Tutorium: Diskrete Mathematik

Daniel Milne-Plückebaum, post@daniel-milne.de

7. November 2015

Die folgenden Übungen, Lösungen und Hilfen basieren auf der Vorlesung *Diskrete Mathematik*, gehalten von Marcus Kracht an der Universität Bielefeld (im Sommersemester 2015), und sind somit idealerweise nur zusammen mit dem zugehörigen Vorlesungsmanuskript zu verwenden. Über Verbesserungsvorschläge und Hinweise auf Fehler freue ich mich sehr. Auch weitere Wünsche für Aufgaben, Lösungen und Hilfen könnt ihr mir jederzeit mitteilen.

Inhaltsverzeichnis

1 Gruppen, Ringe und Körper

1.1 ÜBUNGEN: Gruppen

1. Gib folgende Gruppen explizit an. Welche sind kommutativ?
   (a) $\langle \mathbb{Z}_4, +_4, -_4, 0 \rangle$
   (b) $\langle \mathbb{Z}_1, +_1, -_1, 0 \rangle$
   (c) $\langle \mathbb{Z}_3 - \{0\}, \cdot_3, ^{-1_3}, 1 \rangle$
   (d) $\mathbb{Z}_2^\times$
   (e) $\mathbb{Z}_7^\times$
   (f) $\mathbb{Z}_6^+$
   (g) $\mathrm{Sym}(\{\heartsuit, \diamondsuit\})$
   (h) $\mathrm{Sym}(\{p, q, r\})$
2. Warum lassen sich folgende Dinge nicht zu Gruppen vervollständigen?
   (a) $\mathbb{Z}_4$ mit $\cdot$ (Multiplikation) und 1 (neutrales Element)
   (b) $\mathbb{Z}_6 - \{0\}$ mit $\cdot$ (Multiplikation) und 1 (neutrales Element)
   (c) $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}^*$ mit $\cdot$ (Verkettung) und ϵ (neutrales Element)
3. Gib drei isomorphe Gruppen zu $\mathbb{Z}_3^\times$ an.
4. Gegeben seien die Gruppen $\mathfrak{K} = \langle \{0, 1, 2, 3\}, +, -, 0 \rangle$ und $\mathfrak{L} = \langle \{0, 1, 2, 3\}, \oplus, \ominus, 0 \rangle$ mit

$$
\begin{array}{c|cccc}
+ & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2
\end{array}
\qquad \text{und} \qquad
\begin{array}{c|cccc}
\oplus & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 3 & 0 & 2 \\
2 & 2 & 0 & 3 & 1 \\
3 & 3 & 2 & 1 & 0
\end{array}
$$

Zeige, dass $\mathfrak{K}$ und $\mathfrak{L}$ isomorph sind, wobei der Isomorphismus 2 und 3 vertauscht.

5. Es sei $Q := \{a, b, c, d\}$, wobei a, b, c und d die Ecken eines Quadrates sind. Es sei Q_4 die Gruppe der Kongruenzabbildungen (ausgedrückt als Abbildungen von Q auf sich). Gib die Gruppe explizit an.

1.2 Übungen: Ringe und Körper

1. Warum handelt es sich bei $\langle \mathbb{Z}_8, +_8, -_8, 0, \cdot_8 \rangle$ nur um einen (kommutativen) Ring und nicht um einen Körper? Hat der Ring eine Eins?

2. Gegeben sei die Menge $\{0\}$. Kann man daraus mit den passenden Operationen (a) eine Gruppe, (b) einen (kommutativen) Ring, (c) einen (kommutativen) Ring mit Eins, (d) einen Körper machen?

3. Ist jeder Körper (a) ein (kommutativer) Ring, (b) ein (kommutativer) Ring mit Eins, (c) eine (kommutative) Gruppe?

4. Fasse folgende Gruppen jeweils zu einem Körper zusammen:

   (a) $\langle \mathbb{Z}_3, +_3, -_3, 0 \rangle$ und $\langle \mathbb{Z}_3 - \{0\}, \cdot_3, ^{-1_3}, 1 \rangle$

   (b) $\langle \mathbb{R}, +, -, 0 \rangle$ und $\langle \mathbb{R} - \{0\}, \cdot, ^{-1}, 1 \rangle$

5. Gib die Körper $\mathbb{F}_1$, $\mathbb{F}_2$, $\mathbb{F}_3$ und $\mathbb{F}_5$ explizit an. Wie lautet jeweils die Charakteristik?

6. Betrachte das 7-Tupel $\langle \{\heartsuit, \diamondsuit\}, \star, \bullet, \heartsuit, \because, \circ, \diamondsuit \rangle$ mit

$$\star = \{\langle\langle \heartsuit, \heartsuit \rangle, \heartsuit\rangle, \langle\langle \heartsuit, \diamondsuit \rangle, \diamondsuit\rangle, \langle\langle \diamondsuit, \heartsuit \rangle, \diamondsuit\rangle, \langle\langle \diamondsuit, \diamondsuit \rangle, \heartsuit\rangle\}$$

$$\bullet = \{\langle \heartsuit, \diamondsuit \rangle, \langle \diamondsuit, \heartsuit \rangle\}$$

$$\because = \{\langle\langle \diamondsuit, \diamondsuit \rangle, \diamondsuit\rangle\}$$

$$\circ = \{\langle \diamondsuit, \diamondsuit \rangle\}$$

   (a) Warum handelt es sich dabei *nicht* um einen Körper?

