Diskrete Mathematik

Marcus Kracht
Fakultät LiLi
Universität Bielefeld
Postfach 10 01 31
D-33501 Bielefeld
marcus.kracht@uni-bielefeld.de

3. Juli 2017

Dieser Text ist die Grundlage der Vorlesung gleichen Namens an der Universität Bielefeld. Ich danke Herrn Michaelis und Herrn Milne-Plückebaum für die sorgfältige Durchsicht. Kritik und Anregungen sind jederzeit willkommen.

Inhaltsverzeichnis

Teil I

Vektorräume

Kapitel 1

Gruppen

Definition 1.1 (Gruppe) *Eine **Gruppe** ist ein Quadrupel $\langle G, \cdot, ^{-1}, 1\rangle$, wo G eine Menge und $1 \in G$, das sogenannte **neutrale Element** ist, $^{-1} : G \to G$ eine Funktion, die jedem Element $x \in G$ sein sogenanntes **inverses Element** zuordnet, und $\cdot : G^2 \to G$ eine zweistellige Funktion, die **Verknüpfung**, derart, dass für alle $x, y, z \in G$ gilt*

1. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. $x \cdot (x^{-1}) = (x^{-1}) \cdot x = 1$
3. $x \cdot 1 = 1 \cdot x = x$

*Ist zusätzlich $x \cdot y = y \cdot x$, so heißt die Gruppe **kommutativ** oder **abelsch**. Die Anzahl der Elemente von G heißt die **Ordnung** der Gruppe.*

Im Normalfall lassen wir den Multiplikationspunkt einfach weg und schreiben xy anstelle von $x \cdot y$. Das Assoziativgesetz sieht dann einfach so aus: $x(yz) = (xy)z$. Auch hier lassen wir Klammern in einem Produkt meistens völlig weg, da das Assoziativgesetz dies erlaubt. Dies lässt sich im Übrigen zeigen, was ich jedoch nicht tue, weil die Notation einigermaßen verwirrend sein würde.

Stattdessen gebe ich eine Reihe von Beispielen an.

1. $\langle \mathbb{R} - \{0\}, \cdot, ^{-1}, 1\rangle$
2. $\langle \mathbb{R}, +, -, 0\rangle$
3. $\langle \mathbb{Q} - \{0\}, \cdot, ^{-1}, 1\rangle$

4. $\langle \mathbb{Q}, +, -, 0 \rangle$

5. $\langle \mathbb{Z}, +, -, 0 \rangle$

Dies sind Beispiele von kommutativen Gruppen. Alle diese sind unendlich. Man unterscheide sorgfältig zwischen dem Symbol '$\cdot$' als abstraktem Symbol für die Gruppenoperation und dem Multiplikationspunkt für die reellen bzw. die rationalen Zahlen. Der Unterschied wir in dem Moment augenfällig, wo wir als grundlegende Operation nicht die Multiplikation sondern die Addition wählen. Man beachte auch, dass wir im Falle der Multiplikation die Null herausnehmen müssen. Zwar kann man in den reellen Zahlen mit 0 multiplizieren, aber man kann kein inverses Element finden. Denn das wäre ja eine Zahl k mit $0 \cdot k = 1$. Da $0 \cdot k = 0$, wäre dann $0 = 1$. Das ist aber ein Widerspruch.

Endliche Beispiele gibt es ebenfalls. Es sei $m > 0$ eine natürliche Zahl. Für ganze Zahlen x und y schreiben wir $x \equiv y \pmod{m}$, falls x und y denselben Rest modulo m lassen, das heißt, falls es ganze Zahlen k, k' und p gibt mit $x = km + p$ und $y = k'm + p$. Es ist zum Beispiel $6 \equiv 13 \pmod{7}$, $16 \equiv -1 \pmod{17}$, und so weiter. Dies sei zunächst einmal genau erklärt.

Proposition 1.2 (Modulus, Rest) *Es sei m eine natürliche Zahl > 0 (der sogenannte **Modulus**). Zu jeder ganzen Zahl n existieren dann eindeutig bestimmte ganze Zahlen k und r, sodass $r \in \{0, 1, 2, \cdots, m-1\}$ und $n = km + r$. r wird der **Rest** von n modulo m genannt.*

Beweis. Zunächst zeige ich die Existenz dieser Zahlen. Es sei k^* die größte ganze Zahl derart, das $k^*m \leq n$. (Diese existiert und ist eindeutig.) Dann sei $r^* := n - k^*m$. Zu zeigen ist, dass $0 \leq r^* < m$. Das erste ist klar: da $k^*m \leq n$, ist $r^* \geq 0$. Zweitens ist $r^* < m$. Denn falls nicht, setze $r := r^* - m$, $k := k^* + 1$. Dann ist $r \geq 0$, und es ist $km + r = (k^* + 1)m + (r^* - m) = k^*m + m - m + r^* = n$. Also ist $km \leq n$, im Widerspruch dazu, dass k^* maximal war mit $k^*m \leq n$. Nun zeige ich noch die Eindeutigkeit. Sind k und r zwei Zahlen mit $n = km + r$ und $0 \leq r < m$, so ist $0 = n - n = (km + r) - (k^*m + r^*) = (k - k^*)m + (r - r^*)$. Ist $k \neq k^*$, so ist $|(k - k^*)m| \geq m$. Aber $|r - r^*| < m$, ein Widerspruch. Also $k = k^*$. Dann ist aber auch $r = r^*$. ⊣

Man überlege sich, dass $m = 1$ zwar möglich ist (aber wenig sinvoll); dass negative Zahlen für m ebenfalls möglich sind aber wenig Neues bringen, wohingegen $m = 0$ keinen analogen Satz für Division mit Rest zulässt.

Wir schreiben nun $n \equiv n' \pmod{m}$, falls n und n' denselben Rest modulo m haben.

Wir können dann auch sagen, der Rest von n modulo m ist diejenige Zahl $r \in \{0, 1, \cdots, m-1\}$, für die gilt $n \equiv r \pmod{m}$.

Lemma 1.3 *Genau dann ist $n \equiv n' \pmod{m}$, wenn $n - n'$ durch m teilbar ist.*

Beweis. Es sei $n \equiv n' \pmod{m}$. Dann existieren Zahlen k, r und k' mit $r \in \{0, 1, \cdots, m-1\}$ und $n = km+r$, $n' = k'm+r$. Dann ist $n-n' = (km+r)-(k'm+r) = km - k'm + r - r = (k - k')m$, also ist diese Zahl durch m teilbar. Sei umgekehrt $n - n'$ durch m teilbar, also $n - n' = cm$ für ein c. Ist dann $n = km + r$, so ist $n' = n' + n - n = n - (n - n') = (km + r) - cm = (k - c)m + r$, also $n' \equiv n \pmod{m}$. ⊣

Das Rechnen mit Zahlen modulo m geschieht wie folgt.

Proposition 1.4 *Für die Reste modulo m gelten folgende Rechenregeln.*

1. *Ist $k \equiv k' \pmod{m}$, so ist $-k \equiv -k' \pmod{m}$.*

2. *Ist $k \equiv k' \pmod{m}$ und $\ell \equiv \ell' \pmod{m}$, so $k + \ell \equiv k' + \ell' \pmod{m}$.*

3. *Ist $k \equiv k' \pmod{m}$ und $\ell \equiv \ell' \pmod{m}$, so $k\ell \equiv k'\ell' \pmod{m}$.*

Beweis. Zu 1. Nach Annahme ist $k \equiv k' \pmod{m}$. Also ist $k - k'$ durch m teilbar. Dann ist auch $-k + k' = (-k) - (-k')$ durch m teilbar, also $-k \equiv -k' \pmod{m}$. Zu 2. Nach Annahme (und dem vorigen Lemma) sind sowohl $k - k'$ als auch $\ell - \ell'$ durch m teilbar. Dann ist auch deren Summe durch m teilbar: $(k + k') + (\ell - \ell') = (k + \ell) - (k' + \ell')$. Daher ist $k + \ell \equiv k' + \ell' \pmod{m}$. Zu 3. Nach Annahme ist $k - k'$ und $\ell - \ell'$ durch m teilbar. Nun ist $k\ell - k'\ell' = k\ell - k'\ell + k'\ell - k'\ell' = (k+k')\ell + k'(\ell - \ell')$ ebenfalls durch m teilbar, und deswegen $k\ell \equiv k'\ell' \pmod{m}$. ⊣

Dies besagt intuitiv gesprochen, dass sich die Reste so verhalten wie die Zahlen selbst. Der Rest von $n + n'$ modulo m ist nichts anderes als der Rest von n modulo m plus den Rest von n' modulo m. Jedoch ist dies nicht ganz richtig, weil die Addition zweier Reste eine Zahl größer als m ergeben kann. Exakt wäre es zu sagen, dass das Ergebnis der Rest der Summe der Reste ist. $\mathbb{Z}_m := \{0, 1, \cdots, m-1\}$ sind die sogenannten **Reste modulo** m. Dann definieren wir:

1. $-_m n$ ist der Rest von $-n$ modulo m.

2. $n +_m n'$ ist der Rest $n + n'$ modulo m.

Es gilt dann

Lemma 1.5 *Es sei* $n \equiv r \pmod m$ *und* $n' \equiv r' \pmod m$ *mit* $r \in \{0, 1, \cdots, m-1\}$. *Dann gilt*

- $-n \equiv -r \equiv -_m r \pmod m$
- $n + n' \equiv r + r' \equiv r +_m r' \pmod m$

Man kann sogar genauer die Operationen bestimmen. Es ist im Allgemeinen $-_m r = m - r$ und

$$r +_m r' = \begin{cases} r + r' & \text{falls } r + r' < m \\ r + r' - m & \text{sonst} \end{cases}$$

Der Beweis ist recht einfach und wird hier ausgelassen.

Hier ein konkretes Beispiel. Wir wählen $m = 4$. Dann gibt es vier Reste, nämliche 0, 1, 2 und 3. Diese addieren sich wie folgt.

(1.1)

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Es ist zum Beispiel $3 + 3 = 6$. Da nun $6 \equiv 2 \pmod 4$, so ist $3 +_4 3 = 2$. Ebenso kann man die Inversen bestimmen.

(1.2)

	$-_4$
0	0
1	3
2	2
3	1

Proposition 1.6 $\mathbb{Z}_m^+ := \langle \mathbb{Z}_m, +_m, -_m, 0 \rangle$ *ist eine abelsche Gruppe.*

Beweis. Zu zeigen ist $x +_m (y +_m z) = (x +_m y) +_m z$. Zunächst einmal beachte man, dass $x + y \equiv x +_m y \pmod m$. Daraus folgt dann, dass $x +_m (y +_m z) \equiv x + (y + z) \equiv (x + y) + z \equiv (x +_m y) +_m z \pmod m$. Ebenso zeigt man die anderen Gesetze. ⊣

Wie steht es nun mit der Multiplikation von Resten? Man würde vermuten, dass man wie bei den ganzen Zahlen auch die Menge $\mathbb{Z}_m - \{0\}$, mit der Multiplikation versehen, zu einer Gruppe machen kann. Das scheitert jedoch schon bei der Multiplikation. Nehmen wir $\mathbb{Z}_6$. Es gilt $2 \cdot 3 \equiv 0 \pmod 6$, also ist das Produkt von

2 und 3 nicht definiert. Ein Inverses können die beiden auch nicht haben. Denn wäre $2k \equiv 1 \pmod 6$, so wäre (nach Multiplikation mit 3) $6k \equiv 3 \pmod 6$, was nicht richtig ist, da ja $6k \equiv 0 \cdot k \equiv 0 \pmod 6$. Ganz allgemein kann man zeigen, dass in $\mathbb{Z}_m$ eine Zahl k nur dann ein multiplikatives Inverses besitzt, wenn sie zu m teilerfremd ist. Als Spezialfall interessiert uns hier der Fall, wo m eine Primzahl ist. Dann ist nämlich jede Zahl zu m teilerfremd, die nicht Vielfaches vom m ist.

Proposition 1.7 *Es sei p eine Primzahl. Dann ist $\mathbb{Z}_p{}^\times := \langle \mathbb{Z}_p - \{0\}, \cdot_p, {}^{-1_p}, 1\rangle$ eine abelsche Gruppe.*

Beweis. Das Nachprüfen der Gesetze ist nicht schwierig und erfolgt wie bei der Addition. Im Wesentlichen haben wir zu zeigen, dass die Funktion ${}^{-1_p}$ tatsächlich existiert. Sei dazu $k \neq 0$ mit $k < p$. Wir betrachten die Menge $\{k, 2 \cdot_p k, 3 \cdot_p k, \cdots, (p-1) \cdot_p k, p \cdot_p k\} \subseteq \{0, 1, \cdots, p-1\}$. Ich behaupte, dass diese genau p Zahlen enthält. Daraus folgt dann, dass sie die 1 enthält. Sei dazu $a \cdot_m k = b \cdot_m k$ für $a \leq b \leq p$, also $(b-a) \cdot_m k = 0$, oder auch $(b-a)k \equiv 0 \pmod m$. Dies bedeutet, dass $(b-a)k$ durch p teilbar ist. Da p kein Teiler von ist k, ist p ein Teiler von $b-a$. Aber $b - a < p$. Da $b - a \geq 0$, so haben wir $b - a = 0$, mithin $a = b$. Das beweist die Behauptung. ⊣

Ich unterscheide also $\mathbb{Z}_m{}^+$, die Gruppe der Zahlen $\{0, 1, \cdots, m-1\}$ mit der Addition als Grundoperation, und die Gruppe $\mathbb{Z}_m{}^\times$ der zu m teilerfremden Zahlen mit der Multiplikation als Grundoperation. Während $\mathbb{Z}_m{}^+$ genau m Elemente enthält, ist die Anzahl der Elemente von $\mathbb{Z}_m{}^\times$ etwas komplizierter zu berechnen. (Es gibt dafür eine Formel auf der Grundlage der Primfaktorzerlegung.)

Ein letztes Beispiel. Es sei M eine beliebige Menge. Dann sei $B(M)$ die Menge aller Bijektionen von M nach M. Wir setzen $(f \circ g)(x) := f(g(x))$. Damit haben wir eine Operation auf $B(M)$, die Verkettung. Ferner sei $i_M : x \mapsto x$ die Identitätsabbildung. Ist $f : M \to M$ bijektiv, so existiert eine (eindeutig bestimmte) Funktion $f^{-1} : M \to M$ mit $f^{-1} \circ f = i_M$, also $(f^{-1} \circ f)(x) = x$ für alle $x \in M$.

Proposition 1.8 $\mathrm{Sym}(M) := \langle B(M), \circ, {}^{-1}, i_M\rangle$ *ist eine Gruppe.*

Beweis. Seien $f, g, h \in B(M)$ Funktionen. Dann ist für jedes $x \in M$: $((f \circ g) \circ h)(x) = (f \circ g)(h(x) = f(g(h(x)))$, sowie $(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))$. Daher ist $(f \circ g) \circ h = f \circ (g \circ h)$. ⊣

Ich erwähne hier, dass $\mathrm{Sym}(M)$ nicht kommutativ ist, falls M mehr als zwei Elemente enthält.

Proposition 1.9 *Für eine Gruppe $\langle G, \cdot, {}^{-1}, 1\rangle$ gelten folgende Aussagen.*

1. *Ist $e \in G$ ein Element derart, dass für alle $x \in G$ gilt $x \cdot e = e \cdot x = x$, so ist $e = 1$. (Eindeutigkeit des neutralen Elements)*
2. *Für alle $x, y, y' \in G$ gilt, ist $x \cdot y = x \cdot y'$, so ist $y = y'$.*
3. *Für alle $x, y, y' \in G$ gilt, ist $y \cdot x = y' \cdot x$, so $y = y'$.*
4. *Für alle $x, z \in G$ gilt, ist $x \cdot z = 1$ oder $z \cdot x = 1$, so ist $z = x^{-1}$. (Eindeutigkeit des inversen Elements.)*
5. *Für alle $x, y \in G$, $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.*
6. *Für alle $x \in G$, $(x^{-1})^{-1} = x$.*

Beweis. (1) Es ist $1 \cdot e = e$ (setze $x := 1$), und $1 \cdot e = 1$ (setze $x = e$). Also ist $e = 1$. (2) $y = 1 \cdot y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot (x \cdot y') = (x^{-1} \cdot x) \cdot y' = 1 \cdot y' = y'$. (3) Analog. (4) Es sei $x \cdot z = 1 = x \cdot z'$. Dann ist wegen (4) $z = z' = x^{-1}$. Ebenso folgt aus $z \cdot x = z' \cdot x$, dass $z = z' = x^{-1}$. (5) $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}(xy)) = y^{-1}((x^{-1}x)y) = y^{-1}(1 \cdot y) = y^{-1}y = 1$. Da Inverse eindeutig sind, gilt die Behauptung. (6) $(x^{-1})^{-1}x^{-1} = 1$, nach Definition. Das bedeutet, dass $(x^{-1})^{-1}$ invers zu x^{-1} ist. Aber ebenso ist $xx^{-1} = 1$, also wegen (3) $(x^{-1})^{-1} = x$. ⊣

Daraus bekommen wir folgendes Ergebnis. Liegt die Operation $\cdot$ fest, so ist das neutrale Element und die Inversenbildung eindeutig. Deswegen gibt man bei Gruppen oft nur die Multiplikationstafel an. Es ist aber keineswegs so, dass jede assoziative Operation auf G zu einer Gruppe ergänzt werden kann. Als Beispiel gebe ich die Menge A^* aller Zeichenketten über A mit der Verkettung. Zwar haben wir ein neutrales Element (das leere Wort ε). Es existiert aber kein Element derart, dass $\mathsf{a} \cdot x = \varepsilon$. Mit anderen Worten: es lässt sich keine Inversenoperation definieren.

Ich komme nun auf einen wichtigen Begriff zu sprechen, den der *Isomorphie*. Isomorphie bedeutet übersetzt „Gleichgestaltigkeit". Für jeden Begriff einer Struktur gibt es einen zugehörigen Isomorphiebegriff. So auch für Gruppen. Ich beginne mit einem Beispiel. Es sei eine Gruppe mit zwei Elementen gegeben, nennen wir sie $\diamond$ und $\spadesuit$. Aufgrund der Postulate muss eines von ihnen das neutrale Element sein. Sagen wir, es sei $\diamond$. Dann haben wir $\diamond \cdot x = x$, $x \cdot \diamond = x$, was immer x ist. Und dann müssen wir auch $\spadesuit \cdot \spadesuit = \diamond$ haben. Denn wäre $\spadesuit \cdot \spadesuit = \spadesuit$, so hätten wir $\spadesuit = \diamond$, da ja auch $\spadesuit \cdot \diamond = \spadesuit$. Insgesamt haben wir jetzt die folgenden Tafeln.

(1.3)

$\cdot$	$\diamond$	$\spadesuit$
$\diamond$	$\diamond$	$\spadesuit$
$\spadesuit$	$\spadesuit$	$\diamond$

	$^{-1}$
$\diamond$	$\diamond$
$\spadesuit$	$\spadesuit$

Sei dies die Gruppe $\mathfrak{C}$. Wir hätten aber auch sagen können, dass ♠ das neutrale Element ist. Dann hätten wir folgende Tafeln bekommen.

(1.4)

$\cdot'$	♢	♠
♢	♠	♢
♠	♢	♠

	$^{-1'}$
♢	♢
♠	♠

Sei dies die Gruppe $\mathfrak{D}$. Auf den ersten Blick sieht $\mathfrak{D}$ anders aus als $\mathfrak{C}$. Wenn wir aber die folgende "Umbenennung" der Elemente vornehmen, ist alles wieder beim Alten: $f : ♢ \mapsto ♠, ♠ \mapsto ♢$. Um es etwas genauer zu machen: wenden wir die Abbildung f nicht nur auf den Grundbereich $A = \{♢, ♠\}$ an (wo sie rein gar nichts bewirkt) sondern auf die Tafel von $\cdot_C$ an (welche ja eine Teilmenge von A^3 ist, in der zum Beispiel das Tripel $\langle ♢, ♠, ♠\rangle$ ist), so bekommen wir die Tafel $\cdot'$. Und wenden wir f auf die Tafel von $^{-1}$ an, so bekommen wir die Tafel $^{-1'}$. Und schließlich bildet f das neutrale Element von $\mathfrak{C}$ auf das von $\mathfrak{D}$ ab. Eine solche Abbildung nennen wir einen Isomorphismus.

Definition 1.10 (Homomorphismus, Isomorphismus) *Es seien $\mathfrak{G} = \langle G, \cdot, ^{-1}, 1\rangle$ und $\mathfrak{H} = \langle H, \cdot', ^{-1'}, 1'\rangle$ Gruppen. Eine Abbildung $f : G \to H$ heißt **Homomorphismus** von $\mathfrak{G}$ nach $\mathfrak{H}$, falls für alle $x, y \in G$ folgendes gilt.*

1. $f(1) = 1'$.
2. $f(x^{-1}) = (f(x))^{-1'}$.
3. $f(x \cdot y) = f(x) \cdot' f(y)$.

*f ist ein **Isomorphismus**, falls f bijektiv ist. f ist ein **Automorphismus**, falls $\mathfrak{G} = \mathfrak{G}$. Wir sagen, $\mathfrak{G}$ sei **isomorph** zu $\mathfrak{H}$, falls es einen Isomorphismus von $\mathfrak{G}$ nach $\mathfrak{H}$ gibt.*

Man kann bereits aus dem vorigen Beispiel sehen, dass $G = H$ sein kann, ohne dass die Abbildung die Identität ist. Dennoch müssen wir zwei Dinge sorgsam unterscheiden. Die Gruppe $\mathfrak{D}$ ist *nicht* die Gruppe $\mathfrak{C}$, auch wenn der Grundbereich derselbe ist. Insofern ist die Abbildung f *kein* Automorphismus sondern nur ein gewöhnlicher Isomorphismus.

Wir beginnen mit einem Beispiel.

Proposition 1.11 *Die Abbildung f, welche jeder ganzen Zahl ihren Rest modulo m zuordnet, ist ein Homomorphismus von $\mathbb{Z}$ auf $\mathbb{Z}_m$.*

Beweis. Zu zeigen ist, dass (a) $f(0) = 0$, dass (b) für alle n gilt $f(-n) = -_m f(n)$, und dass (c) für alle n und n' gilt $f(n + n') = f(n) +_m f(n')$. Dies folgt aber aus den oben gezeigten Sätzen. Nach Lemma 1.5 ist $-n \equiv f(-n) \pmod{m}$. Ferner ist $f(-n) \equiv -n \equiv -_m n \equiv -_m f(n) \pmod{m}$. Ebenso ist ⊣

Es mag deswegen so scheinen, als gäbe es nur triviale Automorphismen. Das ist aber nicht der Fall. Ich gebe ein Beispiel einer Gruppe mit nichttrivialen Automorphismen. Diesmal sei es die Gruppe aller zu der Zahl 8 teilerfremden Reste. Dies sind $\{1, 3, 5, 7\}$. Hier ist die Multiplikationstafel.

(1.5)

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Diese Gruppe heiße $\mathfrak{V}_4$. (Die sogenannte *Kleinsche Vierergruppe*. In unserer Nomenklatur könnte man auch ${\mathbb{Z}_8}^\times$ schreiben.) Diese hat vier Elemente, ist aber *nicht* isomorph zu der additiven Gruppe ${\mathbb{Z}_4}^+$. Dies liegt daran, dass in $\mathfrak{V}_4$ gilt $x \cdot x = 1$, während in $\mathbb{Z}_4$ $1 + 1 = 2 \neq 0$ ist. Die Abbildung $f : 1 \mapsto 1, 3 \mapsto 5, 5 \mapsto 3, 7 \mapsto 7$ ist ein nichttrivialer Automorphismus.

Die Argumentation von vorhin zeigt, dass es eigentlich bis auf Isomorphie nur eine einzige Gruppe mit 2 Elementen geben kann. Denn es muss ja das neutrale Element der ersten Gruppe auf das neutrale Element der zweiten Gruppe abgebildet werden, und dann bleibt für das zweite Element keine Wahl.

Proposition 1.12 *Es seien* $\mathfrak{G} = \langle G, \cdot, {}^{-1}, 1\rangle$ *und* $\mathfrak{H} = \langle H, \cdot', {}^{-1'}, 1'\rangle$ *Gruppen mit zwei Elementen. Dann ist* $\mathfrak{G}$ *isomorph zu* $\mathfrak{H}$.

Und damit wissen wir auch, dass $\mathfrak{C}$ isomorph zu $\langle \mathbb{Z}, +_2, -_2, 0\rangle$ ist: dazu muss $\diamond$ auf 0 und ♠ auf 1 abgebildet werden.

Übungen

Übung 1. Es sei $M = \{a, b, c\}$. Wie viele Elemente hat $\mathrm{Sym}(M)$? Geben Sie die Multiplikations- und Inversentafeln an.

Übung 2. Zeigen, dass es bis Isomorphie genau 2 Gruppen mit 4 Elementen geben kann. *Anleitung.* Außer der 1 gibt es noch drei Elemente. Sei $a \neq 1$ ein weiteres Element. Entweder ist nun $a \cdot a = 1$ oder nicht. Falls nicht, so ist $a \cdot a \cdot a \neq 1$ (probieren Sie es aus), und dann haben wir vier Elemente: $1, a, a^2, a^3$. Unsere Gruppe ist isomorph zu $\mathbb{Z}_4$. Sei also $a \cdot a = 1$. Dann nehmen wir ein neues Element, b. Wiederum kann b^3 nicht 1 sein. Ist $b^2 \neq 1$, dann haben wir im Wesentlichen wieder $\mathbb{Z}_4$, und es ist $a = b^2$. Sei also $b^2 = 1$. Nennen wir das vierte Element c. Wieder ist c^3 nicht 1. Und diesmal muss $c^2 = 1$ sein. Die Gruppentafel steht jetzt fest. Wir haben eine Gruppe isomorph zu ${\mathbb{Z}_8}^\times$.

Übung 3. Nehmen wir einen Rhombus, der kein Quadrat ist. Seien die Ecken im Uhrzeigersinn A, B, C und D genannt. Die Selbstabbildungen sind die folgenden: Drehung um 180 Grad, Spiegelung an den beiden Diagonalen.

1. Geben Sie den Effekt dieser Abbildungen auf die Punktmengen an.
2. Zeigen, Sie, dass die Gruppe der Kongruenzabbildungen isomorph zu ${\mathbb{Z}_8}^\times$ ist.

Kapitel 2

Ringe und Körper

Wir betrachten nun eine Menge K, auf der zwei Operationen definiert sind, und zwar so, dass sie bezüglich beider eine kommutative Gruppe bildet.

Definition 2.1 (Ring, Körper) *Eine Struktur $\mathfrak{R} = \langle R, +, -, 0, \cdot \rangle$ ist ein **Ring**, falls*

1. *$\langle R, +, -, 0 \rangle$ eine abelsche Gruppe ist,*
2. *$\cdot : R^2 \to R$ eine assoziative Operation auf R,*
3. *für alle $x, y, z \in R$: $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ sowie $z \cdot (x + y) = (z \cdot x) + (z \cdot y)$. (Distributivität).*

*$\mathfrak{R}$ heißt Ring mit Eins, falls zusätzlich ein Element $1 \in R$ existiert, sodass $1 \cdot x = x \cdot 1 = x$ ist für alle $x \in R$. Obwohl dies eindeutig bestimmt ist, nehmen wir es in die Signatur auf und schreiben $\mathfrak{R} = \langle R, +, -, 0, \cdot, 1 \rangle$. Ein Ring heißt **kommutativ**, falls die Operation $\cdot$ zusätzlich kommutativ ist. Falls R ein kommutativer Ring mit Eins ist sowie zu jedem $x \neq 0$ ein inverses Element x^{-1} bezüglich $\cdot$ existiert, so heißt $\mathfrak{R}$ ein **Körper**. Auch in diesem Fall wird die Operation $^{-1}$ mit in die Signatur aufgenommen. Mit anderen Worten, ist zusätzlich $\langle R - \{0\}, \cdot, ^{-1}, 1 \rangle$ eine abelsche Gruppe, so ist $\mathfrak{R} = \langle R, +, -, 0, \cdot, ^{-1}, 1 \rangle$ ein Körper.*

Wir reden von $-x$ als dem **additiven Inversen** von x, und von x^{-1} (wenn es existiert) als dem multiplikativen Inversen von x.

Ringe unterscheiden sich von Körpern also dadurch, dass es keine Eins geben muss sowie, dass die es nicht unbedingt ein inverses Element bezüglich der Multiplikation geben muss. Beispiele von Ringen.

1. Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring, aber keinen Körper. Die Zahl 2 besitzt kein multiplikatives Inverses. Es gibt allerdings eine Eins.

2. Die geraden Zahlen $2\mathbb{Z}$ bilden ebenfalls einen Ring, aber es existiert keine Eins.

3. Es sei $\mathbb{Z}_m$ die Menge der Reste modulo m, mit der Addition $+_m$, dem Inversen $-_m$ und der Null 0_m. Wir definieren $x \cdot_m y$ als den Rest von xy modulo m. Die entstehende Struktur ist ein Ring. Es gibt eine Eins, nämlich 1_m, aber es existieren nicht notwendig zu jedem von 0 verschiedenen Element ein inverses Elemente, etwa zu 2_6 in $\mathbb{Z}_6$.

4. Es sei $\mathbb{Z}[\sqrt{2}]$ die Menge der Zahlen der Form $a + b\sqrt{2}$, wo a und b ganze Zahlen sind. Wir addieren wie folgt: $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$. Das additive Inverse zu $a + b\sqrt{2}$ ist $(-a) + (-b)\sqrt{2}$. Die Null ist 0. Wir multiplizieren nun wie folgt: $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}$. Dies ist ein Ring. (Die Kommutativität der Multiplikation ist ziemlich einfach zu zeigen, bei der Assoziativität muss man Geduld mitbringen.)

Rechnen wir $\mathbb{Z}_6$ konkret aus.

(2.1)

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Wir sehen, dass es zwar eine 1 gibt, aber nicht notwendig zu jedem von 0 verschiedenen Element ein multiplikatives Inverses (2,3,4 haben keine Inverse).

Hier einige Beispiele für Körper.

1. $\langle \mathbb{Q}, +, -, 0, \cdot, ^{-1}, 1\rangle$ ist ein Körper.

2. $\langle \mathbb{R}, +, -, 0, \cdot, ^{-1}, 1\rangle$ ist ein Körper.

3. $\langle \mathbb{Z}_p, +, -, 0, \cdot, ^{-1}, 1\rangle$ ist ein Körper, falls p eine Primzahl ist. Dieser Körper wird mit $\mathbb{F}_p$ bezeichnet.

In allen diesen Fällen ist der Nachweis recht einfach. Oben haben wir schon gesehen, dass die Bereiche jeweils abelsche Gruppen sind. Das Distributivgesetz ist wie allgemein bekannt sowohl in den rationalen wie in den reellen Zahlen gültig. Daraus folgt, dass es auch in $\mathbb{Z}_p$ gilt. Das Argument geht so. Seien $x, y, z \in \mathbb{Z}_p$. Dann ist $(x+y)\cdot z \equiv (x+_p y)\cdot_p z \pmod p$ ebenso wie $(x\cdot z)+(y\cdot z) \equiv (x\cdot_p z)+_p(y\cdot_p z) \pmod p$. Aus der Tatsache, dass $(x+y)\cdot z = (x\cdot z)+(y\cdot z)$ folgt dann $(x+_p y)\cdot_p z \equiv (x\cdot_p z)+_p(y\cdot_p z) \pmod p$. Also sind diese Elemente gleich.

Wir schreiben den Multiplikationspunkt nicht. Multiplikation bindet außerdem stärker als Addition. Das Distributivgesetz wird deswegen einfach nur wie folgt notiert: $(x + y)z = xz + yz$. Ebenso gilt $z(x + y) = zx + zy$.

Ein besonderer Vorteil der endlichen Körper ist, dass in ihnen gewisse Polynome Nullstellen besitzen, welche keine reellen Nullstellen haben. Betrachten wir das Polynom $p(x) = x^2 + 2$. Es hat keine reellen Nullstellen. Aber als Polynom über $\mathbb{F}_3$ besitzt es Nullstellen. Dies rechnet man durch Einsetzen nach. Setzen wir 0 für x, so bekommen wir $p(0) = 0^2 + 2 = 0 \cdot 0 + 2 = 2$. Setzen wir 1 für x, so bekommen wir $p(1) = 1^2 + 2 = 1 \cdot 1 + 2 = 0$. Setzen wir schließlich 2 ein, so bekommen wir $p(2) = 2^2 + 2 = 2 \cdot 2 + 2 = 1 + 2 = 0$. Also ist über $\mathbb{F}_3$: $x^2 + 2 = (x + 1)(x + 2)$. Dies kann man wiederum durch Ausmultiplizieren bestätigen: $(x + 1)(x + 2) = x^2 + x + 2x + 2 = x^2 + 2$.

Definition 2.2 (Homomorphismus) *Es seien $\mathfrak{R} = \langle R, +_R, -_R, 0_R, \cdot_R\rangle$ und $\mathfrak{S} = \langle S, +_S, -_S, 0_S, \cdot_S\rangle$ Ringe. Eine Abbildung $h : R \to S$ ist ein (**Ring**) **Homomorphismus** von $\mathfrak{R}$ nach $\mathfrak{S}$, falls für alle $x, y \in R$ gilt:*

1. $h(0_R) := 0_S$
2. $h(-_R x) = -_S h(s)$
3. $h(x +_R y) = h(x) +_S h(y)$
4. $h(x \cdot_R y) = h(x) \cdot_S h(y)$

Mit anderen Worten, ist h ist ein Ringhomorphismus, so ist es ein Homomorphomismus der unterliegenden Gruppe, und h respektiert die Multiplikation. Sind $\mathfrak{F} = \langle F, +_F, -_F, 0_F, \cdot_F, {}^{-1_F}, 1_F\rangle$ und $\mathfrak{G} = \langle G, +_G, -_G, 0_G, \cdot_G, {}^{-1_G}, 1_G\rangle$ Körper, so ist ein Homomorphismus eine Abbildung $h : F \to G$, der ein Homomorphismus der Ringe ist und zusätzlich erfüllt:

5. $h(1_F) = 1_G$;
6. $h(x^{-1_F}) = h(x)^{-1_G}$.

Ein Homomorphismus, der bijektiv ist, heißt ***Isomorphismus****. Sind Definitions- und Wertebereich identisch, so heißt h in diesem Fall* ***Automorphismus****.*

Man kann zeigen, dass Homomorphismen von Körpern im Wesentlichen injektiv sein müssen.

Satz 2.3 *Ist $h : F \to G$ ein Homomorphismus von Körpern, so ist h injektiv.*

Beweis. Es seien x und y Elemente von F mit $h(x) = h(y)$. Dann ist $h(x -_F y) = h(x) -_G h(y) = h(x) -_G h(x) = 0_S$. Setze $z := x -_F y$. Dann ist also $h(z) = 0_G$. Angenommen, $z \neq 0_F$. Dann existiert z^{-1_F} und es ist $h(1_F) = h(z \cdot_F z^{-1_F}) = h(z) \cdot_G h(z^{-1_F}) = 0_G \cdot_G h(z)^{-1G} = 0_G$. Auf der anderen Seite muss $h(1_F) = 1_G \neq 0_G$ sein. Widerspruch. Also ist $z = 0_F$, und die Abbildung ist injektiv. ⊣

Die $\mathbb{F}_p$ sind also endliche Körper. In ihnen kann man im Wesentlichen so rechnen, wie in der rationalen Zahlen. Es sind nicht die einzigen endlichen Körper, aber die einzigen, die wir im Folgenden benötigen werden.

Ich gebe zum Schluss noch ein wichtiges Strukturmerkmal von endlichen Körpern. Zunächst eine Notation. Ist x ein beliebiges Element eines Körpers $\mathfrak{K} = \langle K, +, -, 0, \cdot, ^{-1}, 1\rangle$, so definiere nx, wo n eine natürliche Zahl ist, induktiv wie folgt:

$$\begin{aligned} 0x &:= 0 \\ (n+1)x &:= nx + x \end{aligned} \tag{2.2}$$

Ich mache darauf aufmerksam, dass wir diese Abbildung erweitern können: für eine negative Zahl $-n$ definieren wir $(-n)x := -(nx)$.

Definition 2.4 (Charakteristik) *Es sei $\mathfrak{K} = \langle K, +, -, 0, \cdot^{-1}, 1\rangle$ ein endlicher Körper. Dann existiert eine Zahl m derart, dass für alle $x \in K - \{0\}$ gilt: $mx = 0$, aber $nx \neq 0$ für alle $0 < n < m$. Diese Zahl heißt die* ***Charakteristik*** *des Körpers $\mathfrak{K}$. Diese ist immer eine Primzahl.*

Zunächst müssen wir zeigen, dass diese Zahl existiert. Wir nehmen dazu die Eins 1 und addieren sie auf: 1+1, 1+1+1, und so weiter. Da der Körper endlich ist, sind die Elemente nicht alle verschieden. Und so existiert ein kleinstes m derart, dass $1 + 1 + \cdots + 1 = 0$ (m Summanden). Daraus folgt zuänchst einmal, dass für jedes $x \in K$ gilt $mx = x + x + \cdots + x = x(1 + 1 + \cdots + x) = 0$. Ist umgekehrt $nx = 0$ für $x \neq 0$, so besitzt x ein inverses Element, und wir haben $0 = nx = (nx)x^{-1} = n(xx^{-1}) = n1$, sodass n nicht kleiner als m sein kann. Damit haben wir die Existenz der Charakteristik gezeigt. Die Charakteristik muss eine Primzahl sein, denn falls

$m = ab$, so ist $n1 = a(b1)$, und so existiert ein Element y, nämlich $b1$, für das gilt: $ay = 0$. Daraus folgt, dass $y = 0$ oder $a = m$. Ist aber $y = 0$, so haben wir $b1 = 0$, mit anderen Worten $b = m$. Das zeigt, dass m nur zwei Teiler besitzt: 1 und m. m ist also eine Primzahl.

Wir können nun sogar $(m/n)x$ in einem Körper der Charakteristik p definieren.

