 1 e lo stesso n.

Se $n > 1$ e n non è primo, diremo che è *composto*.

Teorema 1.2.5 (Euclide)**.** *Esistono infiniti numeri primi.*

Teorema 1.2.6 (Proprietà fondamentale dei numeri primi)**.** *Sia p un numero primo, e siano a e b due numeri interi. Se $p|ab$ allora $p|a$ oppure $p|b$.*

Teorema 1.2.7 (Teorema fondamentale dell'aritmetica)**.** *Ogni numero intero $n > 1$ può essere scritto come potenze di numeri primi distinti, e tale scrittura è unica, a meno dell'ordine in cui si scrivono i fattori:*

$$n = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}.$$

Capitolo 2

Funzioni aritmetiche

2.1 L'algebra delle funzioni aritmetiche

Definizione 2.1. Una funzione definita sull'insieme dei numeri interi positivi a valori reali o complessi è detta *funzione aritmetica.*
Indichiamo con $\mathcal{A} = \{f : \mathbb{N}^+ \longmapsto \mathbb{C}\}$ l'insieme di tutte le funzioni aritmetiche.

Esempio 2.1. La funzione aritmetica $u : \mathbb{N}^+ \longmapsto \mathbb{C}$ tale che $u(n) = 1$ per ogni n è detta *funzione unità.*

Esempio 2.2. La funzione $\phi : \mathbb{N}^+ \longmapsto \mathbb{C}$ definita da

$$\phi(n) = |\{1 \leq x \leq n; (x, n) = 1\}|$$

è la *funzione di Eulero.*

Esempio 2.3. Definiamo la *funzione* Λ *di Von Mandgoldt.* Per ogni intero $n \geq 1$:

$$\Lambda(n) = \begin{cases} log(p) & \text{se } n = p^m \text{ per un qualche numero primo } p \text{ e } m \geq 1, \\ 0 & \text{altrimenti.} \end{cases} \tag{2.1}$$

Essa gioca un ruolo chiave per quanto riguarda la distribuzione dei numeri primi.

Esempio 2.4. La *funzione* λ *di Liouville* è definita come segue:
$\lambda(1) = 1$, e se $n = p_1^{a_1} \cdots p_k^{a_k}$ poniamo

$$\lambda(n) = (-1)^{a_1 + \cdots a_k}.$$

Esempio 2.5. Per ogni numero complesso α e per $n \geq 1$, definiamo la seguente famiglia di funzioni aritmetiche:

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha.$$

Osserviamo che se $\alpha = 0$, $\sigma_0(n)$ è il *numero* dei divisori di n; mentre se $\alpha = 1$, $\sigma_1(n)$ è la *somma* dei divisori di n

Definizione 2.2. Se f e g sono due funzioni aritmetiche, la loro *somma* è la funzione aritmetica h data da:

$$h(n) = f(n) + g(n).$$

Osservazione 2. Sfruttando l'usuale prodotto interno di $\mathbb{C}$ possiamo dotare l'insieme delle funzioni aritmetiche di un ulteriore operazione di prodotto per scalare come segue:

$$(\lambda f)(n) = \lambda f(n);$$

per ogni $n \in \mathbb{Z}^+$ e per ogni $\lambda \in \mathbb{C}$.

Definizione 2.3. Se f e g sono due funzioni aritmetiche si definisce il *prodotto di Dirichlet* come la funzione aritmetica h data da:

$$h(n) = \sum_{d|n} f(d) g(\frac{n}{d}).$$

Utilizzeremo la notazione $f * g = h$.

Proposizione 2.1.1. *Il prodotto di Dirichlet è commutativo e associativo. Cioè, per ogni funzioni aritmetiche* f, g, k *si ha*

$$f * g = g * f \text{ (proprietà commutativa)}$$

$$(f * g) * k = f * (g * k) \text{ (proprietà associativa).}$$

Dimostrazione. Per prima cosa osserviamo che la definizione di prodotto di Dirichlet può essere riscritta anche nel modo seguente:

$$(f * g)(n) = \sum_{a \cdot b = n} f(a)g(b),$$

e in questo modo la proprietà commutativa risulta evidente. Per quanto riguarda l'associatività si ha

$$\begin{aligned}(f * (g * k))(n) &= \sum_{a \cdot d = n} f(a)(g * k)(d) = \sum_{a \cdot d = n} f(a) \sum_{b \cdot c = d} g(b)k(c) \\ &= \sum_{a \cdot b \cdot c = n} f(a)g(b)k(c).\end{aligned} \tag{2.2}$$

Valutando $((f * g) * k)(n)$ si ottiene la stessa formula. Questo prova che il prodotto di Dirichlet è associativo. □

Proposizione 2.1.2. *L'insieme $\mathcal{A} = \{f : \mathbb{N}^+ \longmapsto \mathbb{C}\}$, munito delle operazioni di somma, prodotto di Dirichlet e prodotto per scalare definite precedentemente risulta una $\mathbb{C}$-algebra associativa, detta algebra delle funzioni aritmetiche.*

Definizione 2.4. La funzione aritmetica I data da

$$I(n) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } n > 1. \end{cases} \tag{2.3}$$

è chiamata *funzione identità.*

Proposizione 2.1.3. *Per ogni f si ha*

$$I * f = f * I = f.$$

Dimostrazione. Si ha

$$(f * I)(n) = \sum_{d|n} f(d)I(\frac{n}{d}) = f(n)$$

poiché $I(\frac{n}{d}) = 1$ se e solo se $d = n$. □

Teorema 2.1.4. *Una funzione aritmetica f è invertibile rispetto al prodotto di Dirichlet se e solo se $f(1) \neq 0$. In questo caso la sua inversa f^{-1} è data dalla seguenti formule ricorsive:*

$$f^{-1}(1) = \frac{1}{f(1)},$$

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{d|n, d<n} f(\frac{n}{d}) f^{-1}(d) \quad per\ n > 1\ .$$

Dimostrazione. Se f è una funzione aritmetica invertibile allora esiste una funzione f^{-1} tale che:

$$(f * f^{-1})(1) = f(1)f^{-1}(1) = I(1) = 1;$$

e quindi $f(1) \neq 0$. Viceversa, data la funzione f, consideriamo l'equazione

$$(f * f^{-1})(n) = I(n)$$

e dimostriamo che, nell'ipotesi $f(1) \neq 0$, essa ammette una ed una sola soluzione f^{-1}. Per $n = 1$ dobbiamo risolvere l'equazione

$$(f * f^{-1})(1) = 1,$$

e, dato che $f(1) \neq 0$, essa ha come unica soluzione $f^{-1}(1) = \frac{1}{f(1)}$. Procediamo ora per induzione supponendo di aver determinato univocamente i valori $f^{-1}(k)$ per ogni intero $k < n$; dobbiamo risolvere l'equazione $(f * f^{-1})(n) = I(n)$, cioè

$$\sum_{d|n} f(\frac{n}{d}) f^{-1}(d) = 0.$$

Quest'ultima si può riscrivere come

$$f(1)f^{-1}(n) + \sum_{d|n, d<n} f(\frac{n}{d}) f^{-1}(d) = 0;$$

se, come abbiamo supposto, sono noti i valori di f^{-1} per tutti i divisori $d < n$, l'equazione ammette una ed una sola soluzione $f^{-1}(n)$. Dunque il teorema è provato. □

Proposizione 2.1.5. *L'insieme delle funzioni aritmetiche f tale che $f(1) \neq 0$ forma un gruppo rispetto al prodotto di Dirichlet, nel quale l'identità è data dalla funzione $I(n)$.*

Dimostrazione. Poiché $(f * g)(1) = f(1)g(1)$, se $f(1) \neq 0$ e $g(1) \neq 0$ allora anche $(f * g)(1) \neq 0$. Questo, insieme ai teoremi 2.1.1, 2.1.3 e 2.1.4, provano la tesi. □

Esempio 2.6. Esempi di funzioni aritmetiche invertibili sono la funzione unità e la funzione ϕ di Eulero; infatti $u(1) = 1$ e $\phi(1) = 1$.

2.1.1 Funzioni aritmetiche moltiplicative

Come abbiamo già fatto osservare, l'insieme delle funzioni aritmetiche f tale che $f(1) \neq 0$ forma un gruppo abeliano rispetto al prodotto di Dirichlet. Introduciamo ora un importante sottogruppo di questo gruppo: le funzioni aritmetiche moltiplicative.

Definizione 2.5. Una funzione aritmetica f si dice *moltiplicativa* se non è identicamente nulla e per ogni m, n interi positivi tali che $(m, n) = 1$ si ha

$$f(m, n) = f(m)f(n)$$

Una funzione f moltiplicativa si dice *completamente moltiplicativa* se si ha anche

$$f(m, n) = f(m)f(n) \quad \text{per ogni } m, n \text{ interi positivi.}$$

Esempio 2.7. La funzione unità $u(n)$ è un banale esempio di funzione completamente moltiplicativa. Mentre la funzione ϕ di Eulero è moltiplicativa ma non è completamente moltiplicativa. Per la dimostrazione si veda [5].

Proposizione 2.1.6. *Se f è una funzione aritmetica moltiplicativa allora $f(1) = 1$.*

Esempio 2.8. Poiché $\Lambda(1) = 0$, la funzione di Von Mangoldt non è moltiplicativa.

Osservazione 3. La proposizione precedente asserisce, in particolare, che una funzione aritmetica moltiplicativa è sempre invertibile rispetto al prodotto di Dirichlet.

Proposizione 2.1.7. *Se g è una funzione aritmetica moltiplicativa, allora la sua inversa g^{-1} rispetto al prodotto di Dirichlet è moltiplicativa.*

Proposizione 2.1.8. *Sia f una funzione aritmetica con $f(1) = 1$. Allora:*

(a) f è moltiplicativa se e solo se

$$f(p_1^{a_1} \cdots p_r^{a_r}) = f(p_1^{a_1}) \cdots f(p_r^{a_r})$$

per ogni numero primo p_i e per ogni intero $a_i \geq 1$.