   (b) Verbessere die Struktur, sodass ein Körper entsteht.

   (c) Welche beiden Gruppen können zu diesem (neuen) Körper zusammengefasst werden?

(d) Denke dir einen weiteren “Quatsch-Körper” aus.

1.3 Hilfe: Definitionen und Beispiele

Die Begriffe **Gruppe**, **Ring** und **Körper** kann man so definieren, dass sie aufeinander aufbauen. Man kann die Begriffe jeweils auch definieren, indem man einfach alle Bedingungen aufzählt, die bereits in die Definitionen der grundlegenderen Begriffe eingegangen sind. Für das Verständnis ist es aber hilfreich, direkt zu sehen, wie die Begriffe zusammenhängen. Beginnen wir also mit dem Begriff der **Gruppe**.

1.3.1 Gruppe

Gruppe (einfach, kommutativ): Eine **Gruppe** ist ein Gebilde mit vier Zutaten: $\mathfrak{G} = \langle G, \star, i_\star, n_\star \rangle$. G ist eine nichtleere **Grundmenge**. $\star$ ist eine zweistellige **Verknüpfung**. $i_\star$ ist eine einstellige **Inversenfunktion (bezüglich $\star$)**. $n_\star$ ist ein Element aus G, nämlich das **neutrale Element (bezüglich $\star$)**. Eine Gruppe, die aus den vier genannten Zutaten besteht, wird durch folgende drei Bedingungen festgezurrt:

1. Für alle Elemente x, y und z der Grundmenge G gilt: $x \star (y \star z) = (x \star y) \star z$.

   Für die Verknüpfung $\star$ gilt also das **Assoziativgesetz**.

2. Für alle Elemente x der Grundmenge G gilt: $x \star i_\star(x) = i_\star(x) \star x = n_\star$.

   Das heißt, dass jedem Element x der Grundmenge G von $i_\star$ ein **$\star$-inverses Element** zugeordnet wird, sodass das $\star$-neutrale Element $n_\star$ herauskommt, wenn man das Element x mit seinem $\star$-inversen Element $\star$-verknüpft.

3. Für alle Elemente x der Grundmenge G gilt: $x \star n_\star = n_\star \star x = x$.

   Diese Bedingung bestimmt das $\star$-neutrale Element näher. Es ist insofern $\star$-neutral, als es, $\star$-verknüpft mit einem Element x, immer einfach wieder x zurückgibt.

Wenn für alle Elemente x und y der Grundmenge auch noch gilt, dass $x \star y = y \star x$, dann gilt das **Kommutativgesetz** für die Verknüpfung $\star$, wodurch die ganze Gruppe zu einer **kommutativen Gruppe** wird.

Schauen wir uns dazu ein Beispiel an.

Beispiel: $\mathbb{Z}_4^+ = \langle \{0, 1, 2, 3\}, +_4, -_4, 0 \rangle$ ist eine **kommutative Gruppe**, wobei $\{0, 1, 2, 3\}$ die **Grundmenge** ist. Aus dieser kommen wir nicht heraus – egal, was wir rechnen. $+_4$ ist die **Verknüpfung** für die Elemente der Grundmenge. $-_4$ ist die **Inversenfunktion (bezüglich $+_4$)** für die Elemente der Grundmenge. Und 0 ist das **neutrale Element (bezüglich $+_4$)**. Wir können $+_4$ und $-_4$ konkret durch folgende

Tabellen angeben:

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

und

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

1.3.2 Ring

Ausgerüstet mit dem Begriff der **kommutativen Gruppe** können wir nun recht leicht den Begriff des **Rings** definieren. Einen **Ring** kann man einfach als eine erweiterte kommutative Gruppe auffassen.

Ring (einfach, kommutativ, unitär): Ein **Ring** ist ein Gebilde mit fünf Zutaten: $\mathfrak{R} = \langle R, \star, i_\star, n_\star, \circledast \rangle$. R ist eine nichtleere **Grundmenge**. $\star$ ist eine zweistellige **Verknüfung**. $i_\star$ ist eine einstellige **Inversenfunktion (bezüglich $\star$)**. $n_\star$ ist ein Element aus R, nämlich das **neutrale Element (bezüglich $\star$)**. $\circledast$ ist ebenfalls eine zweistellige **Verknüpfung**. Der Ring, der aus den fünf Zutaten besteht, wird durch folgende drei Bedingungen festgezurrt:

1. $\langle R, \star, i_\star, n_\star \rangle$ eine eine **kommutative Gruppe**.

   Für einen Teil des Rings, den man zu $\langle R, \star, i_\star, n_\star \rangle$ zusammenfassen kann, gelten also die drei oben genannten Gruppeneigenschaften.

2. Für alle Elemente x, y und z der Grundmenge R gilt: $x \circledast (y \circledast z) = (x \circledast y) \circledast z$.

   Für die Verknüpfung $\circledast$ gilt also das **Assoziativgesetz**.

3. Für alle Elemente x, y und z der Grundmenge R gilt: $(x \star y) \circledast z = (x \circledast z) \star (y \circledast z)$ und $z \circledast (x \star y) = (z \circledast x) \star (z \circledast y)$.

   Für die Verknüpfungen $\star$ und $\circledast$ gilt also das **Distributivgesetz**.