Satz 2.5 *Es sei $\mathfrak{K}$ ein Körper der Charakteristik p und n nicht durch p teilbar. Dann existiert zu x ein eindeutiges Element y derart, dass $ny = x$. Dies wird mit $(1/n)x$ bezeichnet. Wir setzen dann $(m/n)x := m((1/n)x)$.*

Beweis. Es sei r der Rest von n modulo p. Da $\mathbb{F}_p$ ein Körper ist, hat r ein multiplikatives Inverses, also ein s mit $rs \equiv 1 \pmod{p}$. Setze $y := sx$. Dann ist $ry = r(sx) = (rs)x = 1x = x$. ⊣

Satz 2.6 *Ist $\mathfrak{K}$ ein Körper der Charakteristik p, so hat $\mathfrak{K}$ p^n Elemente für ein gewisses n.*

Beweis. Im Vorgriff auf das nächste Kapitel können wir den Beweis kurz halten. Der Körper $\mathfrak{K}$, aufgefasst als die additive Gruppe $\langle K, +, -, 0\rangle$, bildet einen Vektorraum über $\mathbb{F}_p$. (Die äußere Multiplikation ist nx wie in (2.2) definiert.) Damit hat er p^n Elemente für ein gewisses n. ⊣

Das ausführliche Argument ist wie folgt: wir wählen ein Element $x \neq 0$ und betrachten $H_x := \{x, 2x, 3x, \cdots\}$. Ist dies noch nicht $= K$, so existiert ein $y \notin H_x$. Wir betrachten alle Elemente der Form $ax + by$, $0 \leq a, b < p$. Davon existieren p^2 viele, und sie sind alle verschieden. Denn ist $ax + by = a'x + b'y$, so ist $(a - a')x + (b - b')y = 0$. Es ist $-p < a - a' < p$. Ebenso $-p < b - b' < p$. Ist $a - a' \geq 0$, so setzen wir $c := a - a'$, andernfalls $c := a - a' + p$; ebenso setzen wir $d := b - b'$, falls dies ≥ 0 ist, andernfalls sei $d := b - b' + p$. Dann ist $0 \leq c, d < p$ und $cx + dy = 0$. Das bedeutet $cx = (-d)y$. Ist $d \neq 0$, so dividieren wir durch d (siehe Satz 2.5) und erhalten $(-c/d)x = y$, also $y \in H_x$, ein Widerspruch. Ist $c \neq 0$, so erhalten wir $x = (-d/c)y$, also $x \in H_y$, ebenfalls ein Widerspruch. Also $c = d = 0$, woraus folgt, dass $a = a'$ und $b = b'$. (Dies ist kar, wenn $c = a - a'$ und $d = b - b'$ ist. Aber der Fall $c = a - a' + p = 0$ bedeutet $a = a' + p$, also $a \geq p$, ein Widerspruch zur Wahl von p. Ebenso sieht man, dass $d = b - b'$.)

Wir gehen nun immer weiter: induktiv haben wir p^m Elemente der Form $a_1x_1 + a_2x_2 + \cdots + a_mx_m$. Haben wir den Körper nicht ausgeschöpft, so nehmen wir ein neues Element x_{m+1} hinzu und bilden alle Summen $a_1x_1 + a_2x_2 + \cdots + a_{m+1}x_{m+1}$. Diese sind alle verschieden, und wir haben p^{m+1} davon. Gewiss kommt dieser Prozess an ein Ende. Und dann haben wir genau p^n Elemente für ein gewisses n.

Übungen.

Übung 4. Bestimmen Sie die Körper $\mathbb{F}_2$ und $\mathbb{F}_3$, indem Sie die Additions- und Multiplikationstabellen aufschreiben.

Übung 5. Zeigen Sie, dass das Polynom $x^2 - 2$ eine Nullstelle hat in $\mathbb{F}_7$ aber nicht in $\mathbb{F}_5$. Zeigen Sie, dass das Polynom $x^2 + 1$ in $\mathbb{F}_5$ eine Nullstelle hat aber nicht in $\mathbb{F}_7$.

Übung 6. Es bezeichnet i wie gewohnt eine Wurzel von -1. Es ist also $i^2 = -1$. Es ist $\mathbb{Z}[i]$ die Menge der Zahlen der Form $a + bi$ mit $a, b \in \mathbb{Z}$. Die Addition ist definiert durch $(a + bi) + (c + di) := (a + c) + (b + d)i$, das additive Inverse ist $-(a + bi) := (-a) + (-b)i$. Dass Nullelement ist $0 + 0i$. Die Multiplikation ist schließlich definiert durch $(a + bi)(c + di) := (ac - bd) + (ad + bd)i$. Zeigen Sie, dass dies einen Ring bildet.

Übung 7. Wir können eine Abbildung $\varphi : \mathbb{Z}[i] \to \mathbb{F}_{17}$ wie folgt definieren. Für eine Zahl $a + bi$ mit $a, b \in \mathbb{Z}$ sei $\varphi(a + bi) := \varphi(a) + 4\varphi(b)$. Man zeige, dass dies ein Ringhomomorphismus ist.

Übung 8. Zeigen Sie: Die Zahlen $(a + bi)/(c + di)$, wo a, b, c und und d rational sind, bilden einen Körper, den Körper der rational gebrochenen komplexen Zahlen. Dieser wird mit $\mathbb{Q}(i)$ bezeichnet. *Hinweis.* Die multiplikativen Inversen sollten leicht zu bestimmen sein. Einzig die Addition ist etwas schwieriger (wir müssen dabei die Brüche wir gewohnt erweitern).

Übung 9. Im Beweis für Satz 2.6 wurde die Identität $(nx)y = n(xy)$ benutzt. Beweisen Sie, dass sie für alle ganzen Zahlen gilt. *Hinweis.* Induktion über n etabliert das Gesetz für alle natürlichen Zahlen. Benutzen Sie für negative Zahlen die Gleichung $(-n)x := -(nx)$ $(n \in \mathbb{N})$.

Kapitel 3

Vektorräume

Definition 3.1 (Vektorraum) *Es sei* $\mathfrak{K} = \langle K, +_K, -_K, 0, \cdot_K, ^{-1}, 1_K\rangle$ *ein Körper. Ein* ***Vektorraum*** *über* $\mathfrak{K}$ *ist eine Struktur* $\langle V, +_V, -_V, 0_V, \circ\rangle$*, derart, dass*

1. $\langle V, +_V, -_V, 0_V\rangle$ *ein kommutative Gruppe ist,*
2. $\circ : K \times V \to V$ *eine Operation, sodass für alle* $k, k' \in K$ *und* $v, v' \in V$ *gilt*
   (a) $k \circ (k' \circ v) = (k \cdot_K k') \circ v$
   (b) $k \circ (v +_V v') = (k \circ v) +_V (k \circ v')$
   (c) $1_K \circ v = v$
   (d) $(k +_K k') \circ v = (k \circ v) +_V (k' \circ v)$.

Die Elemente von V heißen in diesem Zusammenhang auch ***Vektoren****. Wir sprechen von* $k \circ v$ *als einer* ***Streckung*** *von v um den Faktor k.*

Im Folgenden wird $\circ$ stets wie die Multiplikation geschrieben, das heißt als Punkt oder auch gar nicht. Ebenso wird die Addition im Körper nicht von der Addition im Vektorraum unterschieden. Die Subsripte fallen also ersatzlos weg. Der Kontext wird für Eindeutigkeit sorgen.

Hier einige Beispiele.

Beispiel 1. Es sei $\mathfrak{K} = \langle K, +_K, -_K, 0_K, \cdot_K{}^{-1}, 1_K\rangle$ ein Körper und m eine beliebige Menge. Dann bezeichnet K^M die Menge aller Funktionen von M nach K, die nur an endlich vielen Stellen von Null verschieden sind. (Man nennt das, Funktionen mit endlichem Support.) Ist M insbesondere endlich, so ist K^M schlicht die

Menge *aller* Funktionen von M nach K. Diese bilden einen Vektorraum über K mit folgenden Operationen.

- $(f +_V g)(x) := f(x) +_K g(x)$;
- $(-_V f)(x) := -_K f(x)$;
- $0_V(x) := 0_K$;
- $(k \circ f)(x) := k \cdot_K f(x)$.

Hierbei ist also in der ersten Definition $f +_V g$ die Summe in dem Vektorraum (die wir damit definieren) und $f(x) +_K g(x)$ die Summe aus $f(x)$ und $g(x)$ im Körper, welche bereits definiert ist. ⚽

Beispiel 2. Ich spezialisiere M. Es sei $M = \varnothing$. Dann existiert genau eine Funktion, die leere Funktion, und die ist der Nullvektor. In diesem Fall besitzen wir einen einzigen Vektor, 0. Die Addition ist $0 + 0 = 0$, und die Streckungen sind $k \circ 0 = 0$. ⚽

Beispiel 3. Ein weiterer Spezialfall ist $M = \{0\}$. Dann sind die Vektoren Funktionen, die der Zahl 0 ein Körperelement zuweisen. Wir schreiben (k) für die Funktion f, für die $f(0) = k$. (Die Notation wird später noch häufiger vorkommen.) Die Addition ist $(k +_V k') := (k +_K k')$, die Streckungen sind $k \circ (k') := (k \cdot_K k')$. Der Nullvektor ist (0). ⚽

Beispiel 4. Nehmen wir als Beispiel $M = 3 = \{0, 1, 2\}$ und $K = \mathbb{Q}$. Dann sind die Elemente aus $\mathbb{Q}^3$ Funktionen von $\{0, 1, 2\}$ nach $\mathbb{Q}$. Eine solche Funktion f ist also durch ihre Werte $f(0)$, $f(1)$ und $f(2)$ eindeutig bestimmt. Man schreibt sie wir folgt auf:

$$\begin{pmatrix} f(0) \\ f(1) \\ f(2) \end{pmatrix} \tag{3.1}$$

Die folgenden sind also Elemente von $\mathbb{Q}^3$:

$$\begin{pmatrix} 3 \\ 0.5 \\ -2 \end{pmatrix}, \begin{pmatrix} 6 \\ 1 \\ -4 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}. \tag{3.2}$$

(Der erste Vektor ist zum Beispiel die Funktion $f : 3 \to \mathbb{Q}$ mit $f(0) = 3$, $f(1) = 0.5$ und $f(2) = -2$.) Der zweite Vektor ist eine Streckung des ersten Vektors (mit 2). Der dritte ist der Nullvektor. Wir können in diesem Fall die Addition zweier Vektoren wie folgt konkret aufschreiben.

$$\begin{pmatrix} f(0) \\ f(1) \\ f(2) \end{pmatrix} + \begin{pmatrix} g(0) \\ g(1) \\ g(2) \end{pmatrix} = \begin{pmatrix} f(0) + g(0) \\ f(1) + g(1) \\ f(2) + g(2) \end{pmatrix} \tag{3.3}$$

Ist p eine Primzahl und $m \in \mathbb{N}$, so ist der Vektorraum $\mathbb{F}_p^m$ über dem Körper $\mathbb{F}_p$ endlich und enthält p^m Vektoren. ⚽

Es folgen noch ein paar weitere Beispiele für Vektorräume.

Beispiel 5. Das erste ist $\mathbb{R}$ als Vektorraum über $\mathbb{Q}$. Man betrachtet dabei die reellen Zahlen formal als Vektoren. Sie bilden eine Gruppe $\langle \mathbb{R}, +, -, 0 \rangle$. Multiplikation existiert nur in Form einer Streckung mit einer rationalen Zahl. Das hat zur Folge, dass zum Beispiel die Zahl 2 keine Streckung von $\sqrt{2}$ ist. Denn die einzige Zahl, die mit $\sqrt{2}$ multipliziert 2 ergibt, ist $\sqrt{2}$. Diese ist aber irrational. Die Operation $\circ$ is also nicht weiter als die Einschränkung der Multiplikation von $\mathbb{R}$ auf $\mathbb{Q} \times \mathbb{R}$. Es ist einfach, die Vektorraumaxiome zu verifizieren. ⚽

Beispiel 6. Das nächste Beispiel sind Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. Nennen wir die Menge dieser Funktionen $F(\mathbb{R})$. Diese bilden eine Gruppe mit punktweiser Addition. Wir setzen wie oben

- $(f + g)(x) := f(x) + g(x)$;
- $(-f)(x) := -f(x)$;
- $0(x) := 0$;
- $(k \circ f)(x) := k \cdot f(x)$.

Dies macht $F(\mathbb{R})$ zu einem Vetorraum über $\mathbb{R}$. (Dieser ist nicht identisch mit $\mathbb{R}^{\mathbb{R}}$, weil in letzterem nur solche Funktionen aufgenommen sind, die nur auf endlich vielen Argument von 0 verschieden sind. Die Identitätsabbildung $x \mapsto x$ oder die Parabel $x \mapsto x^2$ sind also in $F(\mathbb{R})$ aber nicht in $\mathbb{R}^{\mathbb{R}}$.) ⚽

Beispiel 7. Und schließlich noch ein endlicher Vektorraum. Nehmen wir $\mathbb{F}_2^3$. Die Elemente sind also (im Wesentlichen) Tripel von Zahlen aus $\mathbb{F}_2^3$. Da $\mathbb{F}_2$ 2 Elemente hat, haben wir insgesamt $2^3 = 8$ Elemente, die wir alle auflisten können:

$$\left(\begin{array}{c}0\\0\\0\end{array}\right),\left(\begin{array}{c}0\\0\\1\end{array}\right),\left(\begin{array}{c}0\\1\\0\end{array}\right),\left(\begin{array}{c}0\\1\\1\end{array}\right),\left(\begin{array}{c}1\\0\\0\end{array}\right),\left(\begin{array}{c}1\\0\\1\end{array}\right),\left(\begin{array}{c}1\\1\\0\end{array}\right),\left(\begin{array}{c}1\\1\\1\end{array}\right). \tag{3.4}$$

Es gibt zwei Streckungen, eine für jedes der zwei Körperelemente. Die Streckung mit 0 bildet jeden Vektor auf den Nullvektor ab. Die Streckung mit 1 bildet jeden Vektor auf sich selbst ab, ist also die Identität. Wir haben ferner für alle Vektoren v: $-v = v$. Die Addition ist die einzig nichttriviale Operation.

$$\left(\begin{array}{c}0\\1\\1\end{array}\right)+\left(\begin{array}{c}1\\0\\1\end{array}\right)=\left(\begin{array}{c}1\\1\\0\end{array}\right) \tag{3.5}$$

⚽

Ich will kurz einige Folgerungen aus den Gesetzen ziehen. Diese verbinden die Operationen auf V mit den Streckungen.

Proposition 3.2 *Für alle $v \in V$ ist $0 \cdot v = 0$ und $-v = (-1) \cdot v$.*

Beweis. Da $0 = 0 + 0$, ist $0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v$. Daraus folgt, indem man von beiden Seiten $0 \cdot v$ abzieht, $0 = 0 \cdot v$. Ferner ist $0 = 1 - 1$, also $0 = 0 \cdot v = (1 - 1) \cdot v = 1 \cdot v + (-1) \cdot v = v + (-1)v$. Da Inverse eindeutig sind, ist $(-1)v = -v$. ⊣

Definition 3.3 (Lineare Abhängigkeit) *Es seien v_i, $i < m$, Vektoren. Eine **Linearkombination** dieser Vektoren ist eine Summe der Form*

$$\sum_{i<m} \lambda_i v_i = \lambda_0 v_0 + \lambda_1 v_1 + \cdots + \lambda_{m-1} v_{m-1} \tag{3.6}$$

wobei $\lambda_i \in K$. Linearkombinationen sind also endliche Summen. Eine Linearkombination von einer unendlichen Menge S von Vektoren ist eine Summe der Form (3.6)*, wo die x_i aus S sind (davon sind nur dann nur endlich viele vertreten). Die Menge aller Linearkombinationen von Vektoren aus einer gegebenen Menge S wird mit $\langle S \rangle$ bezeichnet und heißt die **lineare Hülle** von S. w heißt von den x_i, $i < m$, **linear abhängig**, falls es eine Linearkombination dieser Vektoren ist.*

Es sei $v = \sum_{i<m} \lambda_i x_i$ und $w = \sum_{i<m} \mu_i x_i$. Dann ist

$$v + w = \left(\sum_{i<m} \lambda_i x_i\right) + \left(\sum_{i<m} \mu_i x_i\right) = \sum_{i<m} \lambda_i x_i + \mu_i x_i = \sum_{i<m} (\lambda_i + \mu_i) x_i \tag{3.7}$$

Ebenso ist

$$-v = -\sum_{i<m} \lambda_i x_i = \sum_{i<m} (-\lambda_i) x_i \tag{3.8}$$

sowie

$$\mu v = \mu \left(\sum_{i<m} \lambda_i x_i\right) = \sum_{i<m} \mu(\lambda_i x_i) = \sum_{i<m} (\mu\lambda_i) x_i \tag{3.9}$$

Die lineare Hülle einer Menge S ist also unter den Operationen auf V abgeschlossen. (Allerdings müssen wir eine Feinheit beachten: In (3.7) ist vorausgesetzt, dass v eine Linearkombination derselben Elemente aus S sind. Das lässt aber immer einrichten. Denn man bedenke, dass, wenn $v = \sum_{i<m} \lambda_i x_i$, und x_m ein beliebiger Vektor ist, so setze $\lambda_m := 0$, und wir haben nunmehr $v = \sum_{i<m+1} \lambda_i x_i$.) Der Nullvektor ist auch darin enthalten, wie man unschwer sieht. Daraus folgt unmittelbar

Proposition 3.4 *Es sei $\langle V, +, -, 0, \cdot\rangle$ ein Vektorraum über $\mathfrak{K}$ und $S \subseteq V$. Dann ist $\langle\langle S\rangle, +, -, 0, \cdot\rangle$ ebenfalls ein Vektorraum über $\mathfrak{K}$. (Hierbei sind die Operationen auf $\langle S\rangle$ die natürlichen Einschränkungen der entsprechenden Operationen auf V und werden deswegen ebenso bezeichnet.)*

Definition 3.5 (Unterraum) *Es sei $\langle V, +, -, 0, \cdot\rangle$ ein Vektorraum über K. Ein **Unterraum** von V ist eine beliebige, unter den Operationen von V abgeschlossene Teilmenge von V, zusammen mit den natürlichen Einschränkungen dieser Operationen.*

Nehmen wir noch einmal den $\mathbb{Q}^3$. Die Menge aller Vektoren f, für die $f(1) = 0$, ist ein Unterraum. Denn ist $f(1) = g(1) = 0$, so ist auch $(f + g)(0) = 0$, $(-f)(1) = 0$, sowie $(\lambda f)(1) = \lambda(f(1)) = 0$. Diese Menge ist also wie in der Definition gefordert abgeschlossen unter den Operationen auf $\mathbb{Q}^3$ und bildet Vektoren bildet deswegen einen Unterraum.

Definition 3.6 (Basis) *Eine Menge S von Vektoren heißt **linear unabhängig**, falls kein Vektor von den anderen Vektoren linear abhängig ist, das heißt, wenn $v \notin \langle S - \{v\}\rangle$ für alle $v \in S$. Eine **Basis** des Vektorraums V ist eine Folge $B = \langle b_i : i < \kappa\rangle$, wo $\{b_i : i < \kappa\}$ eine bezüglich Inklusion maximale linear unabhängige Menge ist. κ heißt die **Länge** der Basis und wird mit $|B|$ bezeichnet. (Dies ist eine Kardinalzahl.)*

Eine Basis ist geordnet, wohingegen die Menge der in ihr enthaltenen Vektoren ungeordnet ist. So sind $\langle v, v'\rangle$ und $\langle v', v\rangle$ zwei verschiedene Basen. Diese erzeugen denselben Vektorraum, weil der erzeugte Vektorraum nur von der Menge der Vektoren der Basis abhängt.

Kommen wir noch einmal auf $\mathbb{R}$ als Vektorraum über $\mathbb{Q}$ zurück. Die Menge $\{1, \sqrt{2}\}$ ist linear unabhängig, weil es keine rationalen Zahl q gibt mit $2 = q\sqrt{2}$. Ebenso ist $\{1, \pi, \sqrt{2}\}$ linear unabhängig. (Über $\mathbb{Q}$ gibt es überabzählbare linear unabhängige Mengen reeller Zahlen!)

Lemma 3.7 *Genau dann ist eine Menge S linear unabhängig, wenn aus $\sum_{i<m} \lambda_i x_i = 0$ mit $x_i \in S$ folgt, dass $\lambda_i = 0$ für alle $i < m$.*

Beweis. Ist die Menge S linear abhängig, also $v \in \langle S - \{v\}\rangle$, dann existiert eine Darstellung $v = \sum_{i<m} \lambda_i x_i$, wo $x_i \in S - \{v\}$ für alle $i < m$. Ist $v \notin 0$, so sind nicht alle λ_i gleich Null. Dann haben wir $0 = v - v = (\sum_{i<m} \lambda_i x_i) - v = \sum_{i<m+1} \lambda_i x_i$, falls wir $x_m := v$ und $\lambda_m := -1$ setzen. Es gibt also eine nichttriviale Darstellung der Null. Sei umgekehrt $0 = \sum_{i<m} \lambda_i x_i$, bei der nicht alle λ_i Null sind. Ohne Beschränkung der Allgemeinheit sei $\lambda_{m-1} \neq 0$. Dann ist $\lambda_{m-1} x_{m-1} = \sum_{i<m-1}(-\lambda_i)x_i$, und so $x_{m-1} = \sum_{i<m-1}(-\lambda_i/\lambda_{m-1})x_i$. Das bedeutet, dass S nicht linear unabhängig ist. ⊣Anders ausgedrückt ist eine Menge B eine Basis des Vektorraums, falls sie linear

unabhängig ist und $\langle B\rangle = V$. Denn wenn das Letztere der Fall ist, so gibt es keine Menge C mit $B \subsetneq C \subseteq V$, welche linear unabhängig ist. B ist dann also maximal. Ist B maximal, so ist dann auch $\langle B\rangle = V$. Andernfalls existiert ein $v \in V - \langle B\rangle$, und dann wäre $B \cup \{v\}$ linear unabhängig.

Definition 3.8 (Koordinaten) *Es sei $B = \langle b_i : i < \kappa\rangle$ Basis des Vektorraums V. Zu jedem $v \in V$ existieren dann eindeutig bestimmte Elemente $\lambda_i \in K$, $i < \kappa$, sodass*

$$v = \sum_{i<\kappa} \lambda_i b_i \tag{3.10}$$

*Das Tupel $\langle \lambda_i : i < \kappa\rangle$ heißt der **Koordinatenvektor von** v **zur Basis** B.*

Man beachte: die Koordinaten bilden ebenfalls eine Folge, wie die Basis selbst. Hat man eine Basis B, so haben wir eine Abbildung, die jedem Vektor v seinen Koordinatenvektor zuordnet. Dies ist also eine Bijektion zwischen V und K^κ.

In der Definition stecken zwei Behauptungen: die eine, dass die Koordinaten existieren; die andere, dass sie eindeutig sind. Die Existenz ist klar, sie folgt aus der Definition der Basis. Die Eindeutigkeit folgt mit Lemma 3.7. Sei nämlich

$$v = \sum_{i<m} \lambda_i b_i = \sum_{i<m} \mu_i b_i \tag{3.11}$$

Dann ist

$$0 = v - v = \sum_{i<m} \lambda_i b_i - \sum_{i<m} \mu_i b_i = \sum_{ii<m} (\lambda_i - \mu_i) b_i \tag{3.12}$$

und mit Lemma 3.7 folgt, dass für alle $i < m$ gilt $\lambda_i - \mu_i = 0$, also $\lambda_i = \mu_i$.

Es stellt sich zweierlei heraus. Zunächst einmal gibt es viele verschiedene Basen; es gibt also nicht *die* Basis eines Vektorraums. Zum anderen aber haben Basen stets die gleiche Anzahl Elemente, das heißt, sie sind stets gleich mächtig.

Proposition 3.9 (Basisexistenzsatz) *Jeder Vektorraum hat eine Basis.*

Beweis. Es sei V ein Vektorraum. Wir wählen eine Aufzählung $V = \{v_\alpha : \alpha < \mu\}$ von V. Nun bestimmen wir eine Basis wie folgt. Es sei $B_0 := \emptyset$. Ferner sei

$$B_{\alpha+1} := \begin{cases} B_\alpha & \text{falls } v_\alpha \in \langle B_\alpha \rangle \\ B_\alpha \cup \{v_\alpha\} & \text{sonst} \end{cases} \tag{3.13}$$

Ist α eine Limeszahl (das heißt, eine Ordinalzahl ohne Vorgänger), dann setze

$$B_\alpha := \bigcup_{\beta<\alpha} B_\beta \tag{3.14}$$

Schließlich setze $B := B_\mu$. Wir zeigen: (1) jedes B_α ist linear unabhängig; (2) $\langle B_\mu \rangle = V$. Zu (1). Induktion über den Ordinalzahlrang. B_0 ist sicher linear unabhängig. Für Nachfolgerzahlen ist dies nach Definition richtig. Ist α Limeszahl und sei $0 = \sum_{i<m} \lambda_i x_i$, wo $x_i \in B_\alpha$ und $\lambda_i \neq 0$ für alle $i < m$. Dann existiert ein $\beta < \alpha$, sodass für alle $i < m$ $x_i \in B_\beta$, also $0 = \sum_{i<m} \lambda_i x_i$ mit $\lambda_i \neq 0$ und $x_i \in B_\beta$; mit anderen Worten, B_β ist linear abhängig. Zu (2). Es ist nach Konstruktion für alle α $v_\alpha \in B_{\alpha+1}$. Daher ist für alle v_β, $\beta < \mu$, $v_\beta \in \langle B_\mu \rangle$. Also ist $V = \langle B_\mu \rangle$. Also ist B eine Basis. ⊣

Proposition 3.10 *Es sei V ein Vektorraum über einem Körper $\mathfrak{K}$ und seien B und C Basen von V. Dann ist $|B| = |C|$.*

Beweis. Ich beweise dies nur für den Fall, wo B oder C endlich ist. (In diesem Fall kann man sich leicht überlegen, dass beide Mengen endlich sind.) Sei $B = \{b_i : i < m\}$ und $C = \{c_i : i < n\}$. Wir zeigen zunächst folgende Behauptung: Ist $C \neq B$, so lässt sich für jedes $c \in C$ ein $b \in B$ finden derart, dass $(C - \{c\}) \cup \{b\}$ eine Basis ist. Daraus lässt sich leicht folgern, dass, wenn $|B| \leq |C|$, so existiert eine Basis der Form $(C - D) \cup B$, wo $|D| = |B|$. (Man tausche so viele Elemente aus C durch Elemente aus B aus, wie nur geht.) Da B Basis ist, ist $C - D = \emptyset$, also hat C genauso viele Elemente wie D, also wie B.

Nun also zu der Behauptung. Wir wählen (ohne Beschränkung der Allgemeinheit) $c := c_0$. Da $C - \{c_0\} = \{c_1, \cdots, c_{n-1}\}$ keine Basis ist, existiert ein $b_j \notin \langle C - \{c_0\}\rangle$. (Andernfalls wären sämtliche b_i schon im Erzeugnis von $C - \{c_0\}$, und somit auch jede Linearkombination davon. Dann wäre dies aber eine Basis.) b_i ist linear unabhängig von den c_i mit $0 < i < n$. Es ist also

$$b_j = \sum_{i<n} \lambda_i c_i \tag{3.15}$$

wobei $\lambda_0 \neq 0$. Wir stellen dies wie folgt um:

$$-\lambda_0 c_0 = -b_j + \sum_{0<i<n} \lambda_i c_i \tag{3.16}$$

Daraus folgt dann, dass

$$c_0 = \frac{1}{\lambda_0} b_j + \sum_{0<i<n} -\frac{\lambda_i}{\lambda_0} c_i \tag{3.17}$$

Daraus folgt unmittelbar, dass $C' := \{b_j, c_1, \cdots, c_{n-1}\}$ den Vektorraum erzeugt. Denn nunmehr ist $c_0 \in \langle C'\rangle$, und deswegen ist auch jede Linearkombination von c_0 mit den c_i, $0 < i < n$, in der linearen Hülle von C'. Also ist C' ein Erzeugendensystem von V. C' ist auch linear unabhängig. Nehmen wir an, es existiert eine Darstellung der Null

$$\mu b_j + \sum_{0<i<m} \nu_i c_i = 0 \tag{3.18}$$

wobei nicht alle Koeffizienten Null sind. Insbesondere ist dann $\mu \neq 0$, da sonst schon die c_i, $0 < i < n$, linear abhängig wären. Wir ersetzen b_j:

$$\sum_{i<n} \mu\lambda_i c_i + \sum_{0<i<m} \nu_i c_i = 0 \tag{3.19}$$

Da insbesondere $\lambda_0 \neq 0$, ist dies eine nichttiviale Darstellung des Nullvektors durch die c_i. Aber diese sind linear unabhängig. Widerspruch. Also existiert solch eine Darstellung nicht und C' ist ebenfalls linear unabhängig. ⊣

Definition 3.11 (Dimension) *Es sei V ein Vektorraum über dem Körper $\mathfrak{K}$. Die **Dimension** von V über $\mathfrak{K}$ ist $|B|$, wo B eine Basis von V über $\mathfrak{K}$ ist.*

Aufgrund der eben bewiesenen Sätze ist es unerheblich, welche Basis wir verwenden. Die Dimension ist somit eindeutig bestimmt.

Übungen

In diesen Übungen werden wir Vektorräume über $\mathbb{F}_5$ anschauen.

Übung 10. Geben seien die Vektoren $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ und $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$. Diese sind Vektoren aus ${\mathbb{F}_5}^2$. Sind diese beiden Vektoren in ${\mathbb{F}_5}^2$ linear abhängig? Geben Sie das Erzeugnis von $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ explizit an.

Übung 11. Es sei $v \neq 0$ ein Vektor in $\mathbb{F}_5^2$. Wie viele zu v linear unabhängige Vektoren gibt es?

Übung 12. Lösen Sie folgendes Gleichungssystem (über $\mathbb{F}_5$). Sie können dabei jedes übliche Verfahren verwenden.

$$\begin{aligned} x \quad +2y \quad\ \ +z &= 2 \\ \qquad\ y \quad +3z &= 1 \\ 2x \quad +y \quad +2z &= 3 \end{aligned}$$

Kapitel 4

Lineare Abbildungen und lineare Gleichungen

In diesem Kapitel werden wir sehen, dass man jeden Vektorraum als Raum der Form $\mathfrak{K}^M$ auffassen kann für eine geeignete Menge M. Dazu müssen wir zunächst klären, was es heißt, einen Raum in einer Form aufzufassen.

Definition 4.1 (Lineare Abbildung) *Es seien* $\mathfrak{V} = \langle V, +_V, -_V, 0_V, \circ_V \rangle$ *und* $\mathfrak{W} = \langle W, +_W, -_W, 0_W, \circ_W \rangle$ *Vektorräume über einem Körper* $\mathfrak{K} = \langle K, +_K, -_K, 0_K, \cdot_K, {}^{-1_K}, 1_K \rangle$ *und* $f : V \to W$ *eine Funktion.* f *heißt* ***lineare Abbildung (von*** $\mathfrak{V}$ ***nach*** $\mathfrak{W}$*), falls für alle* $v, w \in V$ *und für alle* $k \in K$ *gilt:*

1. $f(v +_V w) = f(v) +_W f(w)$,
2. $f(k \circ_V v) = k \circ_W f(v)$;
3. $f(0_V) = 0_W$.

Wir werden (auch weiterhin) häufig einfach von einem Vektorraum V sprechen, anstelle vom Vektorraum $\langle V, +_V, -_V, 0_V, \circ_V \rangle$, und die Operationen ohne den auf den Vektorraum verweisenden Index notieren. Die Operation $\circ_V$ wird dabei auch als $\cdot$ statt $\circ$ geschrieben oder sogar ganz weggelassen. Da die Wahl der Operationen über der Menge im Prinzip willkürlich ist, muss man aber streng genommen bei der Formulierung „Vektorraum $\mathfrak{V}$" stets die Operationen und den Nullvektor fixieren.

Analoges gilt für die Sprechweise von einem Körper $\langle K, +_K, -_K, 0_K, \cdot_K, {}^{-1_K}, 1_K \rangle$ einfach als $\mathfrak{K}$ ohne die Aufführung der Operationen und neutralen Elementen und

das Weglassen des Index K bei Verweis auf die Operationen und die neutralen Elemente.

Die dritte Bedingung in Definition 4.1 ist im Übrigen verzichtbar. Denn wählt man für $w := -v$, so folgt aus der ersten Bedingung $f(0) = f(v + (-v)) = f(v) + f(-v) = f(v) + f((-1)v) = f(v) - f(v) = 0$.

Proposition 4.2 *Es sei $f : V \to W$ eine lineare Abbildung und B eine Basis von $\mathfrak{V}$. Dann ist f bereits eindeutig durch seine Werte auf B bestimmt.*

Beweis. Es sei $v \in V$. Nach Definition der Basis existieren b_i, $i < m$, aus B und eindeutige bestimmte $\lambda_i \in K$, $i < m$, sodass $v = \sum_{i<m} \lambda_i x_i$. Also ist

$$f(v) = f(\sum_{i<m} \lambda_i b_i) = \sum_{i<m} f(\lambda_i b_i) = \sum_{i<m} \lambda_i f(b_i) \tag{4.1}$$

Da die Koordinaten eindeutig sind, ist $f(v)$ ebenfalls eindeutig bestimmt. ⊣

Proposition 4.3 *Es seien V und W Vektorräume über $\mathfrak{K}$ und B eine Basis von V. Sei $u : B \to W$ eine beliebige Abbildung. Dann existiert genau eine lineare Abbildung $f : V \to W$ mit $f(b) = u(b)$ für $b \in B$, Diese heißt auch die **lineare Fortsetzung** von u.*

Beweis. Sei $v \in V$. Dann existieren eindeutig bestimmte b_i, $i < m$, und λ_i, $i < m$, mit

$$v = \sum_{i<m} \lambda_i b_i \tag{4.2}$$

Setze nun

$$f(v) := \sum_{i<m} \lambda_i u(b_i) \tag{4.3}$$

Diese Abbildung ist linear; sie ist eindeutig bestimmt aufgrund der Eindeutigkeit der linearen Darstellung von v als Summe von Basisvektoren. Und es ist $f(b) = u(b)$ für alle $b \in B$. ⊣

Es sei nun V ein abstrakter Vektorraum. Ist M eine Menge, so bestehe $\mathfrak{K}^M$ aus Funktionen von M nach K mit endlichem Support. Falls insbesondere M endlich ist, so ist dies schlicht die Menge *aller* Funktionen von M nach K. Anstelle der Vektoren b_i nimmt man jedoch lieber die Zahlen $0, 1, \cdots, m-1$. Der folgende Satz wird nur für Vektorräume formuliert, die eine endliche Basis besitzen. Im unendlichen Fall muss man die Zahl m duch eine Kardinalzahl ersetzen.

Proposition 4.4 *Gegeben sei V ein Vektorraum und $B = \langle b_i : i < m\rangle$ eine endliche Basis. Definiere $\gamma_B : V \to \mathfrak{K}^m$ wie folgt. Ist $v \in V$ und hat $v = \sum_{i<m} \lambda_i b_i$, so sei $\gamma_B(v) := \langle \lambda_i : i < m\rangle$. Diese heiße die* ***Koordinatenfunktion****. Diese ist eine bijektive lineare Abbildung.*

Beweis. Wir haben schon gesehen, dass die Koordinatenfunktion wohldefiniert ist. Nun gilt es zu zeigen, dass sie linear ist. Seien $v, w \in V$. Dann ist $v = \sum_{i<m} \gamma_B(v)(i)b_i$ und $w = \sum_{i<m} \gamma_B(w)(i)b_i$. Also ist

$$\gamma_B(v+w) = \sum_{i<m} \gamma_B(v)(i)b_i + \sum_{i<m} \gamma_B(w)(i)b_i = \sum_{i<m} (\gamma_B(v)(i) + \gamma_B(w)(i))b_i \tag{4.4}$$

Daraus folgt, dass

$$\gamma_B(v+w)(i) = \gamma_B(v)(i) + \gamma_B(w)(i) \tag{4.5}$$

Dies ist aber genau die Addition in $\mathfrak{K}^m$. Ferner ist

$$\gamma_B(\mu v) = \mu\gamma_B(v) = \mu\left(\sum_{i<m} \gamma_B(v)(i)b_i\right) = \sum_{i<m} (\mu\gamma_B(v)(i))b_i \tag{4.6}$$

Daraus folgt, dass

$$\gamma_B(\mu v)(i) = \mu(\gamma_B(v)(i)) \tag{4.7}$$

Dies ist genau die Streckung in $\mathfrak{K}^m$. γ_B ist gewiss injektiv. Denn ist $\gamma_B(v) = \gamma_B(v')$, so ist $\gamma_B(v - v') = \gamma_B(v) - \gamma_B(v') = 0$. Der einzige Vektor, dessen sämtliche Koordinaten Null sind, ist der Nullvektor (Lemma 3.7). γ_B ist aber auch surjektiv. Denn sei ein $j : \{0, 1, \cdots, m-1\} \to K$ gegeben. Dann sei $v := \sum_{i<m} j(i)b_i$. Wir haben dann $\gamma_B(v) = j$. ⊣

Definition 4.5 (Kanonische Basis) *Es sei m eine natürliche Zahl. Sei $\delta_i \in K^m$ wie folgt definiert: $\delta_i(j) := 1$, falls $j = i$ und $\delta_i(j) := 0$ sonst. Dann ist $\langle \delta_i : i < m\rangle$ eine Basis von $\mathfrak{K}^m$, die sogenannte* ***kanonische Basis****. Insbesondere hat $\mathfrak{K}^m$ also eine Basis der Mächtigkeit m.*

Auch hier stecken in der Definition ein paar Behauptungen, die wir erst einmal prüfen müssen. Die δ_i gehören gewiss zu K^m. Sie bilden auch eine linear unabhängige Menge. Denn falls $0 = \sum_{j<m} \lambda_j\delta_j$, so muss gelten:

$$0(i) = \left(\sum_{j<m} \lambda_j\delta_j\right)(i) = \sum_{j<m} \lambda_j\delta_j(i) \tag{4.8}$$

Da $0(i) = 0$ (die $i$te Koordinate des Nullvektors), so ist für jedes i

$$0 = \sum_{j<m} \lambda_j \delta_j(i) = \lambda_i \tag{4.9}$$

Also ist für alle $i < m$ $\lambda_i = 0$. Die Funktionen sind also linear unabhängig.

