# ORDNUNGEN UND VERBÄNDE

HENRI MÜHLE

Wir rekapitulieren einige grundlegende Begriffe aus der Theorie der geordneten Mengen und der Verbandstheorie, und präsentieren drei klassische Ergebnisse: (i) den Darstellungssatz endlicher distributiver Verbände nach G. Birkhoff, (ii) den Satz von R. Dilworth über Kettenzerlegungen geordneter Mengen, sowie (iii) die Inzidenzalgebra nach G.-C. Rota und Möbiusinversion in geordneten Mengen. Dabei orientieren wir uns an Kapitel 12 in P. Camerons Buch "Combinatorics".

## 1. Grundlagen

**Definition 1.1: Teilordnung**

Sei $P$ eine Menge. Eine Relation $R \subseteq P \times P$ heißt Teilordnung auf $P$, wenn sie die folgenden Eigenschaften besitzt.

- Für alle $x \in P$ ist $(x,x) \in R$. (Reflexivität)
- Für alle $x,y \in P$ folgt aus $(x,y) \in R$ und $(y,x) \in R$ stets $x = y$. (Antisymmetrie)
- Für alle $x,y,z \in P$ folgt aus $(x,y) \in R$ und $(y,z) \in R$ stets $(x,z) \in R$. (Transitivität)

**Beispiel 1.2: Duale Ordnung**

Zu jeder Teilordnung $R$ ist die duale Relation $R^d$, definiert durch $(x,y) \in R^d$ genau dann wenn $(y,x) \in R$, wieder eine Teilordnung.

Wir bezeichnen eine Teilordnung üblicherweise mit $\leq$ anstelle von $R$.

**Beispiel 1.3: Teilmengenverband**

Die Teilmengenrelation $\subseteq$ ist eine Teilordnung auf der Potenzmenge $\wp(M)$ einer endlichen Menge $M$, denn:

- für $X \subseteq M$ gilt $X \subseteq X$;
- für $X, Y \subseteq M$ folgt aus $X \subseteq Y$ und $Y \subseteq X$ gerade $X = Y$;
- für $X, Y, Z \subseteq M$ folgt aus $X \subseteq Y$ und $Y \subseteq Z$ gerade $X \subseteq Z$.

**Beispiel 1.4: Teilerverband**

Die Teilerrelation $|$ ist eine Teilordnung auf den natürlichen Zahlen $\mathbb{N}$, denn

- für $a \in \mathbb{N}$ gilt $a \mid a$;
- für $a, b \in \mathbb{N}$ folgt aus $a \mid b$ und $b \mid a$ gerade $a = b$;
- für $a, b, c \in \mathbb{N}$ folgt aus $a \mid b$ und $b \mid c$ gerade $a \mid c$.

Wir erhalten daraus eine endliche Teilordnung, wenn wir uns auf die Menge $D(n)$ aller Teiler einer festen natürlichen Zahl $n$ einschränken.

**DEFINITION 1.5: BEDECKUNGSRELATION**

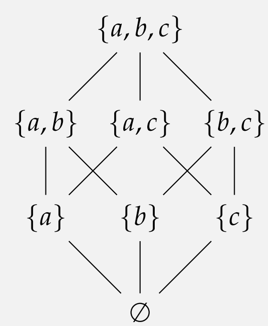
Sei $(P, \leq)$ eine teilgeordnete Menge. Zwei Elemente $x, y \in P$ bilden eine BEDECKUNGSRELATION, wenn $x \leq y$ und für jedes $z \in P$ mit $x \leq z \leq y$ gilt entweder $x = z$ oder $z = y$. Wir schreiben $x \lessdot y$.

**DEFINITION 1.6: ORDNUNGSDIAGRAMM**

Sei $\mathcal{P} = (P, \leq)$ eine teilgeordnete Menge. Das ORDNUNGSDIAGRAMM von $\mathcal{P}$ ist der gerichtete Graph $(P, \lessdot)$. Hierbei gilt die Konvention, dass die Kanten nach oben orientiert sind, also dass $y$ strikt oberhalb von $x$ gezeichnet wird, wenn $x \lessdot y$.

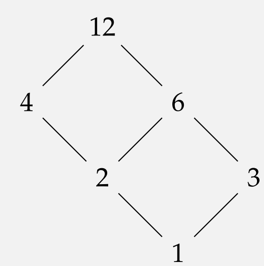
**BEISPIEL 1.7: TEILMENGENVERBAND**

Sei $M = \{a, b, c\}$. Das Ordnungsdiagramm von $\big(\wp(M), \subseteq\big)$ sieht wie folgt aus:




**BEISPIEL 1.8: TEILERVERBAND**

Sei $n = 12$. Das Ordnungsdiagramm von $\big(D(12), |\big)$ sieht wie folgt aus:




**DEFINITION 1.9: DIREKTES PRODUKT**

Seien $\mathcal{P} = (P, \leq_P)$ und $\mathcal{Q} = (Q, \leq_Q)$ zwei teilgeordnete Mengen. Das DIREKTE PRODUKT von $\mathcal{P}$ und $\mathcal{Q}$ ist $\mathcal{P} \times \mathcal{Q} = (P \times Q, \leq)$, wobei für $x, x' \in P$ und $y, y' \in Q$ gilt dass $(x, y) \leq (x', y')$ genau dann, wenn $x \leq_P x'$ und $y \leq_Q y'$.

Für das direkte Produkt von $n$ teilgeordneten Mengen schreiben wir auch $\prod_{i=1}^{n}(P_i, \leq_i)$ anstelle von $(P_1, \leq_1) \times (P_2, \leq_2) \times \cdots \times (P_n, \leq_n)$. Sind alle Faktoren gleich, benutzen wir auch die Potenzschreibweise $(P, \leq)^n$.

**LEMMA 1.10**

Sei $M$ eine endliche Menge mit $n$ Elementen. Weiter sei $\mathbf{2} = \big(\{0,1\}, \leq\big)$ gegeben durch die (nichttriviale) Relation $0 < 1$. Es gilt $\Big(\wp(M), \subseteq\Big) \cong \mathbf{2}^n$.

*Beweis.* Betrachte zu $X \subseteq M = \{m_1, m_2, \dots, m_n\}$ den CHARAKTERISTISCHEN VEKTOR $(a_1, a_2, \dots, a_n)$, der über

$$a_i = \begin{cases} 1, & \text{wenn } m_i \in X, \\ 0, & \text{wenn } m_i \notin X \end{cases}$$

definiert ist. Damit erhalten wir eine Bijektion von $\wp(M)$ nach $\{0,1\}^n$. Seien nun $X, Y \subseteq M$ mit charakteristischen Vektoren $(a_1, a_2, \dots, a_n)$ und $(b_1, b_2, \dots, b_n)$. Es gilt

$$\begin{aligned} X \subseteq Y &\iff \text{für alle } i \in \{1,2,\dots,n\} \text{ gilt } m_i \in X \Rightarrow m_i \in Y \\ &\iff \text{für alle } i \in \{1,2,\dots,n\} \text{ gilt } a_i = 1 \Rightarrow b_i = 1 \\ &\iff \text{für alle } i \in \{1,2,\dots,n\} \text{ gilt } a_i \leq b_i. \end{aligned}$$