(b) Se f è moltiplicativa, allora f è completamente moltiplicativa se e solo se

$$f(p^a) = f(p)^a$$

per ogni numero primo p e per ogni intero $a \geq 1$

Proposizione 2.1.9. *Se f e g sono due funzioni aritmetiche moltiplicative allora il loro prodotto di Dirichlet $(f * g)$ è moltiplicativo.*

Proposizione 2.1.10. *Se sia g che $f * g$ sono funzioni aritmetiche moltiplicative allora f è moltiplicativa.*

2.2 La funzione di Möbius $\mu(n)$

Definizione 2.6. La *funzione di Möbius* μ è definita come segue:

$$\mu(1) = 1;$$

Se $n > 1$, e se $n = p_1^{a_1} \cdots p_k^{a_k}$ allora:

$$\mu(n) = \begin{cases} (-1)^k & \text{se } a_1 = a_2 = \cdots = a_k \\ 0 & \text{altrimenti.} \end{cases} \tag{2.4}$$

Alcuni dei primi valori assunti dalla funzione di Möbius sono:

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1

Osservazione 4. Si noti che $\mu(n) = 0$ se e solo se nella scomposizione in fattori primi di n compare un quadrato maggiore di 1.

Osservazione 5. Poichè $\mu(1) = 1$, la funzione di Möbius è invertibile rispetto al prodotto di Dirichlet.

Proposizione 2.2.1. *La funzione di Möbius è moltiplicativa ma non è completamente moltiplicativa.*

Dimostrazione. Si considerino due interi positivi m, n primi tra loro. Se almeno uno tra m ed n ha un fattore primo che è un quadrato maggiore di 1, allora esso compare anche nella scomposizione di mn, e quindi $\mu(mn)$

e $\mu(n)\mu(m)$ sono entrambi nulli. Altrimenti si scriva $m = p_1 \cdots p_s$ e $n = q_1 \cdots q_t$ dove p_i e q_i sono primi distinti. Allora $\mu(m) = (-1)^s$, $\mu(n) = (-1)^t$ e $\mu(mn) = (-1)^{s+t} = \mu(m)\mu(n)$.
Mentre non è completamente moltiplicativa poiché $\mu(4) = 0$ ma $\mu(2)\mu(2) = 1$. □

Proposizione 2.2.2. *Se $n \geq 1$ si ha*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } n > 1. \end{cases} \tag{2.5}$$

Dimostrazione. La formula è chiaramente vera per $n = 1$. Sia ora $n > 1$ e sia $n = p_1^{a_1} \cdots {p_k}^{a_k}$ la sua scomposizione in fattori primi. Nella somma $\sum_{d|n} \mu(d)$ gli unici addendi che danno contributo non nullo sono quelli relativi a $d = 1$ ed a quei divisori di n che sono prodotto di primi distinti. Allora si ha:

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \cdots + \mu(p_k) + \mu(p_1p_2) + \cdots + \mu(p_{k-1}p_k) + \cdots + \mu(p_1p_2 \cdots p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{s}(-1)^2 + \cdots + \binom{k}{k}(-1)^k = (1-1)^k = 0. \end{aligned} \tag{2.6}$$

□

Osservazione 6. Poiché per definizione

$$I(n) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } n > 1; \end{cases} \tag{2.7}$$

la proposizione 2.2.2 asserisce, utilizzando la notazioni del prodotto di Dirichlet, che $\mu * u = I$, e cioè che $u = \mu^{-1}$ e $\mu = u^{-1}$.

Teorema 2.2.3 (Formula di inversione di Möbius)**.**
Siano f,g due funzioni aritmetiche. Allora

$$g(n) = \sum_{d|n} f(d) \quad \textit{se e solo se} \quad f(n) = \sum_{d|n} g(d)\mu(\frac{n}{d}).$$

Dimostrazione. La formula $g(n) = \sum_{d|n} f(d)$ stabilisce che $g = f * u$. Moltiplicando a destra per $\mu = u^{-1}$ si ottiene che $g * \mu = f$, e cioè

$$f(n) = \sum_{d|n} g(d)\mu(\frac{n}{d}).$$

Viceversa, se $f(n) = \sum_{d|n} g(d)\mu(\frac{n}{d})$ allora $g * \mu = f$ e quindi $g = f * u$; da cui

$$g(n) = \sum_{d|n} f(d).$$

□

Proposizione 2.2.4. *Se $n \geq 1$ risulta:*

$$\sum_{d|n} \phi(d) = n.$$

Dimostrazione. Denotiamo con S l'insieme $\{1, 2, \cdots, n\}$. Distribuiamo gli elementi di S come segue. Per ogni divisore d di n poniamo:

$$A(d) = \{k|(k, n) = d, 1 \leq k \leq n\}.$$

Gli insiemi $A(d)$ formano una collezione disgiunta di insiemi la cui unione è S. Perciò se f(d) denota il numero di elementi contenuti in $A(d)$ avremo:

$$\sum_{d|n} f(d) = n.$$

Ma $(k, n) = d$ se e solo se $(\frac{k}{d}, \frac{k}{d}) = 1$, e $0 < k \leq n$ se e solo se $0 < \frac{k}{d} \leq \frac{n}{d}$. Perciò se poniamo $q = \frac{k}{d}$, vi è una corrispondenza biunivoca tra gli elementi di $A(d)$ e l'insieme $\{q|0 < q \leq \frac{n}{d}, (q, \frac{n}{d}) = 1\}$, la cui cardinalità è $\phi(\frac{n}{d})$. Percui $f(d) = \phi(\frac{n}{d})$ e si ha:

$$n = \sum_{d|n} f(d) = \sum_{d|n} \phi(\frac{n}{d}) = \sum_{d|n} \phi(d).$$

L'ultima uguaglianza segue dal fatto che quando d varia sull'insieme di tutti i divisori di n anche il suo divisore coniugato $\frac{n}{d}$ varia sull'insieme di tutti i divisori di n. □

La funzione di Eulero è correlata alla funzione di Möbius dalla seguente formula:

Teorema 2.2.5.

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d} \tag{2.8}$$

Dimostrazione. La tesi segue immediatamente applicando la formula di inversione di Möbius all'identità $\sum_{d|n} \phi(d) = n$. □

2.3 Il problema delle collane

Presentiamo ora un'applicazione della formula di inversione di Möbius; in particolare vogliamo mostrare come essa possa essere utilizzata per risolvere il cosiddetto *"problema delle collane"*. Introduciamo prima il problema in maniera informale ed intuitiva come segue: supponiamo di voler comporre delle collane utilizzando perline di k colori diversi, e richiediamo che ogni collana sia costituita da esattamente n perline. Quante collane diverse possiamo ottenere?
Con un rapido calcolo si ottiene ad esempio che, se i colori a disposizione sono due, le possibili collane di 4 perline sono in totale 6. Passiamo ora alla formalizzazione matematica del problema.

Definizione 2.7. Un insieme A linearmente ordinato di cardinalità k si dice *alfabeto* di k lettere. Mentre una *parola* di lunghezza n nell'alfabeto A è una funzione $p : \{1, 2, \dots n\} \longmapsto A$.
Una parola p può essere anche rappresentata mediante la lista ordinata dei suoi valori.

Esempio 2.9. Se A={b,n} e $n = 3$, la parola p data da $p(1) = b$, $p(2) = n$ e $p(3) = b$ corrisponde alla lista *bnb*.

Osservazione 7. Il numero totale di parole di lunghezza n su un alfabeto A di k lettere è k^n.

Nella nostra situazione concreta le k lettere corrispondono ai possibili colori delle perline; mentre una parola è una sequenza di n perline infilate una dopo l'altra nel filo che, una volta annodato, realizzerà la collana.

Definizione 2.8. Si dice *periodo* di una parola p un intero h tale che:

$$p(i) = p(i + h)$$

per ogni i. Il minimo tra i periodi di p di dice *periodo* primitivo.

Si controlla facilmente che il periodo della parola p divide la sua lunghezza. Definiamo ora una relazione di equivalenza sull'insieme delle parole di lunghezza n in A.

Definizione 2.9. Diremo che due parole p e q sono *equivalenti* se esiste un intero k tale che per ogni $i, j = 1, 2, \ldots, n$ risulti:

$$j \equiv i + k \pmod{n} \Rightarrow p(i) = q(j).$$

Esempio 2.10. Le parole $p = nbnn$ e $q = nnbn$ sono equivalenti, perché, per ogni $i = 1, 2, 3, 4$, risulta $p(i) = q(j)$ con $j \equiv i + 1 \pmod{4}$.

Definizione 2.10. Ogni classe di equivalenza della reazione appena definita si dice *collana*.

Vogliamo calcolare il numero $C_k(n)$ di collane di lunghezza n nell'alfabeto A.
Osserviamo che due parole equivalenti hanno lo stesso periodo primitivo: possiamo parlare quindi senza ambiguità di *periodo primitivo di una collana*. Inoltre se una collana ha periodo primitivo h, essa corrisponde esattamente ad h parole diverse (tanti sono i modi di tagliare la collana ottenendo parole diverse).