Wenn für alle Elemente x und y der Grundmenge R auch noch $x \circledast y = y \circledast x$ gilt, dann gilt das **Kommutativgesetz** für die Verknüpfung $\circledast$, wodurch der ganze Ring zu einem **kommutativen Ring** wird.
Wenn außerdem ein $n_\circledast$ in der Grundmenge R ist, sodass für alle x in der Grundmenge R gilt, dass $x \circledast n_\circledast = n_\circledast \circledast x = x$, dann hat die Verknüpfung $\circledast$ ebenfalls ein **neutrales Element (bezüglich $\circledast$)**. Das resultierende Gebilde mit sechs Zutaten, $\mathfrak{R} = \langle R, \star, i_\star, n_\star, \circledast, n_\circledast \rangle$, ist dann ein **unitärer Ring** (oder ein **Ring mit Eins**).

Schauen wir uns auch dazu ein Beispiel an:

Beispiel: $\langle\{0,1,2,3,4,5\},+_6,-_6,0,\cdot_6,1\rangle$ ist ein **kommutativer unitärer Ring**. Wir können $+_6$, $-_6$ und $\cdot_6$ konkret durch folgende Tabellen angeben:

$+_6$	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

und

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

und

$\cdot_6$	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 $+_6$ und $-_6$ die Gruppeneigenschaften erfüllen. $\cdot_6$ erfüllt die Gruppeneigenschaften aber nicht (auch nicht für $\{1,2,3,4,5\}$). Dennoch hat $\cdot_6$ ein neutrales Element (bezüglich $\cdot_6$), nämlich die 1.

1.3.3 Körper

Ausgerüstet mit dem Begriff der **(kommutativen unitären) Gruppe** können wir nun recht leicht den Begriff des **Körpers** definieren. Einen **Körper** kann man einfach als einen erweiterten kommutativen unitären Ring auffassen.

Körper: Ein **Körper** ist ein Gebilde mit sieben Zutaten: $\mathfrak{K} = \langle K,\star,i_\star,n_\star,\circledast,i_\circledast,n_\circledast\rangle$. K ist eine nichtleere **Grundmenge**. $\star$ ist eine zweistellige **Verknüfung**. $i_\star$ ist eine einstellige **Inversenfunktion (bezüglich $\star$)**. $n_\star$ ist ein Element aus K, nämlich das erste **neutrale Element (bezüglich $\star$)**. $\circledast$ ist ebenfalls eine zweistellige **Verknüpfung**. $i_\circledast$ ist eine einstellige **Inversenfunktion (bezüglich $\circledast$)**. $n_\circledast$ ist ein Element aus K, nämlich das zweite **neutrale Element (bezüglich $\circledast$)**. Der Körper, der aus den sieben Zutaten besteht, wird durch folgende drei Bedingungen festgezurrt:

1. $\langle K,\star,i_\star,n_\star,\circledast,n_\circledast\rangle$ ist ein **kommutativer unitärer Ring**.

   Für einen Teil des Körpers, den man zu $\langle K,\star,i_\star,n_\star,\circledast,n_\circledast\rangle$ zusammenfassen kann, gelten also die drei oben genannten Ringeigenschaften.

2. $n_\star \neq n_\circledast$.

   Es wird ausgeschlossen, dass das $\star$-neutrale Element $n_\star$ und das $\circledast$-neutrale Element $n_\circledast$ identisch sind. Wären diese beiden Elemente nämlich identisch, ließe sich der sogenannte **Nullring**, $\langle\{0\},+_0,-_0,0,\cdot_0,0\rangle$, zu einem Körper erweitern. Bei einem Körper muss $\langle K-\{0\},\circledast,i_\circledast,n_\circledast\rangle$ aber eine Gruppe sein. Wenn aber $K=\{0\}$, dann $K-\{0\}=\varnothing$. $\varnothing$ kann aber nicht die Grundmenge einer Gruppe sein, da die Grundmenge einer Gruppe nicht leer sein darf (sonst hätte die Gruppe ja kein neutrales Element).

3. Für alle $x \neq n_\star$ in der Grundmenge K gibt es ein $i_\circledast(x)$, sodass $x \circledast i_\circledast(x) = n_\circledast$.

   Das heißt, dass jedem Element x der Grundmenge K, außer dem $\star$-neutralen Element $n_\star$, von $i_\circledast$ ein **$\circledast$-inverses Element** zugeordnet wird, sodass das $\circledast$-neutrale Element $n_\circledast$ herauskommt, wenn man das Element x mit seinem $\circledast$-inversen Element $\circledast$-verknüpft.

   Die Bedingungen 2 und 3 lassen sich auch folgendermaßen zusammenfassen: $\langle K - \{0\}, \circledast, i_\circledast, n_\circledast\rangle$ ist eine **Gruppe**.

Auch dazu betrachten wir ein Beispiel:

Beispiel: $\mathbb{F}_5 = \langle\{0,1,2,3,4\}, +_5, -_5, 0, \cdot_5, {}^{-1_5}, 1\rangle$ ist ein **Körper**. Wir können $+_5$, $-_5$, $\cdot_5$ und ${}^{-1_5}$ konkret durch folgende Tabellen angeben:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

und

	$-_5$
0	0
1	4
2	3
3	2
4	1

und

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

und

	${}^{-1_5}$
0	–
1	1
2	3
3	2
4	4

1.4 Hilfe: Nullgruppe, Nullring, Nullkörper?

Manchmal hilft es, das Verständnis von Begriffen zu vertiefen, indem man sich überlegt, ob es ganz besondere Beispiele dieser Begriffe gibt. Bezogen auf die obigen Strukturbegriffe wollen wir mal schauen, ob es besonders *kleine* Beispiele gibt, also Beispiele mit einer besonders kleinen Grundmenge.