$\square$

**BEISPIEL 1.11: TEILMENGENVERBAND**

Sei $M = \{a, b, c\}$. Das Ordnungsdiagramm von $\big(\wp(M), \subseteq\big)$ unter dem Isomorphismus in Lemma 1.10 sieht wie folgt aus:

$$\begin{tikzcd}
& (1,1,1) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
(1,1,0) \arrow[d, dash] \arrow[dr, dash] & (1,0,1) \arrow[dl, dash] \arrow[dr, dash] & (0,1,1) \arrow[dl, dash] \arrow[d, dash] \\
(1,0,0) \arrow[dr, dash] & (0,1,0) \arrow[d, dash] & (0,0,1) \arrow[dl, dash] \\
& (0,0,0) &
\end{tikzcd}$$

**LEMMA 1.12**

Sei $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_{p \in \mathbb{P}} p^{\alpha_p}$. Es gilt

$$\big(D(n), |\big) \cong \prod_{p \in \mathbb{P}} \big(D(p^{\alpha_p}), |\big).$$

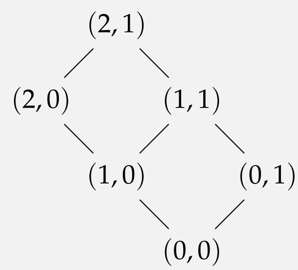
*Beweis.* Offenbar gilt $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ für ein genügend großes $k$. Wir betrachten zu $n$ den PRIMPOTENZVEKTOR $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. Das ist bereits die gewünschte Bijektion. Seien nun $d_1, d_2 \in D(n)$ mit Primpotenzvektoren $(\beta_1, \beta_2, \ldots, \beta_k)$ und $(\gamma_1, \gamma_2, \ldots, \gamma_k)$. Es gilt, dass

$$d_1 \mid d_2 \Longleftrightarrow \text{für alle } i \in \{1, 2, \ldots, k\} \text{ gilt } \beta_i \leq \gamma_i.$$

□

**BEISPIEL 1.13: TEILERVERBAND**

Sei $n = 12 = 2^2 3$. Das Ordnungsdiagramm von $\bigl(D(12), |\bigr)$ unter dem Isomorphismus in Lemma 1.12 sieht dann wie folgt aus:




**DEFINITION 1.14: MAXIMALES ELEMENT, MINIMALES ELEMENT**

Sei $(P, \leq)$ eine teilgeordnete Menge. Ein Element $x \in P$ ist MAXIMAL, wenn für jedes $z \in P$ gilt, dass $z \leq x$.
Dual dazu ist $x$ MINIMAL, wenn es maximal bzgl. der dualen Ordnung ist.

**DEFINITION 1.15: UNTERE SCHRANKE, OBERE SCHRANKE**

Sei $(P, \leq)$ eine teilgeordnete Menge, und seien $x, y \in P$. Ein Element $z \in P$ heißt UNTERE SCHRANKE von $x$ und $y$, wenn $z \leq x$ und $z \leq y$. Weiter heißt $z$ eine MAXIMALE UNTERE SCHRANKE, wenn sie ein maximales Element in der Menge aller unteren Schranken ist.
Dual dazu definieren wir OBERE SCHRANKEN und MINIMALE OBERE SCHRANKEN von $x$ und $y$.

**DEFINITION 1.16: VERBAND; ORDNUNGSTHEORETISCH**

Eine teilgeordnete Menge $(P, \leq)$ heißt VERBAND, wenn zu je zwei Elementen $x, y \in P$ eine größte untere Schranke (INFIMUM), und eine kleinste obere Schranke (SUPREMUM) existiert. Wir schreiben $x \wedge y$ für das Infimum von $x$ und $y$, und $x \vee y$ für das Supremum von $x$ und $y$.

**BEISPIEL 1.17: TEILMENGENVERBAND**

Für jede Menge $M$ ist die teilgeordnete Menge $\bigl(\wp(M), \subseteq\bigr)$ ein Verband. Es gilt $X \wedge Y = X \cap Y$ und $X \vee Y = X \cup Y$.

**BEISPIEL 1.18: TEILERVERBAND**

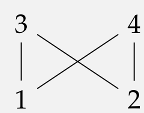
Die teilgeordnete Menge $(\mathbb{N}, |)$ ist ein Verband. Es gilt $a \wedge b = \mathrm{ggT}(a, b)$ und $a \vee b = \mathrm{kgV}(a, b)$.

**BEISPIEL 1.19: FLIEGE**

Sei $F = \{1, 2, 3, 4\}$ und

$$Z = \{(1,1), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (4,4)\}.$$

Die teilgeordnete Menge $(F, Z)$ besitzt das folgende Ordnungsdiagramm.




Offenbar ist $(F, Z)$ kein Verband, da die Menge der unteren Schranken von 3 und 4 zwei maximale Elemente besitzt, nämlich 1 und 2.

**DEFINITION 1.20: VERBAND; ALGEBRAISCH**

Sei $P$ eine Menge, $\wedge$ und $\vee$ zwei binäre Operationen, und 0 und 1 zwei Elemente von $P$. Die Struktur $(P, \wedge, \vee, 0, 1)$ heißt VERBAND, wenn sie die folgenden Eigenschaften erfüllt.

- Für alle $x, y, z \in P$ gilt $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ und $x \vee (y \vee z) = (x \vee y) \vee z$ (ASSOZIATIVITÄT)
- Für alle $x, y \in P$ gilt $x \wedge y = y \wedge x$ und $x \vee y = y \vee x$ (KOMMUTATIVITÄT)
- Für alle $x \in P$ gilt $x \wedge x = x = x \vee x$ (IDEMPOTENZ)
- Für alle $x, y \in P$ gilt $x \wedge (x \vee y) = x = x \vee (x \wedge y)$ (ABSORPTION)
- Für alle $x \in P$ gilt $x \wedge 0 = 0$ und $x \vee 1 = 1$ (EINHEIT)

**SATZ 1.21**

Wenn $P$ endlich ist, sind die ordnungstheoretische und die algebraische Verbandsdefinition äquivalent.

*Beweis.* Sei $(P, \leq)$ ein Verband. Zunächst zeigen wir, dass es ein eindeutig bestimmtes maximales Element 1 in $(P, \leq)$ gibt. Für zwei maximale Elemente $x, y$ von $(P, \leq)$, existiert nach Definition $z = x \vee y$, und es gilt $x \leq z$ und $y \leq z$. Es folgt mit der Maximalität, dass $x = z = y$. Dual folgt die Existenz eines eindeutig bestimmten minimalen Elements. Damit ist die Struktur $(P, \wedge, \vee, 0, 1)$ wohldefiniert. Es bleibt zu zeigen, dass sie die geforderten Eigenschaften besitzt.

Die Assoziativität von Supremum und Infimum lässt sich leicht nachrechnen, Kommutativität und Idempotenz folgen direkt mit der Definition von Supremum und Infimum.

Für $x, y \in P$ gilt offenbar auch, dass aus $x \leq y$ stets $x \wedge y = x$ und $x \vee y = y$ folgt. Damit zeigt man Absorption und Einheit.

Sei nun $(P, \wedge, \vee, 0, 1)$ ein Verband. Wir definieren eine Teilordnung auf $P$ durch $x \leq y$ genau dann wenn $x \wedge y = x$. Die Reflexivität von $\leq$ folgt aus der Idempotenz. Für $x, y \in P$ gilt $x \leq y$ und

$y \leq x$ genau dann wenn $x = x \wedge y$ und $y = y \wedge x$, woraus mit der Kommutativität von $\wedge$ direkt $x = y$ folgt, also gilt die Antisymmetrie. Für $x, y, z \in P$ mit $x \leq y$ und $y \leq z$ folgt nach Definition $x = x \wedge y$ und $y = y \wedge z$, also $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$, und damit $x \leq z$, also gilt die Transitivität.