Proposition 4.4 liefert etwas mehr als nur die Idee, dass wir Vektoren irgendwelche Koordinaten zuordnen können. Er sagt uns, dass die Addition und Streckung des Vektorraums unter dieser Identifikation stets die Addition und Streckung des Vektorraums K^m ist. Das bedeutet wiederum, dass der Raum V von dem Raum K^m nicht unterschieden werden kann. Der einzige Unterschied zwischen den beiden beruht in der Wahl der Elemente.

Definition 4.6 *Es seien V und W Vektorräume über einem Körper K. Dann heißt V **isomorph** zu W, falls es eine bijektive lineare Abbildung von V nach W gibt.*

Lemma 4.7 *Es sei $f : V \to W$ eine injektive lineare Abbildung. Ist dann B eine endliche linear unabhängige Teilmenge von V, so ist $f[B] = \{f(b) : b \in B\}$ eine linear unabhängige Teilmenge von W. Ist zusätzlich f surjektiv und B eine Basis von V, so ist $f[B]$ eine Basis von W.*

Beweis. Angenommen, λ_b, $b \in B$ seien so gewählt, dass $\sum_{b\in B} \lambda_b f(b) = 0$. Dann ist

$$0 = \sum_{b\in B} \lambda_b f(b) = f(\sum_{b\in B} \lambda_b b) \tag{4.10}$$

Da f injektiv ist, ist $\sum_{b\in B} \lambda_b b = 0$. Da B linear unabhängig ist, ist $\lambda_b = 0$ für jedes $b \in B$. Also ist $f[B]$ linear unabhängig. Sei nun zusätzlich f surjektiv und B eine Basis von V. Zu zeigen ist, dass jeder Vektor $w \in W$ eine Darstellung $w = \sum_{b\in B} \mu_b f(b)$ hat. Wähle dazu ein v mit $f(v) = w$; dieses ist eindeutig bestimmt, weil f injektiv ist und existiert, weil f surjektiv ist. Ist B Basis von V, so existieren λ_b mit $v = \sum_{b\in B} \lambda_b\, b$. Dann ist

$$w = f(v) = f(\sum_{b\in B} \lambda\, b) = \sum_{b\in B} f(\lambda_b\, b) = \sum_{b\in B} \lambda_b\, f(b) \tag{4.11}$$

Also ist $f[B]$ Basis. ⊣

Satz 4.8 *Jeder Vektorraum V mit Basis ist zu einem Vektorraum K^B isomorph, wo B eine Menge ist. Ferner ist K^B genau dann isomorph zu K^C, wenn $|B| = |C|$.*

Beweis. (Ich werde dies nicht für unendliche Basen zeigen.) Sei V ein Vektorraum mit endlicher Basis B. Jedem Vektor wird dann eine Funktion $\gamma : B \to K$ zugeordnet. Dies ist der gewünschte Isomorphismus von V nach K^B. Nun zur zweiten Behauptung. Es sei K^B isomorph zu K^C. Dann existiert eine bijektive Abbildung $j : K^B \to K^C$. Nach Lemma 4.7 ist das Bild der kanonischen Basis dann eine Basis von K^C. Dies bedeutet, dass K^C eine Basis der Mächtigkeit $|B|$ hat. Da die kanonische Basis eine Basis von K^C ist, hat K^C auch eine Basis der Mächtigkeit C. Also ist $|B| = |C|$. Sei umgekehrt $|B| = |C|$. Dann existiert eine Bijektion $p : B \to C$. Wähle die Abbildung $f_p : \delta_b \mapsto \delta_{p(b)}$. Diese ist eine Bijektion zwischen einer Basis von K^B und einer Basis von K^C, und somit ein Isomorphismus zwischen diesen Vektorräumen. ⊣

Dieser Satz ist also der zentrale Struktursatz. Er sagt uns, dass wir im Wesentlichen immer annehmen dürfen, dass $V = K^B$ ist, oder im endlichen Fall $V = K^m$, für eine natürliche Zahl m. Diese Vektorräume haben überdies eine kanonische Basis, und diese wird man stets wählen. Wenn wir dies tun, können lineare Abbildungen nunmehr wie bekannt durch sogenannte Matrizenmultiplikation beschrieben werden.

Satz 4.9 *Es sei $f : K^m \to K^n$ eine lineare Abbildung. Dann existieren Zahlen $(a_{ij})_{i<n,j<m}$ derart, dass*

$$f\left(\begin{pmatrix} x_0 \\ \cdots \\ x_{m-1} \end{pmatrix}\right) = \begin{pmatrix} a_{00}x_0 & +a_{01}x_1 & +\cdots & +a_{0,m-1}x_{m-1} \\ a_{10}x_0 & +a_{11}x_1 & +\cdots & +a_{1,m-1}x_{m-1} \\ & & \cdots & \\ a_{n-1,0}x_0 & +a_{n-1,1}x_1 & +\cdots & +a_{n-1,m-1}x_{m-1} \end{pmatrix} \tag{4.12}$$

Das Zahlenschema $A = (a_{ij})_{i<n,j<m}$ heißt auch $n\times m$-**Matrix**. Ist A eine $n\times m$-Matrix und x ein m-dimensionaler Vektor, so bezeichnet Ax das in (4.12) angegebene Produkt. Dies ist ein n-dimensionaler Vektor.

Es sei nun K ein beliebiger Körper. Eine **lineare Gleichung** ist eine Gleichung der Form

$$a_0x_0 + a_1x_1 + \cdots + a_{m-1}x_{m-1} = c \tag{4.13}$$

wo $a_0, \cdots, a_{m-1}, c \in K$ und die x_i Unbekannte (aus K) sind. Fassen wir die Unbekannten zu einem Vektor $v := (x_0, \cdots, x_{m-1})$ zusammen, ist die Abbildung $v \mapsto \sum_{i<m} a_ix_i$ eine lineare Abbildung von K^m nach K. (So etwas nennt man auch eine Linearform.) Gesucht sind also alle Vektoren, deren Bild unter dieser Abbildung genau c ist. Haben wir nun zwei solcher Gleichungen:

$$\begin{aligned} a_{00}x_0 + a_{01}x_1 + \cdots + a_{0,m-1}x_{m-1} &= c_0 \\ a_{10}x_0 + a_{11}x_1 + \cdots + a_{1,m-1}x_{m-1} &= c_1 \end{aligned} \tag{4.14}$$

so definieren wir jetzt

$$f\left(\left(\begin{array}{c} x_0 \\ \cdots \\ x_{m-1} \end{array}\right)\right) := \sum_{i<m} x_i \begin{pmatrix} a_{0i} \\ a_{1i} \end{pmatrix} \tag{4.15}$$

Dies ist eine lineare Abbildung von K^m nach K^2. Gesucht ist ein Vektor $v \in K^m$ mit $f(v) = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$. Auf diese Weise übersetzt man das Lösen linearer Gleichungssysteme in das Finden von Vektoren v, welche einer einzigen Gleichung $f(v) = w$ genügen, wobei $f : K^m \to K^n$.

Proposition 4.10 *Es sei $f : V \to W$ eine lineare Abbildung. Dann bilden die Vektoren v mit $f(v) = 0$ einen Unterraum von V. Dieser heißt der **Kern** von f und wird mit* $\ker(f)$ *bezeichnet.*

Beweis. Ist $f(v) = 0$ und $f(w) = 0$, so ist $f(v + w) = f(v) + f(w) = 0$ sowie $f(\lambda v) = \lambda f(v) = \lambda 0 = 0$. ⊣

Proposition 4.11 *Es sei $f : V \to W$ eine lineare Abbildung und $w \in W$. Ist dann $v \in V$ eine Lösung der Gleichung $f(x) = w$, so ist die Menge aller Lösungen genau $\{v + v' : v' \in \ker(f)\}$.*

Zum Beweis überlegt man sich, dass die Differenz zweier Lösungen jeweils im Kern der Abbildung liegen muss.

Mit $\mathrm{Bild}(f)$ bezeichnen wir die Menge $\{f(v) : v \in V\}$ mit $\mathrm{Bild}(f)$; sie heißt das **Bild** der Abbildung f. Dies ist ein Unterraum von W. Denn ist $u \in \mathrm{Bild}(f)$, so existiert ein $v \in V$ mit $f(v) = u$. Und damit ist $f(kv) = kf(v) = ku$, also ist $ku \in \mathrm{Bild}(f)$ für jedes Körperelement k. Ist ferner $u' \in \mathrm{Bild}(f)$ ein weiterer Bildvektor, so existiert ein $v' \in V$ mit $f(v) = u'$. Dann ist $f(v + v') = f(v) = f(v') = u + u'$, und so ist auch $u + u' \in \mathrm{Bild}(f)$.

Wir wählen nun eine Basis $C = \{c_i : i < p\}$ des Kerns von f. Diese erzeugt einen Unterraum von V, der auch echt sein kann. Ist f injektiv, dann ist $C = \emptyset$. Erzeugt C nicht schon V, so wählen wir noch Vektoren b_i, $i < q$, sodass $C \cup \{b_i : i < q\}$ eine Basis von V ist. Ich behaupte nun, dass die Menge $f[B] := \{f(b_i) : i < q\}$ erstens linear unabhängig ist und zweitens den Raum $\mathrm{Bild}(f)$ erzeugt.

Angenommen, $f[B]$ ist linear abhängig. Dann existieren Zahlen k_i, $i < q$, nicht alle gleich 0, derart, dass $\sum_{i<q} k_i f(b_i) = 0$. Dann ist

$$f(\sum_{i<q} k_i b_i) = \sum_{i<q} k_i f(b_i) = 0 \tag{4.16}$$

Es ist damit $\sum_{i<q} k_i b_i$ im Kern der Abbildung f, somit existieren ℓ_j, $j < p$, derart, dass

$$\sum_{i<q} k_i b_i = \sum_{j<p} \ell_j c_j \tag{4.17}$$

Und das bedeutet, dass

$$\sum_{i<q} k_i b_i - \sum_{j<p} \ell_j c_j = 0 \tag{4.18}$$

wobei nicht alle Zahlen = 0 sind. Das aber widerspricht der Voraussetzung, dass $B \cup C$ eine Basis ist.

Zweitens sei $u \in W$ eine Vektor in Bild(f). Dann existiert ein $v \in V$ mit $f(v) = u$. Ferner existieren Zahlen k_i, $i < q$ und ℓ_j, $j < p$, mit

$$v = \sum_{i<q} k_i b_i + \sum_{j<p} \ell_j c_j \tag{4.19}$$

Dann ist aber

$$u = f(v) = \sum_{i<q} k_i f(b_i) = \sum_{j<p} \ell_j f(c_j) = \sum_{i<q} k_i f(b_i) \tag{4.20}$$

Also ist u im Aufspann von $f[B]$. Ich formuliere dies nun für Vektorräume endlicher Dimension.

Satz 4.12 *Es sei $f : K^m \to K^n$. Dann ist m die Summe der Dimensionen von* ker(f) *und Bild*(f).

Der Witz ist, dass das Bild ja gar nicht Unterraum von V ist. Aber die Abbildung f ist auf dem Aufspann von B injektiv, und deswegen sind der Aufspann von B und sein Bild unter f isomorph.

Proposition 4.13 *Es seien $A = (a_{i,j})_{i<n,j<m}$ und $B = (b_{i,j})_{i<p,j<n}$ Matrizen für Abbildungen $f : K^m \to K^n$ und $g : K^n \to K^p$. Dann ist die Matrix der Abbildung $g \circ f : K^m \to K^p$ die Matrix $B \cdot A = (c_{i,k})_{i<p,k<m}$, wo*

$$c_{i,k} = \sum_{j<n} b_{i,j} a_{j,k} \tag{4.21}$$

Der Beweis ist nicht schwer. Zum Beispiel haben wir

$$\begin{aligned} & \begin{pmatrix} 2 & 1 & -3 \\ 1 & -1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 1 & 3 \\ -2 & 0 \end{pmatrix} \\ = & \begin{pmatrix} 2 \cdot 1 + 1 \cdot 1 + (-3) \cdot (-2) & 2 \cdot 2 + 1 \cdot 3 + (-3) \cdot 0 \\ 1 \cdot 1 + (-1) \cdot 1 + 4 \cdot (-2) & 1 \cdot 2 + (-1) \cdot 3 + 4 \cdot 0 \end{pmatrix} \\ = & \begin{pmatrix} 9 & 7 \\ -8 & -1 \end{pmatrix} \end{aligned} \tag{4.22}$$

Die Identitätsabbildung $K^m \to K^m$ besitzt in jeder Basis die folgende Gestalt. Es ist $E = (\delta_{i,j})_{i,j<m}$, wobei $\delta_{i,j} = 0$, falls $i \neq j$, und $\delta_{i,i} = 1$. Mit $m = 3$ haben wir zum Beispiel

$$E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{4.23}$$

Ob eine Abbildung $K^m \to K^m$ injektiv ist, kann man mit Hilfe der sogenannten Determinante prüfen. Ich definiere die Determinante induktiv über m. Sei $A = (a_{ij})_{i,j<m}$ eine Matrix. Wir schreiben A^{ij} für diejenige Matrix, die aus A durch Streichen der $i$ten Zeile und $j$ten Spalte entsteht. Also $A^{ij} = (b_{ij})_{i,j<m-1}$ mit

$$b_{p,q} = \begin{cases} a_{p,q} & \text{falls } p < i \text{ und } q < j \\ a_{p+1,q} & \text{falls } p \geq i \text{ und } q < j \\ a_{p,q+1} & \text{falls } p < i \text{ und } q \geq j \\ a_{p+1,q+1} & \text{falls } p \geq i \text{ und } q \geq j \end{cases} \tag{4.24}$$

Dann ist $\det(A)$ die sogenannte Determinante, definiert durch

1. $m = 1$ und $\det(A) = a_{00}$;
2. $m > 1$ und

$$\begin{aligned} \det(A) = a_{0,0} \det(A^{00}) - a_{1,0} \det(A^{10}) + a_{2,0} \det(A^{20}) \\ - \cdots + (-1)^{m-1} a_{m-1,0} \det(A^{m-1,0}) \end{aligned} \tag{4.25}$$

Die Determinante einer Matrix wird durch senkrechte Striche anstelle der runden Klammern gekennzeichnet. Sei also die folgende Matrix A gegeben.

$$A = \begin{pmatrix} 1 & 2 & 4 \\ 2 & 3 & 9 \\ 1 & 2 & 1 \end{pmatrix} \tag{4.26}$$

Dann ist $A^{0,0} = \begin{pmatrix} 3 & 9 \\ 2 & 1 \end{pmatrix}$, $A^{2,2} = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$ und $A^{0,1} = \begin{pmatrix} 2 & 9 \\ 1 & 1 \end{pmatrix}$. Damit berechnet sich die Determinante wie folgt.

$$\det(A) = 1 \cdot \det(A^{0,0}) - 2\det(A^{1,0}) + 1 \cdot \det(A^{2,0}) \tag{4.27}$$

$$\begin{aligned} \begin{vmatrix} 1 & 2 & 4 \\ 2 & 3 & 9 \\ 1 & 2 & 1 \end{vmatrix} &= 1 \begin{vmatrix} 3 & 9 \\ 2 & 1 \end{vmatrix} - 2 \begin{vmatrix} 2 & 4 \\ 2 & 1 \end{vmatrix} + 1 \begin{vmatrix} 2 & 4 \\ 3 & 9 \end{vmatrix} \\ &= (3 \cdot 1 - 2 \cdot 9) - 2(2 \cdot 1 - 2 \cdot 4) + 1(2 \cdot 9 - 3 \cdot 4) \\ &= (3 - 18) - 2(2 - 8) + (18 - 12) \\ &= (-15) + 12 + 6 \\ &= 3 \end{aligned} \tag{4.28}$$

Die Inverse zu einer Matrix ist dann wie folgt:

$$A^{-1} = \left(\frac{1}{\det A} (-1)^{i+k} \det(A^{ik}) \right)_{k,i<m} \tag{4.29}$$

Man beachte die Vertauschung von Zeilen und Spalten im Laufindex. Dies bedeutet, dass in Zeile i, Spalte k das Element $\frac{(-1)^{i+k}}{\det(A)} A^{ki}$ steht, also die Determinante, die durch Streichung der $k$ten Zeile und der $i$ten Spalte aus A hervorgeht. An einem Beispiel wird dies klar werden.

Dies führt im Falle der oben angegebenen Matrix zu folgender Inversen.

$$\frac{1}{3} \begin{pmatrix} + \begin{vmatrix} 3 & 9 \\ 2 & 1 \end{vmatrix} & - \begin{vmatrix} 2 & 4 \\ 2 & 1 \end{vmatrix} & + \begin{vmatrix} 2 & 4 \\ 3 & 9 \end{vmatrix} \\ - \begin{vmatrix} 2 & 9 \\ 1 & 1 \end{vmatrix} & + \begin{vmatrix} 1 & 4 \\ 1 & 1 \end{vmatrix} & - \begin{vmatrix} 1 & 4 \\ 2 & 9 \end{vmatrix} \\ + \begin{vmatrix} 2 & 3 \\ 1 & 2 \end{vmatrix} & - \begin{vmatrix} 1 & 2 \\ 1 & 2 \end{vmatrix} & + \begin{vmatrix} 1 & 2 \\ 2 & 3 \end{vmatrix} \end{pmatrix} = \frac{1}{3} \begin{pmatrix} -15 & 6 & 6 \\ 7 & -3 & -1 \\ 6 & 0 & -1 \end{pmatrix} \tag{4.30}$$

Damit kann man Folgendes festhalten. Eine Abbildung $\Re^m \to \Re^n$ ist genau dann bijektiv, wenn $m = n$, und wenn in diesem Fall die Determinante nicht Null ist. Dann bestimmt man die Matrix der Inversen Abbildung wie in (4.29).

Kapitel 5

Eigenwerte

Wie wir gesehen haben, kann man Matrizen auch multiplizieren. Denn wenn $f : K^n \to K^n$ eine lineare Abbildung mit Matrix A ist und $g : K^n \to K^p$ eine lineare Abbildung mit Matrix B, dann ist $g \circ f : K^m \to K^p$ eine lineare Abbildung mit Matrix $B \cdot A$, siehe Proposition 4.13.

Betrachten wir insbesondere den Fall, wo $m = n = p$ ist. Dann lassen sich je zwei Matrizen miteinander multiplizieren. Das Produkt ist auch distributiv: $A(B + C) = AB + AC$ sowie $(B + C)A = BA + CA$. Wir haben also folgendes Ergebnis.

Satz 5.1 *Die $n \times n$-Matrizen über einem Körper bilden einen Ring bezüglich der Addition und Multiplikation.*

Dieser ist nicht notwendig kommutativ.

$$\text{(5.1)} \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

Es gibt aber einen Sonderfall, den wir hier studieren wollen. Ausgangspunkt sei eine einzige quadratische Matrix A. Wir können jedem Polynom $p(x)$ eine Matrix $p(A)$ zuordnen, indem wir anstelle von der Unbekannten x die Matrix A einsetzen, und dann multiplizieren und addieren wie wir es von Matrizen gewohnt sind. Nehmen wir zum Beispiel das Polynom $p(x) = x^2 + x + 1$ und die Matrix

$$\text{(5.2)} \qquad A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

Dann ist

$$\text{(5.3)} \qquad p(A) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^2 + \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 0 & 3 \end{pmatrix}$$

Man beachte, dass der konstante Term a_0 eines Polynoms auch in der Form a_0x^0 geschrieben werden kann, und da A^0 gerade die Einheitsmatrix ist, entspricht diesem $a_0A^0 = a_0E$. Im allgemeinen Fall ist das Polynom von der Form

$$p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \tag{5.4}$$

und dann ist

$$p(A) = a_nA^n + a_{n-1}A^{n-1} + \cdots + a_1A + a_0E \tag{5.5}$$

Das Einsetzen in ein Polynom ist eine Abbildung von Polynomen in den Ring der quadratischen Matrizen über K. Es gilt

- $p(A) + q(A) = (p + q)(A)$.
- $p(A)q(A) = (pq)(A)$.

So ist etwa $x^2 + 2x + 1 = (x + 1)^2$. Und es ist $A^2 + 2A + E = (A + E)^2$, wie man leicht nachrechnet.

Ich weise noch darauf hin, dass das Polynom in (5.4) vom Grad n ist, wenn $a_n \neq 0$. Ist $a_n = 1$, so heißt das Polynom **normiert**. Polynome kann man wie Zahlen dividieren.

Satz 5.2 (Division von Polynomen) *Es sei $p(x)$ ein Polynom vom Grad n, $q(x)$ ein Polynom vom Grad $m < n$. Dann existiert ein Polynom $r(x)$ vom Grad $< m$ und ein weiteres Polynom $c(x)$ vom Grad $n - m$ mit $p(x) = c(x)q(x) + r(x)$.*

Betrachten wir nun das Bild dieser Einsetzungsfunktion: das heißt, betrachten wir die Menge aller Matrizen $p(A)$, wo p ein Polynom ist. Diese bilden einen Ring $R(A)$, der sogar kommutativ ist.

Die Frage, die in diesem Abschnitt behandelt werden soll ist:

Unter welchen Umständen ist $R(A)$ ein Körper?

Wir betrachten dazu alle Polynome q für die $q(A) = 0$ (die Nullmatrix). So etwas muss es geben, denn die Matrizen E, A, A^2 und so weiter können nicht alle linear unabhängig sein, der Vektorraum der quadratischen Matrizen hat die Dimension n^2. Ist $q(A) = 0$ und $r(A) = 0$, und hat r einen kleineren Grad als q, so können wir dividieren: Es gibt Polynome u und v mit $q(x) = u(x)r(x) + v(x)$, wobei der Grad von v kleiner als der von r ist. Ist nun v nicht das Nullpolynom, so haben wir jetzt ein noch kleineres Polynom gefunden, nämlich v, für das $v(A) = 0$.

Satz 5.3 *Es sei A eine quadratische Matrix. Dann existiert ein eindeutig bestimmtes normiertes Polynom $\mu_A(x)$ derart, dass $\mu_A(A) = 0$ und für alle $p(x)$ mit $p(A) = 0$ existiert ein $q(x)$ mit $p(x) = \mu_A(x)q(x)$. Das Polynom $\mu_A(x)$ heißt das **Minimalpolynom** von A.*

Beispiel 8. Die Einheitsmatrix erfüllt $E - E = 0$, ihr Minimalpolynom ist also $x - 1$. Betrachten we nun die folgenden Matrizen.

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{5.6}$$

$\mu_B(x) = x^2 - 1$, denn $B^2 = E$. $\mu_C(x) = x^2 - 2x + 1$. ⚽
Der Satz, auf den ich zusteuere, ist nun dieser:

Satz 5.4 *Genau dann ist $R(A)$ ein Körper, wenn das Minimalpolynom $\mu_A(x)$ von A unzerlegbar ist, das heißt, wenn es keine Polynome $p(x)$, $q(x)$, mindestens vom Grad 1 gibt, sodass $\mu_A(x) = p(x)q(x)$.*

Szenenwechsel. Es sei A eine $n \times n$-Matrix. Ein **Eigenvektor** von A ist ein Vektor v derart, dass eine Zahl λ existiert mit

$$Av = \lambda x \tag{5.7}$$

Dies bedeutet, dass Av eine Streckung von v ist. Es darf durchaus $\lambda = 0$ sein, was immer dann der Fall ist, wenn v im Kern der Abbildung liegt. Hier ist ein Beispiel.

$$\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix} \tag{5.8}$$

Hierbei ist $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ ein Eigenvektor zum Eigenwert.

Proposition 5.5 *Die Eigenvektoren zu einem gegebenen Eigenwert bilden einen Unterraum.*

Beweis. Ist $Av = \lambda v$ und $Av' = \lambda v'$, dann ist $A(v + v') = Av + Av' = \lambda v + \lambda v' = \lambda(v + v')$. Ebenso ist $A(kv) = k(Av) = k(\lambda v) = (k\lambda)v = (\lambda k)v = \lambda(kv)$. ⊣

Wir nun stellen die Gleichung etwas um

$$Av - \lambda v = 0 \tag{5.9}$$

Wir schmuggeln noch die Einheitsmatrix dazwischen und klammern aus:

$$(A - \lambda E)v = 0 \tag{5.10}$$

oder auch

$$(\lambda E - A)v = 0 \tag{5.11}$$

Offenkundig existiert genau dann ein Eigenvektor zum Eigenwert λ, wenn $\det \lambda E - A \neq 0$. Diese Determinante ist ein Polynom in λ. Machen wir dies am Beispiel der oberen Matrix klar.

$$\begin{vmatrix} \lambda & -2 \\ -2 & \lambda \end{vmatrix} = \lambda^2 - 4 \tag{5.12}$$

Dies Polynom besitzt die Nullstellen 2 und -2. Es sollte also auch ein Eigenvektor zum Eigenwert -2 existieren. In der Tat ist $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ ein solcher Vektor.

Definition 5.6 *Das **charakteristische Polynom** von A ist das (normierte) Polynom* $\det(xE - A)$ *und wird mit* $\gamma_A(x)$ *bezeichnet.*

(Bisher hatte ich λ geschrieben, aber das war nur der Name einer Variable, die ich jetzt x nenne.)

Die Eigenwerttheorie ist eine sehr interessante Theorie, weil sie viele wichtige Anwendungen besitzt. Der wichtigste Baustein ist der folgende Satz.

Satz 5.7 *A ist selbst eine Lösung des charakteristischen Polynoms.*

Mit anderen Worten: das Minimalpolynom teilt das charakteristische Polynom.

Dies erlaubt jetzt einen ganz neuen Blick auf unlösbare Gleichungen. Man nehme etwa $\lambda^2 = -1$. Eine Zahl, die dies erfüllt, ist eine Lösung der Gleichung $\lambda^2 + 1 = 0$. Es gibt eine Matrix, deren charakteristisches Polynom genau dieses ist, nämlich

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{5.13}$$

Denn

$$\begin{vmatrix} \lambda & -1 \\ 1 & \lambda \end{vmatrix} = \lambda^2 + 1 \tag{5.14}$$

Und in der Tat ist

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \tag{5.15}$$

Dies alles gilt nun ebenfalls in anderen Körpern. Nehmen wir als Beispiel $\mathbb{F}_3$. Da in diesem Körper $-1 \equiv 2$, vereinfacht sich (5.13) zu

$$\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \tag{5.16}$$

Betrachten nun die Struktur aller 2×2-Matrizen über $\mathbb{F}_3$, die wir aus (5.16) mit Hilfe von Addition, Subtraktion und Multiplikation erzeugen können. Dies sind insgesamt 9 Stück:

$$\begin{aligned} &0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad 2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \quad i = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \\ &2i = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \\ &1 + i = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} \quad 1 + 2i = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \quad 2 + i = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} \\ &2 + 2i = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix} \end{aligned} \tag{5.17}$$

Diese bilden nun einen Körper.

$+$	0	1	2	i	$2i$	$1+i$	$1+2i$	$2+i$	$2+2i$
0	0	1	2	i	$2i$	$1+i$	$1+2i$	$2+i$	$2+2i$
1	1	2	0	$1+i$	$1+2i$	$2+i$	$2+2i$	i	$2i$
2	2	0	1	$2+i$	$2+2i$	i	$2i$	$1+i$	$1+2i$
i	i	$1+i$	$2+i$	$2i$	0	$1+2i$	1	$2+2i$	2
$2i$	$2i$	$1+2i$	$2+2i$	0	i	1	$1+i$	2	$2+i$
$1+i$	$1+i$	$2+i$	i	$1+2i$	1	$2+2i$	2	$2i$	0
$1+2i$	$1+2i$	$2+2i$	$2i$	1	$1+i$	2	$2+i$	0	i
$2+i$	$2+i$	i	$1+i$	$2+2i$	2	$2i$	0	$1+2i$	1
$2+2i$	$2+2i$	$2i$	$1+2i$	2	$2+i$	0	i	1	$1+i$

$\cdot$	0	1	2	i	$2i$	$1+i$	$1+2i$	$2+i$	$2+2i$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	i	$2i$	$1+i$	$1+2i$	$2+i$	$2+2i$
2	0	2	1	$2i$	i	$2+2i$	$2+i$	$1+2i$	$1+i$
i	0	i	$2i$	2	1	$2+i$	$1+i$	$2+2i$	$1+2i$
$2i$	0	$2i$	i	1	2	$1+2i$	$2+2i$	$1+i$	$2+i$
$1+i$	0	$1+i$	$2+2i$	$2+i$	$1+2i$	$2i$	2	1	i
$1+2i$	0	$1+2i$	$2+i$	$1+i$	$2+2i$	2	i	$2i$	1
$2+i$	0	$2+i$	$1+2i$	$2+2i$	$1+i$	1	$2i$	i	2
$2+2i$	0	$2+2i$	$1+i$	$1+2i$	$2+i$	i	1	2	$2i$

Man mag die Axiome einzeln nachprüfen, es gibt jedoch schnellere Verfahren, um dies zu sehen. Denn die Elemente haben die Form $mE + nA$, wo A unsere Matrix ist. Dann ist die Addition einfach komponentweise Addition, und somit haben wir eine abelsche Gruppe bezüglich 0. Multiplikation erfolgt so:

$$(mE + nA)(m'E + n'A) = mm'E + mn'A + m'nA + nn'A^2 = (mm' + 2nn')E + (mn' + m'n)A \tag{5.18}$$

Damit zeigt man leicht, dass die Multiplikation stets assoziativ und kommutativ ist. Bei der Inversenbildung muss man allerdings ein wenig raten.

Nun also zum Beweis von Satz 5.4. Wir nehmen zunächst an, A ist eine Matrix mit Minimalpolynom $\mu_A(x)$, welches zerlegbar ist in $\mu_A(x) = p(x)q(x)$. Da $\mu_A(x)$ minimal ist, ist $p(A) \neq 0$ und $q(A) \neq 0$, aber $p(A)q(A) = \mu_A(A) = 0$. Und so gibt es zwei Elemente $C, D \in R(A)$, die nicht Null sind aber deren Produkt Null ist, nämlich $C = p(A)$ und $D = q(A)$. Dieser Ring kann kein Körper sein. Denn falls C ein Inverses besitzt, etwa F, also $CF = E$, so ist $D = DE = DCF = CDF = 0F = 0$ ($R(A)$ ist kommutativ!), was nicht sein kann.

Sei nun $\mu_A(x)$ unzerlegbar. Wir benötigen folgenden allgemeinen Satz.

Satz 5.8 *Es seien $p(x)$ und $q(x)$ Polynome mit größtem gemeinsamen Teiler $r(x)$. Dann existieren Polynome $a(x)$ und $b(x)$ derart, dass $r(x) = a(x)p(x) + b(x)q(x)$.*

Beweis. Ich werde den Beweis nicht mit Polynomen führen sondern mit Zahlen. Die Lösung besteht in einem Algrotihmus genannt Erweiterter Euklidischer Algorithmus. Wir bestimmen damit zunächst ein größten gemeinsamen Teiler. Gegeben seien Zahlen a_0 und a_1. Wir dividieren mit Rest: $a_0 = c_0a_1 + a_2$, $a_1 = c_1a_2 + a_3$, $a_2 = c_2a_3 + a_4$, und so weiter, bis wir bekommen $a_n = c_na_{n+1} + a_{n+2}$ und $a_{n+1} = c_{n+1}a_{n+2}$. Dann ist offenkundig a_{n+2} der größte gemeinsame Teiler, und wir haben $a_{n+2} = a_n - c_na_{n+1}$. Da ferner $a_{n+1} = a_{n-1} - c_{n-1}a_n$, so setzen wir dies ein und bekommen $a_{n+2} = a_n - c_n(a_{n-1} - c_{n-1}a_n) = a_n(1 + c_nc_{n-1}) - a_{n-1}c_n$. Wir ersetzen jetzt a_n durch eine Kombination aus a_{n-1} und a_{n-2}, und so weiter. ⊣

Sei $C \in R(A)$, also $C = p(A)$ für ein Polynom $p(x)$. Dann ist der größte gemeinsame Teiler von $p(x)$ und $\mu_A(x)$ das Polynom 1, denn $\mu_A(x)$ besitzt keine Teiler kleineren Grades außer den konstanten Polynomen. Somit existieren Polynome $a(x)$ und $b(x)$ mit $1 = a(x)\mu_A(x) + b(x)p(x)$. Dann ist $D := b(A)$ die gesuchte Inverse. Denn $CD = p(A)b(A) = E - a(A)\mu_A(A) = E - a(A)0 = E$.

Übungen

Übung 13. Bestimmen Sie das Minimalpolynom der Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Übung 14. Bestimmen Sie das charakteristische Polynom und die Eigenwerte der folgenden Abbildung über $\mathbb{F}_5$.

$$\begin{pmatrix} 1 & 0 & 3 \\ 2 & 1 & 1 \\ 4 & 1 & 0 \end{pmatrix}$$

Hinweis. Die Nullstellen eines Polynoms kann man durch Ausprobieren finden.

Übung 15. Der Körper der komplexen Zahlen ist isomorph zu dem Körper der reellen Matrizen der Form $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

1. Wie sieht dieser Isomorphismus aus, dh welcher komplexen Zahl entspricht die angegeben Matrix?
2. Wie kann man diesen Sachverhalt ohne Mühe zeigen?

Teil II

Ordnungen und Verbände

Kapitel 6

Partielle Ordnungen

Definition 6.1 (Partielle Ordnung) *Es sei M eine nichtleere Menge und $\leq$ eine zweistellige Relation auf M. $\leq$ heißt **partielle Ordnung**, falls $\leq$ reflexiv, transitiv und antisymmetrisch ist. Dabei ist $\leq$ **reflexiv** falls $x \leq x$ für alle $x \in M$, **transitiv** falls aus $x \leq y$ und $y \leq z$ schon $x \leq z$ folgt für alle $x, y, z \in M$, und $\leq$ heißt **antisymmetrisch**, falls aus $x \leq y$ und $y \leq x$ folgt $x = y$, für alle $x, y \in M$. Das Paar $\langle M, \leq \rangle$ heißt dann eine **partiell geordnete Menge** (Englisch **partially ordered set**, kurz **poset**). $\langle M, \leq \rangle$ und $\langle N, \leq' \rangle$ heißen **isomorph**, falls es eine Abbildung $g : M \to N$ gibt, welche bijektiv ist, und für die gilt $g(x) \leq' g(y)$ gdw. $x \leq y$, für alle $x, y \in M$. g heißt dann ein **Isomorphismus** von $\langle M, \leq \rangle$ auf $\langle N, \leq' \rangle$.*

Es sei nur kurz erwähnt, dass die Eigenschaft der Antisymmetrie etwas anderes ist als die der Asymmetrie (welche nichts weiter ist als die Nicht-Symmetrie). Die Diagonale $\Delta_M := \{\langle x, x \rangle : x \in M\}$ ist eine partielle Ordnung, insbesondere ist sie Antisymmetrisch; aber sie ist auch Symmetrisch.

In Figur 6 haben wir zwei Beispiele von partiell geordneten Mengen. Die Darstellung ist wie folgt. Eine Linie zwischen zwei Knoten, sagen wir a und b, zeigt an, dass $a < b$, was bedeutet, dass $a \leq b$ aber nicht $b \leq a$. Und zwar ist $b \not\leq a$, weil b höher ist als a. Da zwischen b und c keine Linie läuft, ist weder $c \leq d$ noch $d \leq c$. Die Linien zeigen nur unmittelbare Nachbarschaft an. Es gilt $a \leq d$, weil eine Linie von a nach b geht und eine Linie von b nach d. Diese Ordnung ist also transitiv und reflexiv nach Konstruktion. Dass sie antisymmetrisch ist, folgt daraus, dass die Linien stets echt aufsteigend sind. Haben wir $x \leq y$ und $y \leq x$, so sind x und y "auf gleicher Höhe". Dies ist ausgeschlossen.

Definition 6.2 (Infimum, Supremum) *Es sei $\langle M, \leq \rangle$ eine partiell geordnete Menge und $X \subseteq M$. y heißt **obere Schranke von** X, falls $x \leq y$ für alle $x \in X$. y heißt*

Abbildung 6.1: Partiell geordnete Mengen

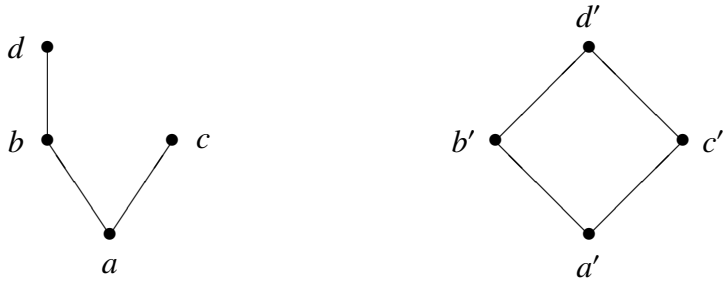
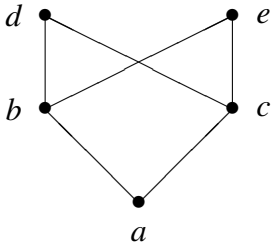


Abbildung 6.2: Kein Verband



untere Schranke von *X, falls* $y \leq x$ *für alle* $x \in X$*. Falls ein eindeutig bestimmtes* $y \in M$ *existiert, sodass* $y \leq z$ *gilt für jede obere Schranke z von X, so heißt y das* ***Supremum*** *von X, in Zeichen* $\sup_{\leq} X$*. Falls ein eindeutig bestimmtes u existiert, sodass* $z \leq u$ *gilt jede untere Schranke z von X, so heißt u das* ***Infimum*** *von X, in Zeichen* $\inf_{\leq} X$*. Ist die Ordnung aus dem Kontext klar, schreiben wir auch* $\inf X$ *statt* $\inf_{\leq} X$ *und* $\sup X$ *statt* $\sup_{\leq} X$*.* $\leq$ *heißt eine* ***Verbandsordnung****, falls* $\sup X$ *und* $\inf X$ *existieren für alle endlichen nichtleeren* $X \subseteq M$*.*

Ein anderer Name für Supremum ist **kleinste obere Schranke**; ein anderer Name für Infimum ist **größte untere Schranke**. Betrachten wir noch einmal die Figur 6. Die linke Menge hat keine Verbandsordnung. Denn es gibt kein Supremum für $\{b, c\}$ oder $\{d, c\}$. Die rechte Menge hat allerdings ein Verbandsordnung. Zum Beispiel ist $\sup_{\leq}\{b', c'\} = d'$. Figur 6 sehen wir eine andere partiell geordnete Menge, die keine Verbandsordnung hat. Denn die Menge $\{b, c\}$ hat zwei obere Schranken, d and e. Es existiert aber keine kleinste obere Schranke.