Alle oben erläuterten Strukturen verlangen, dass die Grundmenge nicht leer ist. Also benötigen wir mindestens ein Element. Schauen wir zuerst, ob das für Gruppen funktioniert. Eine Gruppe ist ein Quadrupel $\langle G, \star, i_\star, n_\star\rangle$, wobei G die Grundmenge ist, in diesem Fall mit einem Element; $n_\star$ – das neutrale Element (bezüglich $\star$) – ist ein Element aus G, also muss $n_\star$ das (einzige) Element in G sein. Damit haben wir: $G = \{n_\star\}$. Jetzt müssen wir nur noch überprüfen, ob $\star$ und $i_\star$ für diese Menge wohldefiniert sind. Offenbar gibt es nicht viel zu tun – wir brauchen nur:

$\star$	$n_\star$
$n_\star$	$n_\star$

und

	$i_\star$
$n_\star$	$n_\star$

Die Gruppeneigenschaften werden von diesen Operationen erfüllt:

1. Das Assoziativgesetz gilt.
2. Wenn man ein Element x der Grundmenge (wir können nur ein einziges Element auswählen) mit seinem $\star$-Inversen (wiederum dem einzigen Element) $\star$-verknüpft, dann kommt das $\star$-neutrale Element (eben das einzige Element) heraus.
3. Wenn man ein Element x der Grundmenge (wir können nur ein einziges Element auswählen) mit dem $\star$-neutralen Element (wiederum dem einzigen Element) $\star$-verknüpft, kommt wieder x (eben das einzige Element) heraus.

Wenn man $\star$ als $+_0$, $i_\star$ als $-_0$ und $n_\star$ selbst als 0 interpretiert, bekommt man $\langle \{0\}, +_0, -_0, 0\rangle$. Eine Gruppe, die das neutrale Element als einziges Gruppenelement enthält, nennt man auch **Nullgruppe**.

Wenn man so eine Nullgruppe noch um die Operation $\circledast$ (mit

$\circledast$	$n_\star$
$n_\star$	$n_\star$

)

erweitert, erhält man einen **Nullring**, da das Assoziativgesetz für $\circledast$ offenbar ebenfalls gilt, und da $\star$ und $\circledast$ das Distributivgesetz erfüllen. Außerdem ist $n_\star$ in so einem Ring gleichzeitig das $\circledast$-neutrale Element: Wenn man ein Element x der Grundmenge (wir können nur ein einziges Element auswählen) mit $n_\star$ (wiederum dem einzigen Element) $\circledast$-verknüpft, kommt wieder x (eben das einzige Element) heraus. Somit ist $\langle \{n_\star\}, \star, i_\star, n_\star, \circledast, n_\star\rangle$ ein **unitärer Nullring**. Spezifiziert haben wir $\langle \{0\}, +_0, -_0, 0, \cdot_0, 0\rangle$ als derartige Struktur.

Zum Schluss kann man sich fragen, ob es auch einen Nullkörper geben kann, also einen Körper, dessen Grundmenge nur ein einziges Element (nämlich 0 bzw. $n_\star$) enthält. Die obige Definition beantwortet diese Frage ganz explizit: Bedingung 2 verlangt, dass das $\star$-neutrale Element vom $\circledast$-neutralen Element *verschieden* sein muss. Damit enthält die Grundmenge eines Körpers immer mindestens *zwei* Elemente. Also kann es keinen Nullkörper geben.

1.5 Hilfe: Fragen und Antworten

Frage: Wie erkennt man, ob eine Gruppe abelsch ist?

Antwort: Eine Gruppe $\langle G, \cdot, ^{-1}, 1\rangle$ ist abelsch, wenn man die Elemente, auf die die Operation $\cdot$ angewendet wird, auch umkehren kann und dasselbe Ergebnis herauskommt. Die Gruppe $\langle B(\{a,b,c\}), \circ, ^{-1}, i_{\{a,b,c\}}\rangle$ ist z.B. nicht abelsch, da
$\{\langle a,b\rangle, \langle b,a\rangle, \langle c,c\rangle\} \circ \{\langle a,c\rangle, \langle b,a\rangle, \langle c,b\rangle\} = \{\langle a,a\rangle, \langle b,c\rangle, \langle c,b\rangle\}$ und
$\{\langle a,c\rangle, \langle b,a\rangle, \langle c,b\rangle\} \circ \{\langle a,b\rangle, \langle b,a\rangle, \langle c,c\rangle\} = \{\langle a,c\rangle, \langle b,b\rangle, \langle c,a\rangle\}$, aber
$\{\langle a,a\rangle, \langle b,c\rangle, \langle c,b\rangle\} \neq \{\langle a,c\rangle, \langle b,b\rangle, \langle c,a\rangle\}$.

Frage: Wie viele Elemente hat $Sym(M)$? Sind das 4 (weil $Sym(M)$ ein Quadrupel ist), 6 (weil $3! = 6$ und 3 die Anzahl der Elemente in M ist), oder 36 (wegen der Multiplikationstabelle)?

Antwort: $Sym(M)$ hat 4 Elemente.