Das Einheitsaxiom zeigt dass für jedes $x \in P$ die Beziehungen $x \leq 1$ und $0 \leq x$ gilt, es existieren also eindeutig bestimmte minimale und maximale Elemente.

Es bleibt zu zeigen, dass für $x, y \in P$ das Element $x \wedge y$ tatsächlich die größte untere Schranke von $x$ und $y$ ist. (Mit der Dualität folgt dann dass $x \vee y$ die kleinste obere Schranke von $x$ und $y$ ist.) Mit Assoziativität und Idempotenz folgt $x \wedge (x \wedge y) = x \wedge y$, also $x \wedge y \leq x$. Damit ist $x \wedge y$ tatsächlich eine untere Schranke von $x$ und $y$. Sei nun $z$ eine andere untere Schranke von $x$ und $y$, dann gilt $z \wedge (x \wedge y) = (z \wedge x) \wedge y = z \wedge y = z$, also $z \leq x \wedge y$. □

Die Korrespondenz in Satz 1.21 lässt sich auf unendliche Grundmengen erweitern, wenn man den ordnungstheoretischen Verbandsbegriff auf den des VOLLSTÄNDIGEN VERBANDS erweitert, indem man fordert, dass Infima und Suprema für beliebige Teilmengen der Grundmenge existieren.

## 2. Birkhoffs Darstellungssatz Distributiver Verbände

**Definition 2.1: Distributiver Verband**

Ein Verband $(P, \wedge, \vee, 0, 1)$ ist DISTRIBUTIV, wenn er die folgende Eigenschaft erfüllt.

- Für alle $x, y, z \in P$ gilt $(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$ und $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$ (DISTRIBUTIVITÄT)

**Beispiel 2.2: Teilmengenverband**

Für jede Menge $M$ ist der Verband $(\wp(M), \subseteq)$ distributiv, da dasselbe für den Durchschnitt und die Vereinigung von Mengen gilt.

**Beispiel 2.3: Teilerverband**

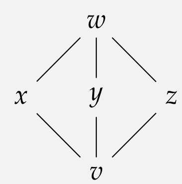
Der Verband $(\mathbb{N}, |)$ ist ebenfalls distributiv, da für zwei Zahlen $a, b \in \mathbb{N}$ mit Primfaktorzerlegung $a = \prod_{p \in \mathbb{P}} p^{\alpha_p}$ und $b = \prod_{p \in \mathbb{P}} p^{\beta_p}$ gilt:

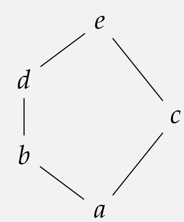
$$\mathrm{ggT}(a, b) = \prod_{p \in \mathbb{P}} p^{\min\{\alpha_p, \beta_p\}} \quad \text{und} \quad \mathrm{kgV}(a, b) = \prod_{p \in \mathbb{P}} p^{\max\{\alpha_p, \beta_p\}},$$

und min und max distributiv sind.

**Beispiel 2.4**

Die kleinsten nicht-distributiven Verbände sind $M_3$ und $N_5$:




Es gilt $(x \wedge y) \vee z = z < w = (x \vee z) \wedge (y \vee z)$, sowie $(b \vee c) \wedge d = d > b = (b \wedge d) \vee (c \wedge d)$.

### DEFINITION 2.5: ORDNUNGSIDEAL, HAUPTIDEAL

Sei $\mathcal{P} = (P, \leq)$ eine teilgeordnete Menge. Eine Teilmenge $X \subseteq P$ heißt ORDNUNGSIDEAL, wenn für alle $x \in X$ und alle $y \leq x$ folgt, dass $y \in X$. Wenn $X$ ein eindeutiges maximales Element besitzt, sprechen wir von einem HAUPTIDEAL.

Jedes Ordnungsideal wird von seinen maximalen Elementen erzeugt. Für ein Ordnungsideal $X$, dessen maximale Elemente die Menge $A$ bilden, schreiben wir auch $A^{\downarrow}$ anstelle von $X$. Falls $A = \{a\}$, schreiben wir kurz $a^{\downarrow}$. Zuletzt sei $\mathcal{I}(\mathcal{P})$ die Menge aller Ordnungsideale von $\mathcal{P}$.

### LEMMA 2.6

Der Durchschnitt und die Vereinigung zweier Ordnungsideale ist wieder ein Ordnungsideal.

*Beweis.* Seien $X$ und $Y$ zwei Ordnungsideale. Wähle $x \in X \cap Y$ und $y \leq x$. Es folgt $x \in X$ und $x \in Y$, und da beide Mengen Ordnungsideale sind, folgt $y \in X$ und $y \in Y$, also $y \in X \cap Y$. Wähle nun $x \in X \cup Y$ und $y \leq x$. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass $x \in X$, und damit $y \in X \subseteq X \cup Y$. □

### DEFINITION 2.7: IDEALVERBAND

Sei $\mathcal{P}$ eine teilgeordnete Menge. Der IDEALVERBAND von $\mathcal{P}$ ist die teilgeordnete Menge $(\mathcal{I}(\mathcal{P}), \subseteq)$.

### LEMMA 2.8

Für jede teilgeordnete Menge $\mathcal{P}$ ist $(\mathcal{I}(\mathcal{P}), \subseteq)$ ein distributiver Verband.

*Beweis.* Das folgt direkt aus der Distributivität des Teilmengenverbands. □

### SATZ 2.9: DARSTELLUNGSSATZ ENDLICHER DISTRIBUTIVER VERBÄNDE [G. BIRKHOFF, 1937]

Ein endlicher Verband $\mathcal{L}$ ist genau dann distributiv, wenn es eine endliche teilgeordnete Menge $\mathcal{P}$ mit $\mathcal{L} \cong (\mathcal{I}(\mathcal{P}), \subseteq)$ gibt.

**LEMMA 2.10**

Sei $\mathcal{P}$ eine endliche teilgeordnete Menge. Für $X \subseteq P$ gilt $X^{\downarrow} = \bigcup_{x \in X} x^{\downarrow}$.

*Beweis.* Sei $y \in X^{\downarrow}$. Nach Definition gibt es ein $\bar{x} \in X$ mit $y \leq \bar{x}$, und damit $y \in \bar{x}^{\downarrow} \subseteq \bigcup_{x \in X} x^{\downarrow}$. Sei umgekehrt $y \in \bigcup_{x \in X} x^{\downarrow}$. Dann gibt es ein $\bar{x} \in X$ mit $y \in \bar{x}^{\downarrow}$, also $y \leq \bar{x}$. Wegen $\bar{x} \in X$, folgt $y \in X^{\downarrow}$. □

Eine Konsequenz von Lemma 2.10 ist, dass die einzigen Ordnungsideale von $\mathcal{P}$, die sich nicht als Vereinigung anderer Ordnungsideale schreiben lassen gerade die Hauptideale sind. Die folgende Definition verallgemeinert diese Idee.

**DEFINITION 2.11: SUPREMUMIRREDUZIBLES ELEMENT**

ei $(L, \leq)$ ein Verband. Ein Element $x \in L \setminus \{0\}$ ist SUPREMUMIRREDUZIBEL wenn für je zwei Elemente $y, z \in L$ mit $x = y \vee z$ folgt, dass $x = y$ oder $x = z$ ist.