Es gibt zwei Sonderfälle, die wir betrachten müssen. Der erste ist der einer einelementigen Teilmenge $X = \{x\}$. Hier ist y genau dann eine oberer Schranke von X, wenn $y \geq x$, und so ist x die kleinste obere Schranke. Diese existiert also immer. Ebenso ist x auch die größte untere Schranke. Der zweite Fall ist $X = \emptyset$. Jedes Element ist eine obere Schranke von der leeren Menge (es gibt nämlich keine Bedingung zu erfüllen). Eine kleinste obere Schranke existiert also immer dann, wenn die Ordnung $\leq$ ein kleinstes Element besitzt. Da man die Existenz von kleinsten bzw. größten Elementen nicht voraussetzen möchte, habe ich in der Definition eine entsprechende Klausel eingebaut.

Beispiele für Verbandsordnungen.

Beispiel 9. Es sei M die Menge aller natürlichen Zahlen mit der üblichen Ordnung $\leq$. Dies ist eine partielle Ordnung. Ferner ist $\inf X$ schlicht das Minimum aller Elemente aus X, $\sup X$ (für endliches X) stets das Maximum aller Elemente aus X. Wir sehen hier auch gleich, dass Suprema unendlicher Mengen nicht existieren müssen, selbst wenn Suprema aller endlichen nichtleeren Mengen existieren; denn M hat kein Supremum. (Es gibt keine größte natürliche Zahl. $\emptyset$ hat aus demselben Grund übrigens auch kein Infimum, weil es kein größtes Element gibt. ⚽

Beispiel 10. Sei Q eine Menge. Dann ist $\subseteq$ eine Verbandsordnung auf $\wp(Q)$, der Potenzmenge von Q. Ist nämlich $X = \{P_1, P_2, \ldots, P_n\}$, so ist

$$\begin{aligned} \inf X &= P_1 \cap P_2 \cap \ldots \cap P_n \\ \sup X &= P_1 \cup P_2 \cup \ldots \cup P_n \end{aligned}$$

⚽

Beispiel 11. Es sei M die Menge der natürlichen Zahlen ohne die Null. Diesmal betrachten wir die Ordnung $|$, die Teilbarkeitsrelation. $m \mid n$ bedeutet, dass m n teilt. Dies ist eine partielle Ordnung und $\inf X$ ist der ggT von X (größter gemeinsamer Teiler) und $\sup X$ das kgV von X (kleinstes gemeinsames Vielfaches). ⚽

Es ist klar, dass wenn $\langle P, \leq \rangle$ eine Verbandsordnung ist und $\langle Q, \leq' \rangle$ isomorph zu $\langle P, \leq \rangle$, so ist auch $\langle Q, \leq' \rangle$ eine Verbandsordnung.

Satz 6.3 *Genau dann ist $\leq$ eine Verbandsordnung auf M, falls Infima und Suprema von zweielementigen Mengen existieren. Ist nämlich $X = \{x_1, x_2, \ldots, x_n\}$, so*

$$\begin{aligned} \sup X &= \sup\{x_n, \sup\{x_{n-1}, \ldots, \sup\{x_2, x_1\}\ldots\}\} \\ \inf X &= \inf\{x_n, \inf\{x_{n-1}, \ldots, \inf\{x_2, x_1\}\ldots\}\} \end{aligned}$$

Beweis. Die Behauptung folgt mittels Induktion aus folgenden zwei Tatsachen: $\sup\{x\} = x$ und $\sup\{x, \sup Y\} = \sup\{x\} \cup Y$. Ersteres ist leicht zu sehen. Wir zeigen die zweite Behauptung. Sei $u \geq \sup\{x, \sup Y\}$. Dann ist $u \geq x$ und $x \geq \sup Y$ und so für jedes $y \in Y$: $u \geq y$. Daraus folgt sofort $u \geq z$ für jedes $z \in \{x\} \cup Y$, also $u \geq \sup(\{x\} \cup Y)$. Nun sei umgekehrt $u \geq \sup(\{x\} \cup Y)$. Dann ist $u \geq y$ für jedes $y \in Y$, also $u \geq \sup Y$. Da auch $u \geq x$, so ist $u \geq \sup\{x, \sup Y\}$. Dies zeigt, dass $\sup\{x, \sup Y\} = \sup(\{x\} \cup Y)$. Analog für Infima. ⊣

Satz 6.4 *Es gelten folgende Gesetze*

$$\begin{array}{lcllcl} \sup\{x, \sup\{y, z\}\} & = & \sup\{\sup\{x, y\}, z\} & \inf\{x, \inf\{y, z\}\} & = & \inf\{\inf\{x, y\}, z\} \\ \sup\{x, x\} & = & x & \inf\{x, x\} & = & x \\ \sup\{x, \inf\{x, y\}\} & = & x & \inf\{x, \sup\{x, y\}\} & = & x \end{array}$$

Beweis. Aus dem vorigen Satz folgt unmittelbar, dass $\sup\{x, \sup\{y, z\}\} = \sup\{x, y, z\}$ sowie $\sup\{z, \sup\{x, y\}\} = \sup\{x, y, z\}$, und so ist das erste Gesetz bewiesen. Ebenso das zweite Gesetz. Gewiss ist $\sup\{x, x\} = \sup\{x\} = x$ und $\inf\{x, x\} = \inf\{x\} = x$. Die letzten beiden Gesetze sieht man so. Es ist $x \geq \inf\{x, y\}$. Also ist $\sup\{x, \inf\{x, y\}\} = x$. Ferner ist $x \leq \sup\{x, y\}$ und so $x = \inf\{x, \sup\{x, y\}\}$. ⊣

Satz 6.5 (Dualitätsprinzip) *Es sei $\mathfrak{M} = \langle M, \leq\rangle$ eine partielle Ordnung. Dann ist auch $\mathfrak{M}^{op} := \langle M, \geq\rangle$ eine partielle Ordnung. Wir nennen $\mathfrak{M}^{op}$ die zu $\mathfrak{M}$* ***duale Ordnung****. Ist ferner $\leq$ eine Verbandsordnung auf M, so auch $\geq$. Ferner ist*

$$\begin{aligned} \inf_{\geq} X &= \sup_{\leq} X \\ \sup_{\geq} X &= \inf_{\leq} X \end{aligned}$$

Beweis. Ist $x \leq x$ für alle x, so auch $x \geq x$. Ist $x \geq y$ und $y \geq z$, so $z \leq y$ und $y \leq x$, also $z \leq x$, was nichts anderes ist als $x \geq z$. Endlich sei $x \geq y$ und $y \geq x$. Dann $x \leq y$ und $y \leq x$, und so $x = y$. Nun zum zweiten Teil. Es sei $\leq$ eine Verbandsordnung. Sei ferner X eine endliche Teilmenge von M. Dann existiert $z := \sup_{\leq} X$. Es sei $u \geq x$ für alle $x \in X$. Dann $x \leq u$ für alle $x \in X$. Daraus folgt $z \leq u$. Also $u \geq z$. Dies bedeutet $z = \inf_{\geq} X$. Analog zeigt man das zweite Gesetz. ⊣

Definition 6.6 (Verband) *Es sei V eine nichtleere Menge und $\sqcap$ und $\sqcup$ zweistellige Operationen auf V. Das Tripel $\langle V, \sqcap, \sqcup\rangle$ heißt **Verband**, falls folgende Gesetze gelten für alle $x, y, z \in V$.*

$$\begin{array}{lcllcl} x \sqcap (y \sqcap z) & = & (x \sqcap y) \sqcap z & x \sqcup (y \sqcup z) & = & (x \sqcup y) \sqcup z \\ x \sqcap y & = & y \sqcap x & x \sqcup y & = & y \sqcup x \\ x \sqcap x & = & x & x \sqcup x & = & x \\ x \sqcap (y \sqcup x) & = & x & x \sqcup (y \sqcap x) & = & x \end{array}$$

Satz 6.7 *1. Es sei $\leq$ eine Verbandsordnung auf M. Setze $x \sqcup y := \sup_{\leq}\{x, y\}$ und $x \sqcap y := \inf_{\leq}\{x, y\}$. Dann ist $\langle M, \sqcap, \sqcup\rangle$ ein Verband.*

2. Es sei $\langle V, \sqcap, \sqcup\rangle$ ein Verband. Setze $x \leq y :\Leftrightarrow x \sqcap y = x$. Dann ist $x \leq y$ genau dann, wenn $x \sqcup y = y$, und $\leq$ ist eine Verbandsordnung auf V. Ferner ist $\sup_{\leq}\{x, y\} = x \sqcup y$ und $\inf_{\leq}\{x, y\} = x \sqcap y$.

Beweis. Der erste Teil ist klar wegen Satz 6.4. Nun zum zweiten Teil. Sei $x \sqcap y = x$. Dann ist $x \sqcup y = (x \sqcap y) \sqcup y = y \sqcup (x \sqcap y) = y$. Ist umgekehrt $x \sqcup y = y$, dann ist $x \sqcap y = x \sqcap (x \sqcup y) = x \sqcap (y \sqcup x) = x$. Wir zeigen nun, dass $\leq$ eine Verbandsordnung ist. (Reflexivität) Da $x \sqcap x = x$, ist $x \leq x$. (Transitivität) Sei $x \leq y$ und $y \leq z$. Dann ist $x \sqcap y = x$ und $y \sqcap z = y$. Daraus folgt $x \sqcap z = (x \sqcap y) \sqcap z = x \sqcap (y \sqcap z) = x \sqcap y = x$. Also ist $x \leq z$. (Antisymmetrie) Sei $x \leq y$ und $y \leq x$. Dann ist $x \sqcap y = x$ und $y \sqcap x = y$. Aber $x \sqcap y = y \sqcap x$; also $x = y$. Also ist $\leq$ eine partielle Ordnung. Es bleibt zu zeigen, dass $\leq$ eine Verbandsordnung ist. Es genügt, die Existenz von Suprema und Infima zweielementiger Mengen nachzuweisen. Wir behaupten nun, dass $\inf_{\leq}\{x, y\} = x \sqcap y$ ist und $\sup_{\leq}\{x, y\} = x \sqcup y$. Sei nämlich $z \geq x$ und $z \geq y$, also $x \sqcup z = z$ sowie $y \sqcup z = z$. Dann ist $x \sqcup y \leq z$, denn $(x \sqcup y) \sqcup z = x \sqcup (y \sqcup z) = x \sqcup z = z$. ⊣

Es besteht also eine eineindeutige Korrespondenz zwischen Verbandsordnungen und Verbänden. Man mache sich dies anhand der Beispiele 9 – 11 klar. Ich mache darauf aufmerksam, dass Folgendes gilt.

$$\begin{array}{lll} x \geq (y \sqcup z) & \text{gdw.} & x \geq y \text{ und } x \geq z \\ x \leq (y \sqcap z) & \text{gdw.} & x \leq y \text{ und } x \leq z \end{array}$$

Ferner ist $x \leq x \sqcup y$ und $x \geq x \sqcap y$, wie man leicht sieht. Auch nützlich ist folgendes Gesetz. Ist $x \leq y$, so $x \sqcup z \leq y \sqcup z$ und $x \sqcap z \leq y \sqcap z$. Nämlich, aus $x \leq y$ folgt $x \leq y \sqcup z$. Ferner ist ja $z \leq y \sqcup z$. Also $x \sqcup z \leq y \sqcup z$. Analog zeigt man, dass aus $x \leq y$ folgt $x \sqcap z \leq y \sqcap z$.

Satz 6.8 (Dualitätsprinzip) *Es sei* $\mathfrak{V} = \langle V, \sqcap, \sqcup \rangle$ *ein Verband. Dann ist auch* $\mathfrak{V}^{op} := \langle V, \sqcup, \sqcap \rangle$ *ein Verband. Wir nennen* $\mathfrak{V}^{op}$ *den zu* $\mathfrak{V}$ ***dualen Verband****. Die Ordnung zu* $\mathfrak{V}^{op}$ *ist die Duale Ordnung zu der Ordnung von* $\mathfrak{V}$.

Das Dualitätprinzip kann man wie folgt ausbeuten. Sei α eine Aussage über Verbände. Es gehe α^{op} aus α durch Austauschen von $\sqcap$ und $\sqcup$, sowie $\leq$ und $\geq$ hervor. Dann ist α^{op} in allen Verbänden gültig genau dann wenn α in allen Verbänden gültig ist. Wir werden allerdings nicht näher präzisieren, was eine Aussage über Verbände ist. Dies sei eine jede sinvolle Aussage, welche außer logischen Symbolen noch $\sqcap$, $\sqcup$, $\leq$ und $\geq$ gebraucht. Zum Beweis muss man sich nur klarmachen, dass man eben (dank der Dualität) $\sqcap$ wahlweise auch als $\sqcup$ interpretieren darf, nur muss dann $\sqcup$ als $\sqcap$ und $\leq$ als $\geq$ interpretiert werden. Wir geben ein Beispiel. Die Aussage

$$(\forall xyz)((x \sqcap y) \sqcup (x \sqcap z) \leq x \sqcap (y \sqcup z))$$

ist in allen Verbänden gültig. Daher ist auch die Aussage

$$(\forall xyz)((x \sqcup y) \sqcap (x \sqcup z) \geq x \sqcup (y \sqcap z))$$

in allen Verbänden gültig.

Definition 6.9 (Verbandshomomorphismus) *Es seien* $\mathfrak{V} = \langle V, \sqcap, \sqcup \rangle$ *und* $\mathfrak{W} = \langle W, \sqcap', \sqcup' \rangle$ *Verbände, und* $h : V \to W$ *eine beliebige Abbildung.* h *heißt* ***Homomorphismus*** *von* $\mathfrak{V}$ *nach* $\mathfrak{W}$*, in Zeichen* $h : \mathfrak{V} \to \mathfrak{W}$*, falls für alle* $x, y \in V$ *gilt*

$$\begin{aligned} h(x \sqcap y) &= h(x) \sqcap' h(y) \\ h(x \sqcup y) &= h(x) \sqcup' h(y) \end{aligned}$$

h *heißt* ***Isomorphismus****, falls* h *bijektiv ist.* h *heißt* ***Endomorphismus****, falls* $\mathfrak{V} = \mathfrak{W}$*, und* ***Automorphismus****, falls* h *sowohl Endomorphismus ist wie auch Isomorphismus.*

Wir merken folgen Tatsache an.

Satz 6.10 *Es seien* $\mathfrak{V} = \langle V, \sqcap, \sqcup \rangle$ *und* $\mathfrak{W} = \langle W, \sqcap', \sqcup' \rangle$ *Verbände und* $h : V \to W$*. Genau dann ist* h *ein Isomorphismus, wenn* h *ein Isomorphismus von* $\langle V, \leq \rangle$ *auf* $\langle W, \leq' \rangle$ *ist.* $\mathfrak{V}$ *ist genau dann zu* $\mathfrak{W}$ *isomorph, wenn* $\langle V, \leq \rangle$ *zu* $\langle W, \leq' \rangle$ *isomorph ist.*

Daher stellt man einen konkreten Verband niemals in Form von Operationstafeln dar. Dies ist im allgemeinen nämlich unübersichtlich. Stattdessen gibt man den Ordnungstyp des Verbands an.

Übungen.

Übung 16. Es sei M eine Menge und $\Pi \subseteq \wp(M)$. Π heißt **Partition** von M, falls (i) $\emptyset \notin \Pi$, (ii) für $S, T \in \Pi$ und $S \neq T$ gilt $S \cap T = \emptyset$, (iii) die Vereinigung aller Mengen aus Π ist M. (Beispiel. $\{\{a\}, \{b, d\}, \{c, e, f\}\}$ ist eine Partition der Menge $\{a, b, c, d, e, f\}$.) Π heißt **feiner** als Σ, falls zu jeder Menge $S \in \Pi$ eine Menge $T \in \Sigma$ existiert mit $S \subseteq T$. Sei $\Pi \leq \Sigma$ falls Π feiner ist als Σ. Sei $\Pi(M)$ die Menge aller Partitionen auf M. Diese sind durch $\leq$ partiell geordnet. (Dies müssen Sie hier nicht zeigen.) Zeichnen Sie $\langle \Pi(M), \leq \rangle$ für $M = \{1, 2, 3, 4\}$.

Übung 17. Eine zweistellige Relation $\sim$ heißt **symmetrisch**, falls aus $x \sim y$ folgt $y \sim x$ für alle $x, y \in M$. $\sim$ heißt **Äquivalenzrelation**, falls $\sim$ reflexiv, symmetrisch und transitiv ist. Sei $A(M)$ die Menge der Äquivalenzrelationen auf M. Zeigen Sie: $\langle \Pi(M), \leq \rangle$ ist isomorph zu $\langle A(M), \subseteq \rangle$. Zeigen Sie so, dass $\langle \Pi(M), \leq \rangle$ eine partiell geordnete Menge ist. *Hinweis.* Ist Π eine Partition, setze $x \sim_\Pi y$ gdw. ein $T \in \Pi$ existiert mit $x, y \in T$. Ist umgekehrt $\approx$ eine Äquivalenzrelation, so sei $[x] = \{y : x \approx y\}$ und $\Pi_\approx := \{[x] : x \in M\}$.

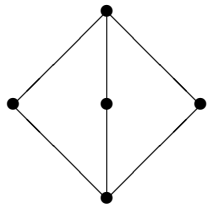
Übung 18. Es sei $\leq$ eine partielle Ordnung auf M. $\leq$ heißt **linear**, falls für je zwei Elemente $x, y \in M$ gilt $x \leq y$ oder $y \leq x$. Zeigen Sie: eine lineare partielle Ordnung ist eine Verbandsordnung.

Übung 19. Es sei $P := \{2^i : i \in \mathbb{N}\}$, und $|$ die Teilbarkeitsrelation (also $m \mid n$ genau dann, wenn ein k existiert mit $mk = n$). Zeigen Sie, dass $\langle P, | \rangle$ isomorph zu $\langle \mathbb{N}, \leq \rangle$ ist.

Übung 20. Zeigen Sie, dass in allen Verbänden gilt

$$(\forall xyz)((x \sqcap y) \sqcup (x \sqcap z) \leq x \sqcap (y \sqcup z))$$

Übung 21. Bestimmen Sie alle Automorphismen des folgenden Verbandes.



Kapitel 7

Distributive Verbände

Ein Element x eines Verbandes $\langle V, \sqcap, \sqcup \rangle$ heißt ein **minimales Element** oder eine **Null**, falls $x \leq y$ für alle $y \in V$. x heißt ein **maximales Element** oder eine **Eins**, falls $x \geq y$ für alle $y \in V$. Es muß weder eine Null noch eine Eins geben; falls es sie gibt, sind sie jeweils eindeutig bestimmt. Man notiert die Null mit 0 oder $\bot$, die Eins mit 1 oder $\top$. Es gilt stets $x \sqcap 1 = x$ und $x \sqcup 0 = x$. Ist X eine beliebige endliche Teilmenge von V, so sei $\bigsqcap X := \inf X$ und $\bigsqcup X := \sup X$. Es ist leicht zu sehen, dass in einem endlichen Verband $\bigsqcap V$ eine Null und $\bigsqcup V$ eine Eins ist.

Satz 7.1 *Ein endlicher Verband hat stets eine Null und eine Eins.*

Hat $\mathfrak{V}$ eine Eins, so ist, wie wir schon gesehen haben, $\inf \varnothing = 1$; hat $\mathfrak{V}$ eine Null, so ist $\sup \varnothing = 0$. Da wir allerdings die Existenz von $\inf \varnothing$ bzw. $\sup \varnothing$ nicht vorausgesetzt hatten, können wir die Existenz einer Null und einer Eins nicht generall annehmen.

Definition 7.2 *Ein Verband heißt **distributiv**, falls für alle $x, y, z \in V$ gilt*

$$\begin{array}{lrcl} (d\sqcup) & x \sqcap (y \sqcup z) & = & (x \sqcap y) \sqcup (x \sqcap z) \\ (d\sqcap) & x \sqcup (y \sqcap z) & = & (x \sqcup y) \sqcap (x \sqcup z) \end{array}$$

Zunächst einmal gilt in *jedem* Verband

$$\begin{aligned} x \sqcap (y \sqcup z) \geq & (x \sqcap y) \sqcup (x \sqcap z) \\ x \sqcup (y \sqcap z) \leq & (x \sqcup y) \sqcap (x \sqcup z) \end{aligned}$$

Zum Beispiel gilt die zweite Behauptung. Denn es ist $x \leq x \sqcup y$ und $x \leq x \sqcup z$, also $x \leq (x \sqcup y) \sqcap (x \sqcup z)$. Ebenso sieht man $y \sqcap z \leq (x \sqcup y) \sqcap (x \sqcup z)$. Daraus folgt dann $x \sqcup (y \sqcap z) \leq (x \sqcup y) \sqcap (x \sqcup z)$.

Die Distributivität gilt also schon dann, wenn wir fordern, dass

$$x \sqcap (y \sqcup z) \leq (x \sqcap y) \sqcup (x \sqcap z)$$
$$x \sqcup (y \sqcap z) \geq (x \sqcup y) \sqcap (x \sqcup z)$$

Man kann zeigen, dass jeweils eine der beiden Forderungen die andere impliziert. Gelte etwa die erste Ungleichung, also de facto die Gleichung (d⊔). Die Gleichung (d⊓) leiten wir dann wie folgt ab.

$$\begin{aligned} & (x \sqcup y) \sqcap (x \sqcup z) \\ = \; & ((x \sqcup y) \sqcap x) \sqcup ((x \sqcup y) \sqcap z) \\ = \; & x \sqcup ((x \sqcup y) \sqcap z) \\ = \; & x \sqcup ((x \sqcap z) \sqcup (y \sqcap z)) \\ = \; & (x \sqcup (z \sqcap x)) \sqcup (y \sqcap z) \\ = \; & x \sqcup (y \sqcap z) \end{aligned}$$

Dabei haben wir zweimal das Distributivgesetz (d⊔) verwendet. Das Dualitätsprinzip sagt uns, dass (d⊔) seinerseits aus (d⊓) folgt.

Ich gebe nun ein allgemeines Verfahren an, wie man distributive Verbände basteln kann und zeige anschließend, dass man über dieses Verfahren zumindest alle endlichen distributiven Verbände bekommt.

Beispiel 12. Es sei X eine Menge, und $\wp(X)$ die Potenzmenge von X. Dann ist $\langle \wp(X), \cap, \cup \rangle$ ein distributiver Verband. $\varnothing$ ist darin eine Null, X eine Eins. Dies ist der **Potenzmengenverband** von X. (Der Beweis dieser Tatsache erfolgte in Formale Methoden 1.) ⚽

Beispiel 13. Es sei n eine natürliche Zahl, und $T(n)$ die Menge der Teiler von n. Dann ist $\langle T(n), \mathrm{ggT}, \mathrm{kgV} \rangle$ ein distributiver Verband, mit 1 als Null (!) und n als Eins. (Dies muss natürlich noch gezeigt werden.) Man beachte, dass $x \leq y$ gilt gdw. x ein Teiler von y ist, was wir auch $x \mid y$ schreiben. Wir nennen dies den **Teilerverband** von n. ⚽

Beispiel 14. Es sei $\mathfrak{P} = \langle P, \leq \rangle$ eine partiell geordnete Menge. Ist $S \subseteq P$, so setze

$$\begin{aligned} \downarrow S &:= \{y : (\exists x \in S)(y \leq x)\} \\ \uparrow S &:= \{y : (\exists x \in S)(y \geq x)\} \end{aligned}$$

Ist $S = \downarrow S$, so heißt S **nach unten abgeschlossen**. Mit anderen Worten, ist $S = \downarrow S$, so folgt aus $x \in S$ und $y \leq x$, dass auch $y \in S$ ist. Man kann nun leicht

zeigen, dass der Schnitt und die Vereinigung zweier nach unten abgeschlossener Mengen wieder nach unten abgeschlossen ist. Seien nämlich S und T nach unten abgeschlossen und $x \in S \cap T$. Es ist zu zeigen, dass für jedes $y \leq x$ auch $y \in S \cap T$ ist. Nach Voraussetzung ist nun aber $x \in S$, und so $y \in S$; ebenfalls ist $x \in T$ und so $y \in T$. Daher $y \in S \cap T$. Ferner, falls $x \in S \cup T$, etwa $x \in S$, und $y \leq x$, so ist $y \in S$, also $y \in S \cup T$. Analog falls $x \in T$. Sei $L(\mathfrak{P})$ die Menge der nach unten abgeschlossenen Mengen. Dann ist $\mathfrak{Vb}(\mathfrak{P}) := \langle L(\mathfrak{P}), \cap, \cup\rangle$ ein distributiver Verband. ⚽

Wir werden nun in dem verbleibenden Teil dieses Kapitels zeigen, dass alle endlichen distributiven Verbände die in Beispiel 14 gegebene Form haben. Jeder endliche distributive Verband ist somit isomorph zu einem Verband der Form $\mathfrak{Vb}(\mathfrak{P})$ für eine partiell geordnete Menge $\mathfrak{P}$ (Satz 7.9).

Definition 7.3 (Irreduzible Elemente) *Es sei $\mathfrak{V} = \langle V, \sqcap, \sqcup\rangle$ ein Verband. $x \in V$ heißt $\sqcup$-**irreduzibel** oder schlicht **irreduzibel**, falls x keine Null ist und aus $x = y \sqcup z$ folgt $x = y$ oder $x = z$. Dual heißt x $\sqcap$-**irreduzibel**, falls x keine Eins ist und aus $x = y \sqcap z$ folgt $x = y$ oder $x = z$.*

Sei x ein Element und y derart, dass $y < x$ aber kein z existiert mit $y < z < x$. In diesem Fall sagen wir, y sei ein **unterer Nachbar** von x und x sei **oberer Nachbar** von y und schreiben $y \prec x$.

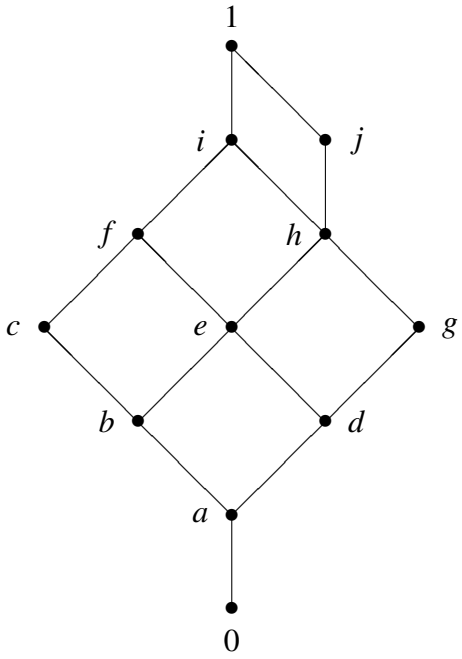
Hilfssatz 7.4 *Sei $\mathfrak{V}$ ein endlicher Verband. Ist $u < x$, so existiert ein unterer Nachbar $y \prec x$ mit $y \leq x$. Ebenso existiert ein oberer Nachbar v von u mit $u \prec v \leq x$.*

Beweis. Wir betrachten die Menge $M := \{z : u \leq z < x\}$. Diese Menge ist nicht leer, da $u \in M$. Ist $M = \{u\}$, so ist u bereits unterer Nachbar von x. Falls nicht, so existiert $u' \in M$ mit $u' \neq u$. Wir haben jetzt $u < u' < x$. Jetzt setzen wir $M' := \{z : u' \leq z < x\}$. Es ist $|M'| < |M|$. Ist $|M'| = 1$, also $M' = \{u'\}$, so ist u' unterer Nachbar von x. Falls nicht, so existiert ein $u'' \in M'$ mit $u'' \neq u'$. Setze $M'' := \{z : u'' \leq z < x\}$. Wir wiederholen dies so oft, bis wir eine Menge $M^{(n)}$ bekommen, die nur ein Element enthält. Dies ist das gesuchte Element. ⊣

Satz 7.5 *Ein Element in einem endlichen Verband ist genau dann irreduzibel, wenn es genau einen unteren Nachbarn hat.*

Beweis. Falls x keinen unteren Nachbarn hat, so ist x schon die Null. Dies folgt aus dem vorigen Hilfssatz 7.4: gewiss hat 0 keinen unteren Nachbarn. Ist nun $x > 0$, so existiert ein y mit $0 \leq y \prec x$. Habe x mindestens zwei untere Nachbarn.

Abbildung 7.1: Ein Distributiver Verband



Seien $u, v \prec x$ und $u \neq v$. Dann ist $u \sqcup v \leq x$. Da $u < u \sqcup v$, so muss schon $u \sqcup v = x$ sein. x ist also nicht irreduzibel. Habe nun x genau einen unteren Nchbarn, y. Wir zeigen, dass x in diesem Fall irreduzibel ist. Nehmen wir an, dass $x = u \sqcup v$. Ist dann $u < x$ und $v < x$, so muss $u \leq y$ und $v \leq y$ sein, mithin $u \sqcup v \leq y < x$. Es ist also $u \sqcup v = x$ nur dann, wenn $u = x$ oder $v = x$. ⊣

Beispiel 15. In dem Verband von Figur 7.1 sind die Elemente a, b, c, d, g und j irreduzibel. ⚽

Beispiel 16. Zum Beispiel ist in dem Teilerverband von n eine Zahl kgV-irreduzibel, falls sie die Potenz einer Primzahl ist (und $\neq 1$, weil die 1 ja hier die Rolle der Null spielt). Ich geben zwei Wege an, dies zu sehen. Der erste ist direkt.

Sei $k = p^m$ für eine Primzahl p und eine natürliche Zahl m. Ist k ein Teiler von

kgV$\{x, y\}$, so muss k entweder x oder y teilen. Denn sei $x = p^a \cdot u$ und $y = p^b \cdot v$ für u, v teilerfremd zu p (Primfaktorzerlegung). Dann ist kgV$\{x, y\} = p^{\max\{a,b\}} \cdot$ kgV$\{u, v\}$. Da p auch das kleinste gemeinsame Vielfache von u und v nicht teilt, so teilt k das kgV aus x und y nur, wenn $m \leq \max\{a, b\}$. Daraus folgt aber, dass entweder $m \leq a$ oder $m \leq b$ sein muss.

Ist aber $k = p^m \cdot y$ für ein $y \neq 1$, welches nicht durch p teilbar ist, so ist $k =$ kgV$\{p^m, y\}$, aber es ist k kein Teiler von p^m oder y. Also ist k nicht irreduzibel.

Nun zum zweiten Weg. Es ist $m \prec n$ genau dann, wenn $m = n/p$ ist für eine Primzahl p, die n teilt. Dies ist eine Übung. Falls nun n keine Primzahlpotenz ist, so existieren zwei Primzahlen p und p', die n teilen. Dann sind n/p und n/p' zwei untere Nachbarn. ⚽

Es sei $\mathfrak{V}$ ein endlicher Verband. Sei Irr $\mathfrak{V}$ die Menge der irreduziblen Elemente von $\mathfrak{V}$. $\langle \text{Irr}\,\mathfrak{V}, \leq \rangle$ ist eine partiell geordnete Menge. Setze $\zeta(x) := \{y \in \text{Irr}\,\mathfrak{V} : y \leq x\}$. Dann ist $\zeta(x)$ eine nach unten abgeschlossene Menge in $\langle \text{Irr}\,\mathfrak{V}, \leq \rangle$.

Hilfssatz 7.6 *Es sei $\mathfrak{V}$ ein distributiver Verband. Dann gilt*

$$\begin{aligned} \zeta(x \sqcup y) &= \zeta(x) \cup \zeta(y) \\ \zeta(x \sqcap y) &= \zeta(x) \cap \zeta(y) \end{aligned}$$

Beweis. Es sei $u \in \zeta(x \sqcup y)$. Dann ist u irreduzibel und $u \leq x \sqcup y$. Daraus folgt $u = u \sqcap (x \sqcup y) = (u \sqcap x) \sqcup (u \sqcap y)$, also ist $u = u \sqcap x$ oder $u = u \sqcap y$. Daher ist $u \leq x$ oder $u \leq y$. Nach Definition heißt dies, dass $u \in \zeta(x)$ oder $u \in \zeta(y)$. Sei nun $u \in \zeta(x)$ oder $u \in \zeta(y)$. Dann $u \leq x$ oder $u \leq y$, und so $u \leq x \sqcup y$. u ist irreduzibel, also $u \in \zeta(x \sqcup y)$. Nun zur zweiten Behauptung. Sei $u \in \zeta(x \sqcap y)$, also $u \leq x \sqcap y$ und u irreduzibel. Dann $u \leq x$ und $u \leq y$ und so $u \in \zeta(x)$ sowie $u \in \zeta(y)$. Ist umgekehrt $u \in \zeta(x)$ und $u \in \zeta(y)$, so $u \leq x$ und $u \leq y$, woraus $u \leq x \sqcap y$ folgt und schließlich $u \in \zeta(x \sqcap y)$. ⊣

Beispiel 17. Wir sehen uns den Verband von Figur 7.1 an. Die irreduziblen Elemente sind a, b, c, c, d, g und j. Damit ist ζ die folgende Abbildung.

(7.1)

x	$\zeta(x)$
0	$\varnothing$
a	$\{a\}$
b	$\{a, b\}$
c	$\{a, b, c\}$
d	$\{a, d\}$
e	$\{a, b, d\}$
f	$\{a, b, c, d\}$
g	$\{a, d, g\}$
h	$\{a, b, d, g\}$
i	$\{a, b, c, d, g\}$
j	$\{a, b, d, g, j\}$
1	$\{a, b, c, d, g.j\}$

⚽

Wir haben damit gezeigt, dass $x \mapsto \zeta(x)$ ein Homomorphismus ist. Nun wollen wir noch zeigen, dass es eine bijektive Abbildung ist. Dazu sei zunächst M eine nach unten abgeschlossene Menge.

Hilfssatz 7.7 *Es sei M eine endliche, nach unten abgeschlossene Menge von irreduziblen Elementen in einem distributiven Verband. Dann gilt $M = \zeta(\bigsqcup M)$.*

Beweis. Mit anderen Worten: Für ein irreduzibles Element u ist $u \leq \bigsqcup M$ genau dann, wenn $u \in M$. Falls $u \in M$, so ist sicher $u \leq \bigsqcup M$. Sei daher $u \leq \bigsqcup M$. Dann ist $u = u \sqcap \bigsqcup M = \bigsqcup \langle u \sqcap y : y \in M \rangle$. Da u $\sqcup$-irreduzibel, ist $u = u \sqcap y$ für ein $y \in M$, also $u \leq y$. Nun ist M nach unten abgeschlossen und u irreduzibel. Also $u \in M$. ⊣

Hilfssatz 7.8 *Es sei $\mathfrak{V}$ ein endlicher Verband. Dann existiert für jedes $x \in V$ eine nach unten abgeschlossene Menge M aus $\sqcup$-irreduziblen Elementen, sodass $x = \bigsqcup M$ ist. Diese Menge ist eindeutig bestimmt, und es ist $M = \zeta(x)$.*

Beweis. Zunächst zeigen wir die Eindeutigkeit. Sei $x = \bigsqcup M = \bigsqcup N$, wo M und N nach unten abgeschlossene Menge irreduzibler Elemente sind. Sei $u \in M$. Dann gilt $u \leq x$, und so $u \leq \bigsqcup N$. Also $u = u \sqcap (\bigsqcup N) = \bigsqcup_{y \in N} (u \sqcap y)$. Da u $\sqcup$-irreduzibel, existiert ein $y \in N$ mit $u = u \sqcap y$; daraus folgt $u \leq y$. Da N nach unten abgeschlossen ist, ist $u \in N$. Daher $M \subseteq N$. Ebenso zeigt man $N \subseteq M$. Nun

zeigen wir, dass $x = \bigsqcup\zeta(x)$. Falls dies nicht der Fall ist, so ist $x > \bigsqcup\zeta(x)$. Sei y ein minimales Element mit der Eigenschaft, dass $y \not\leq \bigsqcup\zeta(x)$, aber $y \leq x$. Solch ein Element muss es geben. Denn x hat diese Eigenschaft. Die Menge der Elemente mit dieser Eigenschaft ist also nichtleer und endlich. Dann hat sie ein kleinstes Element. Wir zeigen, dass y $\sqcup$-irreduzibel ist, woraus folgt $y \in \zeta(x)$, im Gegensatz zu unserer Annahme. Sei also $y = z_1 \sqcup z_2$. Dann ist $z_1 \not\leq \zeta(x)$ oder $z_2 \not\leq \zeta(x)$. Sei etwa $z_1 \not\leq \zeta(x)$. Sicher ist $z_1 \leq x$. Nach Wahl von y ist also $z_1 = y$. Also ist y $\sqcup$-irreduzibel. ⊣

Es lässt sich zeigen, dass die Eindeutigkeit der Zerlegung ein Kriterium dafür ist, ob der Verband distributiv ist oder nicht. Denn sei $x = \bigsqcup M = \bigsqcup N$ für zwei verschiedene, nach unten abgeschlossene Mengen. Dann existiert oBdA ein $u \in M - N$. Also ist $u < \bigsqcup N$. Man kann leicht sehen, dass N kein maximales Element enthält. (Denn dann ist x schon $\sqcup$-irreduzibel und dann muss $x \in M$ sein, woraus sogleich $N \subseteq M$ folgt. Aber $N \subsetneq M$ kann nicht sein, denn daraus folgt $\bigsqcup N < \bigsqcup M$.) Also ist $N = S_1 \cup S_2$, wo S_1 und S_2 jeweils nicht leer sind. Wir können sogar annehmen, dass S_1 und S_2 nach unten abgeschlossen sind. Setze $y := \bigsqcup S_1$ und $z := \bigsqcup S_2$. Dann ist

$$u \sqcap (y \sqcup z) = u \sqcap x = u$$

Angenommen,

$$(u \sqcap y) \sqcup (u \sqcup z) = u$$

Dann ist $u \sqcap y = u$ oder $u \sqcap z = u$, da u $\sqcup$-irreduzibel. Sei etwa $u \sqcap y = u$. Dann $u \in S_1$, da S_1 nach unten abgeschlossen und u $\sqcup$-irreduzibel. Dies widerspricht der Annahme, dass $y \notin N$.