2 Vektorräume

2.1 Übungen: Vektorräume und lineare Abhängigkeit

1. Bestimme die Vektorräume
   (a) $\mathbb{F}_1^2$, $\mathbb{F}_2^2$, $\mathbb{F}_3^2$
   (b) $\mathbb{F}_2^3$ und $\mathbb{F}_3^3$
   (c) $\mathbb{F}_2^4$

2. Es sei $M := \langle\{\heartsuit, \diamondsuit\}, \star, \bullet, \heartsuit, \because, \bigcirc, \diamondsuit\rangle$ ein Körper mit

$$\star = \{\langle\langle\heartsuit,\heartsuit\rangle,\heartsuit\rangle, \langle\langle\heartsuit,\diamondsuit\rangle,\diamondsuit\rangle, \langle\langle\diamondsuit,\heartsuit\rangle,\diamondsuit\rangle, \langle\langle\diamondsuit,\diamondsuit\rangle,\heartsuit\rangle\}$$
$$\bullet = \{\langle\heartsuit,\heartsuit\rangle, \langle\diamondsuit,\diamondsuit\rangle\}$$
$$\because = \{\langle\langle\diamondsuit,\diamondsuit\rangle,\diamondsuit\rangle\}$$
$$\bigcirc = \{\langle\diamondsuit,\diamondsuit\rangle\}$$

   Es sei $N := \{1,2\}$. Bestimme den Vektorraum M^N.

3. Bestimme $\mathbb{F}_5^2$.
   (a) Sind die Vektoren $\begin{pmatrix}1\\2\end{pmatrix}$ und $\begin{pmatrix}3\\1\end{pmatrix}$ linear abhängig?
   (b) Gib das Erzeugnis von $\begin{pmatrix}1\\2\end{pmatrix}$ explizit an.
   (c) Sei $v \neq \vec{0}$ ein Vektor in $\mathbb{F}_5^2$. Wie viele zu v linear unabhängige Vektoren gibt es?

4. Betrachte $\mathbb{F}_5$.

   (a) Wie viele Polynome zweiten Grades gibt es über $\mathbb{F}_5$?

   (b) Welche Nullstellen haben die Polynome?

   (c) Berechne daraus eine Zerlegung der Polynome in Linearfaktoren.

2.2 Übungen: Basen und lineare Abbildungen

1. Betrachte den Vektorraum $\mathbb{F}_3^3$.

   (a) Bestimme eine Menge S, die zwei linear unabhängige Vektoren von $\mathbb{F}_3^3$ enthält.

   (b) Bestimme die lineare Hülle $\langle S\rangle$ von S.

   (c) Schreibe den Unterraum $(\langle S\rangle, +_{\langle S\rangle}, -_{\langle S\rangle}, 0, \circ_{\langle S\rangle})$ von $\mathbb{F}_3^3$ explizit auf.

   (d) Ist S eine Basis von $\mathbb{F}_3^3$? Falls nicht, bestimme eine Basis B_1.

   (e) Bestimme zwei weitere Basen B_2 und B_3 von $\mathbb{F}_3^3$.

   (f) Bestimme die lineare Hülle der Basis B_1 von $\mathbb{F}_3^3$.

   (g) Wie lauten die linearen Hüllen zu B_2 und B_3?

   (h) Bestimme zu den Vektoren $\begin{pmatrix}1\\2\\0\end{pmatrix}$ und $\begin{pmatrix}2\\1\\1\end{pmatrix}$ die B_1-, B_2- und B_3-Koordinaten.

2. Betrachte den Vektorraum $\mathbb{F}_2^4$.

   (a) Gib das Erzeugnis von $\{v_1\}$ an, mit $v_1 = \begin{pmatrix}0\\1\\0\\1\end{pmatrix}$.

   (b) Finde einen von v_1 linear unabhängigen Vektor v_2.

   (c) Gib das Erzeugnis von $\{v_1, v_2\}$ an.

   (d) Finde einen von v_1 und v_2 linear unabhängigen Vektor v_3.

   (e) Gib das Erzeugnis von $\{v_1, v_2, v_3\}$ an.

   (f) Finde einen von v_1, v_2 und v_3 linear unabhängigen Vektor v_4.

   (g) Gib das Erzeugnis von $\{v_1, v_2, v_3, v_4\}$ an.

   (h) Ist $\{v_1, v_2, v_3, v_4\}$ eine Basis von $\mathbb{F}_2^5$? Begründe deine Antwort.

3. Es sei ein Vektor $w_1 \in \mathbb{F}_3^4$ gegeben.

(a) Wie viele Vektoren enthält das Erzeugnis von $\{w_1\}$?

(b) Wie viele Vektoren gibt es, die von w_1 linear unabhängig sind?

(c) Es sei w_2 ein Vektor, der von w_1 linear unabhängig ist. Wie viele Vektoren enthält das Erzeugnis von $\{w_1, w_2\}$?

(d) Wie viele Vektoren gibt es, die von $\{w_1, w_2\}$ linear unabhängig sind?

(e) Es sei w_3 ein Vektor, der von w_1 und w_2 linear unabhängig ist. Wie viele Vektoren enthält das Erzeugnis von $\{w_1, w_2, w_3\}$?

(f) Wie viele Vektoren gibt es, die von $\{w_1, w_2, w_3\}$ linear unabhängig sind?