Wir bezeichnen die Menge aller supremumirreduziblen Elemente von $\mathcal{L} = (L, \leq)$ mit $\mathcal{J}(\mathcal{L})$.

**KOROLLAR 2.12**

Sei $\mathcal{P} = (P, \leq)$ eine endliche teilgeordnete Menge. Es gilt

$$\mathcal{J}\big(\mathcal{I}(\mathcal{P}), \subseteq\big) = \{x^{\downarrow} \mid x \in P\}.$$

**LEMMA 2.13**

Sei $\mathcal{L} = (L, \leq)$ ein endlicher Verband. Jedes Element $x \in L \setminus \{0\}$ ist das Supremum aller $j \in \mathcal{J}(\mathcal{L})$ mit $j \leq x$.

*Beweis.* Zunächst zeigen wir, dass jedes $x \in L \setminus \{0\}$ als Supremum von supremumirreduziblen Elementen dargestellt werden kann, und wir argumentieren mit Induktion über $f(x) = \left|x^{\downarrow}\right|$. Der Induktionsanfang ist durch Elemente $x \in L$ mit $f(x) = 2$ gegeben (da wir $x = 0$ ausgeschlossen haben). Jedes dieser Elemente bildet eine Bedeckungsrelation mit 0, und ist daher offenbar supremumirreduzibel. Nun sei $x \in L \setminus \{0\}$ beliebig, und wir setzen voraus, dass die Behauptung für alle $x' \in L \setminus \{0\}$ mit $f(x') < f(x)$ gilt. Entweder ist $x$ selbst supremumirreduzibel, dann ist nichts zu zeigen, oder $x = y \vee z$ mit $y < x$ und $z < x$. Insbesondere ist $f(y) < f(x)$ und $f(z) < f(x)$, also gilt die Behauptung nach Induktionsvoraussetzung für $y$ und $z$, und damit auch für $x$.

Sei nun $x \in L \setminus \{0\}$. Nach dem vorigen Absatz wissen wir, dass $x = j_1 \vee j_2 \vee \cdots \vee j_s$ für $j_1, j_2, \ldots, j_s \in \mathcal{J}(\mathcal{L})$. Nach Definition des Supremums folgt $j_i \leq x$ für alle $i \in \{1, 2, \ldots, s\}$. Da aus $y \leq x$ stets $x = x \vee y$ folgt, sind wir fertig. □

Nun definieren wir die folgende Abbildung:

$$\beta : L \to \mathcal{I}\big(\mathcal{J}(\mathcal{L})\big), \quad x \mapsto \{j \in \mathcal{J}(\mathcal{L}) \mid j \leq x\}, \tag{1}$$

und wir behaupten dass diese Abbildung der gewünschte Isomorphismus in Satz 2.9 ist.

**LEMMA 2.14**

Die Abbildung $\beta$ ist wohldefiniert.

*Beweis.* Wir müssen zeigen, dass für $x \in L$ das Bild $\beta(x)$ tatsächlich ein Ordnungsideal ist. Sei dazu $j \in \beta(x)$ und $j' \in \mathcal{J}(\mathcal{L})$ mit $j' \leq j$. Mit der Transitivität folgt $j' \leq x$, also $j' \in \beta(x)$. □

**LEMMA 2.15**

Wenn $\mathcal{L}$ ein endlicher distributiver Verband ist, ist die Abbildung $\beta$ eine Bijektion.

*Beweis.* Zunächst zeigen wir, dass $\beta$ injektiv ist. Seien dazu $x, y \in L$ mit $\beta(x) = \{j_1, j_2, \ldots, j_s\} = \beta(y)$. Nach Lemma 2.13 folgt $x = j_1 \vee j_2 \vee \cdots \vee j_s = y$, wie gewünscht.

Nun zeigen wir, dass $\beta$ surjektiv ist. Sei dazu $X \in \mathcal{I}\big(\mathcal{J}(\mathcal{L})\big)$, und schreibe $X = \{j_1, j_2, \ldots, j_s\}$. Sei $y = j_1 \vee j_2 \vee \cdots \vee j_s$. Sei weiter $x \in \mathcal{J}(\mathcal{L})$ mit $x \leq y$. Es gilt

$$x = x \wedge (j_1 \vee j_2 \vee \cdots \vee j_s) = (x \wedge j_1) \vee (x \wedge j_2) \vee \cdots (x \wedge j_s),$$

da $\mathcal{L}$ distributiv ist. Da $x$ supremumirreduzibel ist, folgt $x = x \wedge j_i$ für irgendein $i \in \{1, 2, \ldots, s\}$, also insbesondere $x \leq j_i$. Da $X$ ein Ordnungsideal ist, folgt $x \in X$. Also ist $X = \beta(y)$ nach Lemma 2.13. □

**LEMMA 2.16**

Wenn $\mathcal{L}$ ein endlicher distributiver Verband ist, ist die Abbildung $\beta$ ein Verbandsisomorphismus von $\mathcal{L} = (L, \leq)$ nach $\Big(\mathcal{I}\big(\mathcal{J}(\mathcal{L})\big), \subseteq\Big)$.

*Beweis.* Lemma 2.15 sagt bereits aus, dass $\beta$ in dem Fall eine Bijektion ist. Es bleibt zu zeigen, dass $\beta$ die Verbandsoperationen bewahrt, also dass (i) $\beta(x \wedge y) = \beta(x) \cap \beta(y)$ und (ii) $\beta(x \vee y) = \beta(x) \cup \beta(y)$ für alle $x, y \in L$.

(i) Sei $j \in \mathcal{J}(\mathcal{L})$ mit $j \leq x \wedge y$. Das ist offenbar äquivalent dazu, dass $j \leq x$ und $j \leq y$. Also gilt $\beta(x \wedge y) = \beta(x) \cap \beta(y)$.

(ii) Sei $j \in \mathcal{J}(\mathcal{L})$ mit $j \in \beta(x) \cup \beta(y)$. Dann gilt $j \in \beta(x)$ oder $j \in \beta(y)$, und damit $j \leq x$ oder $j \leq y$, also auf jeden Fall $j \leq x \vee y$. Es folgt $j \in \beta(x \vee y)$. Sei umgekehrt $j \in \beta(x \vee y)$, also $j \leq x \vee y$. Das ist äquivalent zu $j \wedge (x \vee y) = (j \wedge x) \vee (j \wedge y)$, da $\mathcal{L}$ distributiv ist. Da $j$ supremumirreduzibel ist, folgt $j = j \wedge x$ oder $j = j \wedge y$, also $j \leq x$ oder $j \leq y$. Wir erhalten $j \in \beta(x) \cup \beta(y)$. □

*Beweis von Satz 2.9.* Lemma 2.8 zeigt, dass für jede endliche teilgeordnete Menge $\mathcal{P}$ der Verband $(\mathcal{I}(\mathcal{P}), \subseteq)$ stets distributiv ist.

Sei nun $\mathcal{L}$ ein endlicher distributiver Verband, und wähle $\mathcal{P} = \big(\mathcal{J}(\mathcal{L}), \leq\big)$. Lemma 2.16 besagt, dass $\mathcal{L}$ isomorph zu $\big(\mathcal{I}(\mathcal{P}), \subseteq\big)$ ist. □

**BEISPIEL 2.17: TEILMENGENVERBAND**

Sei erneut $M = \{a, b, c\}$. Die supremumirreduziblen Elemente von $\big(\wp(M), \subseteq\big)$ sind $\{a\}, \{b\}$ und $\{c\}$, und diese sind paarweise unvergleichbar. Also ist jede Teilmenge von $M$ ein Ordnungsideal.
(Die supremumirreduziblen Elemente von $M_3$ bilden eine isomorphe Teilordnung.)