Als Anwendung betrachten wir noch einmal den Teilerverband von n. Ein beliebiges Element ist eindeutig darstellbar als das kgV einer bezüglich Teilbarkeit nach unten abgeschlossenen Menge von Primzahlpotenzen. Daraus folgt unmittelbar die Eindeutigkeit der Zerlegung in Primfaktoren.

Satz 7.9 (Darstellungssatz für endliche Distributive Verbände) *Es sei* $\mathfrak{V} = \langle V, \sqcap, \sqcup\rangle$ *ein endlicher distributiver Verband,* $\mathfrak{P} = \langle \operatorname{Irr}\mathfrak{V}, \leq\rangle$ *die partielle Ordnung der* $\sqcup$*-irreduziblen Elemente. Dann ist* $\mathfrak{V}$ *isomorph zu* $\mathfrak{Vb}(\mathfrak{P}) := \langle L(\mathfrak{P}), \cap, \cup\rangle$.

Beweis. Betrachte $x \mapsto \zeta(x)$. Diese Abbildung ist ein Homomorphismus (Hilfssatz 7.6). ζ ist surjektiv wegen Hilfssatz 7.7 und injektiv wegen Hilfssatz 7.8. ⊣

Man beachte, dass man die Distributivität im Wesentlichen für die Eindeutigkeit der Zerlegung braucht. Es ist nämlich in allen endlichen Verbänden jedes Element die Vereinigung $\sqcup$-irreduzibler Elemente, aber da diese Darstellung nicht

eindeutig ist, kann man daraus keinen Isomorphismus konstruieren (sonst wäre ja auch jeder endliche Verband distributiv — und das ist nicht der Fall).

Wir folgern aus dem Darstellungssatz für distributive Verbände ein handliches Kriterium.

Hilfssatz 7.10 *Es sei $\mathfrak{V}$ ein endlicher distributiver Verband. Dann ist $u \leq v$ genau dann, wenn $\zeta(u) \subseteq \zeta(v)$. Ferner ist $u \prec v$ genau dann, wenn $\zeta(v) = \zeta(u) \cup \{x\}$ ist für ein $\sqcup$-irreduzibles x, welches nicht in $\zeta(u)$ ist.*

Beweis. Ist $u \leq v$, so ist jedes Element unterhalb von u auch unterhalb von v, also $\zeta(u) \subseteq \zeta(v)$. Ist umgekehrt $\zeta(u) \subseteq \zeta(v)$, so ist $u = \bigsqcup\zeta(u) \leq \bigsqcup\zeta(v) = v$. Nun sei $\zeta(v) = \zeta(u) \cup \{x\}$ für ein $x \notin \zeta(u)$. Dann ist gewiss $u < v$. Falls ein z existiert mit $u < z < v$, so ist $\zeta(u) \subsetneq \zeta(z) \subsetneq \zeta(v)$. Dies ist nicht möglich. Also $u \prec v$. Sei umgekehrt $u \prec v$. Dann ist sicher $\zeta(u) \subsetneq \zeta(v)$. Sei x minimal bezüglich $\leq$ in der Menge $\zeta(v) - \zeta(u)$. Dann ist $\zeta(u) \cup \{x\}$ nach unten abgeschlossen. Denn ist $p \leq r \in \zeta(u) \cup \{x\}$ ein $\sqcup$-irreduzibles Element, so entweder $r \in \zeta(u)$ oder $r = x$. Im ersten Fall ist $r \in \zeta(u)$, da letztere Menge nach unten abgeschlossen ist. Im zweiten Fall ist entweder $p < x$ und damit $p \in \zeta(u)$, da x minimal war und $\zeta(u)$ nach unten abgeschlossen. Oder aber $x = p$, und so $x \in \zeta(u) \cup \{x\}$. Wir haben also $\zeta(u) \subsetneq \zeta(u) \cup \{x\} \subseteq \zeta(v)$. Da $u \prec v$, gilt $\zeta(v) = \zeta(u) \cup \{x\}$. ⊣

Definition 7.11 (Dimension) *Es sei $\mathfrak{V}$ ein Verband. Eine Folge $F = \langle x_i : 0 \leq i \leq n\rangle$ heißt **Kette**, falls für alle $i < m$, x_i unterer Nachbar von x_{i+1} ist. Darüber hinaus heißt F auch **Kette von** x_0 **nach** x_n. Sei x ein Element und n die größte Zahl — sofern sie existiert — derart, dass eine Kette $\langle y_i : 0 \leq i \leq n\rangle$ existiert mit $y_0 = 0$, $y_n = x$. Dann sagt man, x hat die **Dimension** n.*

Satz 7.12 *Es sei $\mathfrak{V}$ ein distributiver Verband, $x \in V$ ein Element mit Dimension n. Sei $\langle y_i : 0 \leq i \leq m\rangle$ eine beliebige Kette mit $y_0 = 0$, $y_m = x$. Dann ist $m = n$.*

Der Beweis für diesen Satz ist eine Übung. Man sagt, ein Verband ist **kettengleich**, falls für je zwei Elemente x, y gilt: existiert eine Kette von x nach y der Länge n, so hat jede Kette von x nach y die Länge n. Mit Hilfssatz 7.10 folgt jetzt leicht:

Hilfssatz 7.13 *Es sei $\mathfrak{V}$ ein endlicher distributiver Verband. Dann gilt für alle $x \in V$:*

$$\dim x = |\zeta(x)| \ .$$

Ist $\mathfrak{V}$ ein Verband, so schreiben wir $[x, y] := \{z : x \leq z \leq y\}$ und nennen dies ein **Intervall**. Intervalle sind abgeschlossen unter $\sqcup$ und $\sqcap$ und bilden somit wiederum Verbände.

Satz 7.14 *Es sei $\mathfrak{V}$ ein distributiver Verband, und x, y beliebige Elemente. Dann ist das Intervall $[x \sqcap y, x]$ isomorph zu dem Intervall $[y, x \sqcup y]$. Ein Isomorphismus ist gegeben durch die Abbildung $h : z \mapsto z \sqcup y$.*

Beweis. Betrachte die Abbildung $k : z \mapsto z \sqcap x$. Wir behaupten: $k \circ h$ ist die Identität auf $[x \sqcap y, x]$ und $h \circ k$ die Identität auf $[y, x \sqcup y]$. Dazu sei $x \sqcap y \leq z \leq x$. Dann ist $(k \circ h)(z) = (z \sqcup y) \sqcap x = (z \sqcap x) \sqcup (y \sqcap x) = z \sqcup (x \sqcap y) = z$. Sei jetzt $y \leq u \leq x \sqcup y$. Dann $(h \circ k)(u) = (u \sqcap x) \sqcup y = (u \sqcup y) \sqcap (x \sqcup y) = u \sqcap (x \sqcup y) = u$. k und h sind ordnungstreu, das heißt, ist $z \leq z'$ für $z, z' \in [x \sqcap y, x]$, so $h(z) \leq h(z')$ und ist $u, u' \in [y, x \sqcup y]$, so folgt aus $u \leq u'$ bereits $k(u) \leq k(u')$. Ist nun $h(z) \leq h(z')$, so ist $(k \circ h)(z) \leq (k \circ h)(z')$, also $z \leq z'$. Ist $k(u) \leq k(u')$, so ist $(h \circ k)(u) \leq (h \circ k)(u')$, also $u \leq u'$. k und h sind also Ordnungsisomorphismen, und daher Verbandsisomorphismen. ⊣

Als letztes besprechen wir noch eine wichtige Konstruktion in der Algebra, nämlich das **Produkt**. Das Produkt zweier Verbände wird wie folgt definiert. (Wir setzen nicht voraus, dass die Verbände distributiv sind.) Seien $\mathfrak{V} = \langle V, \sqcap, \sqcup \rangle$ und $\mathfrak{W} = \langle W, \sqcap', \sqcup' \rangle$ Verbände. Seien $\langle x_1, y_1 \rangle, \langle x_2, y_2 \rangle \in V \times W$. Dann setze

$$\begin{array}{lcl} \langle x_1, y_1 \rangle \sqcap'' \langle x_2, y_2 \rangle & := & \langle x_1 \sqcap x_2, y_1 \sqcap' y_2 \rangle \\ \langle x_1, y_1 \rangle \sqcup'' \langle x_2, y_2 \rangle & := & \langle x_1 \sqcup x_2, y_1 \sqcup' y_2 \rangle \end{array}$$

$\mathfrak{V} \times \mathfrak{W} := \langle V \times W, \sqcap'', \sqcup'' \rangle$ ist ein Verband. Dies nachzurechnen, ist langwierig, aber nicht schwer. Wir beweisen anstelle dessen folgenden Sachverhalt.

Hilfssatz 7.15 *Es seien $\mathfrak{V}$ und $\mathfrak{W}$ distributive Verbände. Dann ist $\mathfrak{V} \times \mathfrak{W}$ auch ein distributiver Verband.*

Beweis. Wir zeigen nur eines der beiden Gesetze (das andere ist ja dual dazu).

$$\begin{array}{lcl} \langle x_1, y_1 \rangle \sqcap'' (\langle x_2, y_2 \rangle \sqcup'' \langle x_3, y_3 \rangle) & = & \langle x_1, y_1 \rangle \sqcap'' \langle x_2 \sqcup x_3, y_2 \sqcup' y_3 \rangle \\ & = & \langle x_1 \sqcap (x_2 \sqcup x_3), y_1 \sqcap' (y_2 \sqcup' y_3) \rangle \\ & = & \langle (x_1 \sqcap x_2) \sqcup (x_1 \sqcap x_3), (y_1 \sqcap' y_2) \sqcup' (y_1 \sqcap' y_3) \rangle \\ & = & \langle x_1 \sqcap x_2, y_1 \sqcap' y_2 \rangle \sqcup'' \langle x_1 \sqcap x_3, y_1 \sqcap' y_3 \rangle \\ & = & (\langle x_1, y_1 \rangle \sqcap'' \langle x_2, y_2 \rangle) \sqcup'' (\langle x_1, y_1 \rangle \sqcap'' \langle x_3, y_3 \rangle) \end{array}$$

⊣

Übungen

Übung 22. Seien $\mathfrak{P} = \langle P, \leq \rangle$ und $\mathfrak{Q} = \langle Q, \leq \rangle$ Ordnungen $\sqcup$-irreduzibler Elemente von $\mathfrak{V}$ bzw. $\mathfrak{W}$. Definiere die **Summe** $\mathfrak{P} \oplus \mathfrak{Q}$ von $\mathfrak{P}$ und $\mathfrak{Q}$ wie folgt. Setze

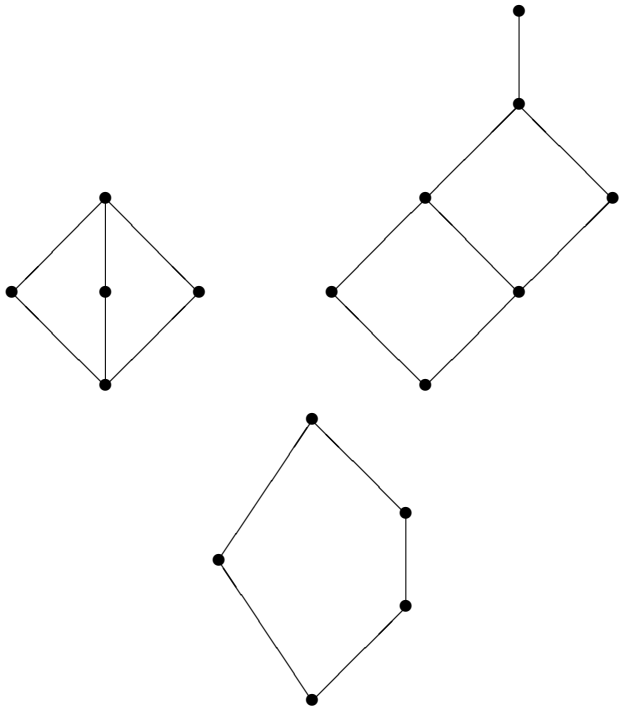
$\mathfrak{P} \oplus \mathfrak{Q} := \langle P + Q, \leq' \rangle$. $P + Q := P \times \{0\} \cup Q \times \{1\}$. Es sei $\langle x, i \rangle \leq' \langle y, j \rangle$ genau dann, wenn $i = j$ und $x \leq y$. (Also: zwei Elemente sind vergleichbar genau dann, wenn sie aus demselben Summanden stammen und dort vergleichbar sind.) Zeigen Sie, dass die Ordnung der $\sqcup$-irreduziblen Elemente von $\mathfrak{V} \times \mathfrak{W}$ die Summe der Ordnungen der $\sqcup$-irreduziblen Elemente von $\mathfrak{P}$ und von $\mathfrak{Q}$ ist, also $\mathfrak{P} \oplus \mathfrak{Q}$. Dh es gilt

$$\mathfrak{Vb}(\mathfrak{V} \times \mathfrak{W}) \cong \mathfrak{Vb}(\mathfrak{V}) \oplus \mathfrak{Vb}(\mathfrak{W})$$

Übung 23. Zeigen Sie, dass ein linearer Verband distributiv ist.

Übung 24. Zeigen Sie: die Behauptung aus Beipiel 16. $m \prec n$ genau dann, wenn $m = n/p$ für eine Primzahl p, die n teilt.

Übung 25. Prüfen Sie, ob die folgenden Verbände distributiv sind.



Hinweis. Verwenden Sie den Darstellungssatz. (Bei 5 Elementen würde der Nachweis der Distributivität bei blindem Ausrechnen das Prüfen von 125 Möglichkeiten erfordern!) Bestimmen Sie die irreduziblen Elemente und prüfen Sie, ob die übrigen Elemente eindeutig durch nach unten abgeschlossene Menge dargestellt werden können.

Übung 26. Beweisen Sie Satz 7.12.

Kapitel 8

Boolesche Algebren

Ein **Verband mit Null und Eins** ist ein Tupel $\langle V, 0, 1, \sqcap, \sqcup\rangle$, wo $\langle V, \sqcap, \sqcup\rangle$ ein Verband, $0 \in V$ eine Null und $1 \in V$ eine Eins ist. Ein Element $x \in V$ heißt ein **Atom**, falls es ein Nullelement gibt und $y < x$ genau dann gilt, wenn $y = 0$ (also wenn x die Dimension 1 hat). Dual dazu sagt man, $x \in V$ ist ein **Coatom**, falls es eine Eins gibt und $y > x$ nur dann gilt, wenn $y = 1$.

Definition 8.1 (Komplement) *Es sei $\mathfrak{V}$ ein Verband mit Null und Eins und $x \in V$. Ein Element $y \in V$ heißt **Komplement** von x, falls $x \sqcap y = 0$ und $x \sqcup y = 1$.*

Ist y Komplement von x, so ist x auch Komplement von y. Komplemente muss es nicht geben, auch nicht, wenn der Verband distributiv ist. Zum Beispiel haben in einem linearen Verband lediglich die Elemente 0 und 1 ein Komplement. (Das Komplement von 0 ist dann 1, das Komplement von 1 ist 0.) Hat ein linearer Verband mehr als zwei Elemente, so haben einige Element kein Komplement. Solche Verbände sind aber distributiv. Trotzdem gilt folgender Satz.

Hilfssatz 8.2 *Es sei $\mathfrak{V}$ ein distributiver Verband mit Null und Eins. Sind y_1 und y_2 Komplemente von x, so ist $y_1 = y_2$.*

Beweis. Es ist $y_1 = y_1 \sqcap 1 = y_1 \sqcap (x \sqcup y_2) = (y_1 \sqcap x) \sqcup (y_1 \sqcap y_2) = 0 \sqcup (y_1 \sqcap y_2) = y_1 \sqcap y_2$. Also $y_1 \leq y_2$. Ebenso zeigt man $y_2 \leq y_1$. ⊣

Definition 8.3 (Boolesche Algebra) *Es sei B eine nichtleere Menge. $\mathfrak{B} = \langle B, 0, 1, -, \cap, \cup\rangle$ ist eine **Boolesche Algebra**, falls $0, 1 \in B$, $-$ eine einstellige und $\cap$ und $\cup$ zweistellige Funktionen sind derart, dass $\langle B, 0, 1, \cap, \cup\rangle$ ein distributiver Verband mit Null und Eins ist, und für jedes $x \in B$ $-x$ ein Komplement von x ist. Sei $\mathfrak{C} =$*

$\langle C, 0', 1', -', \cap', \cup' \rangle$ *eine Boolesche Algebra und* $h : B \to C$. *h heißt* ***Homomorphismus****, in Zeichen* $h : \mathfrak{B} \to \mathfrak{C}$, *falls* $h(0) = 0'$, $h(1) = 1'$, $h(-x) = -'h(x)$, $h(x \cap y) = h(x) \cap' h(y)$ *und* $h(x \cup y) = h(x) \cup' h(y)$ *ist für alle* $x, y \in B$.

Wir ziehen ein paar Folgerungen aus dieser Definition.

Proposition 8.4 *In einer Booleschen Algebra gelten folgende Gesetze.*

$$\begin{array}{lcl} x \cup -x & = & 1 \\ x \cap -x & = & 0 \\ --x & = & x \\ -(x \cup y) & = & (-x) \cap (-y) \\ -(x \cap y) & = & (-x) \cup (-y) \end{array}$$

Die letzten beiden Gesetze heißen die ***de Morganschen Gesetze****.*

Beweis. Die ersten beiden Gesetze folgen unmittelbar aus den Definitionen. Ferner ist x das Komplement von $-x$, und da Komplemente ja nunmehr eindeutig sind, ist $--x = x$. Für das vierte Gesetz muss man zeigen, dass $(x \cup y) \cap ((-x) \cap (-y)) = 0$ und $(x \cup y) \cup ((-x) \cap (-y)) = 1$. Die erste Gleichung ist unmittelbar klar: $(x \cup y) \cap ((-x) \cap (-y)) = (x \cap (-x) \cap (-y)) \cup (y \cap (-x) \cap (-y)) = 0 \cup 0 = 0$. Für die zweite beachte, dass $(x \cup y) \cup ((-x) \cap ((-y)) = (x \cup y \cup (-x)) \cap (x \cup y \cup (-y)) = 1 \cap 1 = 1$. Das fünfte Gesetz ist dual, und wird dual bewiesen. ⊣

Aus dem Darstellungssatz für endliche distributive Verbände folgt nun ein recht schöner Darstellungssatz für Boolesche Algebren. Da Boolesche Algebren distributive Verbände sind (wenn man die Null, die Eins und die Komplementfunktion vergisst), so lassen sich die Elemente von endlichen Booleschen Algebren als Mengen auffassen, und $\cup$ ist die Vereinigung und $\cap$ der Durchschnitt (was wir durch die Notation bereits vorweggenommen haben). Da es immer eine Null und eine Eins gibt müssen wir uns nur noch fragen, für welche distributiven Verbände zu jedem Element ein Komplement existiert. Denn es gilt:

Hilfssatz 8.5 *Es sei* $\mathfrak{V} = \langle V, 0, 1, \sqcap, \sqcup \rangle$ *ein distributiver Verband, in dem jedes Element ein Komplement hat. Es sei* $- : V \to V$ *die Funktion, die jedem Element sein Komplement zuordnet. Dann ist* $\langle V, 0, 1, -, \sqcap, \sqcup \rangle$ *eine Boolesche Algebra.*

Der Beweis ist trivial: der Satz folgt schon aus der Definition.

Hilfssatz 8.6 *Es sei* $\mathfrak{V}$ *ein distributiver Verband und y ein Komplement von x. Dann ist* $\zeta(y)$ *das relative Komplement von* $\zeta(x)$ *in* $\operatorname{Irr}\mathfrak{V}$*; das heißt,* $\zeta(y) = \operatorname{Irr}\mathfrak{V} - \zeta(x)$.

Beweis. Es gilt $\emptyset = \zeta(0) = \zeta(x \sqcap y) = \zeta(x) \cap \zeta(y)$ sowie $\operatorname{Irr} \mathfrak{V} = \zeta(1) = \zeta(x \sqcup y) = \zeta(x) \cup \zeta(y)$. ⊣

Wir schreiben $-\zeta(x)$ anstelle von $\operatorname{Irr} \mathfrak{V} - \zeta(x)$.

Hilfssatz 8.7 *Es sei $\mathfrak{V}$ ein endlicher distributiver Verband. Genau dann hat jedes Element ein Komplement, wenn jedes $\sqcup$-irreduzible Element ein Atom ist.*

Beweis. Zunächst einmal ist jedes Atom irreduzibel. Es sei nun jedes irreduzible Element ein Atom. Dann ist jede Teilmenge von $\operatorname{Irr} \mathfrak{V}$ nach unten abgeschlossen. Betrachte die Abbildung ζ. Setze

$$-x := \bigsqcup - \zeta(x)$$

Dann ist $x \sqcap -x = 0$, denn $\zeta(x \sqcap -x) = \zeta(x) \cap \zeta(-x) = \emptyset = \zeta(0)$, und $x \sqcup -x = 1$, da ja $\zeta(x \sqcup -x) = \zeta(x) \cup \zeta(-x) = \operatorname{Irr} \mathfrak{V} = \zeta(1)$. Nun existiere ein irreduzibles Element u, welches kein Atom ist. Dann existiert ein Atom $x < u$. Die Menge $-\zeta(x)$ enthält u und ist deswegen nicht nach unten abgeschlossen. Also hat x kein Komplement. ⊣

Definition 8.8 (Potenzmengenalgebra) *Es sei X eine Menge. Die **Potenzmengenalgebra** über X ist die Boolesche Algebra $\langle \wp(X), 0, 1, -, \cap, \cup \rangle$, bei der $0 = \emptyset$, $1 = X$, $-A := X - A$ sowie $\cap$ und $\cup$ der Mengenschnitt bzw. die Vereinigung sind.*

Satz 8.9 (Darstellungssatz für endliche Boolesche Algebren) *Es sei $\mathfrak{B}$ eine endliche Boolesche Algebra und X die Menge der Atome von $\mathfrak{B}$. Dann ist $\mathfrak{B}$ isomorph zu der Potenzmengenalgebra über X.*

Dies folgt unmittelbar aus dem Darstellungssatz für distributive Verbände und dem Hilfssatz 8.7. Man setze einfach $X := \operatorname{Irr}(\mathfrak{v})$.

Betrachte nun die Menge $\{0, 1\}$. Setze $\leq := \{\langle 0, 0\rangle, \langle 0, 1\rangle, \langle 1, 1\rangle\}$. Dies ist eine partielle Ordnung. Damit ist

	$-$
0	1
1	0

$\cap$	0	1
0	0	0
1	0	1

$\cup$	0	1
0	0	1
1	1	1

Wir bezeichnen mit **2** die Algebra $\langle \{0, 1\}, 0, 1, -, \cap, \cup \rangle$. Diese Algebra spielt eine wichtige Rolle im Aufbau von Booleschen Algebren.

Hilfssatz 8.10 *Es sei 2^n die Menge aller Folgen der Länge n von Elementen aus $\{0,1\}$. Sei $\vec{x} \leq \vec{y}$ genau dann, wenn $x_i \leq y_i$ für alle $i \leq n$. Dann ist*

$$\begin{array}{lcl} \vec{x} \cap \vec{y} & = & \langle x_i \cap y_i : 1 \leq i \leq n \rangle \\ \vec{x} \cup \vec{y} & = & \langle x_i \cup y_i : 1 \leq i \leq n \rangle \\ -\vec{x} & = & \langle -x_i : 1 \leq i \leq n \rangle \end{array}$$

*Diese Algebra ist das n–fache Produkt von **2** mit sich selbst.*

Nehmen wir den einfachsten nichttrivialen Fall, $n = 2$. Hier hat die Algebra 4 Elemente, $\langle 0,0\rangle$, $\langle 0,1\rangle$, $\langle 1,0\rangle$ und $\langle 1,1\rangle$. Die Operationen $-$ und $\cap$ sind wie folgt.

(8.1)

	$-$
$\langle 0,0\rangle$	$\langle 1,1\rangle$
$\langle 0,1\rangle$	$\langle 1,0\rangle$
$\langle 1,0\rangle$	$\langle 0,1\rangle$
$\langle 1,1\rangle$	$\langle 0,0\rangle$

$\cap$	$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 1,0\rangle$	$\langle 1,1\rangle$
$\langle 0,0\rangle$	$\langle 0,0\rangle$	$\langle 0,0\rangle$	$\langle 0,0\rangle$	$\langle 0,0\rangle$
$\langle 0,1\rangle$	$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 0,0\rangle$	$\langle 0,1\rangle$
$\langle 1,0\rangle$	$\langle 0,0\rangle$	$\langle 0,0\rangle$	$\langle 1,0\rangle$	$\langle 1,0\rangle$
$\langle 1,1\rangle$	$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 1,0\rangle$	$\langle 1,1\rangle$

Satz 8.11 *Es sei $\mathfrak{B}$ eine endliche Boolesche Algebra. Dann ist $\mathfrak{B}$ isomorph zu dem n-fachen Produkt von **2**, wobei n die Anzahl der Atome von $\mathfrak{B}$ ist.*

Beweis. Es sei X die Menge der Atome von $\mathfrak{B}$. Sei $X = \{x_1, x_2, \ldots, x_n\}$. Sei y ein Element aus B. Sei $f(y) = \langle u_i(y) : 1 \leq i \leq n\rangle$, wobei $u_i(y) = 1$ falls $x_i \leq y$ und 0 sonst. Es ist nicht schwer zu zeigen, dass $y \leq z$ genau dann, wenn $f(y) \leq f(z)$. Dies bedeutet, dass f ein Homomorphismus ist von $\mathfrak{B}$ in die Algebra $\mathbf{2} \times \mathbf{2} \times \ldots \mathbf{2}$. Jeder Folge $\vec{u}$ entspricht das Element $\bigcup\langle x_i : u_i = 1\rangle$, also ist die Abbildung f surjektiv. Sie ist injektiv, da $y = z$ genau dann, wenn für jedes $i \leq n$ gilt $x_i \leq y$ genau dann wenn $x_i \leq z$; also ist dies gleichwertig mit $f(y) = f(z)$. ⊣

Übungen

Übung 27. Es sei 2^n die Menge aller n–langen Folgen aus 0 und 1. Ist $\vec{x}, \vec{y} \in 2^n$, so ist der **Hammingabstand** von $\vec{x}$ und $\vec{y}$, $d_H(\vec{x}, \vec{y})$, die Anzahl aller $i \leq n$ sodass $x_i \neq y_i$. Zeigen Sie: die Dimension von $\vec{x}$ ist gleich $d_H(\vec{0}, \vec{x})$.

Übung 28. Es sei $\mathfrak{B} = \langle B, 0, 1, -, \cap, \cup\rangle$ eine Boolesche Algebra und $x \in B$. Sei $B_x := \{y : x \geq y\}$. Zeigen Sie, dass $\langle B_x, \leq\rangle$ die Ordnung einer Booleschen Algebra ist. Bestimmen Sie die zugehörigen Operationen. Wir bezeichnen die entstehende Boolesche Algebra mit $\mathfrak{B}_x$.

Übung 29. Zeigen Sie, dass die Abbildung $y \mapsto y \cap x$ ein Homomorphismus ist von $\mathfrak{B}$ auf $\mathfrak{B}_x$.

Übung 30. Es seien $\mathfrak{V}$ und $\mathfrak{W}$ endliche Verbände und $h : \mathfrak{V} \to \mathfrak{W}$ ein Homomorphismus. Zeigen Sie, dass $h^{-1}(x)$ entweder leer ist oder ein Intervall in $\mathfrak{V}$. *Anleitung.* Man muss also zeigen, dass für $u, v \in h^{-1}(x)$ gilt: $u \cap v, u \cap v \in h^{-1}(x)$.

Übung 31. Ein **Filter** in einer Booleschen Algebra ist eine Menge $F \subseteq B$ derart, dass (1.) $1 \in F$, (2.) falls $x \in F$ und $x \leq y$ so auch $y \in F$, und (3.) sind $x, y \in F$ so auch $x \cap y \in F$. Zeigen Sie, dass für jeden Homomorphismus $h : \mathfrak{B} \to \mathfrak{C}$ von Booleschen Algebren gilt: $h^{-1}(1)$ ist ein Filter.

Teil III

Kombinatorik und Graphen

Kapitel 9

Binomialkoeffizienten

Es sei M eine beliebige Menge. Dann bezeichnen wir mit $\sharp M$ die Anzahl der Elemente von M, genannt die **Mächtigkeit** von M. Im Folgenden setzen wir stets voraus, dass Mengen endlich sind. Dann ist die Mächtigkeit eine natürliche Zahl. 0 ist eine natürliche Zahl, und es gibt genau eine Menge M mit $\sharp M = 0$, nämlich die leere Menge, bezeichnet mit $\emptyset$. Wir betrachten nun ein paar Konstruktionen aus der Mengenlehre und schauen nach, wie sich die Anzahlen der konstruierten Mengen bestimmen. Zunächst ein Satz, der sich unmittelbar aus den Definitionen ergibt.

Hilfssatz 9.1 *Es seien M und N endliche Mengen. Genau dann ist $\sharp M = \sharp N$, wenn eine bijektive Abbildung $f : M \to N$ existiert.*

Satz 9.2 *Es seien M und N endlich Mengen. Dann ist*

$$\sharp(M \cup N) = \sharp M + \sharp N - \sharp(M \cap N)$$

Ist insbesondere M disjunkt zu N, so ist

$$\sharp(M \cup N) = \sharp M + \sharp N$$

Satz 9.3 *Es seien M_i, $1 \leq i \leq n$, Mengen. Dann ist*

$$\sharp(M_1 \times M_2 \times \ldots \times M_n) = \prod_{i=1}^{n} \sharp M_i$$

Satz 9.4 *Es seien M und N endliche Mengen, $m := \sharp M$, $n := \sharp N$. Es bezeichne N^M die Menge aller Funktionen von M nach N. Dann ist*

$$\sharp N^M = n^m$$

Beweis. Es sei $M = \{x_1, x_2, \ldots, x_m\}$. Einer Funktion $f : M \to N$ ordnen wir die Folge $\Phi(f) := \langle f(x_1), f(x_2), \ldots, f(x_m)\rangle$ zu. Diese Zuordnung ist bijektiv. $\Phi : N^M \to N \times N \times \ldots \times N$ (m-mal). Also ist nach Satz 9.3 $\sharp N^M = \prod_{i=1}^{m} n = n^m$. ⊣

Wir wollen nun als erstes ein nicht so einfaches Problem betrachten, welches in vielen verschiedenen Gewändern auftritt. Einige äquivalente Formulierungen wollen wir auch angeben, bevor wir daran gehen, diese Zahlen durch explizite Formeln zu bestimmen. Es sei M eine endliche Menge und k eine natürliche Zahl. Dann bezeichne $\binom{M}{k}$ die Menge der k-elementigen Teilmengen von M. Wir interessieren uns für die Anzahl der Elemente der Menge $\binom{M}{k}$, also der Anzahl der k-elementigen Teilmengen von M. Falls $\sharp M = n$, so sei diese Anzahl mit $\binom{n}{k}$ bezeichnet. Es ist klar, dass diese Anzahl nur von $\sharp M$ abhängt. Bevor wir also zur Bestimmung von $\binom{n}{k}$ übergehen, wollen wir uns Anzahlprobleme ansehen, welche auch zu den Zahlen $\binom{n}{k}$ führen.

Beispiel 18. Es sei $\mathfrak{B}$ eine Boolesche Algebra. Sei $d(\mathfrak{B}, k)$ die Anzahl der Elemente der Dimension k in $\mathfrak{B}$. Nach dem Darstellungssatz für endliche Boolesche Algebren können wir annehmen, $\mathfrak{B}$ sei die Potenzmengenalgebra einer Menge X. Die Elemente von $\mathfrak{B}$ sind die Teilmengen X; die irreduziblen Elemente sind die Atome, dh die Mengen der Form $\{x\}$, $x \in X$. Die Dimension von $Y \subseteq X$ ist genau die Anzahl der Atome unterhalb von Y, und dies ist nichts anderes als die Anzahl der Elemente von Y. Die Elemente von $\mathfrak{B}$ der Dimension k entsprechen somit eineindeutig den k-elementigen Teilmengen von X. Sei nun $n := \sharp X$. Dann ist also $d(\mathfrak{B}, k) = \binom{n}{k}$. ⚽

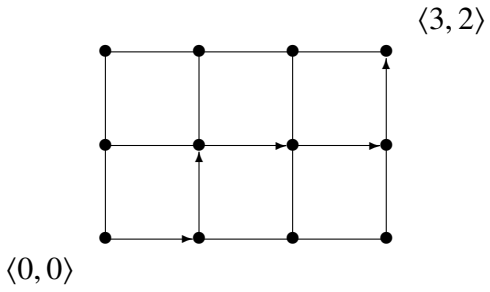
Beispiel 19. Es sei $m(n, k)$ die Anzahl aller Folgen der Länge n über $\{a, b\}$, welche a genau k mal enthalten. Wir betrachten die Abbildung X, welche der Folge $F = x_1 x_2 \ldots x_n$ die Menge $X(F) := \{i : x_i = a\}$ zuordnet. Es ist $X(F) \subseteq \{1, 2, \ldots, n\}$. X ist bijektiv. Genau dann kommt a in F k-mal vor, wenn $\sharp X(F) = k$. Also haben wir eine Bijektion zwischen den Folgen, welche a k-mal enthalten und den Teilmengen von $\{1, 2, \ldots, n\}$ der Mächtigkeit k. Also ist $m(n, k) = \binom{n}{k}$. ⚽

Beispiel 20. Der Term $(x + y)^n$ kann in eine Summe von Termen der Form $a(n, k)x^k y^{n-k}$ zerlegt werden, wobei $0 \leq k \leq n$. Allgemein bekannt ist der Fall $n = 2$: $(x + y)^2 = x^2 + 2xy + y^2$. Also $a(2, 0) = 1$, $a(2, 1) = 2$ und $a(2, 2) = 1$. Wir fragen nach den Zahlen $a(n, k)$. Dazu überlegen wir wie folgt. Offensichtlich kann man $(x + y)^n$ stur ausmultiplizieren; dann entsteht eine Summe von Termen

der Form $u_1u_2 \dots u_n$, wobei $u_i = x$ oder $u_i = y$. Wir nennen dies einen **Elementarsummanden** von $(x + y)^n$. Jeder Elementarsummand kommt in dieser Summe genau einmal dran. Da beim Multiplizieren die Reihenfolge unerheblich ist, können wir einen Elementarsummanden umschreiben in $x^k y^{n-k}$ für ein $k \leq n$. Dabei ist k gerade die Anzahl aller i für die $u_i = x$. Um also die Zahl $a(n, k)$ zu finden, müssen wir letztlich nur wissen, wie viele Folgen $U = u_1u_2 \dots u_n$ es gibt, in denen x genau k mal auftritt. Also ist nach dem vorigen Beispiel $a(n, k) = \binom{n}{k}$. ⚽

Beispiel 21. Es sei ein Gitter von Punkten der Ebene gegeben. Es bestehe aus den Punkten (i, j), wo $0 \leq i \leq m$ und $0 \leq j \leq n$. Ein **Weg der Länge** k in dem Gitter ist eine Folge von Punkten $P_0, P_1, P_2, \dots, P_k$, wo P_{i+1} jeweils Nachbar von P_i ist. Der Abstand zwischen zwei Punkten P und Q des Gitters, $d(P, Q)$, ist das kleinste k derart, dass ein Weg von P nach Q der Länge k existiert. Ist $P = (p_1, p_2)$ und $Q = (q_1, q_2)$, so ist $d(P, Q) = |p_1 - q_2| + |p_2 - q_2|$. Es interessiert uns die Anzahl der kürzesten Wege zwischen P und Q. Wir nennen sie $w(m, n)$. Das folgende Bild zeigt eine kürzesten Weg von $\langle 0, 0\rangle$ nach $\langle 3, 2\rangle$, nämlich

(9.1) $\langle 0, 0\rangle, \langle 1, 0\rangle, \langle 1, 1\rangle, \langle 2, 1\rangle, \langle 3, 1\rangle, \langle 3, 2\rangle$



(Eine Anwendung: der Stadtplan vieler amerikanischer Städte entspricht einem solchen Gitter. Um von einer beliebigen Kreuzung zu einer anderen zu gelanden, kann man nur entlang des Gitters laufen. Der Abstand wie oben definiert ist gerade die sogennante **Taximetrik**, sofern das Gitter aus quadratischen Zellen besteht. Denn dieser Abstand bestimmt ziemlich genau die Rechnung, die man fürs Taxi bezahlen muss...) Man kann sich überlegen, dass es reicht, wenn man $P = (0, 0)$ wählt, und $Q = (m, n)$. Der Abstand ist gerade $m + n$. Ein kürzester Weg $W = (P, P_1, P_2, \dots, P_{n+m})$ geht dann immer nach rechts oder oben, niemals nach links oder unten. Das bedeutet, dass, wenn $P_i = (p_i, q_i)$ ist, so ist $P_{i+1} = (p_i + 1, q_i)$ oder $P_{i+1} = (p_i, q_i + 1)$. Einem solchen Weg ordnen wir eine Folge $O(W) = \langle \eta_i : 1 \leq$

$i \leq m+n\rangle$ der Länge $m+n$ zu, wo $\eta_i = o$ falls $P_i = (p_{i-1}+1, q_{i-1})$ und $\eta_i = r$, falls $P_i = (p_{i-1}, q_{i-1}+1)$. Die Vorschrift $W \mapsto O(W)$ definiert eine Bijektion zwischen den kürzesten Wegen von $(0,0)$ nach (m,n) und den $n+m$-langen Folgen über $\{o,r\}$, welche genau n mal o enthalten. Also ist $w(m,n) = \binom{m+n}{n}$. ⚽

Gehen wir nun zu der Bestimmung von $\binom{n}{k}$ über. Dazu zunächst noch ein neues Zählprinzip. Es sei M eine Menge und $\Pi \subseteq \wp(M) - \{\emptyset\}$ eine Menge von Teilmengen von M. Π heißt **Partition** von M, falls jedes Element von M in genau einer Menge von Π liegt. Ist $\Pi = \{P_1, P_2, \ldots, P_k\}$, so ist natürlich $\sharp M = \sum_{i=1}^{k} \sharp P_i$. Der besondere Fall, wo alle P_i die gleiche Mächtigkeit haben, ist besonders hervorhebenswert.