(g) Es sei w_4 ein Vektor, der von w_1, w_2 und w_3 linear unabhängig ist. Wie viele Vektoren enthält das Erzeugnis von $\{w_1, w_2, w_3, w_4\}$?

(h) Wie viele Vektoren gibt es, die von $\{w_1, w_2, w_3, w_4\}$ linear unabhängig sind?

4. Es sei $f : \mathbb{F}_3^4 \to \mathbb{F}_3^2$ eine lineare Abbildung mit

$$f(\begin{pmatrix} 0 \\ 2 \\ 0 \\ 2 \end{pmatrix}) = \begin{pmatrix} 2 \\ 1 \end{pmatrix},\ f(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}) = \begin{pmatrix} 0 \\ 2 \end{pmatrix},\ f(\begin{pmatrix} 0 \\ 0 \\ 2 \\ 0 \end{pmatrix}) = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \text{ und } f(\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}) = \begin{pmatrix} 1 \\ 2 \end{pmatrix}.$$ Berechne

(a) $f(\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix})$

(b) $f(\begin{pmatrix} 2 \\ 2 \\ 1 \\ 2 \end{pmatrix})$

(c) $f(\begin{pmatrix} -1 \\ 0 \\ -2 \\ 1 \end{pmatrix})$

2.3 Hilfe: Definitionen und Beispiel

2.3.1 Vektorraum

Erst einmal allgemein: Was ist ein Vektorraum über einem Körper $\mathfrak{K}$? (Merkt euch gleich, dass ein Vektorraum immer einen dazugehörigen Körper $\mathfrak{K}$ benötigt!)

Vektorraum: Sei $\mathfrak{K}$ ein Körper $\langle K, \star, i_\star, n_\star, \circledast, i_\circledast, n_\circledast \rangle$. Ein **Vektorraum über** $\mathfrak{K}$ ist ein Quintupel $\langle V, \star_V, i_{\star_V}, n_{\star_V}, \circ \rangle$, das folgende Eigenschaften erfüllt:

1. $\langle V, \star_V, i_{\star_V}, n_{\star_V} \rangle$ ist eine kommutative Gruppe.
2. $\circ : K \times V \to V$ ist eine zweistellige Operation, sodass für alle $k, k' \in K$ und alle $v, v' \in V$ gilt:
   (a) $k \circ (k' \circ v) = (k \circledast k') \circ v$
   (b) $k \circ (v \star v') = (k \circ v) \star (k \circ v')$
   (c) $n_{\star_V} \circ v = v$
   (d) $(k \star k') \circ v = (k \circ v) \star (k' \circ v)$

Die Elemente von V sind **Vektoren**. $k \circ v$ ist eine **Streckung** von v um den Faktor k.

Schauen wir uns nun ein vollständig ausbuchstabiertes **Beispiel** an:

Körper: $\mathbb{F}_3 := \langle \{0,1,2\}, +_3, -_3, 0, \cdot_3, ^{-1_3}, 1 \rangle$ mit

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

und

	$-_3$
0	0
1	2
2	1

und

$\cdot_3$	1	2
1	1	2
2	2	1

und

	$^{-1_3}$
1	1
2	2

Menge: $M := \{1, 2\}$

Vektorraum: $\mathbb{F}_3^M = \mathbb{F}_3^2 = \langle V, +_V, -_V, \vec{0}, \circ \rangle$ mit

$$V = \{\{\langle 1,0\rangle, \langle 2,0\rangle\}, \{\langle 1,0\rangle, \langle 2,1\rangle\}, \{\langle 1,0\rangle, \langle 2,2\rangle\}, \{\langle 1,1\rangle, \langle 2,0\rangle\}, \{\langle 1,1\rangle, \langle 2,1\rangle\}, \{\langle 1,1\rangle, \langle 2,2\rangle\}, \{\langle 1,2\rangle, \langle 2,0\rangle\}, \{\langle 1,2\rangle, \langle 2,1\rangle\}, \{\langle 1,2\rangle, \langle 2,2\rangle\}\}$$

- $(f +_V g)(x) := f(x) +_3 g(x)$
- $(-_V f)(x) := -_3 f(x)$
- $\vec{0}(x) := 0$
- $(k \circ f)(x) := k \cdot_3 f(x)$

Für die Vektoren schreiben wir anstatt $\{\langle 1,1\rangle, \langle 2,0\rangle\}$ usw. einfach $\begin{pmatrix}1\\0\end{pmatrix}$ $(= \begin{pmatrix}f(1)\\f(2)\end{pmatrix})$ usw.

Dann haben wir $V = \{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}2\\0\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix}, \begin{pmatrix}2\\2\end{pmatrix}\}$, also insgesamt 9 Vektoren, die die Grundmenge unseres Vektorraums bilden. Beachtet, dass das neutrale

Element $\vec{0}$ des Vektorraums nicht die Zahl 0 ist, sondern der **Nullvektor** $\begin{pmatrix}0\\0\end{pmatrix}$.

Beispielrechnungen sind dann:

- $\begin{pmatrix}0\\1\end{pmatrix} +_V \begin{pmatrix}2\\2\end{pmatrix} = \begin{pmatrix}0 +_3 2\\2 +_3 2\end{pmatrix} = \begin{pmatrix}2\\0\end{pmatrix}$
- $-_V \begin{pmatrix}2\\0\end{pmatrix} = \begin{pmatrix}-_3\ 0\\-_3\ 1\end{pmatrix} = \begin{pmatrix}0\\2\end{pmatrix}$
- $\vec{0}(1) = 0$
- $2 \circ \begin{pmatrix}2\\2\end{pmatrix} = \begin{pmatrix}2 \cdot_3 2\\2 \cdot_3 2\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix}$

2.3.2 Weitere Begriffe

Es gibt noch ein paar weitere Begriffe, die man sich im Zusammenhang mit Vektorräumen klar machen sollte. Auch diese wollen wir uns anhand unseres Beispiels ansehen.