BEISPIEL 2.18: TEILERVERBAND

Die supremumirreduziblen Elemente von $\big(D(12),|\big)$ sind 2, 3, und 4 (gerade die möglichen Potenzen der Primteiler von $n$). Die Ordnungsideale entsprechen gerade den partiellen Produkten aller möglichen Potenzen der Primteiler von $n$.
(Die supremumirreduziblen Elemente von $N_5$ bilden eine isomorphe Teilordnung.)

## 3. DER SATZ VON DILWORTH

DEFINITION 3.1: KETTE, ANTIKETTE

Eine teilgeordnete Menge $(P,\leq)$ heißt ANTIKETTE, wenn für $x,y\in P$ aus $x\leq y$ stets $x=y$ folgt. Wir nennen in dem Fall $|P|$ ihre WEITE.
Es heißt $(P,\leq)$ KETTE, wenn für alle $x,y\in P$ stets $x\leq y$ oder $y\leq x$ gilt. Wir nennen in dem Fall $|P|-1$ ihre LÄNGE.

BEISPIEL 3.2: TEILMENGENVERBAND

Die supremumirreduziblen Elemente von $\big(\wp(M),\subseteq\big)$ bilden eine Antikette der Weite $|M|$.

BEISPIEL 3.3: TEILERVERBAND

Die supremumirreduziblen Elemente von $\big(D(n),|\big)$ bilden eine disjunkte Vereinigung von Ketten, gegeben durch die Primteiler von $n$. Die Längen dieser Ketten sind durch die Exponenten der Primteiler in der Primfaktorzerlegung von $n$ bestimmt.

DEFINITION 3.4: ZERLEGUNG

Eine ZERLEGUNG von $(P,\leq)$ ist eine Mengenpartition $P=D_1\uplus D_2\uplus\cdots\uplus D_s$, wobei für $i\in\{1,2,\ldots,s\}$ und $x,y\in D_i$ gilt, wenn $x\lessdot y$ in $(D_i,\leq)$, dann $x\lessdot y$ in $(P,\leq)$.

LEMMA 3.5: W

nn $\mathcal{P}$ eine Kette der Länge $s$ enthält, dann existiert keine Zerlegung von $\mathcal{P}$ in weniger als $s+1$ Antiketten.
Wenn $\mathcal{P}$ eine Antikette der Weite $s$ enthält, dann existiert keine Zerlegung von $\mathcal{P}$ in weniger als $s$ Ketten.

*Beweis.* Für eine beliebige Kette $C$ und eine beliebige Antikette $A$ gilt $|A\cap C|\leq 1$, da alle Elemente in diesem Durchschnitt paarweise vergleichbar, und paarweise unvergleichbar sein müssen. Damit folgt die Behauptung. □

SATZ 3.6: [L. MIRSKY, 1971]

Sei $\mathcal{P}=(P,\leq)$ eine endliche teilgeordnete Menge, und sei $s$ die größte Länge einer Kette in $\mathcal{P}$. Dann besitzt $\mathcal{P}$ eine Zerlegung in genau $s+1$ Antiketten.

*Beweis.* Für $x \in P$ definiere die HÖHE von $x$ als

$$h(x) = \begin{cases} 0, & x \text{ ist minimal,} \\ \sup_{m \leq x \text{ minimal}} \{ |C| - 1 \mid C \text{ ist Kette, und } x, m \in C \}, & \text{sonst.} \end{cases}$$

Definiere $A_i = \{x \in P \mid h(x) = i\}$. Nach Voraussetzung ist $A_i = \emptyset$ for $i > s$, und es gilt $P = A_0 \uplus A_1 \uplus \cdots \uplus A_s$. Sei nun $x \in A_i$ und $x < y$. Dann existiert eine Kette $x_0 < x_1 < \cdots < x_i = x < y$, also gilt $h(x) < h(y)$. Es folgt, dass $(A_i, \leq)$ für jedes $i \in \{0, 1, \ldots, s\}$ eine Antikette ist. □

**SATZ 3.7: SATZ VON DILWORTH [R. DILWORTH, 1950]**

Sei $\mathcal{P} = (P, \leq)$ eine endliche teilgeordnete Menge, und sei $s$ die größte Weite einer Antikette in $\mathcal{P}$. Dann besitzt $\mathcal{P}$ eine Zerlegung in genau $s$ Ketten.

*Beweis.* Wir beweisen diesen Satz mittels vollständiger Induktion über die Kardinalität von $P$. Ist $|P| = 1$, dann gilt die Aussage offenbar. Wir nehmen also an, das die Aussage für alle teilgeordneten Mengen der Kardinalität $< |P|$ gilt. Wir fixieren ein minimales Element $x \in P$ und unterscheiden zwei Fälle. Sei $P' = P \setminus \{x\}$.

(i) $x$ ist mit keinem Element in $P'$ vergleichbar. Die größte Weite einer Antikette in $(P', \leq)$ ist demnach $s - 1$, und nach Induktionsvoraussetzung läßt sich $(P', \leq)$ in $s - 1$ Ketten zerlegen. Die Menge $\{x\}$ ist selbst eine Kette, also gilt die Behauptung.

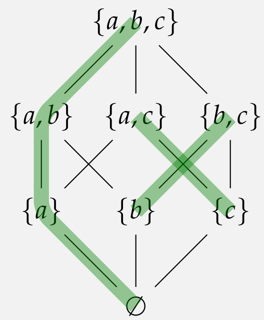
(ii) Es gibt mindestens ein Element in $P'$ das größer als $x$ ist. Sei nun $s'$ die größte Weite einer Antikette in $(P', \leq)$. Offenbar gilt $s' \in \{s, s-1\}$. Wenn $s' = s - 1$, dann verfahren wir analog zu (i). Andernfalls finden wir nach Induktionsvoraussetzung eine Zerlegung von $(P', \leq)$ in $s$ Ketten $C_1, C_2, \ldots, C_s$. Für $i \in \{1, 2, \ldots, s\}$, definiere $T_i = \{x' \in C_i \mid x \leq x'\}$ und $B_i = C_i \setminus T_i$. Die Menge $B = B_1 \cup B_2 \cup \cdots \cup B_s$ enthält alle Elemente von $P'$, die nicht mit $x$ vergleichbar sind. Wir färben die Elemente von $B$ mit $s$ Farben, nämlich erhält $x' \in C_i$ die Farbe $i$.

Sei $r$ die größte Weite einer Antikette in $(B, \leq)$; nach Voraussetzung ist $r < s$. Nach Induktionsvoraussetzung können wir $(B, \leq)$ in $r$ Ketten $C'_1, C'_2, \ldots, C'_r$ zerlegen. Für $i \in \{1, 2, \ldots, r\}$ sei $x'_i$ das maximale Element von $C'_i$. Wenn eine Farbe $i$ mehrfach in $\{x'_1, x'_2, \ldots, x'_r\}$ auftaucht, sagen wir in den Elementen $x'_{i_1}, x'_{i_2}, \ldots, x'_{i_{r'}}$, definiere $U$ als die Menge aller einfarbigen, zusammenhängenden Segmente von $C'_{i_j}$ die $x'_{i_j}$ enthalten. Es gilt $U \subseteq C_i$, also ist $U$ selbst eine Kette. Sei $u$ das minimale Element von $U$, und $j$ der Index sodass $u \in C'_j$. Dann ergänze $C'_j$ um $U$, und entferne die entsprechenden Anteile von $U$ aus den übrigen Ketten in $B$.