Hilfssatz 9.5 *Es sei M eine Menge und $\Pi \subseteq \wp(M)$ eine Partition von M, bei der alle Mengen die gleiche Mächtigkeit p haben. Dann ist $\sharp M = p \cdot \sharp\Pi$.*

Wir wählen nun als M die Menge aller Folgen der Länge k von Elementen aus N, wobei kein Element wiederholt werden darf. Es habe N die Mächtigkeit n. Dann gibt es genau

$$n^{\underline{k}} := n \cdot (n-1) \cdot \ldots \cdot (n-k+1) \tag{9.2}$$

Elemente in M. Eine rekursive Definition dieser Zahl ist wie folgt ($k \leq n$).

$$\begin{aligned} n^{\underline{0}} &:= 1 \\ n^{\underline{k+1}} &:= (n-k) \cdot n^{\underline{k}} \end{aligned} \tag{9.3}$$

Zu jeder Folge $F = (x_1, x_2, \ldots, x_k)$ sei $\mu(F) := \{x_1, x_2, \ldots, x_k\}$. Da F kein Element wiederholt, ist $\sharp\mu(F) = k$. Betrachte nun zu jeder k-elementigen Teilmenge X von N die Menge $\Phi(X) := \{F : \mu(F) = X\}$. Dann ist das System

$$\Pi := \{\Phi(X) : X \subseteq N, \sharp X = k\} \tag{9.4}$$

eine Partition von M. Ferner hat jedes $\Phi(X)$ die gleiche Anzahl Elemente, nämlich $k^{\underline{k}}$. Für letzteren Ausdruck überlegt man sich, dass er gleich $k!$ ist. Nach dem Hilfssatz 9.5 ergibt sich nun

Satz 9.6

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{n!}{k!(n-k)!}$$

Übungen

Übung 32. Ein Lottoziehung ist eine Ziehung von 6 Zahlen aus 49. Wie viele verschiedene Ziehungen gibt es? Angenommen, man darf 7 Zahlen tippen. Wie hoch ist die Wahrscheinlichkeit, 6 bzw. 5 bzw. 4 richtige Zahlen getippt zu haben? (Hier ist Wahrscheinlichkeit die Anzahl der gewünschten Ergebnisse geteilt durch die Anzahl aller möglichen Ergebnisse.)

Übung 33. In einem Verband bezeichne $d(x)$ die Dimension des Elementes x. Man beweise folgende Dimensionsformel für distributive Verbände.

$$d(x \sqcap y) + d(x \sqcup y) = d(x) + d(y)$$

Hinweis. Bedienen Sie sich der Tatsache, dass $d(x) = \sharp\zeta(x)$.

Übung 34. Wir betrachten eine Abstimmung, an der genau n Personen beteiligt sind; es wird ferner nur über eine Sache abgestimmt, und man darf nur mit 'ja' oder 'nein' stimmen. (Es gibt also keine Enthaltungen.) Ergebnisse der Abstimmung sind: 'ja' (mehr Ja- als Nein-Stimmen), 'nein' (mehr Nein- als Ja-Stimmen), 'unentschieden' (genauso viele Ja- wie Nein-Stimmen). Wie stark ist das Gewicht einer einzelnen Stimme? Intuitiv würde man sagen, das Gewicht sei $1/n$. Ein amerikanischer Richter namens Banzhaff wollte es genauer wissen. Er definierte das Gewicht einer Stimme als die Anzahl der Situationen, in der diese eine Stimme den Ausschlag gibt geteilt durch die Anzahl aller möglichen Situationen. Man stellt sich dabei vor, dass zunächst alle anderen Personen abstimmen und bekommt ein Ergebnis E. Dann wirft man seine Stimme in den Ring und bekommt das endgültige Ergebnis E'. Wenn $E' \neq E$, so hat die eigene Stimme den Ausschlag gegeben. Man nennt das so definierte Gewicht den **Banzhaff-Index**. Wir notieren ihn $\mathrm{bz}(n)$. Wie groß ist $\mathrm{bz}(7)$? Was lässt sich in Bezug auf die naive Hypothese sagen? Wenn Sie können, geben Sie eine Formel für $\mathrm{bz}(n)$ an. *Hinweis.* Man wird nicht umhin kommen, in der Formel für $\mathrm{bz}(n)$ zwischen geraden n und ungeraden n zu unterscheiden. Dies spiegelt sich im Übrigen auch in der Art der Ergebnisse E und E' wider.

Übung 35. An einem Bridgeturnier nehmen $4n$ Personen teil, die an n Tischen spielen. Jeder Spieler benötigt einen Partner, und jedes Paar Spieler benötigt ein weiteres Paar als Gegner. Eine Konfiguration ist eine Einteilung von Spielern in Gruppen bestehend aus zwei Paaren. Wie viele Konfigurationen gibt es?

Übung 36. In einem Haus wohnen Autobesitzer, die zusammen a Autos besitzen, und es gibt genau p Parkplätze. Auf wie viele Weisen können die Autobesitzer ihre Autos auf die Parkplätze stellen? *Anmerkung.* Wir nehmen an, dass die größtmögliche Anzahl Autos auf die Stellplätze geparkt wird. Ist $p \geq a$, so werden alle Autos geparkt. Falls aber $p < a$, so müssen einige Autos halt woanders geparkt werden ...

Kapitel 10

Verteilungen

Wir ziehen zunächst noch einige nützliche Folgerungen aus der Definition von $\binom{n}{k}$. Die Anzahl aller $k+1$-elementigen Teilmengen einer Menge mit $n+1$ Elementen kann wie folgt bestimmt werden. Man wähle ein Element $x \in M$. Für $X \subseteq M$ der Mächtigkeit $k+1$ gibt es zwei Fälle. **Fall 1.** $x \notin X$. Dann ist X eine $k+1$-elementige Teilmenge von $M-\{x\}$. **Fall 2.** $x \in X$. Dann ist $X-\{x\}$ eine k-elementige Teilmenge von $M-\{x\}$. Dies führt zu folgender Gleichung.

$$\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k} \tag{10.1}$$

Aus dieser Vorschrift ergibt sich ein leichtes Verfahren, wie man die Binomialkoeffizienten berechnen kann. Dies ist als das Pascalsche Dreieck bekannt, benannt nach Blaise Pascal (1623 – 1662).

$$\begin{array}{ccccccccccc} & & & & & 1 & & & & & n=0 \\ & & & & 1 & & 1 & & & & n=1 \\ & & & 1 & & 2 & & 1 & & & n=2 \\ & & 1 & & 3 & & 3 & & 1 & & n=3 \\ & 1 & & 4 & & 6 & & 4 & & 1 & n=4 \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \quad n=5 \end{array} \tag{10.2}$$

Man beginnt mit der ersten Zeile für $n = 0$. Anschließend füllt man das dreieckige Schema aus. Jede Zahl mit Ausnahme der Randzahlen hat zwei obere Nachbarn. Jede Zahl ist die Summe ihrer oberen Nachbarn. Zum Beispiel ist $10 = 4 + 6$, da 10 die oberen Nachbarn 4 und 6 hat.

Ferner haben wir gezeigt, dass $(x+y)^n = \sum_{i=0}^{n} \binom{n}{k} x^k y^{n-k}$. Setzen wir $x = y = 1$, so bekommen wir

$$\sum_{i=0}^{n} \binom{n}{k} = 2^n \tag{10.3}$$

Dies ist auch deswegen klar, weil $\binom{n}{k}$ die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge ist. Es gibt insgesamt 2^n solcher Teilmengen.

Setzen wir $x = 1$, $y = -1$, dann ergibt sich

$$\sum_{i=0}^{n} (-1)^k \binom{n}{k} = 0 \tag{10.4}$$

Also: die alternierende Summe über die Binomialkoeffizienten ist gleich 0. Etwa ist $1 - 4 + 6 + 4 - 1 = 0$. Ist n ungerade, so folgt dies unmittelbar aus der Tatsache, dass $\binom{n}{k} = \binom{n}{n-k}$ ist sowie mit jedem Term $(-1)^k \binom{n}{k}$ auch der Term $(-1)^{n-k} \binom{n}{n-k} = -(-1)^k \binom{n}{k}$ auftritt.

Im Folgenden wollen wir uns nun mit sogenannten Verteilungsproblemen befassen. Einige solcher Probleme haben wir schon vorher kennengelernt. Im Wesentlichen ist das Problem so beschrieben. Wir wollen n Bälle auf r Fächer verteilen. Wie viele Möglichkeiten gibt es? Ein analoges Problem ist dieses. Wir haben eine Menge B mit n Elementen und eine Menge F mit r Elementen. Wie viele Funktionen gibt es von B nach F? Dies haben wir schon errechnet. Die Anzahl ist r^n. Wir können nun einerseits Bedingungen an die Funktionen stellen; das heißt, wir bestimmen beispielsweise nur die injektiven, oder nur die surjektiven oder nur die bijektiven Funktionen. Auf der anderen Seite können wir auch von der Identität der Objekte absehen. Das heißt konkret, wir können annehmen, dass die Bälle bzw. die Fächer ununterscheidbar sind. Beide Möglichkeiten werden oft benutzt. Der Unterschied zwischen *unterscheidbar* und *ununterscheidbar* kommt zum Beispiel in dem Unterschied zwischen einer Menge und einer nichtwiederholenden Folge heraus. Die Folge F ordnet jedem Folgenglied einen Platz zu; die zugehörige Menge der Folgenglieder tut dies nicht. Sie sieht von der Reihenfolge ab. Wir veranschaulichen den Unterschied durch ein Beispiel. Es sei $B = \{1, 2, 3, 4\}$ und

$F = \{a, b, c\}$. Betrachte folgende Verteilungen:

$$\begin{array}{ll} V_1 & V_2 \\ a{:}() & a{:}() \\ b{:}(1) & b{:}(234) \\ c{:}(234) & c{:}(1) \end{array}$$

(10.5)

$$\begin{array}{ll} V_3 & V_4 \\ a{:}() & a{:}(3) \\ b{:}(3) & b{:}(124) \\ c{:}(124) & c{:}() \end{array}$$

Falls wir sowohl die Bälle unterscheiden wie die Fächer, so sind alle Verteilungen verschieden. Falls wir die Fächer nicht unterscheiden aber die Bälle, so sind V_1 und V_2 sowie V_3 und V_4 nicht mehr zu unterscheiden. Am besten sieht man das so: wir entfernen von den Fächern die Namen a, b und c. Dann haben wir nur noch die Information, dass bei V_1 beispielsweise ein Fach keinen Ball, ein anderes den Ball 1 und ein drittes die Bälle 2, 3 und 4 enthält. Anders ausgedrückt: falls wir durch Vertauschen der Namen der Fächer eine Verteilung V in die Verteilung V' überführen können, so sind V und V' in dem Falle gleich, wo wir die Fächer nicht mehr unterscheiden. Man sieht nun ebenso, dass, wenn wir die Bälle nicht mehr unterscheiden, nunmehr V_1 und V_3 gleich sind. Falls wir schließlich weder Fächer noch Bälle unterscheiden wollen, so sind alle vier Verteilungen gleich.

Ich gehe nunr die vier Verteilungen der Reihe nach durch.

Bälle und Fächer sind unterschieden. Betrachten wir die Verteilung V_1. Wir können sie als Funktion betrachten, die jedem Ball sein Fach zuordnet. V_1 ist dann $\{\langle 1, b\rangle, \langle c, 2\rangle, \langle c, 3\rangle, \langle c, 4\rangle\}$. In diesem Fall entspricht also die Anzahl der Verteilungen der Mächtigkeit der Menge F^B, wo F^B die Menge der Funktionen von B nach F bezeichnet.

Satz 10.1 $|M^N| = |M|^{|N|}$. *Hat also M m Element und N n Element, so hat M^N genau m^n Elemente.*

Beweis. Sei $M = \{x_0, x_1, \cdots, x_{m-1}\}$ und $N = \{y_0, y_1, \cdots, y_{n-1}$. Wir repräsentieren die Funktion durch eine n-lange Folge $\langle x_{j_0}, x_{j_1}, \cdots, x_{j_{n-1}}\rangle$, wo x_{j_i} dasjenige Element aus M ist, auf das y_i abgebildet wird. Mit anderen Worten, die Funktion $f : M \to N$ bekommt als Code die Folge $\sharp f := \langle f(y_0), f(y_1), \cdots, f(y_{n-1})\rangle$. Die Anzahl dieser Folgen ist nun genau das n-fache Produkt von $|M|$. Das ist aber m^n. ⊣

Bälle werden nicht unterschieden, Fächer schon. Ist nun der Ball nicht unterschieden, das Fach aber schon, so benötigen wir eine andere Repräsentation. Eine Möglichkeit ist wie folgt: wir notieren anstelle des Namens der Bälle nur deren Anzahl. So wird dann aus V_1 nurmehr $\{\langle a, 0\rangle, \langle b, 1\rangle, \langle c, 3\rangle\}$. Eine alternative Repräsentation benutzt sogenannte Multimengen. Diese sind technisch äquivalent.

Multimengen sind dasselbe wir ungeordnete Folgen. Die Definition mag etwas umständlich erscheinen, aber sie ist relativ einleuchtend, wenn man sie von der praktischen Seite her sieht. Eine ungeordnete Folge ist eine Folge, in der es nicht auf den Platz ankommt, den ein Element einnimmt. Dies drücken wir so aus, dass wir eine ungeordnete Folge als die Menge aller geordneten Folgen auffassen, welche durch Umordnung ineinander übergehen.

Definition 10.2 *Es sei X eine Menge, und F und G n-lange Folgen von Elementen aus X. Für $x \in X$ sei $j(x, F)$ die Anzahl der Folgenglieder, welche gleich x sind. Dies heiße der* ***Index*** *von x in F. Wir setzen $F \approx G$, falls für alle Elemente x aus X gilt $j(x, F) = j(x, G)$. Die Menge $M(F) := \{G : G \approx F\}$ heißt auch eine* ***Multimenge*** *M mit Elementen aus X oder* ***ungeordnete Folge****. Die* ***Mächtigkeit*** *von M ist definiert als die Länge von F.*

Diese Definition ist nicht besonders handlich. Wir notieren Multimengen so:

$$\{a, b, b, a, c, d, d, a, d\}_m \tag{10.6}$$

Der Index $_m$ deutet an, dass es sich um eine Multimenge handelt. Teilmengen von X sind Multimengen, in denen der Index eines jeden Elements nur 0 oder 1 ist. Wie auch sonst üblich, ist die oben hingeschriebene Folge nur ein Vertreter. Dieselbe Multimenge ist beschrieben durch

$$\{d, d, d, c, b, b, a, a, a\}_m \tag{10.7}$$

Netrachten wir die Verteilungen, wo wir Fächer unterscheiden, nicht aber Bälle. Eine Verteilung entspricht dann genau einer Multimenge über F, in der die Summe der Indizes gerade $|B|$ ist. Die Summe aller Indizes $j(x, F)$ ist aber gerade die Mächtigkeit der durch F repräsentierten Multimenge. Die Anzahl der Multimengen der Mächtigkeit r über einer Menge B der Mächtigkeit n lässt sich durch einen Trick berechnen. Ohne Beschränkung der Allgemeinheit ist $B = \{1, 2, \ldots, n\}$. Zu jeder Multimenge gibt es genau eine Auflistung der Elemente, die monoton wachsend ist. (Etwa ist $\{1, 1, 2, 2, 3\}_m$ eine solche Auflistung, nicht aber $\{3, 1, 1, 2, 2\}_m$.) Sei $M = \{x_1, x_2, \ldots, x_r\}_m$ eine Multimenge mit $x_i \leq x_{i+1}$. Nun setze $A(M) :=$

$\{x_1, x_2+1, x_3+2, x_4+3, \ldots, x_r+r-1\}$. $A(M)$ ist wohlgemerkt eine Menge, und es ist $x_i+i-1 < x_{i+1}+i$, nach Wahl der x_i. $A(M)$ ist eine r-elementige Teilmenge von $\{1, 2, \ldots, n+r-1\}$. Sei $Y \subseteq \{1, 2, \ldots, n+r-1\}$ eine r-elementige Menge, etwa $Y = \{y_1, y_2, \ldots, y_r\}$ mit $y_i < y_{i+1}$. Dann setze $B(Y) := \{y_1, y_2-1, y_3-2, \ldots, y_r-r+1\}$. $B(Y)$ ist der Repräsentant einer Multimenge der Mächtigkeit r über B. Diese Beziehung ist bijektiv. Also ergibt sich folgender Satz.

Satz 10.3 *Die Anzahl der Multimengen der Mächtigkeit k über einer Menge der Mächtigkeit n ist*

$$\binom{n+k-1}{k} = \frac{(n+k-1)^{\underline{k}}}{k!} \tag{10.8}$$

Bälle werden unterschieden, Fächer nicht. Seien nun um gekehrt die Bächer unterschieden, nicht aber die Fächer. Fächer sind Mengen von Bällen (die ja wohlunterschieden sind). Wir können also eine Verteilung auch als Funktion von Fächern nach Mengen von Bällen auffassen. So ist V_1 die Funktion $a \mapsto \emptyset, b \mapsto \{1\}, c \mapsto \{2, 3, 4\}$. Da jeder Ball in nur einem Fach liegt, sind diese Mengen paarweise disjunkt. Wir entfernen nun den Bezug zu den Fächern, indem wir nur noch das Mengensystem $\{f(x) : x \in F, f(x) \neq \emptyset\}$ betrachten, hier also $\{\{1\}, \{2, 3, 4\}\}$.

In dieser Darstellung entspricht einer Verteilung schlicht eine Partition der Menge B in höchstens (!) r Mengen. (Partitionsmengen dürfen nicht leer sein, Fächer schon.) Ist $r > n$, so existiert keine solche Partition. Die Anzahl der Partitionen einer n-elementigen Menge in r nichtleere Mengen bezeichnet man mit $S_{n,r}$.

Satz 10.4 *Die Anzahl der Verteilungen von n Bällen auf r Fächer, wobei Bälle nicht unterschieden werden, ist genau*

$$\sum_{i \leq r} S_{n,i} = S_{n,0} + S_{i,1} + \cdots + S_{n,r} \tag{10.9}$$

Weder Bälle noch Fächer werden unterschieden. Falls wir nun auch noch die Bälle nicht mehr unterscheiden, so ist die Anzahl der Möglichkeiten gerade die Anzahl der Möglichkeiten, die Zahl n in höchstens r von Null verschiedene Summanden zu zerlegen. Diese Zahl nennen wir $P_{n,r}$. Zum Beispiel ist $P_{7,3} = 4$,

denn

$$\begin{aligned} 7 &= 1+1+5 \\ &= 1+2+4 \\ &= 1+3+3 \\ &= 2+2+3 \end{aligned} \tag{10.10}$$

Über die Zahlen $S_{n,r}$ und $P_{n,r}$ lässt sich keine leichte Berechnungsvorschrift angeben. Es gilt aber folgender Sachverhalt.

Satz 10.5 *Sei $n > 0$. Es ist $P_{n,1} = 1$, $P_{n,2} = \frac{n}{2}$, falls n gerade und $P_{n,2} = \frac{n-1}{2}$, falls n ungerade.*

Beweis. Es ist klar, dass eine beliebige Zahl sich nur auf eine Weise als Summe einer einzigen Zahl darstellen lässt. Nun sei $n = 2k$ eine gerade Zahl. Dann ist für beliebiges i mit $0 < i < n$, $n = i + (n - i)$. Um Doppelzählungen zu vermeiden, überlegen wir uns, dass, falls $i > k$ ist, $n - i < k$ ist. Wir betrachten deswegen nur solche Summen $i_1 + i_2$, in denen $i_1 \leq i_2$ ist. (Dieses Verfahren wendet man ganz allgemein bei der Bestimmung der $P_{n,r}$ an.) Zu jeder Zahl i mit $0 < i \leq k$ gibt es genau eine Zerlegung von n, nämlich $n = i + (n - i)$, und es ist $i \leq n - i$. Für zwei Darstellungen $i + (n - i) = j + (n - j)$ mit $0 < i, j \leq k$ gilt $i = j$. Wir haben also exakt k viele solcher Darstellungen, das heißt genau $\frac{n}{2}$ viele. Falls nun n ungerade ist, also $n = 2k + 1$, muss man beachten, dass wiederum $0 < i \leq k$ muss. Dies ergibt den Wert $\frac{n-1}{2}$. ⊣

Will man $P_{n,r}$ für $r > 2$ exakt ausrechnen, muss man einige Mühe aufwenden. Betrachten wir kurz den Fall $r = 3$. Zwei Darstellungen $n = i_1 + i_2 + i_3$ und $n = j_1 + j_2 + j_3$ sind gleich, falls $\{i_1, i_2, i_3\} = \{j_1, j_2, j_3\}$. Eine Darstellung $n = i_1 + i_2 + i_3$ kann man immer so wählen, dass $i_1 \leq i_2 \leq i_3$. Ist dann $i_1 + i_2 + i_3 = j_1 + j_2 + j_3$ mit $j_1 \leq j_2 \leq j_3$, so gilt $i_1 = j_1$ und $i_2 = j_2$ und $i_3 = j_3$, oder aber es gilt $\{i_1, i_2, i_3\} \neq \{j_1, j_2, j_3\}$ (das heißt, die Darstellungen sind ungleich). Dies bedeutet, dass wir jede Darstellung tatsächlich nur einmal zählen. Nun geht man so vor. Man wählt i_1, und bestimmt die Anzahl aller Darstellungen von $n - i_1$ in Summen $i_2 + i_3$, wo $i_1 \leq i_2 \leq i_3$. Dies bedeutet, wir wollen nur solche Darstellungen von $n - i_1$ betrachten, in denen alle Summanden $\geq i_1$ sind. Man überlege sich, dass dies gerade die Anzahl aller Darstellungen von $n - 3i_1 + 2$ in Summen $k_1 + k_2$, $k_1, k_2 > 0$, ist. Denn ist $n - 3i_1 + 2 = k_1 + k_2$, so ist

$$n - i_1 = (k_1 + i_1 - 1) + (k_2 + i_1 - 1) \tag{10.11}$$

Mit $k_1 > 0$ ist $k_1 + i_1 - 1 \geq i_1$, und mit $k_1 \leq k_2$ ist $k_1 + i_1 - 1 \leq k_2 + i_1 - 1$. Dies erledigt die Darstellung von $n - i_1$. Nun muss man im Prinzip nur aufsummieren. Man beachte, dass man stets $i_1 \leq \frac{n}{3}$ hat. Größere i_1 muss man nicht betrachten.

4 Bälle auf 3 Fächer zu verteilen. Zu guter Letzt führe ich das Beispiel zu Ende. Werden sowohl Bälle als auch Fächer unterschieden, haben wir $3^4 = 81$ Verteilungen. Werden die Bälle nicht unterschieden, die Fächer aber wohl, so haben wir $\binom{4+3-1}{4} = \binom{6}{4} = \frac{6\cdot5\cdot4\cdot3}{4\cdot3\cdot2\cdot1} = 15$ Verteilungen.

(10.12)

1	$\{a,a,a,a\}_m$
2	$\{a,a,a,b\}_m$
3	$\{a,a,a,c\}_m$
4	$\{a,a,b,b\}_m$
5	$\{a,a,b,c\}_m$
6	$\{a,a,c,c\}_m$
7	$\{a,b,b,b\}_m$
8	$\{a,b,b,c\}_m$
9	$\{a,b,c,c\}_m$
10	$\{a,c,c,c\}_m$
11	$\{b,b,b,b\}_m$
12	$\{b,b,b,c\}_m$
13	$\{b,b,c,c\}_m$
14	$\{b,c,c,c\}_m$
15	$\{c,c,c,c\}_m$

Für die anderen Verteilungen gibt es keine geschlossenen Formeln, deshalb zähle ich sie nur auf. Können wir Bälle unterscheiden, Fächer nicht, so bekommen wir $S_{4,1} + S_{4,2} + S_{4,3}$ Verteilungen. Es ist $S_{4,1} = 1$, da es nur eine Partitionsmenge geben darf. Aus der Aufzählung ergibt sich, dass $S_{4,2} = 7$ und $S_{4,3} = 6$. Insgesamt

ergeben sich 14 Verteilungen.

(10.13)

1	$\{\{1,2,3,4\}\}$
2	$\{\{1\},\{2,3,4\}\}$
3	$\{\{2\},\{1,3,4\}\}$
4	$\{\{3\},\{1,2,4\}\}$
5	$\{\{4\},\{1,2,3\}\}$
6	$\{\{1,2\},\{3,4\}\}$
7	$\{\{1,3\},\{2,4\}\}$
8	$\{\{1,4\},\{2,3\}\}$
9	$\{\{1,2\},\{3\},\{4\}\}$
10	$\{\{1,3\},\{2\},\{4\}\}$
11	$\{\{1,4\},\{2\},\{3\}\}$
12	$\{\{2,3\},\{1\},\{4\}\}$
13	$\{\{2,4\},\{1\},\{3\}\}$
14	$\{\{3,4\},\{1\},\{2\}\}$

Und zum Schluss noch der Fall, wo weder Bälle noch Fächer unterschieden werden. Wir notieren in den Verteilungen nur noch die Anzahl der Elemente. Dann bekommen wir $P_{4,1} = 1$, $P_{4,2} = 2$ und $P_{4,3} = 1$. Denn die Verteilungen 2 - 5 fallen zusammen, ebenso die Verteilungen 6 - 9 und die Verteilungen 10 - 14. Wir haben nur noch 4 verschiedene Verteilungen.

Übungen

In den folgenden Aufgaben werden recht große Zahlen auftreten. Aus diesem Grunde ist es von Vorteil, die Aufgaben stets abstrakt zu lösen und nicht nur auszurechnen (was mit Hilfe des Computers nicht schwer sein dürfte). Man kann schon einiges erreichen, wenn man nur die Formeln bestimmt hat, nach denen man ausrechnen muss.

Übung 37. Eine Tüte Gummibären enthalte stets genau 50 Gummibären. Gummibären gibt es in genau 3 Farben. Es sei von jeder Farbe mindestens ein Gummibär in einer Tüte enthalten. Wie viele verschiedene Farbmischungsverhältnisse gibt es? Geben Sie zunächst eine Benennung der Zahl in Form einer Formel an (welcher Typ von Zählkoeffizient) und berechnen Sie seinen Wert.

Übung 38. Desgleichen wie in der vorigen Übung, aber ohne die Bedingung, dass eine bestimmte Farbe auftreten muss. *Hinweis.* Vergessen Sie bitte auch diesmal nicht, eine Formel anzugeben, bevor Sie sich an's Ausrechnen machen!

Übung 39. Wie in den vorigen beiden Aufgaben. Nun seien aber die Farben konkret gegeben: rot, gelb und grün. Bestimmen Sie also die Farbmischungsverhältnisse rot:gelb:grün mit und ohne die Bedingung, dass eine Farbe mindestens einmal vertreten sein muss.

Übung 40. Stellen sie alle Verteilungen von drei Kugeln auf drei Fächer dar. Wie viele gibt es wenn man (a) Kugeln und Fächer unterscheidet, (b) nur Fächer unterscheidet, (c) nur Kugeln unterscheidet, (d) weder Kugeln noch Fächer unterscheidet?

Übung 41. Es sei $N = \{1, 2, \ldots, n\}$. Einer Multimenge K über N ordnen wir als *Typ* die Folge $\langle j(1, F), j(2, F), \ldots, j(n, F)\rangle$. Zeige zunächst: jeder Multimenge über N entspricht genau eine Folge natürlicher Zahlen

$$\mathfrak{j} = \langle j(1), j(2), \ldots, j(n)\rangle \ .$$

Gegeben eine solche Folge, bestimmen Sie die Anzahl der geordneten Folgen G, deren ungeordnetes Gegenstück gerade der Multimenge des Typs $\mathfrak{j}$ entspricht. Diese Anzahl bezeichnet man mit

$$\binom{q}{j(1), j(2), \ldots, j(n)} \tag{10.14}$$

wobei $q = j(1) + j(2) + \ldots + j(n)$. *Hinweis.* Insbesondere ist im Falle $n = 2$ diese Zahl dann $\binom{q}{j(1), j(2)}$, welches (in anderer Notation) der allbekannte Binomialkoeffizient ist.

Kapitel 11

Graphen

Ein Paar $\mathfrak{G} = \langle E, K\rangle$, wo E eine beliebige, nichtleere Menge ist und $K \subseteq \binom{E}{2}$, heißt ein **Graph**. Falls nichts anderes gesagt wird, ist E endlich, und damit ist natürlich auch K endlich. E ist die Menge der **Ecken** und K die Menge der **Kanten** des Graphen. Eine Kante ist also nichts anderes als eine Paarmenge $\{u, v\} \subseteq E$. Wir schreiben oft uv (oder vu) für die Kante $\{u, v\}$. Wir sagen, u und v seien **benachbart** oder **adjazent** (in $\mathfrak{G}$), falls $uv \in K$. Ist ferner $u \in k$, $k \in K$, so heißt u mit k **inzident**. Zwei Kanten k und ℓ heißen **inzident**, falls $k \cap \ell \neq \emptyset$, das heißt, wenn sie eine gemeinsame Ecke haben. Ein paar Beispiele für Graphen.

Beispiel 22. Es sei $K = \binom{E}{2}$. Dann heißt der Graph **vollständig**. Im Fall, wo $E = n$ (also die Menge $\{0, 1, \cdots, n-1\}$) wird dieser Graph mit K_n bezeichnet. ⚽

Beispiel 23. Sei $E = S \cup T$, wobei $S \cap T = \emptyset$. Ferner bestehe jede Kante aus je einem Element aus S und einem Element aus T. Dann heißt der Graph **bipartit**. Er heißt vollständig bipartit, falls $K = \{\{u, v\} : u \in S, v \in T\}$. Ist $\sharp S = m$ und $\sharp T = n$, so bezeichnen wir den Graphen mit $K_{m,n}$. ⚽

Beispiel 24. Sei $E = \{e_1, e_2, \ldots, e_n\}$, und $K = \{\{e_i, e_{i+1}\} : 0 < i < n\}$. Dieser Graph heißt **linearer Graph der Länge** $n - 1$. ⚽

Beispiel 25. Sei $E = \{e_1, e_2, \ldots, e_n\}$ und $K = \{\{e_i, e_{i+1}\} : 0 < i < n\} \cup \{\{e_n, e_1\}\}$. Dieser Graph heißt schlicht ein **Kreis** der **Länge** $n-1$. (Wir können auch schreiben $K = \{\{e_i, e_j\} : j \equiv i + 1 \pmod{n}\}$.) ⚽

Beispiel 26. Es sei E die Menge der Folgen der Länge n über $\{0,1\}$. Es sei $d(\vec{x},\vec{y}) := \sharp\{i : x_i \neq y_i\}$ der sogenannte **Hammingabstand** von $\vec{x}$ und $\vec{y}$. Betrachte $K = \{\{\vec{x},\vec{y}\} : d(\vec{x},\vec{y}) = 1\}$. Dieser Graph heißt **(Hyper–)Würfel der Dimension** n. Für $n = 2$ ist dies genau ein Quadrat, für $n = 3$ genau der allbekannte Würfel. ⚽

Beispiel 27. Der **Petersen–Graph** sieht wie folgt aus. Es ist $E = E_i \cup E_a$, wobei $E_i = \{i_0, i_1, \ldots, i_4\}$ und $E_a = \{a_0, a_1, \ldots, a_4\}$. $K = K_a \cup K_{ia} \cup K_i$, wobei $K_a = \{\{i_m, i_n\} : m \equiv n+1 \pmod 5\}$, $K_{ia} = \{\{i_k, a_k\} : 0 \leq i < 5\}$ und $K_i = \{\{i_p, i_q\} : q \equiv p+2 \pmod 5\}$. Man kann sich den Petersen–Graph so vorstellen: $\langle E_i, K_i\rangle$ ist der sogenannte *Drudenfuß*, dem ein Fünfeck $\langle E_a, K_a\rangle$ umschrieben wird. ⚽

Zwei Graphen $G = \langle E, K\rangle$ und $H = \langle F, L\rangle$ heißen **isomorph**, falls es eine bijektive Abbildung $h : E \to F$ gibt, derart, daß für alle $u, v \in E$ gilt $uv \in K$ genau dann, wenn $h(u)h(v) \in L$. (Wir können dies etwas prägnanter ausdrücken. Es bezeichne $h[K] := \{\{h(u), h(v)\} : uv \in K\}$. Dann verlangen wir $h[K] = L$.) Es sind alle vollständigen Graphen mit gleicher Eckenzahl isomorph. Dies haben wir schon in der Schreibweise K_n zum Ausdruck gebracht; diese drückt lediglich eine Abhängigkeit von $n = \sharp E$ und nicht von E aus. Ebenso ist für den Isomorphietyp eines vollständigen bipartiten Graphen lediglich die Mächtigkeit der Mengen S und T ausschlaggebend.

Definition 11.1 *Es sei $\mathfrak{G} = \langle E, K\rangle$ ein Graph und u eine Ecke von $\mathfrak{G}$. Dann heißt $N(u) := \{v : uv \in K\}$ die Menge der **Nachbarn** von u. Für $S \subseteq E$ sei $N(S) := \{v : uv \in K$ für ein $u \in S\}$. Ferner ist $d(u) := \sharp N(u)$ der **Grad** von u. Ist $d(u) = 0$, so heißt u **isoliert**. $N^k(S)$ für $S \subseteq E$ sei wie folgt definiert.*

$$\begin{array}{lcl} N^0(S) & := & S \\ N^{k+1}(S) & := & N^k(S) \cup N(N^k(S)) \end{array} \tag{11.1}$$

*$Z(S) := \bigcup_{i\in\mathbb{N}} N^i(S)$ heißt die **Zusammenhangskomponente** von S. $\mathfrak{G}$ heißt **zusammenhängend**, falls $E = Z(\{x\})$ für ein $x \in E$ gilt.*

Es ist $N^k(S)$ die Menge aller Ecken, die von einer Ecke aus S in höchstens k Schritten erreichbar sind. Für endliche Graphen gilt: es existiert ein k dergestalt, daß $Z(S) = N^k(S)$ ist für alle k.

Definition 11.2 *Es sei $G = \langle E, K\rangle$ ein Graph und $S \subseteq E$. Dann sei $d(S)$ die kleinste Zahl derart, daß mit $E = N^d(S)$. Falls diese nicht existiert, so setze $d(S) := \infty$. Der **Durchmesser** von G ist*

$$d(G) := \max_{S\subseteq E, S\neq\emptyset} d(S) \tag{11.2}$$

Falls G endlich, so ist $d(G)$ endlich genau dann, wenn G zusammenhängend ist. Dann ist sogar $d(G) < \sharp E$.

Satz 11.3 *In einem endlichen Graphen gilt stets*

$$\sum_{u \in E} d(u) = 2 \cdot \sharp K \tag{11.3}$$

Beweis. Die linke Summe zählt alle Paare $\langle u, v \rangle$ derart, daß $uv \in K$. Da nun stets $u \neq v$ gilt, wenn $uv \in K$, so entspricht jeder Kante genau zwei Paaren. ⊣

Satz 11.4 *In jedem Graphen ist die Anzahl der Ecken ungeraden Grades eine gerade Zahl.*

Beweis. Sei E_u die Menge der Ecken, für die $d(u)$ ungerade ist, und E_g die Menge aller Ecken, für die $d(u)$ gerade ist. Dann ist nach dem vorigen Satz $2 \cdot \sharp K = \sum_{u \in E} d(u) = \sum_{u \in E_u} d(u) + \sum_{u \in E_g} d(u)$. Es ist $\sum_{u \in E_g} d(u)$ stets gerade, also ist auch $\sum_{u \in E_u} d(u)$ gerade. Dann ist E_u gerade. Das war zu zeigen. ⊣

Es sei nun als erstes ein Satz gezeigt, der gewissermaßen die erste Anwendung der Graphentheorie überhaupt darstellt, nämlich die Lösung des Königsberger Brückenproblems. In abstrakter Form dargestellt, lautet es so: *existiert eine Folge $F = k_1 k_2 \dots k_r$ von Kanten aus K derart, daß jede Kante aus K genau einmal auftritt, und so daß k_i mit k_{i+1} für $1 \leq i < r$ und k_r mit k_1 jeweils inzident sind*? Eine solche Folge heißt ein **Euler-Zug**. Ferner verabreden wir, eine Folge $u_1 u_2 \dots u_r$ von Ecken einen **Weg** der Länge $r - 1$ zu nennen, wenn $u_i u_{i+1} \in K$ für alle $1 \leq i < r$. Ein Weg ist **geschlossen**, falls $u_r = u_1$. Ist F ein Euler-Zug, so definiert dieser einen eindeutig bestimmten Weg. Denn seien $k_i k_{i+1}$ zwei aufeinanderfolgende Kanten aus F, dann hat $k_i \cap k_{i+1}$ genau ein Element. Es sei also u_{i+1} das eindeutig bestimmte v mit $v \in k_i \cap k_{i+1}$, und es sei u_1 das eindeutig bestimmte v mit $k_1 = v u_2$, u_{r+1} das eindeutig bestimmte v mit $k_r = u_r v$. Wir nennen einen Weg **nichtwiederholend**, falls $u_i = u_j$ nur dann gilt wenn $i = j$ oder $\{i, j\} = \{1, r\}$. Ein nichtwiederholender, geschlossener Weg heiße **Kreis**.