Linearkombinationen sind z.B.

- $2 \circ \begin{pmatrix}1\\1\end{pmatrix} + 1 \circ \begin{pmatrix}2\\2\end{pmatrix} + 1 \circ \begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}(2 \cdot_3 1) +_3 (1 \cdot_3 2) +_3 (1 \cdot_3 0)\\(2 \cdot_3 1) +_3 (1 \cdot_3 2) +_3 (1 \cdot_3 2)\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}$
- $0 \circ \begin{pmatrix}2\\2\end{pmatrix} + 2 \circ \begin{pmatrix}0\\0\end{pmatrix} + 2 \circ \begin{pmatrix}2\\2\end{pmatrix} = \begin{pmatrix}(0 \cdot_3 2) +_3 (2 \cdot_3 0) +_3 (2 \cdot_3 2)\\(0 \cdot_3 1) +_3 (2 \cdot_3 0) +_3 (2 \cdot_3 2)\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix}$

Damit ist $\begin{pmatrix}1\\0\end{pmatrix}$ eine Linearkombination aus $\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}2\\2\end{pmatrix}$ und $\begin{pmatrix}0\\2\end{pmatrix}$; und $\begin{pmatrix}1\\1\end{pmatrix}$ ist eine Linearkombination aus $\begin{pmatrix}2\\2\end{pmatrix}$ und $\begin{pmatrix}0\\0\end{pmatrix}$.

Betrachten wir nur den Vektor $\begin{pmatrix}1\\0\end{pmatrix}$. Die Menge aller Linearkombinationen aus $\begin{pmatrix}1\\0\end{pmatrix}$, $\langle\{\begin{pmatrix}1\\0\end{pmatrix}\}\rangle$, ist die **lineare Hülle** von $\begin{pmatrix}1\\0\end{pmatrix}$. Alle Linearkombinationen sind:

- $0 \circ \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}$
- $1 \circ \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}$

- $2 \circ \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}2\\0\end{pmatrix}$

Also ist $\langle\{\begin{pmatrix}1\\0\end{pmatrix}\}\rangle = \{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}2\\0\end{pmatrix}\}$ die Menge aller Vektoren, die sich aus $\begin{pmatrix}1\\0\end{pmatrix}$ und den Körperelementen 0, 1, 2 erzeugen lassen.

$U = \langle\langle\{\begin{pmatrix}1\\0\end{pmatrix}\}\rangle, +_V, -_V, \vec{0}, \circ\rangle$ ist ebenfalls ein Vektorraum über $\mathbb{F}_3$, ein **Unterraum von V**. $+_V$, $-_V$ und $\circ$ werden natürlich entsprechend eingeschränkt.

Außerdem gilt: Eine Menge T von Vektoren heißt **linear unabhängig**, falls kein Vektor von den anderen Vektoren linear abhängig ist. Zum Beispiel ist die Menge $\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}\}$ linear unabhängig, da es keine Linearkombination gibt, sodass

- $n \circ \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\2\end{pmatrix}$ oder
- $m \circ \begin{pmatrix}2\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}$.

Falls ein Vektor v von einem Vektor w linear abhängig ist, so ist natürlich auch w von v linear abhängig, da das Körperelement n, das zusammen mit v w ergibt, ein Inverses m hat, welches zusammen mit w v ergibt.

$\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}\}$ ist auch eine **Basis** des Vektorraums V, da $\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}\}$ linear unabhängig ist und sich alle Vektoren aus V durch Linearkombinationen der Vektoren aus $\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}\}$ schreiben lassen.

2.4 Übungen: Matrizen, Bilder, Kerne, Determinanten

1. Es sei $f : \mathbb{F}_3^4 \to \mathbb{F}_3^2$ eine lineare Abbildung mit

$$f(\begin{pmatrix}1\\0\\0\\0\end{pmatrix}) = \begin{pmatrix}1\\1\end{pmatrix},\ f(\begin{pmatrix}0\\1\\0\\0\end{pmatrix}) = \begin{pmatrix}2\\2\end{pmatrix},\ f(\begin{pmatrix}0\\0\\1\\0\end{pmatrix}) = \begin{pmatrix}0\\1\end{pmatrix} \text{ und } f(\begin{pmatrix}0\\0\\0\\1\end{pmatrix}) = \begin{pmatrix}2\\1\end{pmatrix}.$$

   (a) Bestimme die zu der Abbildung korrespondierende Matrix.

(b) Berechne $f(\begin{pmatrix}2\\2\\2\\2\end{pmatrix})$, $f(\begin{pmatrix}1\\2\\2\\1\end{pmatrix})$ und $f(\begin{pmatrix}0\\1\\1\\2\end{pmatrix})$.