Wir erhalten $r$ Ketten $C''_1, C''_2, \ldots, C''_r$ die immernoch eine Zerlegung von $(B, \leq)$ bilden, und deren Anzahl von einfarbigen, zusammenhängenden Segmenten echt kleiner ist als zuvor. Wir können also folgern, dass eine Wiederholung dieses Prozesses irgendwann terminiert. Insbesondere dann, wenn wir eine Zerlegung von $(B, \leq)$ in $r$ Ketten erreicht haben, deren maximale Elemente alle verschiedene Farben haben. Seien $\tilde{C}_1, \tilde{C}_2, \ldots, \tilde{C}_r$ diese Ketten. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass das maximale Element von $\tilde{C}_i$ die Farbe $i$ hat. Für $i \in \{1, 2, \ldots, r\}$, definiere $\tilde{T}_i = \tilde{C}_i \cup T_i$, und definiere $\tilde{T}_{r+1} = \{x\} \cup T_r$ und $\tilde{T}_i = T_i$ für $i \in \{r+2, r+3, \ldots, s\}$. Das ist die gewünschte Zerlegung von $\mathcal{P}$ in $s$ Ketten. □

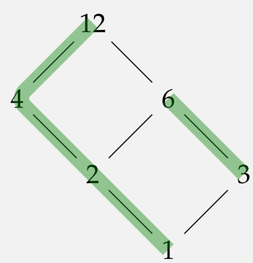
**Beispiel 3.8: Teilmengenverband**

Sei $M = \{a,b,c\}$. Die größte Weite einer Antikette in $\bigl(\wp(M),\subseteq\bigr)$ ist 3, und eine Zerlegung in drei Ketten ist zum Beispiel die folgende.




**Beispiel 3.9: Teilerverband**

Die größte Weite einer Antikette in $\bigl(D(12),|\bigr)$ ist 2, und eine Zerlegung in zwei Ketten ist zum Beispiel die folgende.




## 4. Die Inzidenzalgebra einer teilgeordneten Menge

**Definition 4.1: Lineare Erweiterung**

Sei $(P,\leq)$ eine teilgeordnete Menge. Eine Kette $(P,\prec)$ heißt LINEARE ERWEITERUNG von $(P,\leq)$, wenn für $x,y\in P$ aus $x\leq y$ stets $x\prec y$ folgt.

**Beispiel 4.2: Teilmengenverband**

Sei $M=\{a,b,c\}$. Eine lineare Erweiterung von $\bigl(\wp(M),\leq\bigr)$ ist zum Beispiel

$$\emptyset\prec\{a\}\prec\{b\}\prec\{c\}\prec\{a,b\}\prec\{a,c\}\prec\{b,c\}\prec\{a,b,c\}.$$

**Beispiel 4.3: Teilerverband**

Eine lineare Erweiterung von $\bigl(D(12),|\bigr)$ ist zum Beispiel

$$1\prec 2\prec 3\prec 4\prec 6\prec 12.$$

**DEFINITION 4.4: INTERVALL**

Sei $\mathcal{P} = (P, \leq)$ eine teilgeordnete Menge, und seien $x, y \in P$. Die Menge $[x, y] = \{z \in P \mid x \leq z \leq y\}$ ist das von $x$ und $y$ erzeugte INTERVALL in $\mathcal{P}$.

**DEFINITION 4.5: INZIDENZALGEBRA**

Sei $\mathcal{P} = (P, \leq)$ eine endliche teilgeordnete Menge. Die INZIDENZALGEBRA $\mathcal{A}(\mathcal{P})$ von $\mathcal{P}$ ist die Menge aller Funktionen $f : P \times P \to \mathbb{R}$ mit $f(x, y) = 0$ wenn $x \not\leq y$. Dabei sind Addition und skalare Multiplikation punktweise definiert, und die Multiplikation zweier Funktionen $f, g \in \mathcal{A}(\mathcal{P})$ als Faltung

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

**PROPOSITION 4.6**

Sei $\mathcal{P} = (P, \leq)$ eine endliche teilgeordnete Menge mit $|P| = n$. Dann ist die Inzidenzalgebra $\mathcal{A}(\mathcal{P})$ isomorph zu einer Unteralgebra der Algebra aller oberen Dreiecksmatrizen. Eine Funktion $f \in \mathcal{A}(\mathcal{P})$ ist genau dann invertierbar, wenn $f(x, x) \neq 0$ für alle $x \in P$.

*Beweis.* Sei $\prec$ eine lineare Erweiterung von $\mathcal{P}$, sodass wir $P = \{x_1, x_2, \ldots, x_n\}$ schreiben können mit $i \leq j$ genau dann wenn $x_i \prec x_j$. Wir bilden eine Funktion $f : P \times P \to \mathbb{R}$ auf die $n \times n$-Matrix $A = (a_{i,j})_{1 \leq i,j \leq n}$ ab, wobei $a_{i,j} = f(x_i, x_j)$. Dann ist $A$ eine obere Dreiecksmatrix, und diese Abbildung ist ein Isomorphismus, da für zwei Funktionen $f, g \in \mathcal{A}(\mathcal{P})$ mit zugehörigen Matrizen $A = (a_{i,j}), B = (b_{i,j})$ gilt, dass

$$(f \cdot g)(x_i, x_j) = \sum_{x_i \prec x_k \prec x_j} f(x_i, x_k) g(x_k, x_j) = \sum_{i \leq k \leq j} a_{i,k} b_{k,j} = \sum_{1 \leq k \leq n} a_{i,k} b_{k,j}.$$

Insbesondere ist $(f \cdot g)(x_i, x_j) = 0$, wenn $x_i \not\leq x_j$, also $f \cdot g \in \mathcal{A}(\mathcal{P})$.

Nun sei $f \in \mathcal{A}(\mathcal{P})$ so, dass $f(x, x) \neq 0$ für alle $x \in P$. Es folgt, dass die zugehörige Matrix $A$ invertierbar ist. Wir definieren nun eine Funktion $g \in \mathcal{A}(\mathcal{P})$ mit $(f \cdot g)(x, x) = 1$ und $(f \cdot g)(x, y) = 0$ für $x \neq y$. Die Eindeutigkeit der Inversen zeigt dann, dass $g = f^{-1}$. Sei dazu

$$g(x, y) = \begin{cases} 0, & \text{wenn } x \not\leq y, \\ f(x, x)^{-1}, & \text{wenn } x = y, \\ -f(x, x)^{-1} \left( \sum_{x < z \leq y} f(x, z) g(z, y) \right), & \text{wenn } x < y. \end{cases} \tag{2}$$

Das ist wohldefiniert, da im Fall $x < y$ für jedes $x < z \leq y$ die Werte für $g(z, y)$ induktiv berechnet werden können. Es gilt dann offenbar $(f \cdot g)(x, x) = 1$ und $(f \cdot g)(x, y) = 0$ falls $x \not\leq y$. Nun sei $x < y$. Dann gilt

$$\begin{aligned} (f \cdot g)(x, y) &= \sum_{x \leq z \leq y} f(x, z) g(z, y) \\ &= f(x, x) g(x, y) + \sum_{x < z \leq y} f(x, z) g(z, y) \end{aligned}$$

$$
\begin{aligned}
&= f(x,x)\big(-f(x,x)^{-1}\big)\left(\sum_{x<z\leq y} f(x,z)g(z,y)\right) + \sum_{x<z\leq y} f(x,z)g(z,y)\\
&= -\left(\sum_{x<z\leq y} f(x,z)g(z,y)\right) + \sum_{x<z\leq y} f(x,z)g(z,y)\\
&= 0.
\end{aligned}
$$

Also ist $g$ tatsächlich invers zu $f$. □

Wir interessieren uns besonders für drei Funktionen in $\mathcal{A}(\mathcal{P})$.