Satz 11.5 *In einem Graphen existiert ein Euler-Zug genau dann, wenn der Graph zusammenhängend ist und keine Ecke einen ungeraden Grad hat.*

Beweis. Die Bedingungen sind notwendig. Denn wenn $\mathfrak{G}$ nicht zusammenhängend ist, gibt es keine Ecke, von der aus alle Ecken erreichbar sind. Ferner: ist W ein Euler-Zug der Länge r, so ist u_i, $1 < i \leq r$, stets inzident mit $u_i u_{i+1}$ und $u_{i-1} u_i$ (und diese Kanten sind verschieden). Genauso ist u_{r+1} mit $u_1 u_{r+1}$ und

$u_r u_{r+1}$ inzident. Jede Ecke ist also mit einer geraden Anzahl Kanten inzident. Nun also zur Umkehrung. Zunächst einmal zeigen wir: in einem Graphen, in dem jede Ecke geraden Grad hat, existiert ein Kreis durch einen gegebene Ecke. Sei u_1 also gegeben. Wir wählen eine beliebige zu u_1 adjazente Ecke u_2. Sei $\mathfrak{G}_1 := \langle E, K - \{\{u_1, u_2\}\}\rangle$. In $\mathfrak{G}_1$ haben u_1 und u_2 ungeraden Grad. Also existiert eine zu u_2 adjazente Ecke u_3. Es gilt $u_3 \neq u_1$ (sowie auch $u_3 \neq u_2$). Induktiv definieren wir eine Folge u_i, derart daß $u_1 u_2 \dots u_i$ ein nichtwiederholender Weg ist. Ferner setzen wir

$$\mathfrak{G}_i := \langle E, K - \{\{u_i, u_{i+1}\} : 1 \leq j < i\}\rangle \tag{11.4}$$

Ist $u_i \neq u_1$, so hat u_i einen ungeraden Grad in $\mathfrak{G}_i$. (Denn wir haben aus $\mathfrak{G}$ genau eine mit u_i inzidente Kante entnommen.) Also existiert in $\mathfrak{G}_i$ eine zu u_i inzidente Ecke u_{i+1}. Ist $u_{i+1} = u_j$ für ein $j \leq i$, so gilt sicher $j < i - 1$. Also haben wir einen Kreis. Ist andererseits u_{i+1} verschieden von allen u_j, so ist $u_1 u_2 \dots u_{i+1}$ ein nichtwiederholender Weg. Nun haben wir zwar noch nicht gezeigt, daß ein Kreis durch u_1 existiert, aber wir können aus K nun die Kantenmenge des eben konstruierten Kreises entfernen und erhalten so einen Graphen, in dem jede Ecke einen geraden Grad hat, und insbesondere ist der Grad von u_1 nicht Null ist (da wir keine mit u_1 inzidente Kante entnommen haben). Nun machen wir das gleiche Spiel nochmal mit dem neuen Graphen. Es ist klar, daß bei diesem Wegnehmen jede Kante einmal drankommt. Also ist u_1 in einem Kreis, da es in einer Kante ist. Dies zeigt unsere erste Behauptung. Der Satz folgt nun so. Wir wählen einen Kreis K_1 mit Kantenmenge γ_1. $W_1 := K_1$. Dann sei $\mathfrak{G}^1 := \langle E, K - \gamma_1\rangle$. Da wir zu jedem Punkt genau zwei inzidente Kanten entnehmen, hat in $\mathfrak{G}^1$ jede Ecke geraden Grad. Falls die Kantenmenge noch nicht leer ist, existiert eine Kante in $K - \gamma_1$. Es existiert sogar eine Kante $uv \notin \gamma_1$, derart, daß eine Ecke auf dem Kreis liegt, etwa u. Wir wählen nun in $\mathfrak{G}^1$ einen Kreis K_2 durch u. Nun definieren wir einen neuen Weg wie folgt: wir schieben bei u in K_1 den Kreis K_2 ein. Das Ergebnis ist ein geschlossener Weg W, auf dem keine Kante wiederholt wird. Sei γ_2 seine Kantenmenge. Wir setzen $\mathfrak{G}^2 := \langle E, K - \gamma_2\rangle$. Wir fahren so fort. Es existiert eine Kante uv, die nicht in γ_2 liegt, aber mit einer Ecke aus W_2 inzident ist. Andernfalls ist $\mathfrak{G}$ nicht zusammenhängend. ⊣

Übungen.

Übung 42. Bestimmen Sie den Durchmesser des n-dimensionalen Würfels und des Petersen-Graphs.

Übung 43. Geben Sie für beliebiges n einen Graphen mit n Ecken an, der den Durchmesser 2 hat, sowie einen Graphen mit Durchmesser $n - 1$.

Übung 44. Es sei $\mathfrak{G}$ ein Grpah ohne isolierte Ecken. Ein Weg in $\mathfrak{G}$ heißt **offener Euler-Zug**, falls alle Kanten genau einmal vorkommen, aber die erste Ecke nicht mit der letzten Ecke übereinstimmt. Zeigen Sie: genau dann gibt es in einem Graphen einen offenen Euler-Zug, wenn der Graph zusammenhängend ist und genau zwei Ecken einen ungeraden Grad haben. *Hinweis.* Da ist also gerade die Verallgemeinerung des Problems vom Haus des Nikolaus. Führen Sie dieses durch einen kleinen Trick auf Satz 11.5 zurück. Seien nämlich u und v genau die Ecken mit ungeradem Grad. Dann füge man zu dem Graphen die Kante uv hinzu. Dann geht alles wir gewünscht (beweisen!). Einzige Schwierigkeit: es kann sein, daß uv schon Kante des Graphen ist (wie beim Haus des Nikolaus). In diesem Fall muß man wieder einen kleiner Trick anwenden, der hier aber nicht verraten wird.

Übung 45. Zeigen Sie: genau dann ist $\mathfrak{G} = \langle E, K\rangle$ unzusammenhängend, wenn es zwei Mengen A und B gibt derart, daß $E = A + B$, $A \cap B = \emptyset$, und $K \subseteq \binom{A}{2} \cup \binom{B}{2}$.

Übung 46. Es habe $\mathfrak{G}$ keine isolierten Ecken. Zeigen Sie, daß $\mathfrak{G}$ genau dann zusammenhängend ist, wenn es einen geschlossenen Weg gibt, der jede Kante mindestens einmal enthält. *Hinweis.* Dieser Weg muß kein Euler–Zug sein!

Teil IV

Wahrscheinlichkeit

Kapitel 12

Wahrscheinlichkeitsräume

Die Definition von Wahrscheinlichkeitsräumen ist etwas komplex. Bevor ich die vollständige Version geben kann, werde ich zunächst einige Spezialfälle vorstellen. Intuitiv gesprochen treten Ereignisse mit einer gewissen Wahrscheinlichkeit auf. Wenn man eine Münze wirft, so wird sie entweder Kopf oder Zahl zeigen, und jedes dieser Ereignisse wird gleich häufig sein, was wir dadurch erklären, dass die Wahrscheinlchkeit des Ereignisses "Die Münze zeigt Kopf." genau $\frac{1}{2}$ ist und die Wahrscheinlichkeit von "Die Münze zeigt Zahl." ebenfalls genau $\frac{1}{2}$. Im Kontext der Wahrscheinlichkeitstheorie reden wir aber nicht von Ereignissen sondern von **Ergebnissen**. Dieser Wortwahl werde ich mich anschließen. Ähnlich ist es beim Würfel. Wir haben hier sechs verschiedene Ergebnisse, jedem von ihnen geben wir die gleiche Wahrscheinlichkeit, die dann $\frac{1}{6}$ sein muss. Wenn wir allerdings zwei Würfel haben, sagen wir einen roten und einen grünen, so gibt es 36 Ergebnisse, die wir durch Paare (i, j) repräsentieren können, wo i der Zahl auf dem roten Würfel entspricht und j der Zahl auf dem grünen Würfel. Alle sind wiederum gleich wahrscheinlich, und wir geben ihnen deshalb die Wahrscheinlichkeit $\frac{1}{36}$.

Um ein anderes Beispiel zu geben, nehmen wir jetzt als Ergebnisse nicht die Paare (i, j) sondern die Summe $i + j$. Das heißt, obwohl wir das Paar sehen, notieren wir als Ergebnis nur die Summe der Augen. In diesem Fall haben die Ergebnisse nicht mehr die gleiche Wahrscheinlichkeit. Wir haben als Ergebnisse die

Zahlen 2 bis 12, und die Wahrscheinlichkeiten sind wie folgt.

$$\begin{array}{llllll} p(2) & = \frac{1}{36} & p(3) & = \frac{2}{36} & p(4) & = \frac{3}{36} \\ p(5) & = \frac{4}{36} & p(6) & = \frac{5}{36} & p(7) & = \frac{6}{36} \\ p(8) & = \frac{5}{36} & p(9) & = \frac{4}{36} & p(10) & = \frac{3}{36} \\ p(11) & = \frac{2}{36} & p(12) & = \frac{1}{36} & & \end{array} \tag{12.1}$$

Man rechnet leicht nach, dass die Summe der Wahrscheinlichkeiten 1 ist. Wir haben also diesmal *keine* Gleichverteilung. Das heißt, die Ergebnisse sind in diesem Fall nicht alle gleich wahrscheinlich.

Warum ist das so? Die Erklärung kommt von dem vorigen Beispiel. Wir haben insgesamt 5 Möglichkeiten, eine 6 zu würfeln. Das sind die Paare $(1, 5)$, $(2, 4)$, $(3, 3)$, $(4, 2)$ und $(1, 5)$. Da wir jedem Paar die Wahrscheinlichkeit gegeben haben, bekommen wir $\frac{5}{36}$.

Kehren wir zu dem einfachen Würfel zurück. Es gibt 6 Ergebnisse, die durch die Zahlen 1 bis 6 repräsentiert werden. Außer den Ergebnissen gibt es auch sogenannte **Ereignisse**. Dies sind Mengen von Ergebnissen. Nehmen wir das Ereignis, eine gerade Zahl zu würfeln. Dieses ist offensichtlich die Menge $\{2, 4, 6\}$. Denn die Ergebnisse sind genau diejenigen, von denen wir sagen, wir hätten bei diesem Ergebnis eine gerade Zahl gewürfelt. Die Wahrscheinlichkeit eines Ereignisses ist nun die Summe der Wahrscheinlichkeiten der darin enthaltenen Ergebnisse.

Im endlichen Fall besitzen wir also eine Menge Ω von Ergebnissen (den Ergebnisraum) und eine Funktion $p : \Omega \to [0, 1]$ mit

$$\sum_{\omega \in \Omega} p(\omega) = 1 \tag{12.2}$$

Ist $A \subseteq \Omega$ eine Menge von Ergebnissen (also ein Ereignis), so setzen wir

$$P(A) := \sum_{\omega \in A} p(\omega) \tag{12.3}$$

Man beachte, dass ich einen anderen Buchstaben gewählt habe, nämlich P. Wir sagen, P sei die **Wahrscheinlichkeit** und dass p die ihre **Dichte** or **Verteilung** sei. Die Dichte wird also von Ergebnissen bestimmt, währen die Wahrscheinlichkeit auf Ereignissen definiert ist. Ist $\omega \in \Omega$ ein Ergebnis, so ist $P(\{\omega\}) = p(\omega)$. Da nun keinerlei Verwirrung eintreten kann, schreibt man $P(\omega)$ anstelle von $P(\{\omega\})$. Aus

diesen Definitionen können wir ein paar Folgerungen ableiten.

$$P(\varnothing) = 0 \tag{12.4}$$

$$P(\Omega) = 1 \tag{12.5}$$

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) \tag{12.6}$$

Die ersten beiden Folgerungen sind klar. Wir erwarten erstens, dass stets ein Ergebnis eintritt, sodass das Ereignis $\varnothing$ ("kein Ergebnis") niemals eintreten kann, also die Wahrscheinlichkeit 0 haben muss. Auf der anderen Seite tritt immer eines der vorgegebenen Ergebnisse ein. Aufgrund von (12.2) und der dritten Gleichung haben wir die zweite. Wenden wir uns also der dritten Behauptung zu. Wir leiten sie her, indem wir erst einmal einen Spezialfall ansehen, nämlich dass $A \cap B = \varnothing$. In diesem Fall ist

$$P(A + B) = \sum_{\omega \in A \cup B} p(\omega) = \sum_{\omega \in A} p(\omega) + \sum_{\omega \in B} p(\omega) = P(A) + P(B) \tag{12.7}$$

Dies ist nach Definition so. Falls nun $A \cap B \neq \varnothing$, so ist $A \cup B = A \cup (B - A)$, und diese Mengen sind disjunkt. Also ist $P(A \cup B) = P(A) + P(B - A)$. Ebenfalls ist $B = (B - A) \cup (B \cap A)$, wiederum mit disjunktion Mengen. Daraus folgt dann $P(B) = P(B - A) + P(A \cap B)$ oder auch $P(B - A) = P(B) - P(A \cap B)$. Zusammen ergibt sich die Formel $P(A \cup B) = P(A) + P(B) - P(A \cap B)$. Schließlich sei noch angemerkt, dass, wenn die A_i, $1 \leq i \leq n$, paarweise disjunkte Mengen sind, so ist

$$P(\bigcup_{i=1}^{n} A_i) = P(A_1) + P(A_2) + \cdots + P(A_n) \tag{12.8}$$

Dies ist alles, was man wissen muss, sofern Ω endlich ist.

Das ändert sich in dem Moment, wo Ω unendlich ist. Dann müssen wir die Strategie gründlich ändern. Nehmen wir zum Beispiel an, dass Ω die Menge der natürlichen Zahlen ist. Nehmen wir weiter an, jede Zahl hat die gleiche Wahrscheinlichkeit. In diesem Fall ist die Wahrscheinlichkeit einer jeder Zahl gleich — 0! Und das würde bedeutet, dass die Wahrscheinlichkeit eines beliebigen Ereignisses (= Menge von natürlichen Zahlen) ebenfalls gleich 0 ist. Dieser Zugang funkioniert also nicht mehr. In der Tat geht man hier umgekehrt vor: die Wahrscheinlichkeiten werden nicht den Ergebnissen gegeben sondern den Ereignissen. So würden wir zum Beispiel sagen, dass die Wahrscheinlichkeit, eine beliebige Zahl sei gerade, sei $\frac{1}{2}$, ebenso wie die Wahrscheinlichkeit, dass sie ungerade sei. Dies lässt sich allerdings nicht mehr mit den Wahrscheinlichkeiten für einzelne

Ergebnisse rechtfertigen. Damit dieser Ansatz funktioniert, müssen wir den Raum der Ereignisse speziell wählen. Wir müssen annehmen, dass es sich um eine boolesche Algebra handelt. Genauer verlangt man, dass in dieser Algebra auch der Schnitt (und die Vereinigung) einer abzählbaren Familie von Elementen existiert. Eine solche Struktur heißt eine σ–**Algebra**.

Beispiel 28. Hier ist ein nichttriviales Beispiel einer booleschen Algebra, welche nicht die volle Potenzmengenalgebra ist. Und zwar nehmen wir zunächst die Mengen $U(k, n)$ aller Zahlen, die bei Division durch n den Rest k lassen (also ist dann $0 \leq k \leq n-1$). Diese Mengen sollen die Wahrscheinlichkeit $\frac{1}{n}$ bekommen. Die davon erzeugte boolesche Algebra ist die Algebra aller Vereinigungen solcher Mengen. (Der Schnitt $U(n, k) \cap U(n', k')$ ist nach dem sogenannten Chinesischen Restsatz eine Vereinigung von Mengen der Form $U(\mathrm{kgV}\{n, n'\}, p)$ für gewisse p.) Eine σ-Algebra bekommen wir, indem wir beliebige abzählbare Schnitte und Vereinigungen zulassen. ⚽

Definition 12.1 *Ein **Wahrscheinlichkeitsraum** ist ein Tripel $\langle \Omega, \mathfrak{A}, P \rangle$, wo Ω eine Menge ist, die Menge der **Ergebnisse**, $\mathfrak{A} \subseteq \wp(\Omega)$ eine σ-Algebra, die Algebra der **Ereignisse** und $P : \mathfrak{A} \to [0, 1]$ eine Funktion, welche folgende Eigenschaften hat.*

1. $P(\varnothing) = 0$
2. $P(\Omega) = 1$,
3. *Falls A_i, $i \in I$, paarweis disjunkt sind und $|I| \leq \omega$, dann*

$$P(\bigcup_{i \in I} A_i) = \sum_{i \in I} P(A_i)$$

Eine Anmerkungen zur Notation. $\mathfrak{A}$ ist immer eine Algebra von Mengen über Ω. Deswegen schreiben wir auch nicht $0_{\mathfrak{A}}$ oder 0 für das Nullelement, sondern $\varnothing$. Die Operationszeichen sind Vereinigung ($\cup$), Schnitt ($\cap$) und relatives Komplement ($-$). Man beachte also, dass $-A = \Omega - A$.

Es folgen einige Beispiele.

Beispiel 29. Der Laplace Raum. Es sei Ω eine endlichen Menge mit n Elementen. $\mathfrak{A} := \wp(\Omega)$. Schließlich sei $P(A) := \frac{|A|}{n}$. In diesem Raum hat jedes Ergebnis die gleiche Wahrscheinlichkeit, nämlich $\frac{1}{n}$. Die obenstehenden Beispiele (eine faire Münze, ein Würfel) sind solche Räume. ⚽

Beispiel 30. Der Bernoulli Raum. Sei $\Omega = \{0, 1\}$, $\mathfrak{A} = \wp(\Omega)$. Mit $p := p(1)$, haben wir $q := p(0) = 1 - p$. 1 repräsentiert das Ergebnis des "Erfolgs", während 0 den "Mißerfolg" repräsentiert. Wetten sehen im Allgemeinen so aus. Mannschaft A spielt gegen Mannschaft B in einem Spiel. Mannschaft A gewinnt mit Wahrscheinlichkeit 75%, oder 0,75. Also ist $p = 0,75$ und $q = 0,25$. Der Bernoulli Raum ist der kleinste Wahrscheinlichkeitsraum, aber seine Nützlichkeit kann man kaum überschätzen. Man sagt, das Maß der Ungerechtigkeit einer "unfairen Münze", ist q/p gegen den Spieler. Wenn die Münze tatsächlich fair ist, dann ist $p = q = 1/2$ und dieser Quotient ist 1. Im dem Beispiel ist er $0,75/0,25 = 3$. Falls das Wettbüro der Überzeugung ist, dass die Chancen 3:1 stehen, dass A gewinnt, und Sie wetten zehn Euro dagegen, dann bietet Ihnen das Wettbüro höchstens 40 Euro, wenn A nicht gewinnt, und 0 wenn A gewinnt. Falls das Wettbüro kein Geld machen will, und die Chancen richtig einschätzt, so wird es genau 40 Euro zahlen. Allgemeiner sind die Zahlen wie folgt. Falls die Chancen $r : 1$ gegen Sie sind, dann bekommen Sie für jeden gesetzten Euro $r + 1$, falls Sie gewinnen und 0 Euro sonst. Um zu sehen, dass dies gerecht ist, muss man wissen, dass Sie in 1 von $r + 1$ (!) Fällen gewinnen. Und dann bekommen Sie $r + 1$ Euro. Macht 1 Euro im Durchschnitt. Langfristig wird niemand dadurch gewinnen. Der Beweis dafür wird noch geführt werden. Intuitiv ist es jedoch plausibel. Man beachte, dass Wettbüros natürlich Geld machen wollen, und so werden sie Wege finden, Ihnnen effektiv weniger als $r + 1$ Euro zu geben. Zum Beispiel sind im französischen Roulette die Chancen effektiv $\frac{1}{37}$, weil es ja noch die Null gibt, aber der Einsatzmultiplikator ist 36. Wetten Sie 10 Euro auf "rot", so bekommen Sie 20 Euro, falls Sie gewinnen. Aber Ihre Chancen sind nur $\frac{18}{37}$, etwas weniger als $\frac{1}{2}$. ⚽

Beispiel 31. Der Diskrete Raum. Ein Raum heißt **diskret**, falls $\mathfrak{A} = \wp(\Omega)$. In diesem Fall ist jede Menge von Ergebnissen ein Ereignis und besitzt eine Wahrscheinlichkeit. Insbesondere ist für jedes $\omega \in \Omega$ die Menge $\{\omega\}$ in $\mathfrak{A}$. Und wir haben $p(\omega) := P(\{\omega\})$. Dann gilt

$$P(A) = \sum_{\omega \in A} p(\omega) \tag{12.9}$$

Dies ist jedoch nur dann definiert, wenn Ω endlich oder abzählbar unendlich ist. Wir werden allerdings keine Räume gebrauchen, die von dieser Art sind. ⚽

Ich stelle jetzt einige abstrakte Konstruktionen für Wahrscheinlichkeitsräume vor. Sei $f : X \to Y$ eine Funktion und $U \subseteq X$ sowie $V \subseteq Y$. Dann setze

$$f[U] := \{h(x) : x \in U\} \tag{12.10}$$

$$f^{-1}[V] := \{x \in U : f(x) \in V\} \tag{12.11}$$

$f[U]$ wird das **direct image** von U unter f genannt und $f^{-1}[V]$ das **Urbild** von V unter f. Falls nun $\mathfrak{B} \subseteq \wp(V)$ eine boolesche Algebra ist so ist auch $\{f^{-1}[B] : B \in \mathfrak{B}\}$ eine boolesche Algebra. Der Beweis ist wie folgt.

1. $f^{-1}[\varnothing] = \varnothing$.
2. $f^{-1}[V \cup W] = f^{-1}[V] \cup f^{-1}[W]$. Denn $x \in f^{-1}[V \cup W]$ gdw. $f(x) \in V \cup W$ gdw. $f(x) \in V$ oder $f(x) \in W$ gdw. $x \in f^{-1}[V]$ oder $x \in f^{-1}[W]$.
3. $f^{-1}[Y - V] = X - f^{-1}[V]$. Denn $x \in f^{-1}[Y - V]$ gdw. $f(x) \in Y - V$ gdw. $f(x) \in Y$ und $f(x) \notin V$ iff $x \in X$ und nicht $x \in f^{-1}[V]$ gdw. $x \in X - f^{-1}[V]$.
4. $f^{-1}[V \cap W] = f^{-1}[V] \cap f^{-1}[W]$. Folgt aus (2) und (3), kann aber auch direkt gezeigt werden.

Sei nun eine Wahrscheinlichkeitsfunktion $P : \mathfrak{A} \to [0, 1]$ gegeben. Dann können wir einer Menge in $\mathfrak{B}$ nur dann eine Wahrscheinlichkeit zuordnen, wenn ihr volles Urbild in $\mathfrak{A}$ ist. Wir sagen also, $f : \Omega \to \Omega'$ sei **kompatibel mit** $\mathfrak{A}$, falls $f^{-1}[B] \in \mathfrak{A}$ für alle $B \in \mathfrak{B}$. In diesm Fall kann man jeder Menge aus $\mathfrak{B}$ eine Wahrscheinlichkeit zuweisen über

$$P'(B) := P(f^{-1}[B]) \tag{12.12}$$

Dies ist in der Tat eine Wahrscheinlichkeitsfunktion.

1. $P'(\Omega') = P(f^{-1}[\Omega']) = P(\Omega) = 1$.
2. $P'(\varnothing) = P(f^{-1}[\varnothing]) = P(\varnothing) = 0$.
3. Falls A und B disjunkt sind, so sind auch $f^{-1}[A]$ und $f^{-1}[B]$ disjunkt, und in diesem Fall ist $P'(A \cup B) = P(f^{-1}[A \cup B]) = P(f^{-1}[A] \cup f^{-1}[B]) = P(f^{-1}[A]) + P(f^{-1}[B]) = P'(A) + P'(B)$.

Proposition 12.2 *Sei $\langle \Omega, \mathfrak{A}, P\rangle$ ein endlicher Wahrscheinlichkeitsraum, $\mathfrak{B}$ eine boolesche Algebra über Ω' und $f : \Omega \to \Omega'$ eine surjektive Funktion kompatibel mit $\mathfrak{A}$. Setze $P'(B) := P(f^{-1}[A])$. Dann ist $\langle \Omega', \mathfrak{A}', P'\rangle$ ein Wahrscheinlichkeitsraum.*

Wir werden dies wie folgt ausschlachten. $\mathfrak{A}$ ist endlich und hat die Atome $A_1, \ldots, A_n$. Dann sei $\Omega' = \{1, \ldots, n\}$ und wir definieren f durch $f(x) := i$, wo $x \in A_i$. Dies ist wohldefiniert: jedes Element ist in einem und nur einem Atom der Algebra enthalten. Diese Funktion ist kompatibel mit $\mathfrak{A}$. Denn sei $S \subseteq \Omega'$. Dann ist

$$f^{-1}[S] = \bigcup_{i \in S} A_i \in \mathfrak{A} \tag{12.13}$$

Hier ist ein Beispiel. Sei etwas $\Omega = \{1, 2, 3, 4, 5, 6\}$, und

$$\mathfrak{A} = \{\varnothing, \{1, 2\}, \{3, 4, 5, 6\}, \Omega\}. \tag{12.14}$$

Dies ist eine boolesche Algebra, und sie hat zwei Atomw, $\{1, 2\}$ und $\{3, 4, 5, 6\}$. Jetzt definieren wir $f(1) := f(2) := \alpha$ und $f(3) := f(4) := f(5) := f(6) := \beta$. Dann ist $f(\varnothing) = \varnothing$, $f(\{1, 2\}) = \{\alpha\}$, $f(\{3, 4, 5, 6\}) = \{\beta\}$, and $f(\Omega) = \{\alpha, \beta\}$. Und schließlich wählen wir folgende Wahrscheinlichkeiten: $P(\{1, 2\}) = \frac{1}{3}$, $P(\{3, 4, 5, 6\}) = \frac{2}{3}$. Dann setzen wir $P'(\{\alpha\}) := \frac{1}{3}$ und $P'(\{\beta\}) = \frac{2}{3}$. Man beachte, dass der ursprüngliche Raum ein Lapace-Raum ist. Wir werfen einen Würfel und jedes Ergebnis hat dieselbe Wahrscheinlichkeit. Aber wir haben nur 4 Ereignisse darüber betrachtet. Das Ergebnis kann nunmehr als Bernoulli-Raum betrachtet werden mit $p = \frac{1}{3}$.

Dies besitzt eine unmittelbare Folge. Wir sagen, $\langle \Omega, \mathfrak{A}, P \rangle$ sei **reduzibel** auf $\langle \Omega', \mathfrak{A}', P' \rangle$, falls es eine Funktion $f : \Omega \to \Omega'$ gibt derart, dass $\mathfrak{A} = \{f^{-1}[B] : B \in \mathfrak{A}'\}$ und $P'(B) = P(f^{-1}[B])$ für alle $B \in \mathfrak{A}'$. Der zweite Raum hat also möglicherweise weniger Ereignisse, aber hat bis auf Isomorphie dieselbe Ereignisstruktur wie eine Teilalgebra von $\mathfrak{A}$, mit den entsprechenden Wahrscheinlichkeiten.

Proposition 12.3 *Jeder endliche Wahrscheinlichkeitsraum ist reduzibel auf einen diskreten Wahrscheinlichkeitsraum.*

Dies bedeutet, dass wir bei einem endlichen Raum im Grunde immer davon ausgehen können, dass die Atome Ergebnisse sind. Aber die abstrakte Theorie erlaubt eine Flexibilität, die durchaus sinnvoll ist.

Als nächstes schauen wir uns eine andere Standardsituation an. Seien Ω_1 und Ω_2 Ergebnismengen von Eexperimenten E_1 und E_2, respectively. Dann ist $\Omega_1 \times \Omega_2$ die Ergebnismenge von einem Experiment, wo erst E_1 und dann E_2 durchgeführt werden. Zum Beispiel nehme man an, wir werfen eine Münze und dann einen Würfel. Dann ist das Ergebnis des kombinierten Experiments ein Paar $\langle \ell, m \rangle$, wo $\ell \in \{\mathrm{H}, \mathrm{T}\}$ und $m \in \{1, 2, 3, 4, 5, 6\}$. Was für Ereignisse müssen wir nun ansetzen? Wenn $A_1 \in \mathfrak{A}_1$ und $A_2 \in \mathfrak{A}_2$, so haben wir gewiss das Ereignis $A_1 \times A_2$. Aber dies reicht nicht, um eine boolesche Algebra zu bekommen. Denn die Menge der

Produkte ist nicht unter Vereinigung und Komplement abgeschlossen, wohl aber unter Schnitt. Sei etwa $\Omega_1 = \Omega_2 = \{0, 1\}$ und $\mathfrak{A}_1 = \mathfrak{A}_2 = \wp(\{0, 1\})$. Die Menge $\{\langle 0, 1\rangle, \langle 1, 0\rangle\}$ ist die Vereinigung der Mengen $\{1\} = \{\langle 0, 1\rangle\}$ und $\{1\}\times\{0\} = \{\langle 1, 0\rangle\}$. Aber sie hat nicht die Form $A \times B$ für irgendwelche A, B.

Stattdessen nehmen wir also als Ereignisse sämtliche Vereinigungen von Produkten.

$$\mathfrak{A}_1 \otimes \mathfrak{A}_2 := \left\{ \bigcup_{i=1}^{p} A_i \times B_i : \text{ for all } i\text{: } A_i \in \mathfrak{A}_1, B_i \in \mathfrak{A}_2 \right\} \tag{12.15}$$

Die Wahrscheinlichkeiten sind wie folgt.

$$(P_1 \times P_2)(A \times B) := P_1(A) \cdot P_2(B) \tag{12.16}$$

Es ist ein wenig trickreich zu zeigen, dass dies tatsächlich einen Wahrscheinlichkeitsraum definiert. Der Grund ist, dass wir eine solche Vereinigung immer als Vereinigung disjunkter Mengen darstellen können. Ich mache dies für den Fall vor, wo wir zwei Mengen haben. Man beachte, dass $(A \times B) \cap (A' \cap B') = (A \cap A') \times (B \cap B')$. Dies und (12.6) ergibt

$$P((A \times B) \cup (A' \times B')) = P(A \times B) + P(A' \times B') - P((A \cap A') \times (B \cap B')) \tag{12.17}$$

Dies erinnert an die Tatsache, dass der Schnitt von zwei Rechtecken wieder ein Rechteck ist. Wenn wir also die Summe von Wahrscheinlichkeiten nehmen, so kann es passieren, dass wir gewisse Mengen mehrfach zählen.

Die Wahrscheinlichkeiten der Mengen auf der rechten Seite sind definiert; und so ist die der Menge auf der linken.

Definition 12.4 *Seien $\mathcal{P}_1 = \langle \Omega_1, \mathfrak{A}_1, P_1\rangle$ und $\mathcal{P}_2 = \langle \Omega_2, \mathfrak{A}_2, P_2\rangle$ Wahrscheinlichkeitsräume. Dann ist $\mathcal{P}_1 \otimes \mathcal{P}_2 := \langle \Omega_1 \times \Omega_2, \mathfrak{A}_1 \otimes \mathfrak{A}_2, P_1 \times P_2\rangle$ ein Wahrscheinlichkeitsraum, der sogenannte* ***Produktraum****.*

Ich gebe eine Anwendung. Es sei eine Bernoulli Experiment mit $p = 0,6$ gegeben. Dies definiert einen Raum $\mathcal{P}$. Wir wiederholen nun dieser Experiments. Alternativ dazu können wir ein einziges Experiment durchführen, in dem der Wahrscheinlichkeitsraum nunmehr $\mathcal{P} \otimes \mathcal{P}$ ist. Die Algebra der Ereignisse ist die Potenzmengenalgebra $\wp(\{0, 1\} \times \{0, 1\})$. Ferner haben wir

$$p(\langle 0, 0\rangle) = 0,36,\ p(\langle 0, 1\rangle) = p(\langle 1, 0\rangle) = 0,24,\ p(\langle 1, 1\rangle) = 0,16 \tag{12.18}$$

Die Wahrscheinlichkeiten summieren sich zu 1, wie man leicht nachprüft.

Kapitel 13

Bedingte Wahrscheinlichkeit

Nehmen wir an, eine Person hat 3 Kinder. Nehmen wir ferner an, dass die Wahrscheinlichkeit, dass ein Kind eine Junge ist, genau $\frac{1}{2}$ sei. Die Wahrscheinlichkeit, genau einen Jungen und zwei Mädchen zu haben, ist dann $\frac{3}{8}$. (Das ist gerade $\binom{3}{1}$ dividiert durch 8.) Nun nehmen wir an, Sie wissen, dass A wenigstens ein Mädchen hat.Was ist die Wahrscheinlichkeit dafür, dass A genau einen Jungen hat? Die Wahrscheinlichkeit kann nicht dieselbe sein. Denn man beachte, dass die Wahrscheinlichkeit, dass A drei Jungen hat, nunmehr Null sein muss. Wüsste man nicht, dass A (wenigstens) ein Mädchen hat, so wäre die Wahrscheinlichkeit, drei Jungen zu haben, genau $\frac{1}{8}$. Nun ist sie 0. Die Wahrscheinlichkeiten haben sich also geändert.

Machen wir uns an die Berechnung. Die Wahrscheinlichkeit, wenigstens ein Mädchen zu haben, ist $\frac{7}{8}$. Die Wahrscheinlichkeit, genau einen Jungen zu haben, ist $\frac{3}{8}$. Wenn es genau einen Jungen gibt, so gibt es wenigstens ein Mädchen, also stehen die Wahrscheinlichkeiten im Verhältnis 3 : 7. Also erwarten wir, dass die Wahrscheinlichkeit, genau einen Jungen zu haben *unter der Bedingung, wenigstens ein Mädchen zu haben*, genau $\frac{3}{7}$ ist. Wie sind wir darauf gekommen? Wir betrachten dazu ein Ereignis A und fragen, was seine Wahrscheinlichkeit ist *unter der Bedingung, dass B*. Wir müssen insgesamt vier Fälle unterscheiden. A kann der Fall sein oder nicht, ebenso kann B der Fall sein oder nicht. Da wir nun aber ausgeschlossen haben, dass B nicht der Fall ist, haben wir den Raum der Möglichkeiten von 4 auf 2 reduziert. Die Wette steht $P(A \cap B) : P((-A) \cap B)$. Also ist die Wahrscheinlichkeit, dass A der Fall ist unter der Bedingung, dass B, in Zeichen $P(A|B)$, genau

$$P(A|B) = \frac{P(A \cap B)}{P(A \cap B) + P((-A) \cap B)} = \frac{P(A \cap B)}{P(B)} \tag{13.1}$$

Definition 13.1 *Die **bedingte Wahrscheinlichkeit** von A unter der Bedingung, dass B, in Zeichen P(A|B), ist genau*

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \tag{13.2}$$

Diese Zahl ist nicht definiert für $P(B) = 0$.

Der letzte Satz ist einigermaßen wichtig. Es ist nicht nur so, dass die Berechnungsformel keinen Wert ergibt, wenn $P(B) = 0$. Es macht auch intuitiv keinen Sinn, einen zu geben. Denn was soll bittesehr die Wahrscheinlichkeit eines Ereignisses sein unter einer Bedingung, die nie eintreten kann? In der klassischen Logik sagt man, aus einer Kontradiktion folge alles. Ist also B ausgeschlossen, so können wir ebenso behaupten, A trete *immer* ein (also $P(A) = 1$) wie auch, A trete *nie* (also $P(A) = 0$). Oder irgendwas dazwischen. Aber das kann ja nicht sein. Also ist $P(A|B)$ in diesem Fall offenkundig nicht sinnvoll definierbar.

(13.2) ist bekannt als das **Bayessche Gesetz der bedingten Wahrscheinlichkeiten**. Wir können daraus eine Menge Folgerungen ziehen. Zunächst einmal können wir die Wahrscheinlichkeit $P(A \cap B)$ berechnen.

$$P(A \cap B) = P(A|B)P(B) \tag{13.3}$$

Ferner, da $A = (A \cap B) \cup (A \cap (-B))$ und die Mengen disjunkt sind, haben wir

$$P(A) = P(A|B)P(B) + P(A| - B)P(-B) \tag{13.4}$$

Das bedeutetn, dass die Wahrscheinlichkeit eines Ereignisses auf der Basis der bedingten Wahrscheinlichkeiten einer Mengenfamilie B_i, $i \in I$, errechnet werden kann, sofern diese Familie eine Partition von Ω bildet. (Das bedeutet, dass die B_i nichtleer und paarweise disjunkt sein müssen, sowie $\bigcup_{i \in I} B_i = \Omega$.)

Drehen wir die Rollen von A and B in (13.2) um, so bekommen wir

$$P(B|A) = \frac{P(B \cap A)}{P(A)} = \frac{P(A \cap B)}{P(B)} \cdot \frac{P(B)}{P(A)} = P(A|B) \cdot \frac{P(B)}{P(A)} \tag{13.5}$$

Solange also die einzelnen Wahrscheinlichkeiten bekannt sind (oder die Chancen von A relativ zu B), können wir die Wahrscheinlichkeit von B unter der Bedingung, dass A ausrechnen, sofern wir die Wahrscheinlichkeit von A unter der Bedingung, dass B, kennen. Um zu sehen, warum dies so wichtig ist, nehmen wir

noch einmal den Münzwurf. Angenommen, wir haben eine unfaire Münze mit $p = 0,4$; das sei die Wahrscheinlichkeit, Kopf (K) zu werfen. Werfen Sie die Münze nunmehr zehn Mal. Nehmen wir nun an, Sie werfen die Folge

$$\text{K, Z, Z, K, K, Z, K, K, Z, Z} \tag{13.6}$$

Statt, dass K wie erwartet 4 mal auftritt, tritt es hier 5 mal auf. Wir können nun berechnen, wie groß die Wahrscheinlichkeit ist, dass *dieses* Ergebnis unter der genannten Wahrscheinlichkeit eintritt. Es ist

$$\binom{10}{5} \cdot 0,4^5 \cdot 0,6^5 = 0,201 \tag{13.7}$$

Nehmen wir nun an, die Münze ist fair. Dann ist die Wahrscheinlichkeit

$$\binom{10}{5} \cdot 0,5^5 \cdot 0,5^5 = 0,236 \tag{13.8}$$

Die Wahrscheinlichkeit, K 5 mal zu werfen, ist größer, wenn die Münze fair ist, als wenn sie es nicht ist und stattdessen $p = 0,4$.