Teorema 2.3.1. *Il numero $C_k(n)$ delle collane di lunghezza n nell'alfabeto A di cardinalità k è dato da:*

$$C_k(n) = \frac{1}{n} \sum_{d|n} \phi(\frac{n}{d}) k^d.$$

Dimostrazione. Per ogni intero $h = 1, 2, \ldots, n$, indichiamo con $F(h)$ il numero di collane di lunghezza n aventi periodo primitivo h. Si ha quindi

$$C_k(n) = \sum_{h|n} F(h).$$

Dunque il numero di parole di lunghezza n in A è dato da

$$k^n = \sum_{h|n} hF(h).$$

La formula di inversione di Möbius fornisce dunque:

$$F(h) = \frac{1}{h} \sum_{h|n} \mu(\frac{h}{d}) k^d,$$

per cui

$$C_k(n) = \sum_{h|n} F(h) = \sum_{h|n} \frac{1}{h} \sum_{d|h} \mu(\frac{h}{d}) k^d = \frac{1}{n} \left(\sum_{h|n} \frac{n}{h} \sum_{d|n} \mu(\frac{h}{d}) k^d \right);$$

e la somma interna, per il teorema 2.2.5, è uguale a $\phi(\frac{n}{d})$; dunque,

$$C_k(n) = \frac{1}{n} \sum_{d|n} \phi(\frac{n}{d}) k^d,$$

come volevamo. □

Capitolo 3

Algebre di Incidenza

Definiamo l'algebra di incidenza di un insieme parzialmente ordinato. La trattazione può essere condotta in ambito più generale, ma ci limitiamo a considerare algebre di incidenza su campi anziché su anelli.

Definizione 3.1. Sia K un campo, e sia A uno spazio vettoriale su K munito di una operazione binaria aggiuntiva da $A \times A$ ad A, che denotiamo con $\cdot$. Diremo che A è un'*algebra* su K se per ogni $x, y, z \in A$ e per ogni $a, b \in K$ vale:

- $(x + y) \cdot z = x \cdot z + y \cdot z$;
- $x \cdot (y + z) = x \cdot y + x \cdot z$;
- $(ax) \cdot (by) = (ab)(x \cdot y)$.

Definizione 3.2. Siano $(X, \leq)$ un insieme parzialmente ordinato localmente finito e K un campo. *L'algebra di incidenza* $I(X, K)$ di X su K è

$$I(X, K) = \{f : X \times X \longmapsto K | f(x, y) = 0 \quad se \quad x \not\leq y\}$$

con le operazioni date da

$$(f + g)(x, y) = f(x, y) + g(x, y),$$
$$(rf)(x, y) = rf(x, y),$$
$$(f \cdot g)(x, y) = \sum_{x \leq z \leq y} f(x, z)g(z, y),$$

$\forall f, g \in I(X,K), r \in K$ e $x, y, z \in X$.

Osservazione 8. Si noti che il prodotto definito da $(f \cdot g)(x,y) = \sum_{x \leq z \leq y} f(x,z)g(z,y)$, detto *prodotto di convoluzione*, è ben definito in quanto X è localmente finito.

Proposizione 3.0.1. *Con le operazioni definite precedentemente $I(X,K)$ è una K-algebra associativa.*

Dimostrazione. E' facile verificare che $I(X,K)$ sia uno spazio vettoriale rispetto alle operazioni di somma tra funzioni e di prodotto per scalare. Proviamo la distributività da destra dell'operazione di prodotto rispetto alla somma.

$$\begin{aligned}[(f+g)\cdot h](x,y) &= \sum_{x\leq z\leq y} (f+g)(x,z)h(z,y) = \sum_{x\leq z\leq y} [f(x,z)+g(z,y)]h(z,y) = \\ &= \sum_{x\leq z\leq y} f(x,z)h(z,y) + g(x,z)h(z,y) = \sum_{x\leq z\leq y} f(x,z)h(z,y) + \\ &+ \sum_{x\leq z\leq y} g(x,z)h(z,y) = (f\cdot h)(x,y) + (g\cdot h)(x,y).\end{aligned} \tag{3.1}$$

Analogamente si prova la distributività da sinistra.
Infine si ha:

$$\begin{aligned}(af)\cdot(bg) &= \sum_{x\leq z\leq y} (af)(x,z)(bg)(z,y) = \sum_{x\leq z\leq y} af(x,z)bg(z,y) = \\ &\sum_{x\leq z\leq y} abf(x,z)g(z,y) = (ab)(f\cdot g).\end{aligned} \tag{3.2}$$

□

Definizione 3.3. Se A è un sottoinsieme di X, la funzione $\delta_A \in I(X,K)$ definita da:

$$\delta_A(x,y) = \begin{cases} 1 & \text{se } x = y \in A \\ 0 & \text{altrimenti .} \end{cases} \tag{3.3}$$

è detta *funzione caratteristica di A*. Se $A = X$ poniamo $\delta_X = \delta$.

Proposizione 3.0.2. *Data $f \in I(X,K)$, si ha:*
$(f \cdot \delta)(x,y) = f(x,y) \quad e \quad (\delta \cdot f)(x,y) = f(x,y)$.
Quindi δ è l'identità dell'algebra di incidenza.

Dimostrazione. Si ha: $(f \cdot \delta)(x,y) = \sum_{x \leq z \leq y} f(x,z)\delta(z,y) = f(x,y)\delta(x,y)$. Si è sfruttato il fatto che nella sommatoria l'unico addendo non nullo è quello che si ottiene per $z = y$. Analogamente si prova che $(\delta \cdot f)(x,y) = f(x,y)$. □

Al fine di determinare quali elementi di $I(X,K)$ siano invertibili, enunciamo la seguente proposizione.

Teorema 3.0.3. *Sia X un insieme parzialmente ordinato localmente finito e K un campo. Un elemento $f \in I(X,K)$ possiede un inverso bilatero se e solo se $f(x,x) \neq 0$ per ogni $x \in X$.*

Dimostrazione. Se $f(x,x) \neq 0$ per ogni $x \in X$, si controlla facilmente che l'inversa bilatera di f è la funzione f^{-1} così definita:

$$f^{-1}(x,x) = \frac{1}{f(x,x)} \text{ per ogni } x \in X,$$

$$f^{-1}(x,y) = \frac{-1}{f(y,y)} \sum_{x \leq z < y} f^{-1}(x,z) \cdot f(z,y) \text{ per } x < y.$$

Viceversa, se f ammette inversa bilatera f^{-1}, allora $f \cdot f^{-1} = \delta$, quindi per ogni $x \in X$ si ha:

$$1 = \delta(x,x) = (f \cdot f^{-1})(x,x) = f(x,x)f^{-1}(x,x)$$

e dunque $f(x,x) \neq 0$. □

Definiamo ora le principali funzioni che appartengono ad una qualsiasi algebra di incidenza.

Definizione 3.4. Sia $\zeta \in I(X,K)$ definita nel modo seguente:

$$\zeta(x,y) = \begin{cases} 1 & \text{se } x \leq y, \\ 0 & \text{altrimenti .} \end{cases} \tag{3.4}$$

che chiameremo *funzione zeta* di X.

Osservazione 9. La funzione ζ è invertibile grazie al teorema 3.0.3.

Proposizione 3.0.4. *Sia $[x, y]$ un intervallo dell'insieme parzialmente ordinato $(X; \leq)$. Allora $\zeta^2(x, y)$ fornisce la cardinalità dell'intervallo $[x, y]$.*

Dimostrazione. La dimostrazione segue immediatamente dalla definizione di prodotto di convoluzione. □

Definizione 3.5. Si definisce $\chi \in I(X, K)$, detta *funzione catena*, nel modo seguente:

$$\chi(x, y) = \begin{cases} 1 & \text{se } x < y, \\ 0 & \text{altrimenti .} \end{cases} \tag{3.5}$$

Proposizione 3.0.5. *Sia K un campo di caratteristica zero e sia $[x, y]$ un intervallo dell'insieme parzialmente ordinato $(X; \leq)$. Allora:*

(i) $\chi^n(x, y)$ fornisce il numero di catene distinte di lunghezza n dell'intervallo $[x, y]$;

(ii) $\sum_{k>0} \chi^k(x, y)$ fornisce il numero di catene tra x ed y.

Dimostrazione. L'affermazione (i) si dimostra procedendo per induzione su n. Per $n = 1$ l'affermazione segue dalla definizione di funzione catena. Supponiamo ora che l'affermazione sia valida per un valore $1 \leq n$; abbiamo:

$$\chi^{n+1} = \sum_{x \leq z \leq y} \chi^n(x, z)\chi(z, y) = \sum_{x \leq z < y} \chi^n(x, z);$$

per ipotesi di induzione, l'ultima somma fornisce il numero di catene di lunghezza $n + 1$ tra x ed y, da cui la tesi. L'affermazione (ii) è ovvia, osservando che grazie alla (i) solo un numero finito di addendi è diverso da zero. □

Osservazione 10. Osserviamo che $\zeta = \chi + \delta$ e inoltre formalmente si ha: $\frac{1}{\zeta} = \delta - \chi + \chi^2 - \chi^3 + \dots$.
Grazie al teorema precedente, vi è solo un numero finito di addendi che compaiono a secondo membro il cui valore è diverso da zero quando valutati in (x, y).

Definizione 3.6. Definiamo la *funzione di copertura* $\kappa \in I(X, K)$ come segue:

$$\kappa(x, y) = \begin{cases} 1 & \text{se } x \text{ è coperto da } y, \\ 0 & \text{altrimenti .} \end{cases} \tag{3.6}$$

Definizione 3.7. La *funzione di Möbius* dell'insieme parzialmente ordinato $(X, \leq)$ è per definizione:

$$\mu_X = \zeta^{-1}.$$

Le proprietà di questa funzione, oggetto principale dell'intera trattazione, verranno presentate in maniera dettagliata nella sezione seguente.

3.1 Sottoalgebre

Proposizione 3.1.1.
Se $(X', \leq)$ *è un sottoordine di* $(X, \leq)$*, allora* $I(X', K)$ *è una sottoalgebra di* $I(X, K)$*.*

Introduciamo ora un'importante classe di sottolagebre.