- Die Deltafunktion $\delta(x,y) = \begin{cases} 1, & \text{wenn } x = y,\\ 0, & \text{sonst.}\end{cases}$
- Die Zetafunktion $\zeta(x,y) = \begin{cases} 1, & \text{wenn } x \leq y,\\ 0, & \text{sonst.}\end{cases}$
- Die Möbiusfunktion $\mu(x,y) = \begin{cases} 1, & \text{wenn } x = y,\\ -\sum_{x<z\leq y}\mu(z,y), & \text{wenn } x < y,\\ 0, & \text{sonst.}\end{cases}$

Die Definition der Möbiusfunktion ist äquivalent zu der Darstellung

$$
\sum_{x\leq z\leq y} \mu(x,y) = \begin{cases} 1, & \text{wenn } x = y,\\ 0, & \text{sonst.}\end{cases} \tag{3}
$$

**Lemma 4.7**

Sei $\mathcal{P}$ eine endliche teilgeordnete Menge. Es gilt $\mu\cdot\zeta = \delta$. Mit anderen Worten, $\mu$ und $\zeta$ sind zueinander invers in $\mathcal{A}(\mathcal{P})$.

*Beweis.* $\zeta$ ist nach Proposition 4.6 offenbar invertierbar, und es gilt $\zeta^{-1}(x,y) = 0$, wenn $x \not\leq y$, und $\zeta^{-1}(x,x) = 1$ für alle $x \in P$. Nun sei $x < y$. Wir erhalten

$$
\begin{aligned}
\zeta^{-1}(x,y) &= -\zeta(x,x)^{-1}\left(\sum_{x<z\leq y}\zeta(x,z)\zeta^{-1}(z,y)\right)\\
&= -\sum_{x<z\leq y}\zeta^{-1}(z,y).
\end{aligned}
$$

Damit erfüllt $\zeta^{-1}$ genau die Definition von $\mu$, und aus der Eindeutigkeit von $\mu$ folgt $\zeta^{-1} = \mu$. □

**Lemma 4.8**

Sei $(P,\leq)$ eine endliche teilgeordnete Menge. Es gilt $\mu : P\times P \to \mathbb{Z}$.

*Beweis.* Das folgt direkt aus der Definition. Für alle $x \in P$ ist $\mu(x,x)$ ganzzahlig (nämlich genau 1), und für $x < y$ ist $\mu(x,y)$ induktiv als Summe über Teilintervalle definiert. □

LEMMA 4.9

Sei $(P, \leq)$ eine Kette endlicher Länge. Dann gilt $\mu(x,y) = \begin{cases} 1, & \text{wenn } x = y, \\ -1, & \text{wenn } x \lessdot y, \\ 0, & \text{sonst.} \end{cases}$

*Beweis.* Sei zunächst $x \lessdot y$. Nach Definition der Möbiusfunktion folgt dann $\mu(x,y) = -\mu(y,y) = -1$. (Dies gilt in jeder teilgeordneten Menge.) Seien nun $x < y$ so, dass sie eine Kette der Länge $k \geq 2$ bilden. Wir zeigen $\mu(x,y) = 0$ mittels Induktion über $k$. Wenn $k = 2$, dann ist $x \lessdot z \lessdot y$, und es gilt $\mu(x,y) = -\mu(z,y) - \mu(y,y) = 1 - 1 = 0$ wie gewünscht. Für $k$ beliebig folgt $\mu(x,y) = -\sum_{x<z\leq y} \mu(z,y)$. Sei $z'$ das eindeutige Element mit $x \leq z' \lessdot y$. Es ergibt sich nach Induktionsvoraussetzung, dass $\mu(z,y) = 0$ für alle $x \leq z < z'$. Damit ist $\mu(x,y) = -\mu(z',y) - \mu(y,y) = 1 - 1 = 0$. $\square$

LEMMA 4.10

Seien $\mathcal{P} = (P, \leq_P)$ und $\mathcal{Q} = (Q, \leq_Q)$ zwei endliche teilgeordnete Mengen, und seien $\mu_{\mathcal{P}}$ und $\mu_{\mathcal{Q}}$ die entsprechenden Möbiusfunktionen. Es gilt $\mu_{\mathcal{P}\times\mathcal{Q}}\big((x,x'),(y,y')\big) = \mu_{\mathcal{P}}(x,y)\mu_{\mathcal{Q}}(x',y')$.

*Beweis.* Nach (3) und der Definition des direkten Produkts gilt

$$\left(\sum_{x\leq_P z\leq_P y} \mu_{\mathcal{P}}(x,y)\right)\left(\sum_{x'\leq_Q z'\leq_Q y'} \mu_{\mathcal{Q}}(x',y')\right) = \sum_{(x,x')\leq(z,z')\leq(y,y')} \mu_{\mathcal{P}}(x,y)\mu_{\mathcal{Q}}(x',y').$$

Diese Identität nimmt genau dann den Wert 1 an, wenn $x = y$ und $x' = y'$, und ist andernfalls 0. Damit erfüllt die Funktion $f : (P \times Q) \times (P \times Q)$ gegeben durch $f\big((x,x'),(y,y')\big) = \mu_{\mathcal{P}}(x,y)\mu_{\mathcal{Q}}(x',y')$, die Gleichung (3). Da die Möbiusfunktion eindeutig ist, muss also $f = \mu_{\mathcal{P}\times\mathcal{Q}}$ gelten. $\square$

LEMMA 4.11

Die Möbiusfunktion in $\big(\wp(M), \subseteq\big)$ ist gegeben durch

$$\mu(X,Y) = \begin{cases} (-1)^{|Y|-|X|}, & \text{wenn } X \subseteq Y, \\ 0, & \text{sonst.} \end{cases}$$

*Beweis.* Das Intervall $[X,Y]$ ist offenbar isomorph zu $\big(\wp(Y \setminus X), \subseteq\big)$. Nach Lemma 1.10 ist es also isomorph zu $\mathbf{2}^{|Y|-|X|}$. Mit Lemmas 4.9 und 4.10 folgt dann $\mu(X,Y) = (-1)^{|Y|-|X|}$ wie gewünscht. $\square$

**Beispiel 4.12: Teilmengenverband**

Sei $M = \{1,2,3\}$. Die Matrix zu $\mu$ in $\mathcal{A}\big(\wp(M),\subseteq\big)$ (bzgl. der linearen Erweiterung aus Beispiel 4.2) ist die folgende.

$$\begin{pmatrix} 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1\\ 0 & 1 & 0 & 0 & -1 & -1 & 0 & 1\\ 0 & 0 & 1 & 0 & -1 & 0 & -1 & 1\\ 0 & 0 & 0 & 1 & 0 & -1 & -1 & 1\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