Nun wollen wir eine ganz andere Frage stellen: *gegeben diese Wurffolge*, was ist die Wahrscheinlichkeit dafür, dass die Münze mit $p = 0,4$ unfair ist gegenüber der Wahrscheinlichkeit, dass sie fair ist? Um dies zu beantworten, sei B das Ereignis, dass die Münze mit $p = 0,4$ unfair ist, N das Ereignis, dass sie fair ist. Sei ferne F das Ereignis, dass die Münze in einem 10 fachen Wurd 5 mal Kopf zeigt. Wir nehmen an (was etwas unrealistisch ist), dass entweder N oder B der Fall ist. Also ist $P(N) + P(B) = 1$. Setze $\alpha := P(B)$. Wir haben dann

$$P(F|B) = 0,201, P(F|N) = 0,236 \tag{13.9}$$

Wir wollen nun den Wert von $P(B|F)$ bestimmen. Dies ist

$$P(B|F) = P(F|B) \cdot \frac{P(B)}{P(F)} = 0,201 \cdot \frac{\alpha}{P(F)}. \tag{13.10}$$

Wir müssen also noch die Wahrscheinlichkeit von F wissen. Es ist

$$\begin{aligned} P(F) &= P(F \cap B) + P(F \cap N) \\ &= P(F|B)P(B) + P(F|N)P(N) \\ &= 0,201\alpha + 0,236(1-\alpha) = 0,236 - 0,035\alpha. \end{aligned} \tag{13.11}$$

Also bekommen wir

$$P(B|F) = 0,201 \cdot \frac{\alpha}{0,236 - 0,035\alpha} \tag{13.12}$$

Falls B und N gleich wahrscheinlich sind, haben wir $\alpha = 1/2$ und so

$$P(B|F) = 0,201 \cdot \frac{1}{2(0,236 - 0,0185)} = 0,201 \cdot \frac{1}{0,438} = 0,4621. \tag{13.13}$$

Also ist die Wahrscheinlichkeit, dass die Münze unfair ist, $0,4621$ und dementsprechend ist $0,5379$ die Wahrscheinlichkeit, dass sie fair ist, *unter der Bedingung, dass sie nur unfair mit* $p = 0,4$ *sein kann, wobei beide Hypothesen gleiche Wahrscheinlichkeit besitzen*.

Diese Argumentation ist sehr häufig, sie ist gewissermaßen zur Routine in den experimentellen Wissenschaften geworden. Man hat mehrere Hypothesen, sagen wir H_1, H_2, $\cdots$, H_n, welche sogenannte "a priori" Wahrscheinlichkeiten haben, $P(H_i)$, $i = 1, 2, \cdots, n$. Mit diesen bestimmt man die Wahrscheinlichkeit, dass ein Ereignis E eintritt. Dies sind dann die Wahrscheinlichkeiten $P(E|H_i)$. Man führt das Experiment durch und erhält E. Nun ist die Frage: was ist die Wahrscheinlichkeit von den Hypothesen H_i, nun, da das Experiment den Ausgang E genommen hat? Man möchte, in der Sprache der experimentellen Wissenschaft, die "a posteriori Wahrscheinlichkeiten" der Hypothesen H_i bestimmen. Diese sind nach Definition $P(H_i|E)$. Abstrakt kann man diese wie folgt bestimmen. Wir haben

$$P(H_i|E) = P(E|H_i)\frac{P(H_i)}{P(E)} \tag{13.14}$$

Alles, was wir bestimmen müssen, ist $P(E)$. Wir machen hier dasselbe, wie vorher. Wir haben angenommen, dass die Hypothesen die Wahrscheinlichkeiten $P(H_i)$ besitzen, und dass diese Wahrscheinlichkeiten sich zu 1 addieren. Eine dieser Hypothesen tritt ein. Also ist $\Omega = \bigcup_{i=1}^{n} H_i$, wobie die Mengen paarweise disjunkt sind. Also haben wir $E = \bigcup_{i=1}^{n}(E \cap H_i)$. Und so bekommen wir

$$P(E) = \sum_{i=1}^{n} P(E|H_i)P(H_i) \tag{13.15}$$

Dies setzen wir in (13.14) ein und bekommen

$$P(H_i|E) = P(E|H_i)\frac{P(H_i)}{\sum_{i=1}^{n} P(E|H_i)P(H_i)} \tag{13.16}$$

Falls A nicht von B abhängt, erwarten wir, dass die bedingte Wahrscheinlichkeit $P(A|B)$ gleich $P(B)$ ist. Dies bedeutet, dass $P(A \cap B) = P(A|B)P(B) = P(A)P(B)$. Dies führt zu folgender Definition.

Definition 13.2 (Unabhängigkeit) *Es seien A und B Ereignisse in einem Wahrscheinlichkeitsraum $\mathcal{P} = \langle \Omega, \mathfrak{A}, P \rangle$. Wir nennen A und B* ***unabhängig (voneinander)****, falls $P(A \cap B) = P(A) \cdot P(B)$. Seien $\mathfrak{B}_1$ und $\mathfrak{B}_2$ zwei Unteralgebren von $\mathfrak{A}$. $\mathfrak{B}_1$ und $\mathfrak{B}_2$ heißen* ***unabhängig****, falls für alle $B_1 \in \mathfrak{B}_1$ und $B_2 \in \mathfrak{B}_2$ gilt $P(B_1 \cap B_2) = P(B_1) \cdot P(B_2)$.*

Ich gebe ein Beispiel, das später noch auftreten wird. Man betrachte den Raum $\mathcal{P} \otimes \mathcal{Q}$, wo $\mathcal{P} = \langle \Omega, \mathfrak{A}, P \rangle$ und $\mathcal{Q} = \langle \Omega', \mathfrak{A}', P' \rangle$. Die Mengen $A \times B$ haben die Wahrscheinlichkeiten $P_2(A \times B) := P(A)P(B)$. Dies bedeutet, dass

$$\begin{aligned} P_2(A \times \Omega') &= P(A) \cdot P'(\Omega') = P(A) \\ P_2(\Omega \times B) &= P(\Omega) \cdot P'(B) = P(B) \end{aligned} \tag{13.17}$$

Nun haben wir

$$\begin{aligned} P_2((A \times \Omega') \cap (\Omega \times B)) &= P_2((A \cap \Omega) \times (\Omega \cap B)) \\ &= P_2(A \times B) = P(A) \cdot P(B) \\ &= P_2(A \times \Omega') \cdot P_2(\Omega \times B) \end{aligned} \tag{13.18}$$

Proposition 13.3 *Die Mengen $A \times \Omega'$ und $\Omega \times B$ sind unabhängig in dem Raum $\mathcal{P} \otimes \mathcal{Q}$.*

Sei ferner $\mathfrak{B}_1$ die Algebra der Mengen der Form $A \times \Omega'$ und $\mathfrak{B}_2$ die Algebra der Mengen der Form $\Omega \times B$. Zunächst zeigen wir, dass dies in der Tat Unteralgebren sind.

Proposition 13.4 *Seien $\mathfrak{A}$ und $\mathfrak{B}$ nichttriviale boolesche Algebren. Die Abbildung $i_1 : A \mapsto A \times 1_B$ ist eine Einbettung von $\mathfrak{A}$ in $\mathfrak{A} \otimes \mathfrak{B}$. Ebenso ist die Abbildung $i_2 : B \mapsto 1_A \times B$ eine Einbettung von $\mathfrak{B}$ in $\mathfrak{A} \otimes \mathfrak{B}$.*

Beweis. Zunächst zeige ich, dass die Abbildung i_1 injektiv ist: seien dazu A, C Mengen mit $A \times 1_B = C \times 1_B$. Da $1_B \neq \varnothing$ bedeutet dies, dass es ein $b \in 1_B$ gibt. Für jedes $a \in A$, ist $\langle a, b \rangle \in A \times 1_B$, also $\langle a, b \rangle \in C \times 1_B$, und so $a \in C$. Ebenso ist für alle $c \in C$, $\langle c, b \rangle \in C \times 1_B$, und so $\langle c, b \rangle \in C \times 1_B$, weshalb $c \in A$. Also ist $A = C$. $i_1(A \cup C) = (A \cup C) \times 1_B = (A \times 1_B) \cup (C \times 1_B) = i_1(A) \cup i_1(C)$. Auch ist

$i_1(-A) = (-A)\times 1_B = A\times(-1_B)\cup(-A)\times(-1_B)\cup -(A\times 1_B) = (-A)\times 1_B = -i_B(A)$. Ebenso zeigt man die zweite Behauptung. ⊣

Die Algebren $i_1(\mathfrak{A})$ und $i_2(\mathfrak{A})$ sind unabhängig, wie wir gerade gezeigt haben. Sie stellen die Algebra der Ereignisse dar, dass wir das Experiment zum ersten Mal durchführen ($\mathfrak{B}_1$) und zum zweiten Mal ($\mathfrak{B}_2$). Das Beruhigende ist, dass die Gruppierung der beiden Experimente in ein einziges die Wahrscheinlichkeiten der Ereignisse nicht ändert.

Satz 13.5 *Seien $\mathcal{P} = \langle\Omega, \mathfrak{A}, P\rangle$ und $\mathcal{Q} = \langle\Omega', \mathfrak{A}', P'\rangle$ Wahrscheinlichkeitsräume. Dann sind die Algebren $i_{\Omega'}[\mathfrak{A}] = \{A\times\Omega' : A\in\mathfrak{A}\}$ und $j_\Omega[\mathfrak{A}'] = \{\Omega\times B : B\in\mathfrak{A}'\}$ unabhängige Unteralgebren von $\mathfrak{A}\otimes\mathfrak{A}'$.*

Nachtrag

Der Fall der nachträglichen Anpassung der Wahrscheinlichkeiten wirft Fragen auf, denen man sich stellen sollte. Ich wähle noch einmal den Fall, wo wir wissen, dass die Münze fair ist oder nicht und dass sie dann mit $4:6$ Kopf zeigt. Die Wahrscheinlichkeit $P(p = 0,4)$ werde mit α bezeichnet. Wir führen nun das Experiment n mal durch, und das Ergebnis sei k mal Kopf. (Es ist möglich, das Argument mit identischen Ergebnis — indem man einen gewissen fixen Ausgang des Experiments benutzt anstelle des Ereignisses "k mal K". Dies ist so, weil wir ja verschiedene Sequenzen in ein einziges Ereignis zusammenfassen, die aber dieselbe Wahrscheinlichkeit haben. Man sollte im Allgemeinen aber große Vorsicht walten lassen.) Wir schreiben $\beta(n,k)$ für die Wahrscheinlichkeit, dass dies geschieht, wenn die Münze unfair ist. Und wir schreiben $\nu(n,k)$ für die Wahrscheinlichkeit, dass dies passiert, wenn die Münze fair ist. Wir haben

$$\nu(n,k) = \binom{n}{k}\frac{1}{2^n} \tag{13.19}$$

$$\beta(n,k) = \binom{n}{k}0,4^k 0,6^{n-k} \tag{13.20}$$

Die unbedingte, a priori Wahrscheinlichkeit von "k mal Kopf" ist jetzt

$$\begin{aligned}&\nu(n,k)P(p=0,5) + \beta(n,k)P(p=0,4)\\ =&\binom{n}{k}(0,5^n(1-\alpha) + 0,4^k 0,6^{n-k}\alpha)\end{aligned} \tag{13.21}$$

Wir sind an der a posteriori Wahrscheinlichkeit interessiert, dass die Münze mit $p = 0,4$ gezinkt ist, sofern sich "k mal Kopfëreignet hat. Diese Wahrscheinlichkeit

ist

$$
\begin{aligned}
& P(p = 0,4|k \text{ mal Kopf}) \\
=& P(k \text{ mal Kopf}|p = 0,4)\frac{P(p = 0,4)}{P(k \text{ mal Z})} \\
=& \binom{n}{k} 0,4^k 0,6^{n-k} \frac{\alpha}{\binom{n}{k}(0,5^n(1-\alpha) + 0,4^k 0,6^{n-k}\alpha)} \\
=& 0,4^k 0,6^{n-k} \frac{\alpha}{0,5^n(1-\alpha) + 0,4^k 0,6^{n-k}\alpha} \\
=& \frac{\alpha}{(0,5/0,4)^k (0,5/0,6)^{n-k}(1-\alpha) + \alpha}
\end{aligned} \tag{13.22}
$$

Für eine reelle Zahl ρ schreibe

$$
f_\rho(\alpha) := \frac{\alpha}{\rho(1-\alpha) + \alpha} \tag{13.23}
$$

Der spezielle Fall oben betraf $n = 10$ und $k = 5$. In diesem Fall ist die a posteriori Wahrscheinlichkeit gegeben eine a priori Wahrscheinlichkeit α

$$
f(\alpha) = 0,201 \frac{\alpha}{0,236 - 0,035\alpha} \tag{13.24}
$$

In diesem Fall ist also $\rho = 0,236/0,201$. Dies ist das Update unserer a priori Wahrscheinlichkeiten. Es ergeben sich mehrere Fragen. Erstens, ist es wichtig, welche a priori Wahscheinlichkeiten wir gewählt hatten? Die Antwort ist leicht: es ist in der Tat wichtig. Um das zu sehen, setze man einfach neue Werte in die Funktion f ein. Sei zum Beispiel $\alpha = 0,25$. Dann haben wir

$$
\begin{aligned}
f(0,25) =& \frac{0,201}{4(0,236 - 0,035/4)} \\
=& \frac{0,201}{0,944 - 0,035} \\
=& \frac{0,201}{0,909} \\
=& 0,2211
\end{aligned} \tag{13.25}
$$

Wenn man also der Meinung ist, die Wahrscheinlichkeit dafür, dass die Münze fair ist, sei $0,75$, dann wird man dies jetzt mit der Wahrscheinlichkeit $0,7789$ glauben. Zweite Frage: gibt es a priori Wahrscheinlichkeiten, die sich durch das

Experiment nicht ändern? Intuitiv gesprochen sind das Annahmen, die durch das Experiment absolut bestätigt wurden. Wir fragen also, ob es α gibt derart, dass

$$f(\alpha) = \alpha \tag{13.26}$$

Oder

$$0,201\frac{\alpha}{0,236 - 0,035\alpha} = \alpha \tag{13.27}$$

Die erste Lösung ist $\alpha = 0$. Unter Ausschluss dieses Extremfalls können wir durch α dividieren und bekommen

$$\begin{aligned} \frac{0,201}{0,236 - 0,035\alpha} &= 1 \\ 0,201 &= 0,236 - 0,035\alpha \\ 0,035\alpha &= 0,035 \\ \alpha &= 1 \end{aligned} \tag{13.28}$$

Es gibt also zwei (!) a priori Wahrscheinlichkeiten, die nicht durch das Experiment geändert werden. Diese sind $\alpha = 0$ and $\alpha = 1$. Sie repräsentieren einerseits die Gewissheit, dass die Münze fair ist, und die Gewissheit, dass sie es nicht ist. Gerade die zweite Tatsache ist etwas merkwürdig. Wie kann bittesehr das Faktum, dass die Münze 5 mal Kopf zeigt nicht unsere Meinung berühren, dass die Münze unfair ist? Die Antwort ist einfach: ist die Wahrscheinlichkeit der Hypothese 1, so muss sie gelten. Das Ereigniss kann eintreten, aber eine alternative Hypothese ist bereits ausgeschlossen. Keine endliche Evidenz kann das ändern.

Man ist versucht, diese Zahlen wie folgt zu interpretieren. Sicher, die a posteriori Wahrscheinlichkeiten ist $f(\alpha)$ und nicht α. Wenn wir dies wissen, können wir uns fragen: was wäre denn, wenn wir schon mit $f(\alpha)$ anstelle von α angefangen hätten? Dann würden wir offenkunding bei $f^2(\alpha) = f(f(\alpha))$ landen. Und hätten wir *damit* angefangen, so wären wir jetzt bei $f^3(\alpha)$, und so weiter. Es stellt sich heraus, dass die Folge der $f^n(\alpha)$ folgende Eigenschaft hat. Ist $\alpha = 1$ so ist $f(\alpha) = 1$, und dann haben wir schon ein Gleichgewicht. Ebenso, wenn $\alpha = 0$ ist. Wenn $0 < \alpha < 1$, dann ist $f(\alpha) < \alpha$, und wir bekommen eine fallende Folge

$$\alpha > f(\alpha) > f^2(\alpha) > f^3(\alpha) > \dots \tag{13.29}$$

Denn

$$0,201\frac{\alpha}{0,236 - 0,035\alpha} < \alpha \tag{13.30}$$

ist gleichbedeutend ($\alpha \neq 0$ (!)) mit

$$0,201\frac{1}{0,236-0,035\alpha} < 1 \tag{13.31}$$

was wiederum nichts anderes ist als

$$0,201 < 0,236 - 0,035\alpha \tag{13.32}$$

oder

$$0,035\alpha < 0,035 \tag{13.33}$$

Mit anderen Worten: $\alpha < 1$, was der Fall ist.

Der Grenzwert dieser Folge ist 0. Und in diesem Fall haben wir, dass die a posteriori Wahrscheinlichkeiten auch die a priori Wahrscheinlichkeiten sind. $\alpha = 0$ ist eine stabile Lösung. Jede Abweichung führt uns wieder zu ihr zurück. Die andere Gleichgewichtslösung, $\alpha = 1$, ist dagegen instabil. Man ist geneigt, dies als alleinige Lösung anzusehen.

Aber das ist nicht korrekt. Denn was wir tun, ist, dieselben Daten mehrfach zu verwenden, um unsere Wahrscheinlichkeiten erneut zu revidieren. Dies ist gleichbedeutend damit, dass wir das Experiment mehrfach (mit gleichem Ausgang) wiederholen. Aner wir haben das Experiment gar nicht wiederholt, wir haben es nur *einmal* durchgeführt. Insofern dürfen wir unsere Wahrscheinlichkeiten auch nur *einmal* revidiered. Um zu dem Schluss zu kommen, dass wir den sicheren Glauben, als effektiv das Wissen haben, dass die Münze fair ist, ist nicht durch das Experiment gedeckt und deshalb gefährlich. In der Wahrscheinlichkeitstheorie ist Wissen zeitabhängig. Wahrscheinlichkeiten sind es deswegen auch. Experimente raten uns dazu, Wahrscheinlichkeiten anzupassen. Wenn wir das getan haben, sinde die Daten eingepreist worden und dürfen nicht noch einmal verwendet werden. Natürlich können sie dazu dienen, anderer Leute Wahrscheinlichkeiten zu ändern, aber das ist eine andere Sache. Dies zu wissen, ist sehr wichtig. So hat man lange Zeit überall lesen können, dass Spinat gut für uns ist, weil es Eisen enthält. Man würde aufgrund der Vielzahl an Quellen denken, dass es sich hier um eine fest etablierte Tatsache handelt. In der Tat aber gründeten sich all diese Ratschläge auf eine einzige Untersuchung, die vor vielen Jahrzehnten durchgeführt worden war. Die wiederholte Erwähnung dieser Studie sollte dann eben *nicht* zur erneuten Anpassung der Wahrscheinlichkeiten führen.

Wir können auch formal beweisen, dass dies ist, was wir erwarten sollten. Man beachte folgende Gleichung.

$$\begin{aligned} f_\rho(f_\rho(\alpha)) =& \frac{\frac{\alpha}{\rho(1-\alpha)+\alpha}}{\rho\left(1-\frac{\alpha}{\rho(1-\alpha)+\alpha}\right)+\frac{\alpha}{\rho(1-\alpha)+\alpha}} \\ =& \frac{\alpha}{\rho(\rho(1-\alpha)+\alpha-\alpha)+\alpha} \\ =& \frac{\alpha}{\rho^2(1-\alpha)+\alpha} \\ =& f_{\rho^2}(\alpha) \end{aligned} \tag{13.34}$$

Schauen wir auf die Zahl ρ, dass wir k von n mal gewinnen. Diese Zahl ist

$$\pi_{k,n} = (0,5/0,4)^k(0,5/0,6)^{n-k} \tag{13.35}$$

Man beachte, dass

$$\pi_{2k,2n} = \pi_{k,n}^2 \tag{13.36}$$

Wir schließen daraus, dass $f^2(\alpha) = f_{\pi_{10,20}}(\alpha))$. Das bestärkt die Behauptung, dass das zweimalige Anpassen der Wahrscheinlichkeiten der zweimaligen Durchführung des Experiments mit gleichem Ausgang entspricht.

Kapitel 14

Zufallsvariable

Es sei $\mathcal{P} = \langle \Omega, \mathfrak{A}, P \rangle$ ein Wahrscheinlichkeitsraum und $X : \Omega \to \mathbb{R}$. Wir nennen X eine **Zufallsvariable**, wenn für jedes $a \in \mathbb{R}$ und $I = [a, b]$ gilt $X^{-1}(\{a\}) \in \mathfrak{A}$ und $X^{-1}[I] \in \mathfrak{A}$. Der Grund für diese Bedingung ist, dass wir wollen, dass $X^{-1}[A] \in \mathfrak{A}$ wann immer A eine gewisse Menge von rellen Zahlen ist (im Allgemeinen eine sogenannte Borel Menge, aber es genügt zu verlangen, dass das Urbild einer Einermenge bzw. eines Intervals in der Algebra ist). Falls $\mathcal{P}$ diskret ist, so ist jede Funktion in die reellen Zahlen eine Zufallsvariable.

Beispiel 32. Nehmen wir an, ein Arzt habe zwei Sorten von Patienten, eine mit Versicherung A und die andere mit Versicherung B. Versicherung A zahlt pro Besuch 40 Euro für ihre Versicherten, Versicherung B 55. Es ist $\Omega = \{A, B\}$, $\mathfrak{A} = \wp(\Omega)$. Die Funktion $X : \{A, B\} \to \mathbb{R}$ definiert durch $f(A) := 40$ und $f(B) := 55$ ist eine Zufallsvariable über dem Raum $\langle \{A, B\}, \wp(\{A, B\}), P \rangle$, wo $P(A) = p$ und $P(B) = 1 - p$. Angenommen, $p = \frac{1}{3}$; wie viel Geld bekommt der Arzt im Durchschnitt von jedem Patienten? Die Antwort ist

$$\frac{1}{3} \cdot 40 + \frac{2}{3} \cdot 55 = 50 \tag{14.1}$$

Dieser Wert ist bekannt als der *Erwartungswert* der Zufallsvariablen X. ⚽

Definition 14.1 (Erwartungswert) *Der **Erwartungswert** einer Zufallsvariable X ist definiert durch*

$$\mathrm{E}(X) := \sum_{x \in \mathbb{R}} x \cdot P(X = x) \tag{14.2}$$

wobei $P(X = x) = P(X^{-1}(\{x\}))$.

Wir sehen, dass dies nur dann definiert ist, wenn $X^{-1}(\{x\})$ ein Ereignis ist. Wir betrachten einen Spezialfall, wenn P eine Dichtefunktion p hat und der Raum höchstens abzählbar ist. Dann kann man die Formel wie folgt umschreiben.

$$\mathrm{E}(X) := \sum_{\omega\in\Omega} X(\omega)\cdot p(\omega) \tag{14.3}$$

Es gibt sehr viele Anwendungen für diese Definition. Zum Beispiel haben die Worten des Deutschen eine bestimmte Wahrscheinlichkeit, und die Funktion, X, die jedem Wort seine Länge zuordnet, ist eine Zufallsvariable auf dem diskreten Raum aller Mengen von Worten des Deutschen. Dann ist also $\mathrm{E}(X)$ die erwartete Länge eines beliebigen Wortes. Dies ist nicht die Durchschnittslänge, die ja wie folgt berechnet wird.

$$\frac{\sum_{\vec{x}\in L} X(\vec{x})}{|L|} \tag{14.4}$$

Denn hier geht jedes Wort mit gleichem Gewicht ein. Sondern es ist gewissermaßen die gewichtete Durchschnittslänge. Sie erlaubt zum Beispiel abzuschätzen, wie viel Buchstaben ein Text hat, wenn er n Worte enthält. Oder auch: man wähle aus einem Text zufällig ein Wort aus. Welche Länge erwarten wir?

Kehren wir noch einmal zum Beispiel 32 zurück. Die Durchschnittliche Versicerhungssumme ist $47,50$ Euro (das Mittel der beiden Beträge). Aber der Arzt bekommt mehr, weil er im Durchschnitt mehr Patienten hat, die die besser zahlende Versicherung haben. Bei einem anderen Arzt mag das natürlich anders sein.

Nehmen wir wieder an, wir haben eine Zufallsvariable X auf einem Raum $\mathcal{P}$. Es wird aus der Definition klar, dass X kompatibel mit der Ereignisalgebra ist und dieses deswegen einen Wahrscheinlichkeitsraum auf dem Bild $X[\Omega]$ definiert, wie in Kapitel 12 besprochen. Statt also über Versicherungen und Patienten zu reden, können wir auch direkt über Zahlungen sprechen. Der Raum ist dann $\{40, 55\}$ und die Wahrscheinlichkeiten sind $P'(40) = \frac{1}{3}$ und $P'(55) = \frac{2}{3}$.

Dies ist eine andere Art, auf das Thema zu sehen, und es gibt keinen Vorzug der einen Art über die andere. Es hilft aber zu verstehen, warum es auch andere Räume als Laplace-Räume gibt. Nehmen wir nämlich an, dass Ω ein Raum von Ergebnissen ist; falls wir sonst nichts weiter wissen, ist die beste Annahme, die wir machen können, die, dass alle Ergebnisse die gleiche Wahrscheinlichkeit haben. Dies ist die "Nullhypothese". So erwarten wir, dass Würfel fair sind und jede Zahl die Wahrscheinlichkeit $\frac{1}{6}$ besitzt. Aber wenn wir nun zwei Würfel zugleich werfen und nur die Summe mitteilen, so haben die Ergebnisse 2, 3, bis

12, die aber aus gutem Grund nicht gleich wahrscheinlich sind. Denn sie entstehen aus der Zusammelegung von Ergebnissen, die wir als gleich wahrscheinlich annehmen müssen. Wir definieren eine Variable $X(\langle x, y\rangle) := x + y$. Im zweiten Schritt betrachten wir den induzierten Wahrscheinlichkeitsraum auf der Menge $\{2, 3, \cdots, 12\}$. Die Wahrscheinlichkeit einer Zahl z ist $X^{-1}(\{z\})$. Der neue Raum ist kein Laplace-Raum.

Nehmen wir an, dass $A \subseteq \Omega$. Dann setze

$$I(A)(\omega) := \begin{cases} 1 & \text{falls } \omega \in A \\ 0 & \text{sonst.} \end{cases} \tag{14.5}$$

Die Funktion $I(A)$ heißt auch die **characteristische Funktion** von A. Sie ist eine Zufallsvariable, und wir können ihren Erwartungswert berechnen.

$$\mathrm{E}\, I(A) = \sum_{\omega\in\Omega} p(\omega) I(A)(\omega) = \sum_{\omega\in A} p(w) = P(A) \tag{14.6}$$

Proposition 14.2 *Es sei A endlich. Dann ist* $\mathrm{E}\, I(A) = P(A)$. ⊣

Sind X und Y Zufallsvariable, so können wir neue Funktionen $X + Y$, αX und $X \cdot Y$ wie folgt definieren.

$$(X + Y)(\omega) := X(\omega) + Y(\omega) \tag{14.7}$$
$$(\alpha X)(\omega) := \alpha \cdot X(\omega) \tag{14.8}$$
$$(X \cdot Y)(\omega) := X(\omega) \cdot Y(\omega) \tag{14.9}$$

Diese sind nicht unbedingt wieder Zufallsvariable.

Proposition 14.3 *Es seien X und Y Zufallsvariable. Falls $X + Y$ und αX Zufallsvariable sind, gilt*

$$\mathrm{E}(X + Y) = \mathrm{E}(X) + \mathrm{E}(Y) \tag{14.10}$$
$$\mathrm{E}(\alpha X) = \alpha\, \mathrm{E}(X) \tag{14.11}$$

Beweis. Ausrechnen. Wir nehmen der Einfachheit halber an, P habe eine Dichte.

$$\begin{aligned}
\mathrm{E}(X+Y) &= \sum_{\omega\in\Omega}(X+Y)(\omega)p(\omega)\\
&= \sum_{\omega\in\Omega}(X(\omega)+Y(\omega))p(\omega)\\
&= \sum_{\omega\in\Omega}X(\omega)p(\omega)+Y(\omega)p(\omega)\\
&= \sum_{\omega\in\Omega}X(\omega)p(\omega)+\sum_{\omega\in\Omega}Y(\omega)p(\omega)\\
&= \mathrm{E}(X)+\mathrm{E}(Y)
\end{aligned} \tag{14.12}$$

Also

$$\begin{aligned}
\mathrm{E}(\alpha X) &= \sum_{\omega\in\Omega}(\alpha X)(\omega)p(\omega)\\
&= \sum_{\omega\in\Omega}\alpha X(\omega)p(\omega)\\
&= \alpha\sum_{\omega\in\Omega}X(\omega)p(\omega)\\
&= \alpha\,\mathrm{E}(X)
\end{aligned} \tag{14.13}$$

⊣

Diese Formeln sind sehr wichtig. Ich gebe eine unmittelbar Anwendung. Nehmen wir an, wir haben einen Bernoulli-Raum $\mathcal{P}$ und eine Zufallsvariable X. Der Erwartungswert is $\mathrm{E}(X)$. Der Erwartungswert ist für jeden Patienten gleich, egal wer kommt. Es sind 50 Euro pro Patient, also 100 für zwei Patienten. Machen wir also ein Bernoulli-Experiment und führen es zweimal durch. Dies können wir auch als einen einzigen Raum sehen, $\mathcal{P}\otimes\mathcal{P}$. Jetzt haben wir die Zufallsvariablen $X_1(\langle x,y\rangle) = X(x)$ und $X_2(\langle x,y\rangle) = X(y)$. Die erste Variable gibt den Wert des ersten "Experiments" und die zweite den des zweiten. Die Variable $\frac{1}{2}(X_1+X_2)$ gibt uns das arithmetische Mittel dieser Werte.

$$\mathrm{E}\left(\frac{1}{2}(X_1+X_2)\right) = \mathrm{E}(X) \tag{14.14}$$

Oder auch: der Erwartungswert von X_1+X_2 ist $2\,\mathrm{E}(X)$. Dies kann man leicht auf eine n-fache Ausführung verallgemeinern.

Der Erwartungswert ist nicht unbedingt ein Wert, den die Variable tatsächlich annimmt; ein Beispiel haben wir schon gesehen. Ein Wert für die Abweichung, die die Variable von ihrem Erwartungswert zeigt, ist die sogenannte **Varianz**.

$$\mathrm{V}(X) = \mathrm{E}(X - \mathrm{E}(X))^2 \tag{14.15}$$

Nehmen wir zum Beispiel die Varianz der Identität auf einem Bernoulli Raum. Zunächst einmal müssen wir den Erwartungswert ausrechnen. Es sei $p := p(1)$ und $q := p(0) = 1 - p$.

$$\mathrm{E}\, I = p \cdot 1 + q \cdot 0 = p \tag{14.16}$$

Es gibt zwei Ergebnisse, 0 und 1, und die Zufallsvariable wirft 0 auf 0 und 1 auf 1. Also ist

$$\begin{aligned} \mathrm{V}\, I &= p \cdot (1 - \mathrm{E}\, I)^2 + q \cdot (0 - \mathrm{E}\, I)^2 \\ &= p(1-p)^2 + q(-p)^2 \\ &= pq^2 + qp^2 \\ &= pq(q+p) \\ &= pq \end{aligned} \tag{14.17}$$

Dies wird später noch nützlich sein. Die **Standardabweichung** von X, $\sigma(X)$, ist wie folgt definiert

$$\sigma(X) := \sqrt{\mathrm{V}(X)} \tag{14.18}$$

Man beachte, dass $X - \mathrm{E}(X)$ eine Zufallsveriable ist, die für jedes ω die Differenz $X(\omega) - \mathrm{E}(X)$ ausgibt. Diese Differenz wird quadriert, und dies wird über alle ω summiert. Aber die Summe ist durch die Wahrscheinlichkeiten gewichtet. Im Falle des Arztes bekommen wir $(X - \mathrm{E}(X))(A) = -10$ und $(X - \mathrm{E}(X))(B) = 5$. Also ist

$$\mathrm{V}(X) = \frac{1}{3} \cdot (-10)^2 + \frac{2}{3} \cdot 5^2 = \frac{150}{3} = 50 \tag{14.19}$$

(Dies ist auch der Erwartungswert. Das ist reiner Zufall.) Also ist $\sigma(X) = \sqrt{50} \approx 7.071$. Die Zahlung, die der Arzt bekommt, weicht im Mittel um 7.071 Euro vom Erwartungswert, also 50 Euro, ab. Die Standardabweichung misst also die zu erwartende Abweichung der Zahlungen. Ist diese 0, so gibt es keinerlei Abweichungen. Je größer sie wird, um so größer die zu erwartende Abweichung.

Die Formel für die Varianz kann wie folgt vereinfacht werden.

$$\mathrm{V}(X) = \mathrm{E}(X^2) - (\mathrm{E}(X))^2 \tag{14.20}$$

Zum Beweis beachte man, dass

$$\begin{aligned} \mathrm{E}(X - \mathrm{E}\,X)^2 &= \mathrm{E}(X - \mathrm{E}\,X)(X - \mathrm{E}\,X) \\ &= \mathrm{E}(X^2 - 2X \cdot \mathrm{E}\,X + (\mathrm{E}\,X)^2) \\ &= \mathrm{E}(X^2) - 2\,\mathrm{E}((\mathrm{E}\,X) \cdot X) + (\mathrm{E}\,X)^2 \\ &= \mathrm{E}(X^2) - 2(\mathrm{E}\,X)(\mathrm{E}\,X) + (\mathrm{E}\,X)^2 \\ &= \mathrm{E}(X^2) - (\mathrm{E}\,X)^2 \end{aligned} \tag{14.21}$$

Wir werden die Notation $X = x$ verwenden, um die Menge alle Ergebnisse zu bezeichnen, bei denen X den Wert x annimmt.

Definition 14.4 (Unabhängigkeit) *Seien X und Y Zufallsvariable auf einem Raum. Diese heißen* ***unabhängig****, falls für alle* $x, y \in \mathbb{R}$ *gilt* $P(X = x \cap Y = y) = P(X = x) \cdot P(Y = y)$.

Satz 14.5 *Es seien X und Y unabhängige Zufallsvariable. Dann ist* $\mathrm{E}(X \cdot Y) = \mathrm{E}\,X \cdot \mathrm{E}\,Y$ *und* $\mathrm{V}(X + Y) = \mathrm{V}\,X + \mathrm{V}\,Y$.

Beweis. Zur ersten Behauptung. Nehmen wir an, dass X die Werte $\{x_i : i \in I\}$

annimmt und Y die Werte $\{y_j : j \in J\}$.

$$
\begin{aligned}
\mathrm{E}(X \cdot Y) &= \mathrm{E}\left(\sum_{i\in I} x_i I(A_i)\right)\left(\sum_{j\in J} y_j I(B_j)\right) \\
&= \mathrm{E}\left(\sum_{i\in I, j\in J} x_i y_j I(A_i \cap B_j)\right) \\
&= \left(\sum_{i\in I, j\in J} x_i y_j \,\mathrm{E}\, I(A_i \cap B_j)\right) \\
&= \left(\sum_{i\in I, j\in J} x_i y_j P(A_i \cap B_j)\right) \\
&= \left(\sum_{i\in I, j\in J} x_i y_j P(A_i) P(B_j)\right) \\
&= \left(\sum_{i\in I} x_i P(A_i)\right)\left(\sum_{j\in J} y_j P(B_j)\right) \\
&= (\mathrm{E}\, X) \cdot (\mathrm{E}\, Y)
\end{aligned}
\tag{14.22}
$$

Man beachte, dass die Unabhängigkeit in Form der Gleichung $P(A_i \cap B_j) = P(A_i) \cdot P(B_j)$ eingeht. Der Erwartungswert vertauscht auch mit unendlichen Summen, sofern diese absolut summierbar sind. Jetzt zur zweiten Behauptung. Wenn X und Y unabhängig sind, so auch $X - \alpha$ und $Y - \beta$ für irgendwelche reelle Zahlen α und β. Insbesondere sind $X - \mathrm{E}\, X$ und $Y - \mathrm{E}\, Y$ unabhängig. Und so so $\mathrm{E}((X - \mathrm{E}\, X)(Y - \mathrm{E}\, Y)) = \mathrm{E}(X - \mathrm{E}\, X) \cdot \mathrm{E}(Y - \mathrm{E}\, Y) = 0$. Daraus leiten wir die zweite Behauptung wie folgt an.

$$
\begin{aligned}
\mathrm{V}(X + Y) &= \mathrm{E}((X - \mathrm{E}\, X) + (Y - \mathrm{E}\, Y))^2 \\
&= \mathrm{E}(X - \mathrm{E}\, X)^2 - 2\,\mathrm{E}(X - \mathrm{E}\, X)(Y - \mathrm{E}\, Y) + \mathrm{E}(Y - \mathrm{E}\, Y)^2 \\
&= \mathrm{V}\, X + \mathrm{V}\, Y
\end{aligned}
\tag{14.23}
$$

⊣

Dies ist ein Spezialfall eines viel allgemeineren Resultats, welches ähnlich ist zu Satz 13.5.

Satz 14.6 *Es seien $\mathcal{P}$ und $\mathcal{Q}$ Wahrscheinlichkeitsräume undX und Y Zufallsvariable über $\mathcal{P}$ und $\mathcal{Q}$. Definiere die folgende Zufallsvariable X^1 und Y^2:*

$$\begin{aligned} X^1(\langle\omega_1, \omega_2\rangle) &:= X(\omega_1) \\ Y^2(\langle\omega_1, \omega_2\rangle) &:= Y(\omega_2) \end{aligned} \tag{14.24}$$

X^1 und Y^2 sind unabhängige Zufallsvariable über $\mathcal{P} \otimes \mathcal{Q}$.

Der Beweis ist recht einfach. $X^1 = \omega_1 = (X = \omega_1) \times \Omega'$ und $Y^2 = \omega_2 = \Omega' \times (Y = \omega_2)$, und deswegen ist nach Definition

$$P(X^1 = \omega_1 \cap Y^2 = \omega_2) = P(X^1 = \omega) \cdot P(X^2 = \omega_2) \tag{14.25}$$

Index

Literatur

Aigner, Martin. *Diskrete Mathematik*. Braunschweig/Wiesbaden: Vieweg Verlag, 1993.

Burris, Stanley und H. P. Sankappanavar. *A Course in Universal Algebra*. Graduate Texts in Mathematics 78. Springer, 1981.

Davey, B. A. und H. A. Priestley. *Introduction to Lattices and Order*. 2. Aufl. Cambridge: Cambridge University Press, 1991.