Definizione 3.8.
Sia X un insieme parzialmente ordinato, e sia E una relazione di equivalenza sull'insieme degli intervalli non vuoti di X. Una funzione $f \in I(X, K)$ si dice *E-funzione* se per ogni coppia di intervalli $[x, y]$ e $[u, v]$ di X si ha: $[x, y]E[u, v]$ implica $f(x, y) = f(u, v)$. Cioè f è costante sulle classi di equivalenza di E. Sia $I(X_E, K)$ la collezione delle E-funzioni.

Definizione 3.9. Sia E una relazione di equivalenza sull'insieme degli intervalli non vuoti di X. Diremo che E è *compatibile con la relazione d'ordine* se: per ogni $f, g \in I(X_E, K)$ il prodotto $f \cdot g$ appartiene ancora ad $I(X_E, K)$.

Osservazione 11. In generale, $I(X_E, R)$ è una sottoalgebra di I(X, K) se e solo se E è compatibile con la relazione d'ordine.

Proposizione 3.1.2. *Siano* X *un insieme parzialmente ordinato localmente finito,* K *un campo ed* E *una relazione d'equivalenza sull'insieme degli intervalli non vuoti di* X*. Supponiamo che, per ogni coppia di intervalli, se*

$[x,y]E[u,v]$ allora esiste una mappa biettiva $\phi : [x,y] \longmapsto [u,v]$ tale che per ogni $z \in [x,y]$ vale:

$$[x,z]E[u,\phi(z)] \text{ e } [z,y]E[\phi(z),v].$$

Allora $I(X_E,K)$ è una sottoalgebra di $I(X,K)$.

Dimostrazione. Siano $f,g \in I(X_E,K)$ e $[x,y]E[u,v]$, si ha:

$$\begin{aligned}(f\cdot g)(x,y) &= \sum_{x\leq z\leq y} f(x,z)g(z,y)\\ &= \sum_{x\leq z\leq y} f(u,\phi(z))g(\phi(z),v)\\ &= \sum_{u\leq t\leq v} f(u,t)g(t,v)\\ &= (f\cdot g)(u,v).\end{aligned} \tag{3.7}$$

Quindi $I(X_E,K)$ è una sotto algebra di $I(X,K)$. □

Enunciamo senza dimostrare la seguente proposizione.

Proposizione 3.1.3. *Siano X un insieme parzialmente ordinato localmente finito, K un campo ed E una relazione d'equivalenza sull'insieme degli intervalli non vuoti di X. Se $I(X_E,K)$ è una sotto algebra dell'algebra di incidenza $I(X,K)$ allora:*

(i) $\delta \in I(X_E,K)$

(ii) $I(X_E,K)^* = I(X_E,K) \cap I(X,K)^*$

In particolare, $\mu \in I(X_E,K)$.

Definizione 3.10. Siano X un insieme parzialmente ordinato e K un campo. Sia E è una relazione d'equivalenza sull'insieme degli intervalli non vuoti di X. Se E è compatibile con la relazione d'ordine, allora la sotto algebra di incidenza $I(X_E,K)$ è detta *algebra di incidenza ridotta di X su K* e si denota con $Red_E(I(X,K))$. Se E è la relazione d'equivalenza definita dall'isomorfismo tra intervalli, allora la sotto algebra è detta *algebra di incidenza ridotta standard di X su K*.

Definizione 3.11. Siano $f, g \in I(X, K)$, il *prodotto di Hadamard* tra f e g, che denotiamo con $f \star g$, è definito da:

$$(f \star g)(x, y) = f(x, y)g(x, y)$$

per ogni $x, y \in X$.

Proposizione 3.1.4. *Siano X un insieme parzialmente ordinato e K un campo. Sia A una sotto algebra di $I(X, K)$. Se A è una sotto algebra di incidenza ridotta allora:*

(i) $\zeta \in A$

(ii) se $f, g \in A$, *allora* $f \star g \in A$.

Dimostrazione. Abbiamo già osservato in precedenza che, se A è una sotto algebra di incidenza ridotta definita dalla relazione d'equivalenza $\sim$, la funzione ζ appartiene sempre ad A. Inoltre se gli intervalli $[x_1, y_1]$ e $[x_2, y_2]$ sono equivalenti, allora $f(x_1, y_1) = f(x_2, y_2)$ e $g(x_1, y_1) = g(x_2, y_2)$. Segue quindi che $(f \star g)(x_1, y_1) = (f \star g)(x_2, y_2)$. Quindi A è chiusa rispetto al prodotto di Hadamard. □

Osservazione 12. Nel caso in cui il sostegno X sia finito, nella proposizione precedente vale anche l'implicazione inversa. Per la dimostrazione si veda [4].

L'esempio più naturale di algebra di incidenza ridotta è l'algebra di incidenza ridotta standard. Concludiamo questo capitolo riportando due esempi che mostrano l'utilità di tali sotto algebre.

Definizione 3.12. Sia $s \in \mathbb{C}$ fissato. Una *serie di Dirichlet* è una qualunque serie della forma

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

dove i coefficienti a_n sono numeri complessi.

Esempio 3.1. Consideriamo l'algebra di incidenza $I(\mathbb{Z}_0^+, \mathbb{C})$, dove $\mathbb{Z}_0^+$ è ordinato secondo il suo ordinamento naturale. Se $\simeq$ indica la relazione di isomorfismo tra intervalli di $\mathbb{Z}_0^+$, si ha che $[x, y] \simeq [u, v]$ se e solo se $y - x = v - u$.

Di conseguenza, se una funzione f appartiene all'algebra di incidenza ridotta standard, essa è determinata univocamente dai valori $f(0,n)$ per ogni $n \in \mathbb{Z}_0^+$. In questa situazione c'è una rappresentazione più familiare dell'algebra di incidenza ridotta standard.
Per ogni funzione $f \in Red_{\simeq}(I(\mathbb{Z}_0^+, \mathbb{C}))$ poniamo $a_n = f(0,n)$ e consideriamo la biezione:

$$f \longmapsto a_o + a_1 t + a_2 t^2 \cdots.$$

Abbiamo così costruito una mappa:

$$\rho : Red_{\simeq}(I(\mathbb{Z}_0^+, \mathbb{C})) \longmapsto \mathbb{C}[[t]],$$

dove $\mathbb{C}[[t]]$ è l'anello delle serie di potenze a coefficienti in $\mathbb{C}$. Vediamo come la moltiplicazione tra elementi in $Red_{\simeq}(I(\mathbb{Z}_0^+, \mathbb{C}))$ corrisponda alla moltiplicazione tra serie di potenze. Se

$$g \longmapsto b_o + b_1 t + b_2 t^2 \cdots,$$

allora

$$\begin{aligned}(f \cdot g)(0,n) &= \sum_{i=0}^{n} f(0,i) g(i,n) \\ &= \sum_{i=0}^{n} f(0,i) g(0,n-i) \\ &= \sum_{i=0}^{n} a_i b_{n-i}.\end{aligned} \tag{3.8}$$

Si può dimostrare che $Red_{\simeq}(I(\mathbb{Z}_0^+, \mathbb{C}))$ e $\mathbb{C}[[t]]$ sono isomorfe, tramite ρ, come $\mathbb{C} - algebre$. In particolare:

$$\zeta \longmapsto 1 + t + t^2 + \cdots = \frac{1}{1-t}.$$

Da cui $\zeta^{-1} = \mu = 1 - t$. Quindi,

$$\mu(x,y) = \begin{cases} 1 & \text{se } x = y, \\ -1 & \text{se } y = x + 1, \\ 0 & \text{altrimenti.} \end{cases} \tag{3.9}$$

Esempio 3.2. Sia $\mathbb{N}$ l'insieme degli interi postivi ordinati per divisibilità e sia

$$A = \{f \in I(\mathbb{N}, \mathbb{C}) | f(x_1, y_1) = f(x_2, y_2) \text{ se } \frac{y_1}{x_1} = \frac{y_2}{x_2}\}.$$

La sottoalgebra A è una algebra di incidenza ridotta che contiene l'algebra di incidenza ridotta standard. Se $f \in A$ si ha che $f(x, y) = f(1, \frac{y}{x})$, quindi f è univocamente determinata di valori $f(1, n)$ per ogni intero positivo n.
Anche in questo caso esiste una rappresentazione comoda dell'algebra di incidenza ridotta. Se $f \in A$ poniamo $a_n = f(1, n)$ e consideriamo la biezione

$$f \longmapsto \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

dove s è un numero complesso fissato. Se

$$g \longmapsto \sum_{n=1}^{\infty} \frac{b_n}{n^s},$$

allora

$$\begin{aligned}(f \cdot g)(1, n) &= \sum_{r|n} f(1, n) g(r, n) \\ &= \sum_{r|n} f(1, r) g(1, \frac{n}{r}) \\ &= \sum_{r|n} a_n b_{\frac{n}{r}}.\end{aligned} \tag{3.10}$$

Questo mostra che la moltiplicazione in A corrisponde alla moltiplicazione tra serie di Dirichlet. Anche in questo caso si ha che che $Red_{\simeq}(I(\mathbb{N}, \mathbb{C}))$ è isomorfa ad una sottoalgebra dell'algebra delle serie di Dirichlet.
In particolare,

$$\zeta \longmapsto \sum_{n=1}^{\infty} \frac{1}{n^s}$$

è la funzione Zeta di Riemann.