**Lemma 4.13**

Die Möbiusfunktion in $\big(D(n),|\big)$ ist gegeben durch

$$\mu(a,b) = \begin{cases} (-1)^d, & \text{wenn } b/a \text{ das Produkt von } d \text{ verschiedenen Primzahlen ist,}\\ 0, & \text{sonst.} \end{cases}$$

*Beweis.* Das Intervall $[a,b]$ ist offenbar isomorph zu $\big(D(b/a),|\big)$. Wenn $b/a$ genau $k$ Primteiler hat, ist dieses Intervall nach Lemma 1.12 isomorph zum direkten Produkt von $k$ Ketten, deren Länge durch den Exponenten des entsprechenden Primteilers ist. Die Möbiusfunktion einer Kette ist nach Lemma 4.9 nur dann verschieden von Null, wenn die Kette höchstens Länge 1 hat, also wenn der entsprechende Primfaktor höchstens einmal vorkommt. Mit Lemma 4.10 folgt die Behauptung. □

**Beispiel 4.14: Teilerverband**

Die Matrix zu $\mu$ in $\mathcal{A}\big(D(12),|\big)$ (bzgl. der linearen Erweiterung aus Beispiel 4.3) ist die folgende.

$$\begin{pmatrix} 1 & -1 & -1 & 0 & 1 & 0\\ 0 & 1 & 0 & -1 & -1 & -1\\ 0 & 0 & 1 & 0 & -1 & 0\\ 0 & 0 & 0 & 1 & 0 & -1\\ 0 & 0 & 0 & 0 & 1 & -1\\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

**Beispiel 4.15: $M_3$**

Die Matrix zu $\mu$ in $\mathcal{A}(M_3)$ ist die folgende.

$$\begin{pmatrix} 1 & -1 & -1 & -1 & 2\\ 0 & 1 & 0 & 0 & -1\\ 0 & 0 & 1 & 0 & -1\\ 0 & 0 & 0 & 1 & -1\\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

**Satz 4.16: Möbiusinversion**

Sei $\mathcal{P}$ eine endliche teilgeordnete Menge und seien $f, g \in \mathcal{A}(\mathcal{P})$. Die folgenden Beziehungen sind dann äquivalent:

(a) $$f(x,y) = \sum_{x \le z \le y} g(x,z);$$

(b) $$g(x,y) = \sum_{x \le z \le y} f(x,z)\mu(z,y).$$

*Beweis.* Nehmen wir zunächst an, dass (a) gilt. Wir erhalten:

$$\begin{aligned}
\sum_{x \le z \le y} f(x,z)\mu(z,y) &= \sum_{x \le z \le y} \left( \sum_{x \le z' \le z} g(x,z') \right) \mu(z,y) \\
&= \sum_{x \le z \le y} \left( \sum_{x \le z' \le y} g(x,z')\zeta(z',z) \right) \mu(z,y) \\
&= \sum_{x \le z' \le y} g(x,z') \left( \sum_{x \le z \le y} \zeta(z',z)\mu(z,y) \right) \\
&= \sum_{x \le z' \le y} g(x,z') \left( \sum_{z' \le z \le y} \zeta(z',z)\mu(z,y) \right) \\
&= \sum_{x \le z' \le y} g(x,z')\delta(z',y) \\
&= g(x,y).
\end{aligned}$$

Gelte nun (b). Wir haben:

$$\begin{aligned}
\sum_{x \le z \le y} g(x,z) &= \sum_{x \le z \le y} \left( \sum_{x \le z' \le z} f(x,z')\mu(z',z) \right) \\
&= \sum_{x \le z \le y} \left( \sum_{x \le z' \le y} f(x,z')\mu(z',z)\zeta(z,y) \right) \\
&= \sum_{x \le z' \le y} f(x,z') \left( \sum_{x \le z \le y} \mu(z',z)\zeta(z,y) \right) \\
&= \sum_{x \le z' \le y} f(x,z')\delta(z',y) \\
&= f(x,y).
\end{aligned}$$

$\square$

**Korollar 4.17: Prinzip von Inklusion und Exklusion**

Sei $\{A_1, A_2, \ldots, A_n\}$ eine Familie von Teilmengen einer endlichen Menge $X$. Die Anzahl der Elemente, die in keiner dieser Mengen liegen ist gerade

$$\sum_{J\subseteq\{1,2,\ldots,n\}} (-1)^{|J|}|A_J|,$$

wobei $A_J = \bigcap_{j\in J} A_j$.

*Beweis.* Wir definieren die folgenden Funktionen

$$f(I) = \Bigl|A_I \setminus \bigcup_{I\subsetneq J} A_J\Bigr| \quad \text{und} \quad g(I) = \bigl|A_I\bigr|.$$

Unter der Voraussetzung, dass $A_\emptyset = X$, suchen wir also den Wert von $f(\emptyset)$. Es gilt

$$\sum_{I\subseteq J} f(J) = \sum_{I\subseteq J}\Bigl|A_J - \bigcup_{J\subsetneq K} A_K\Bigr| = \Bigl|A_I \setminus \bigcup_{I\subsetneq J} A_J\Bigr| + \sum_{I\subsetneq J}\Bigl|A_J \setminus \bigcup_{J\subsetneq K} A_K\Bigr| = \bigl|A_I\bigr| = g(I).$$

Mittels Möbiusinversion im Teilmengenverband $\Bigl(\wp\bigl(\{1,2,\ldots,n\}\bigr),\supseteq\Bigr)$, siehe Satz 4.16 und Lemma 4.11, folgt dann

$$f(I) = \sum_{I\subseteq J}(-1)^{|J\setminus I|}g(J).$$

Setzen wir nun $I = \emptyset$ ein, folgt die Behauptung. □

**Beispiel 4.18**

Für $n = 2$ beschreibt Korollar 4.17 die bekannte Relation

$$\bigl|A_1 \cup A_2\bigr| = \bigl|A_1\bigr| + \bigl|A_2\bigr| - \bigl|A_1 \cap A_2\bigr|,$$

da für die Anzahl aller Elemente, die nicht in $A_1$ oder $A_2$ liegen, gilt:

$$\begin{aligned}\bigl|X\bigr| - \bigl|A_1 \cup A_2\bigr| &= \bigl|X \setminus (A_1 \cup A_2)\bigr|\\ &= (-1)^0\bigl|A_\emptyset\bigr| + (-1)^1\bigl|A_{\{1\}}\bigr| + (-1)^1\bigl|A_{\{2\}}\bigr| + (-1)^2\bigl|A_{\{1,2\}}\bigr|\\ &= \bigl|X\bigr| - \bigl|A_1\bigr| - \bigl|A_2\bigr| + \bigl|A_1 \cap A_2\bigr|.\end{aligned}$$

Sei abschließend $\mu(n) = \begin{cases}(-1)^d, & \text{wenn } n = p_1p_2\cdots p_d,\\ 0, & \text{sonst}\end{cases}$ die klassische zahlentheoretische Möbiusfunktion. (In dieser Definition sollen die vorkommenden $p_i$ allesamt Primzahlen sein.)

**Korollar 4.19: Zahlentheoretische Möbiusinversion**

Für $f,g : \mathbb{N} \to \mathbb{R}$ sind äquivalent.

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

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

*Beweis.* Das folgt aus Satz 4.16 und Lemma 4.13. □