3.2 La funzione di Möbius di un insieme parzialmente ordinato

In questa sezione vengono presentate le proprietà della funzione di Möbius di un generico insieme parzialmente ordinato; nonché presi in esame alcuni dei più classici esempi in cui è possibile determinarne completamente i valori assunti. Richiamiamo quindi la seguente definizione:

Definizione 3.13. La *funzione di Möbius* dell'insieme parzialmente ordinato $(X, \leq)$ è per definizione:

$$\mu = \zeta^{-1}.$$

Parleremo di funzione di Möbius dell'insieme parzialmente ordinato $(X, \leq)$ o, equivalentemente, della funzione di Möbius dell'algebra di incidenza $I(X, K)$. Scriveremo μ_X anziché μ quando vorremo mettere in evidenza l'insieme parzialmente ordinato a cui ci si riferisce.
Una proprietà cruciale della funzione μ è, chiaramente, quella di essere la funzione inversa di ζ, da cui segue la seguente proposizione.

Proposizione 3.2.1. *Sia X un insieme parzialmente ordinato localmente finito, K un campo e sia $\mu \in I(X, K)$ la funzione di Möbius dell'algebra di incidenza. Allora:*

(1) $\mu(x, x) = 1$ *per ogni* $x \in X$,

(2) per ogni $x < y$ *vale* $\sum_{x \leq z \leq y} \mu(x, z) = 0$,

(3) per ogni $x < y$ *vale* $\sum_{x \leq z \leq y} \mu(z, y) = 0$.

Dimostrazione. Segue immediatamente dal fatto che $(\mu \cdot \zeta)(x, y) = \delta(x, y) = (\zeta \cdot \mu)(x, y)$. □

Corollario 3.2.2. *Sia X un insieme parzialmente ordinato localmente finito, K un campo e sia $\mu \in I(X, K)$ la funzione di Möbius dell'algebra di incidenza. Indichiamo con 1_K l'elemento neutro del gruppo moltiplicativo K^*. Allora per ogni $x, y \in X$ $\mu(x, y)$ appartiene al sottoanello $< 1_K >$.*

Dimostrazione. Per dimostrare l'affermazione procediamo per induzione forte sulla cardinalità $|[x, y]|$ dell'intervallo di estremi x e y.

Per $n = 0$ l'intervallo $|[x, y]|$ si riduce all'insieme $\{x\}$ e per la proposizione 3.2.1 $\mu(x, x) = 1$.
Supponiamo ora vera la tesi per ogni $a, b \in X$ tale che $|[a, b]| < n$ e siano $x, y \in X$ tale che $|[x, y]| = n$. Per la proposizione 3.2.1 si ha:

$$\sum_{x \leq z < y} \mu(x, z) = -\mu(x, y);$$

dove per ogni $z \in [x, y]$, $z \neq y$, si ha $|[x, z]| < n$. Allora per ipotesi di induzione per ogni $z \in [x, y]$, $z \neq y$, $\mu(x, z) \in < 1_K >$ e quindi anche $\mu(x, y)$ appartiene a $< 1_K >$. □

Corollario 3.2.3. *Sia X un insieme parzialmente ordinato localmente finito e sia $\mu \in I(X, \mathbb{C})$ la funzione di Möbius dell'algebra di incidenza di X su $\mathbb{C}$. Allora per ogni $x, y \in X$ $\mu_X(x, y)$ è un numero intero.*

Dimostrazione. Segue dal corollario 3.2.3 e dal fatto che $< 1_{\mathbb{C}} >= \mathbb{Z}$. □

Corollario 3.2.4. *Sia X una catena. Allora:*

$$\mu(x, y) = \begin{cases} 1 & \text{se } x = y, \\ -1 & \text{se } y \succ x, \\ 0 & \text{altrimenti.} \end{cases} \tag{3.11}$$

Dimostrazione. Segue immediatamente dal teorema 3.2.1. □

Esempio 3.3. Come abbiamo visto nell'esempio 3.1, la funzione di Möbius di $I(\mathbb{Z}_0^+, \mathbb{C})$ è data da:

$$\mu(x, y) = \begin{cases} 1 & \text{se } x = y, \\ -1 & \text{se } y = x + 1, \\ 0 & \text{altrimenti.} \end{cases} \tag{3.12}$$

Esempio 3.4. Sia U un insieme finito, e $\mathcal{B}(U)$ l'algebra di Boole dei suoi sottoinsiemi. Se A, B sono due sottoinsiemi di U tali che $A \subseteq B$, risulta:

$$\mu(A, B) = (-1)^{|B|-|A|}.$$

Per provarlo, procediamo per induzione su $|B| - |A|$. Per $|B| - |A| = 0$ l'affermazione è banalmente vera. Supponiamola ora vera per ogni coppia di

sottoinsiemi $C \subseteq D$ per cui $|C| - |D| = k$, e consideriamo $A, B \subseteq U$ tali che $A \subseteq B$ e $|B| - |A| = k + 1$. Per il teorema 3.2.1 abbiamo:

$$\mu(A,B) = -\sum_{A \subseteq C \subset B} \mu(A,C) = -\sum_{i=0}^{k} \sum_{A \subseteq C \subset B, |C| = |A| + i} \mu(A,C);$$

per ipotesi di induzione, l'ultima espressione si può riscrivere come

$$-\sum_{i=0}^{k} \sum_{A \subseteq C \subset B, |C| = |A| + i} (-1)^i = -\sum_{i=0}^{k} \binom{k+1}{i} (-1)^i;$$

ora, tenendo conto che

$$\sum_{i=0}^{k+1} \binom{k+1}{i} (-1)^i = 0,$$

l'ultima espressione vale proprio $(-1)^{k+1}$.

Riportiamo un'altra conseguenza del teorema 3.2.1 la quale mostra che per calcolare $\mu(x,y)$, ci si può limitare a considerare l'insieme parzialmente ordinato costituito dall'intervallo $[x,y]$.

Corollario 3.2.5. *Sia X un insieme parzialmente ordinato e $x, y \in X$. Allora $\mu_X(x,y) = \mu_{[x,y]}(x,y)$.*

Dimostrazione. Segue immediatamente procedendo per induzione sulla cardinalità dell'intervallo $[x,y]$ e utilizzando la proposizione 3.2.1. □

Nella sezione precedente abbiamo visto che $\zeta = \delta + \chi$ e che, grazie al teorema 3.0.5, $\chi^n(x,y)$ fornisce il numero di catene da x ad y di lunghezza n. Da questo si ottiene il seguente:

Teorema 3.2.6. *(P.Hall) Sia X un insieme parzialmente ordinato localmente finito e $x, y \in X$. Per ogni intero positivo n denotiamo con $C_n(x,y)$ l'insieme delle catene distinte di lunghezza n da x a y in X. Allora:*

$$\mu(x,y) = \sum_{n=0}^{\infty} (-1)^n |C_n(x,y)| \tag{3.13}$$

Dimostrazione. Per $n \geq 1$, grazie al teorema 3.0.5, risulta $|C_n(x,y)| = \chi^n(x,y)$. Mentre per $n = 0$:

$$|C_0(x,y)| = \begin{cases} 1 & \text{se } x = y, \\ 0 & \text{altrimenti;} \end{cases} \tag{3.14}$$

quindi $|C_0(x,y)| = \delta(x,y)$. Allora si ha:

$$\begin{aligned} \mu(x,y) = \zeta^{-1}(x,y) = (\delta + \chi)^{-1}(x,y) &= \delta(x,y) - \chi(x,y) + \chi^2(x,y) - \chi^3(x,y) \cdots \\ &= |C_0(x,y)| - |C_1(x,y)| + |C_1(x,y)| - |C_3(x,y) \cdots \end{aligned} \tag{3.15}$$

□

Osservazione 13. In realtà la somma $\sum_{n=0}^{\infty} (-1)^n |C_n(x,y)|$ è finita; infatti essendo $[x,y]$ finito si ha che $\chi^n = 0$ per n sufficientemente grande.

Abbiamo osservato che per calcolare $\mu(x,y)$ in un insieme parzialmente ordinato localmente finito X possiamo supporre, senza perdere di generalità, che $X = [x,y]$. Insiemi parzialmente ordinati di questo tipo sono sempre dotati di minimo e massimo, che indichiamo rispettivamente con 0 e 1. Diventa quindi importante saper calcolare il valore $\mu(0,1)$. A tale scopo la seguente proposizione fornisce un procedimento ricorsivo.

Proposizione 3.2.7. *Sia X un insieme parzialmente ordinato dotato di minimo e massimo, rispettivamente 0 e 1.*
Sia poi $x_0 \in X \setminus \{0,1\}$, allora:

$$\mu_X(0,1) = \mu_{X \setminus \{x_0\}}(0,1) + \mu_X(0,x_0) \cdot \mu_X(x_0,1).$$

Dimostrazione. Sia $C_n(0,1)$ la collezione di tutte le catene da 0 a 1 di lunghezza n in X. Inoltre denotiamo con $D_n(0,1)$ l'insieme di quelle catene di $C_n(0,1)$ che non contengono x_0 e poniamo $E_n(0,1) = C_n(0,1) \setminus D_n(0,1)$. Ogni catena di lunghezza n da 0 a 1 o contiene x_0 oppure o non lo contiene, quindi si ha:

$$|C_n(0,1)| = |D_n(0,1)| + |E_n(0,1)|.$$

Sia ora α una catena di E_n, la quale necessariamente contiene x_0. Quindi per un certo numero intero j, la catena α può essere spezzata in una catena

β da 0 a x_0 di lunghezza j e in una catena γ da x_0 a 1 di lunghezza $n-j$. In altre parole ogni volta che si sceglie una catena di lunghezza j da 0 a x_0 e una catena di lunghezza k, con $k+j=n$, da x_0 a 1 si ottiene una catena di lunghezza n da 0 a 1 che contiene x_0, e tale corrispondenza è biunivoca. Ricordiamo inoltre che per il teorema 3.2.6 abbiamo:

$$\mu_{X\setminus\{x_0\}}(0,1) = |D_0| - |D_1| + |D_2| - |D_3| + \cdots .$$

In definitiva:

$$\begin{aligned}
\mu_X(0,1) &= \sum_{n=0}^{\infty} (-1)^n |C_n(0,1)| \\
&= \sum_{n=0}^{\infty} (-1)^n \left(|D_n(0,1)| + |E_n(0,1)|\right) \\
&= \sum_{n=0}^{\infty} (-1)^n |D_n(0,1)| + \sum_{n=0}^{\infty} (-1)^n |E_n(0,1)| \\
&= \mu_{X\setminus\{x_0\}}(0,1) + \sum_{n=0}^{\infty} \sum_{k+j=n} (-1)^k (-1)^j |C_k(0,x_0)||C_j(x_0,1)| \\
&= \mu_{X\setminus\{x_0\}}(0,1) + \sum_{n=0}^{\infty} (-1)^n |C_n(0,x_0)| \cdot \sum_{n=0}^{\infty} (-1)^n |C_n(x_0,1)| \\
&= \mu_{X\setminus\{x_0\}}(0,1) + \mu_X(0,x_0) \cdot \mu_X(x_0,1).
\end{aligned} \tag{3.16}$$

□

Confrontiamo ora la funzione di Möbius di due insiemi parzialmente ordinati che siano isomorfi oppure anti-isomorfi. Ricordiamo la seguente:

Definizione 3.14. Siano $(X, \leq_X)$ e $(Y, \leq_Y)$ due insiemi parzialmente ordinati, e sia $\rho : X \longmapsto Y$ una funzione biettiva.

(1) ρ si dice *isomorfismo d'ordine* se:

$$x_1 \leq_X x_2 \text{ se e solo se } \rho(x_1) \leq_Y \rho(x_2).$$

(2) ρ si dice *anti-isomorfismo d'ordine* se:

$$x_1 \leq_X x_2 \text{ se e solo se } \rho(x_1) \geq_Y \rho(x_2).$$

Proposizione 3.2.8. *Siano $(X, \leq_X)$ e $(Y, \leq_Y)$ due insiemi parzialmente ordinati localmente finiti. Sia $\rho : X \longmapsto Y$ una funzione biettiva. Allora per ogni $x_1, x_2 \in X$ si ha:*

(1) Se ρ è un isomorfismo d'ordine allora:

$$\mu_X(x_1, x_2) = \mu_Y(\rho(x_1), \rho(x_2)).$$

(2) Se ρ è un anti-isomorfismo d'ordine allora:

$$\mu_X(x_1, x_2) = \mu_Y(\rho(x_2), \rho(x_1)).$$

Dimostrazione. Dimostriamo solo la la (1) poichè per la (2) si procede in modo analogo. Poichè per ipotesi $x_1 \leq x_2 \Leftrightarrow \rho(x_1) \leq \rho(x_2)$, per ogni $x_1, x_2 \in X$ si ha:

$$\zeta_X(x_1, x_2) = \zeta_Y(\rho(x_1), \rho(x_1)).$$

Da cui segue che $\mu_X = \mu_Y$. □

Corollario 3.2.9. *Sia X^* il duale d'ordine dell'insieme parzialmente ordinato X, e μ^* la sua funzione di Möbius. Allora per ogni coppia di elementi x, y si ha:*

$$\mu^*(x, y) = \mu(y, x).$$

Dimostrazione. Segue dalla proposizione precedente e dal fatto che X e X^* sono anti-isomorfi. □

Molti insiemi parzialmente ordinati che si incontrano nell'ambito della teoria del calcolo combinatorio sono isomorfi al prodotto diretto in insiemi parzialmente ordinati più semplici. Il teorema seguente mostra che, quando un insieme parzialmente ordinato Z è il prodotto di posets X e Y, la funzione di Möbius di Z può essere facilmente ottenuta a partire dalle funzioni di Möbius di X e Y. Ricordiamo allora la seguente:

Definizione 3.15. Siano $(X, \leq_X)$ e $(Y, \leq_Y)$ due insiemi parzialmente ordinati. L'insieme parzialmente ordinato $Z = (X \times Y, \leq_Z)$ con la relazione d'ordine definita da $(x_1, y_1) \leq_Z (x_2, y_2)$ se e solo se $x_1 \leq_X x_2$ e $y_1 \leq_Y y_2$ si dice *prodotto diretto* degli insiemi parzialmente ordinati X e Y.

Osservazione 14. Se $Z = (X \times Y, \leq_Z)$ è il prodotto diretto di due insiemi parzialmente ordinati localmente finiti X ed Y, allora Z è esso stesso localmente finito. Inoltre:

$$\delta_Z((x_1, y_1), (x_2, y_2)) = \delta_X(x_1, x_2) \cdot \delta_Y(y_1, y_2),$$

e

$$\zeta_Z((x_1, y_1), (x_2, y_2)) = \zeta_X(x_1, x_2) \cdot \zeta_Y(y_1, y_2).$$

Teorema 3.2.10. *(Teorema del prodotto) Siano X e Y due insiemi parzialmente ordinati localmente finiti, e $Z = (X \times Y, \leq_Z)$ il loro prodotto diretto. Allora per $x_1, x_2 \in X$ e $y_1, y_2 \in Y$ si ha:*

$$\mu_Z((x_1, y_1), (x_2, y_2)) = \mu_X(x_1, x_2)\mu_Y(y_1, y_2).$$

Dimostrazione. Sia $f \in I(Z, K)$ definita da:

$$f((x_1, y_1), (x_2, y_2)) = \mu_X(x_1, x_2)\mu_Y(y_1, y_2).$$

Mostriamo che $\zeta_Z \cdot f = \delta_Z$. Si ha:

$$\begin{aligned}
(\zeta_Z \cdot f)((x_1, y_1), (x_2, y_2)) = & \\
&= \sum_{(x_1,y_1) \leq (x,y) \leq (x_2,y_2)} \zeta_Z((x_1, y_1), (x, y)) \cdot f((x, y), (x_2, y_2)) \\
&= \sum_{(x_1,y_1) \leq (x,y) \leq (x_2,y_2)} \zeta_X(x_1, x) \cdot \zeta_Y(y_1, y) \cdot \mu_X(x, x_2) \cdot \mu_Y(y, y_2) \\
&= \sum_{x_1 \leq x \leq x_2, y_1 \leq y \leq y_2} \zeta_X(x_1, x) \cdot \mu_X(x, x_2) \cdot \zeta_Y(y_1, y) \cdot \mu_Y(y, y_2) \\
&= \delta_X(x_1, x_2) \cdot \delta_Y(y_1, y_2) \\
&= \delta_Z((x_1, y_1), (x_2, y_2)).
\end{aligned} \tag{3.17}$$

Poichè l'inversa di ζ_Z è μ_Z, segue che $\mu_Z = f$. □

Mostriamo l'utilità di questo risultato calcolando la funzione di Möbius di $(\mathbb{N}, |)$.

Esempio 3.5. Sia $\mathbb{N}$ l'insieme dei numeri interi positivi ordinati per divisibilità. Calcoliamo la funzione di Möbius di $\mathbb{N}$.

Se n divide m, allora l'intervallo $[n, m]$ è isomorfo all'intervallo $[1, \frac{m}{n}]$; è quindi sufficiente calcolare $\mu(1, n)$ per ogni intero positivo n. Se $n = 1$, allora $\mu(1, 1) = 1$. Sia ora $n > 1$, e supponiamo che $n = p_1^{e_1} \cdot p_2^{e_2} \dots p_r^{e_r}$ sia la sua scomposizione in fattori primi. Per ogni $i = 1, 2 \dots, r$, sia $D_i = [1, p_i^{e_i}]$. Il teorema fondamentale dell'aritmetica assicura che la scomposizione in fattori primi di n è unica a meno dell'ordine dei fattori; quindi l'intervallo $[1, n]$ è isomorfo al prodotto diretto degli insiemi parzialmente ordinati D_i per $i = 1, 2 \dots, r,$. Utilizzando il teorema del prodotto ed il corollario 3.2.4, abbiamo:

$$\mu(n, m) = \mu(1, n) = \begin{cases} 1 & \text{se } n = 1, \\ (-1)^r & \text{se } e_i = 1 \text{ per ogni } i, \\ 0 & \text{altrimenti.} \end{cases} \tag{3.18}$$

In altri termini $\mu_{\mathbb{N}}(n, m) = \mu(\frac{m}{n})$, dove μ indica la funzione di Möbius della teoria dei numeri.

Definizione 3.16. Sia X un insieme parzialmente ordinato localmente finito. Indichiamo con $Int(X)$ l'insieme parzialmente ordinato degli intervalli di X (compreso l'intervallo vuoto), ordinati per inclusione.

Proposizione 3.2.11. *Se X è localmente finito allora $Int(X)$ è localmente finito.*

Dimostrazione. Osserviamo prima di tutto che, se $[x_1, y_1], [x_2, y_2]$ sono due intervalli non vuoti di X tali che $[x_1, y_1] \leq [x_2, y_2]$ in $Int(X)$, allora risulta $x_2 \leq x_1 \leq y_1 \leq y_2$. Sia $S = [[x_1, y_1], [x_2, y_2]]$ un intervallo non vuoto di $Int(X)$ con $[x_1, y_1] \neq \emptyset$. Allora si ha che $[x, y] \in S$ se e soltanto se risulta $x_2 \leq x \leq x_1$ e $y_1 \leq y \leq y_2$. Quindi se X è localmente finito anche $Int(X)$ lo è. □

Osservazione 15. La proposizione precedente implica che se $[x_1, y_1], [x_2, y_2]$ sono due intervalli non vuoti di X tali che $[x_1, y_1] \leq [x_2, y_2]$ in $Int(X)$, allora la funzione:

$$\theta : [[x_1, y_1], [x_2, y_2]] \longmapsto [x_2, x_1]^* \times [y_1, y_2]$$

definita da $\theta([x, y]) = (x, y)$, è un isomorfismo d'ordine.

Teorema 3.2.12. *Sia X un insieme parzialmente ordinato localmente finito. Per ogni coppia $[x_1, y_1], [x_2, y_2] \in Int(X)$ si ha:*

$$\mu_{Int(x)}([x_1, y_1], [x_2, y_2]) = \begin{cases} \mu_X(x_2, x_1) \cdot \mu_X(y_1, y_2) & \text{se } [x_1, y_1] \neq \emptyset, \\ -\mu_X(x_2, y_2) & \text{se } [x_1, y_1] = \emptyset. \end{cases} \tag{3.19}$$

Dimostrazione. Il caso in cui $[x_1, y_1] \neq \emptyset$ segue dall'osservazione precedente applicando il teorema del prodotto. Supponiamo ora che $[x_1, y_1] = \emptyset$ e sia $[x_2, y_2] \in Int(X)$ non vuoto. Allora per la proposizione 3.2.1 si ha:

$$\begin{aligned} \mu_{Int(x)}(\emptyset, [x_2, y_2]) &= - \sum_{\emptyset < [x,y] \leq [x_2,y_2]} \mu_{Int(x)}([x, y], [x_2, y_2]) \\ &= - \sum_{[x,y] \leq [x_2,y_2]} \mu_X(x_2, x) \cdot \mu_X(y, y_2) \\ &= - \sum_{x_2 \leq x \leq y \leq y_2} \mu_X(x_2, x) \cdot \mu_X(y, y_2) \\ &= - \sum_{x_2 \leq x \leq y \leq y_2} \mu_X(x_2, x) \cdot \zeta_X(x, y) \cdot \mu_X(y, y_2) \\ &= - \sum_{x_2 \leq x \leq y \leq y_2} \delta_X(x_2, y) \cdot \mu_X(y, y_2) \\ &= -\mu_X(x_2, y_2). \end{aligned} \tag{3.20}$$

□

3.2.1 La formula di inversione di Möbius

Le algebre di incidenza sono state sviluppate come ambiente naturale in cui generalizzare la formula di inversione di Möbius della teoria dei numeri che abbiamo visto nel capitolo precedente. I seguenti due teoremi, dovuti al matematico italo americano Gian Carlo Rota [6], sono noti come teoremi di inversione di Möbius dell'insieme parzialmente ordinato X. Enunciamo i risultati ottenuti da Rota utilizzando i concetti di filtro e di ideale di un insieme parzialmente ordinato. Ricordiamo quindi le seguenti definizioni.

Definizione 3.17. Sia $(X, \leq)$ un insieme parzialmente ordinato. Un *ideale* di X è un suo sottoinsieme I tale che: $x \in I, y \leq x \Rightarrow y \in I$. La nozione duale di ideale è quella di *filtro*. Un filtro di X è un suo sottoinsieme F tale che: $x \in F, x \leq y \Rightarrow y \in F$.

Definizione 3.18. Siano X un insieme parzialmente ordinato e $x \in X$. L'insieme $I_x = \{y \in X | y \leq x\}$ è *l'ideale principale di X generato da x* e, dualmente, $U_x = \{y \in X | x \leq y\}$ è il *filtro principale di X generato da x.*

Esempio 3.6. L'insieme parzialmente ordinato $(\mathbb{N}, |)$ è ad ideali principali finiti ma ogni filtro principale è infinito. Infatti per ogni $n \in \mathbb{N}$ l'ideale principale generato da n è dato da $I_n = \{d \in \mathbb{N} | d \text{ divide } n\}$; che è chiaramente un insieme finito. Mentre l'insieme $U_n = \{d \in \mathbb{N} | n \text{ divide } d\}$ è infinito.

Teorema 3.2.13. *Siano X un insieme parzialmente ordinato localmente finito, K un campo e f una funzione da X a K. Supponiamo che per ogni $x \in X$ il filtro principale di X generato da x sia finito. Allora:*

$$g(x) = \sum_{x \leq y} f(y) \text{ se e solo se } f(x) = \sum_{x \leq y} \mu(x,y) g(y).$$

Dimostrazione. Supponiamo che $g(x) = \sum_{x \leq y} f(y)$. Allora:

$$\begin{aligned}
\sum_{x \leq y} \mu(x,y) g(y) &= \sum_{x \leq y} \mu(x,y) \sum_{y \leq z} f(z) \\
&= \sum_{x \leq y} \mu(x,y) \sum_{y \leq z} \zeta(y,z) f(z) \\
&= \sum_{x \leq y} \sum_{y \leq z} \mu(x,y) \zeta(y,z) f(z) \\
&= \sum_{y \leq z} \sum_{x \leq y} \mu(x,y) \zeta(y,z) f(z) \\
&= \sum_{y \leq z} \left(\sum_{x \leq y} \mu(x,y) \zeta(y,z) \right) f(z) \\
&= \sum_{x \leq y \leq z} \delta(x,z) f(z) = f(x)
\end{aligned} \tag{3.21}$$

L'implicazione inversa si dimostra in maniera del tutto analoga. □

La versione duale, in cui si richiede invece che gli ideali principali di X siano finiti, è la seguente.

Teorema 3.2.14. *Siano X un insieme parzialmente ordinato localmente finito, K un campo e f una funzione da X a K. Supponiamo che per ogni $x \in X$ l'ideale principale di X generato da x sia finito. Allora:*

$$g(x) = \sum_{y \leq x} f(y) \text{ se e solo se } f(x) = \sum_{y \leq x} \mu(y,x) g(y).$$

Esempio 3.7. Consideriamo l'insieme parzialmente ordinato $(\mathbb{N}, |)$. Applicando il teorema 3.2.14 si ottiene la formula di inversione di Möbius della teoria dei numeri:

$$g(n) = \sum_{d|n} f(d) \quad \text{se e solo se} \quad f(n) = \sum_{d|n} g(d)\mu(\frac{n}{d}).$$

Esempio 3.8. Nel caso in cui X sia la catena $(\mathbb{N}, \leq)$, dove $\leq$ è l'ordinamento naturale, tenendo conto dei valori della funzione di Möbius calcolati nel corollario 3.2.4, la formula di inversione assume la seguente forma:

$$g(x) = \sum_{i=0}^{x} f(i) \text{ per ogni } x > 0,$$

se e solo se

$$f(x) = g(x) - g(x-1) \text{ per ogni } x > 0.$$

Il seguente esempio mostra come sia possibile ottenere il principio di inclusione-esclusione utilizzando la formula di inversione.

Esempio 3.9. Sia U un insieme finito e sia

$$\Sigma = \{A_1, A_2, \ldots, A_n\}$$

una famiglia di sottoinsiemi di U. Sia G la funzione che associa ad ogni sottofamiglia $\mathcal{F}$ di Σ la cardinalità dell'intersezione dei suoi sottoinsiemi:

$$g : \mathcal{P}(\Sigma) \longmapsto \mathbb{N}, \quad g(\mathcal{F}) = card\left(\bigcap_{A\in\mathcal{F}} A\right).$$

Sia poi f la funzione che associa ad ogni sottofamiglia $\mathcal{F}$ di Σ il numero di elementi di U che stanno in tutti gli insiemi di $\mathcal{F}$, ma in nessuno degli insiemi di $\Sigma \setminus \mathcal{F}$; in altri termini,

$$f(\mathcal{F}) = card\left(\bigcap_{A\in\mathcal{F}} A \cap \bigcap_{B\in\Sigma\setminus\mathcal{F}} B^C\right).$$

Dato che $g(\mathcal{F})$ conta gli elementi x tali che $\mathcal{G} = \{A \in \Sigma; x \in A\}$ per qualche famiglia $\mathcal{G}$ tale che $\mathcal{F} \subseteq \mathcal{G} \subseteq \Sigma$, abbiamo:

$$g(\mathcal{F}) = \sum_{\mathcal{F}\subseteq\mathcal{G}\subseteq\Sigma} f(\mathcal{G}),$$

da cui, per il teorema 3.2.13,

$$f(\mathcal{F}) = \sum_{\mathcal{F}\subseteq\mathcal{G}\subseteq\Sigma} \mu(\mathcal{F},\mathcal{G})g(\mathcal{G}).$$

Ponendo $\mathcal{F} = \emptyset$, e ricordando che $\mu(\mathcal{F},\mathcal{G}) = (-1)^{|\mathcal{G}|-|\mathcal{F}|}$, otteniamo la formula di Sylvester.

3.3 Alcune applicazioni

In questa sezione presentiamo alcune ulteriori applicazioni della formula di inversione di Möbius di particolare interesse sia dal punto di vista del calcolo combinatorio che dal punto di vista algebrico.

Esempio 3.10. *Sia F un campo finito con q elementi. Vogliamo calcolare il numero $A(n)$ di polinomi monici, irriducibili di grado n a coefficienti in F.*

Sia $F \subseteq K$ una estensione di campo di grado n. Allora K è il campo di spezzamento del polinomio riducibile $f_n(x) = x^{q^n} - x$; infatti ogni elemento del gruppo moltiplicativo K^* risolve l'equazione $x^{q^n-1} - 1 = 0$. Se α è un elemento non nullo di K che annulla il polinomio irriducibile $p_\alpha(x) \in F[x]$, allora $p_\alpha(x)$ divide $f_n(x)$. Inoltre, poiché $F[\alpha]$ è un sotto campo di K, segue che il grado di $p_\alpha(x)$ divide n. Poiché esiste un unico campo finito di ordine q^n nella chiusura algebrica di F, ogni polinomio irriducibile $q(x) \in F[x]$ il cui grado divida n deve dividere $f_n(x)$. Il prodotto di tutti i polinomi monici ed irriducibili in $F[x]$ il cui grado divide n è proprio $x^{q^n} - x$. In effetti per quanto detto prima tutti i polinomi monici irriducibili su $F[x]$ il cui grado divide n sono fattori di $x^{q^n} - x$. Questi sono, chiaramente, tutti i fattori irriducibili di $f_n(x)$. D'altra parte $f_n(x)' = -1$, per cui $f_n(x)$ non ha radici multiple nel suo campo di spezzamento. Pertanto ogni polinomio monico che compare nella fattorizzazione di $f_n(x)$ vi appare un'unica volta.
Per ogni d, poniamo:

$$\Sigma_d = \{p(x) \in F[x] |\ p(x) \text{ monico, irriducibile e } deg(p(x)) = d\} \qquad (3.22)$$

Quindi

$$x^{q^n} - x = \prod_{d|n} \prod_{p(x)\in\Sigma_d} p(x)$$

e dall'uguaglianza tra i gradi di questi due polinomi:

$$q^n = deg(x^{q^n} - x) = \sum_{d|n} \sum_{p(x)\in\Sigma_d} deg(p(x)) = \sum_{d|n} d \cdot A(d).$$

Utilizzando la formula di inversione di Möbius otteniamo

$$n \cdot A(n) = \sum_{d|n} \mu(d,n) \cdot q^d,$$

da cui

$$A(n) = \frac{1}{n} \cdot \sum_{d|n} \mu(d,n) \cdot q^d.$$

Esempio 3.11. *Vogliamo calcolare una espressione per l'ennesimo polinomio ciclotomico.*

Sia n un intero positivo. Una *radice n-esima dell'unità* è un numero complesso z tale che $z^n = 1$. Un numero complesso z è poi detto *radice primitiva n-esima dell'unità* se n è il più piccolo numero intero positivo tale che $z^n = 1$. L'insieme S delle soluzioni dell'equazione $x^n - 1 = 0$ forma un gruppo ciclico di ordine n rispetto al prodotto tra numeri complessi, il cui insieme dei generatori è costituito dalle $\phi(n)$ radici primitive n-esime dell'unità. Il numero complesso $\zeta_n = e^{i\frac{2\pi}{n}} = cos(\frac{2\pi}{n}) + isen(\frac{2\pi}{n})$ è una radice primitiva n-esima dell'unità, e tutte le radici primitive n-esime dell'unità sono

$$\{\zeta_n^k; (k,n) = 1, 1 \leq k \leq n\}.$$

Il polinomio

$$\phi_n(x) = \prod_{1\leq k\leq n,(k,n)=1} (x - \zeta_n^k),$$

le cui radici sono tutte e sole le radici primitive n-esime dell'unità, è detto *n-esimo polinomio ciclotomico*. Poiché ogni $s \in S$ è una radice primitiva d-esima dell'unità per un qualche divisore d di n si ha:

$$\prod_{\zeta\in S} (x - \zeta) = x^n - 1 = \prod_{d|n} \phi_d(x).$$

Per induzione si può dimostrare che che $\phi_n(x)$ è un polinomio monico a coefficienti interi. Se x è un numero reale sufficientemente grande, allora $\phi_d(x)$ è

positivo per ogni divisore d di n. Possiamo quindi valutare il logaritmo delle due quantità presenti a primo e secondo membro, ottenendo:

$$ln(x^n - 1) = \sum_{d|n} ln(\phi_d(x)).$$

usando l'inversione di Möbius abbiamo:

$$\begin{aligned} ln(\phi_n(x)) &= \sum_{d|n} \mu(d,n) \cdot ln(x^d - 1) \\ &= \sum_{d|n} \mu(\frac{n}{d}) \cdot ln(x^d - 1) \\ &= ln(\prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}). \end{aligned} \tag{3.23}$$

Quindi per x sufficientemente grande abbiamo:

$$\phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}.$$

Poiché la funzione $\prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$ è razionale, possiamo scrivere

$$\prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})} = \frac{a(x)}{b(x)},$$

dove $a(x)$ e $b(x)$ sono polinomi primi tra loro a coefficienti interi. Supponiamo che $b(x)$ sia di grado almeno 1 e scriviamo:

$$\frac{a(x)}{b(x)} = \alpha(x) + \frac{\beta(x)}{b(x)},$$

dove $\alpha(x)$ e $\beta(x)$ sono polinomi a coefficienti interi e $deg(\beta(x)) \leq deg(b(x))$. Allora per x sufficientemente grande si ha $|\frac{\beta(x)}{b(x)}| < 1$; e quindi poiché sia $\phi_n(x)$ che $\alpha(x)$ assumono valori interi se valutati su numeri interi, necessariamente $\beta(x) = 0$.
In definitiva $\prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$ è un polinomio che coincide con $\phi_n(x)$ per infiniti valori di x; e quindi per ogni x.

Esempio 3.12. *Sia $Z = \{z_1, z_2, \ldots, z_n\}$ un insieme di elementi algebricamente indipendenti e che commutano tra di loro. Le funzioni simmetriche elementari $a_1, a_2, \ldots, a_n$ negli elementi di Z sono definite da*

$$a_k = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} z_{i_1} \cdot z_{i_2} \cdots z_{i_k},$$

per $k = 1, 2, \ldots, n$.
Le somme di potenze simmetriche $s_1, s_2, \ldots$ *sono definite da*

$$s_k = \sum_{i=1}^{n} z_i^k,$$

per $k = 1, 2, \ldots$. *Vogliamo esprimere le funzioni simmetriche elementari in termini delle somme di potenze simmetriche.*

Fissiamo $k \in \mathbb{Z}^+$. Sia S un insieme finito con k elementi e sia F l'insieme di tutte le funzioni da S a Z. Per $f \in F$, diremo che il polinomio

$$p(f) = \prod_{s \in S} f(s)$$

è il *polinomio associato* ad f. Inoltre, per $H \subseteq F$, sia

$$p(H) = \prod_{g \in H} p(g).$$

Se $f \in F$, definiamo il nucleo di f come quella partizione π di S i cui blocchi $B_1, B_2, \ldots, B_n$ sono dati da

$$B_i = \{s \in S | f(s) = z_i\}, \quad i = 1, 2, \ldots, k.$$

Osserviamo che una funzione f ha come nucleo la partizione discreta se e solo se f è iniettiva. Data una partizione π di S, definiamo la funzione

$$G(\pi) = p(H),$$

dove H è l'insieme delle funzione il cui nucleo è π, e

$$G_{\geq}(\pi) = p(H'),$$

dove H' è l'insieme delle funzioni il cui nucleo è maggiore o uguale a π nel reticolo $P(S)$ delle partizioni di S. Dalla definizione della funzione simmetrica a_k segue immediatamente che

$$G(0) = k! \cdot a_k. \tag{3.24}$$

Sia ora σ una partizione costituita da n_1 blocchi di cardinalità 1, n_2 blocchi di cardinalità $2, \ldots, n_k$ blocchi di cardinalità k. Vogliamo ora provare che

$$G_{\geq}(\sigma) = s_1^{n_1} s_2^{n_2} \ldots s_k^{n_k}. \tag{3.25}$$

Siano $B_1, B_2, \ldots, B_m$ i blocchi associati a σ. Osserviamo che una funzione $f \in F$ è tale che $ker(f) \geq \sigma$ se e solo se f è costante sugli elementi di B_i per ogni i. Quindi, il polinomio $p(f)$ è uguale ad uno dei termini dello sviluppo del prodotto $s_1^{n_1} s_2^{n_2} \ldots s_k^{n_k}$. Sommando su tutti i polinomi $p(f)$ tali che $ker(f) \geq \sigma$ si ottiene la 3.25. Ora, è chiaro che

$$G_{\geq}(0) = \sum_{\sigma \in P(S)} G(\sigma).$$

Usando l'inversione di Möbius otteniamo

$$a_k = \frac{1}{k!} \cdot \sum_{\sigma \in P(S)} \mu(0, \sigma) \cdot G_{\geq}(\sigma). \tag{3.26}$$

Siano ora $\pi_1, \pi_2 \in P(S)$ due partizioni di S tali che $\pi_1 \leq \pi_2$. Siano $B_1, B_2, \ldots, B_r$ i blocchi di π_2 e supponiamo che per $i = 1, 2, \ldots, r$ il blocco B_i sia l'unione di n_i blocchi di π_1. Allora si può dimostrare che in questo caso la funzione di Möbius è data da:

$$\mu_{P(S)}(\pi_1, \pi_2) = (-1)^{N(\pi_1) - N(\pi_2)} \cdot \prod_{i=1}^{r} (n_i - 1)!,$$

dove $N(\pi_1)$ e $N(\pi_2)$ rappresentano rispettivamente il numero di blocchi delle partizioni π_1 e π_2.
Sostituendo questa espressione nella 3.26 e ricordando che $G_{\geq}(\sigma) = s_1^{n_1} s_2^{n_2} \ldots s_k^{n_k}$, otteniamo il risultato cercato.

Bibliografia

[1] M. Barnabei e F. Bonetti, *Matematica discreta elementare*, Bologna, Pitagora, 1994

[2] E. Szpilrajn, *Sur l'extension de l'ordre partial*, Fund. Math. 16 (1930), 386-389

[3] M.Artin, *Algebra*, Torino, Bollati Boringhieri, 1997

[4] E. Spiegel e C.J. O'Donnel, *Incidence algebras*, New York, M. Dekker, 1997

[5] T. M. Apostol, *Introduction to analytic number theory*, New York, Springer-Verlag, 1976

[6] G. C. Rota, *On the foundations of combinatorial theory 1: Theory of Möbius Functions*, Z. Wahr Scheinlichkeits Theorie und Verw. Gabiete **2** (1964)