2. Es sei $f : \mathbb{F}_3^4 \to \mathbb{F}_3^2$ eine lineare Abbildung mit

$$f(\begin{pmatrix}0\\2\\0\\2\end{pmatrix}) = \begin{pmatrix}2\\1\end{pmatrix},\ f(\begin{pmatrix}1\\0\\0\\0\end{pmatrix}) = \begin{pmatrix}0\\2\end{pmatrix},\ f(\begin{pmatrix}0\\0\\2\\0\end{pmatrix}) = \begin{pmatrix}1\\1\end{pmatrix} \text{ und } f(\begin{pmatrix}0\\0\\0\\1\end{pmatrix}) = \begin{pmatrix}1\\2\end{pmatrix}.$$

   (a) Bestimme die zu der Abbildung korrespondierende Matrix.

   (b) Berechne $f(\begin{pmatrix}2\\2\\2\\2\end{pmatrix})$, $f(\begin{pmatrix}1\\2\\2\\1\end{pmatrix})$ und $f(\begin{pmatrix}0\\1\\1\\2\end{pmatrix})$.

3. Es sei folgende Matrix über $\mathbb{F}_3$ gegeben: $A = \begin{pmatrix}0 & 2 & 2 & 1\\1 & 0 & 0 & 0\\0 & 1 & 2 & 2\end{pmatrix}$.

   (a) Welche lineare Abbildung wird von A definiert?

   (b) Berechne die Bilder der Vektoren $\begin{pmatrix}0\\1\\2\\2\end{pmatrix}$ und $\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$.

   (c) Bestimme den Kern von A.

   (d) Bestimme das Bild von A.

4. Es sei folgende Matrix über $\mathbb{F}_5$ gegeben: $B = \begin{pmatrix}3 & 2 & 3 & 1 & 4\end{pmatrix}$.

   (a) Welche lineare Abbildung wird von B definiert?

   (b) Berechne die Bilder der Vektoren $\begin{pmatrix}2\\4\\0\\0\\3\end{pmatrix}$ und $\begin{pmatrix}3\\0\\3\\3\\2\end{pmatrix}$.

   (c) Bestimme den Kern von B.

(d) Bestimme das Bild von B.

5. Berechne die Determinanten der folgenden Matrizen. Sind die linearen Abbildungen, die sie definieren, invertierbar?

   (a) $\begin{pmatrix} 2 \end{pmatrix}$ über $\mathbb{F}_5$.

   (b) $\begin{pmatrix} 2 & 4 \\ 3 & 6 \end{pmatrix}$ über $\mathbb{F}_7$.

   (c) $\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 2 & 0 & 0 \end{pmatrix}$ über $\mathbb{F}_3$.

   (d) $\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ über $\mathbb{F}_2$.

2.5 Hilfe: Beispiele

2.5.1 Matrizen

Gegeben sei der Vektorraum $\mathbb{F}_3^4$ mit der kanonischen Basis $B := \{\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}\}$. (Die Reihenfolge der Basisvektoren sei festgelegt.) Gegeben sei außerdem der Vektorraum $\mathbb{F}_3^2$ mit der Basis $B := \{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$.
Nun definieren wir die lineare Abbildung $f : \mathbb{F}_3^4 \to \mathbb{F}_3^2$ mit

$$f(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}) = \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \; f(\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}) = \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \; f(\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}) = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \text{ und } f(\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}) = \begin{pmatrix} 1 \\ 2 \end{pmatrix}.$$

Das definiert eine lineare Abbildung, weil jedem Vektor einer Basis von $\mathbb{F}_3^4$ (und somit jedem Vektor von $\mathbb{F}_3^4$) ein Vektor des Zielvektorraums $\mathbb{F}_3^2$ zugeordnet wird. Dann existieren Zahlen a_{ij} mit $1 < i < 3, 1 < j < 5$ und

$$f(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}) = \begin{pmatrix} x_1 a_{11} & + & x_2 a_{12} & + & x_3 a_{13} & + & x_4 a_{14} \\ x_1 a_{21} & + & x_2 a_{22} & + & x_3 a_{23} & + & x_4 a_{24} \end{pmatrix}$$

für alle Vektoren aus $\mathbb{F}_3^4$. Beispielsweise haben wir

$$f(\begin{pmatrix}1\\2\\0\\2\end{pmatrix}) = f(1\cdot\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+2\cdot\begin{pmatrix}0\\1\\0\\0\end{pmatrix}+0\cdot\begin{pmatrix}0\\0\\1\\0\end{pmatrix}+2\cdot\begin{pmatrix}0\\0\\1\\0\end{pmatrix})$$

$$= f(1\cdot\begin{pmatrix}1\\0\\0\\0\end{pmatrix}) + f(2\cdot\begin{pmatrix}0\\1\\0\\0\end{pmatrix}) + f(0\cdot\begin{pmatrix}0\\0\\1\\0\end{pmatrix}) + f(2\cdot\begin{pmatrix}0\\0\\1\\0\end{pmatrix})$$

$$= 1\cdot f(\begin{pmatrix}1\\0\\0\\0\end{pmatrix}) + 2\cdot f(\begin{pmatrix}0\\1\\0\\0\end{pmatrix}) + 0\cdot f(\begin{pmatrix}0\\0\\1\\0\end{pmatrix}) + 2\cdot f(\begin{pmatrix}0\\0\\1\\0\end{pmatrix})$$

$$= 1\cdot\begin{pmatrix}2\\1\end{pmatrix} + 2\cdot\begin{pmatrix}0\\2\end{pmatrix} + 0\cdot\begin{pmatrix}1\\1\end{pmatrix} + 2\cdot\begin{pmatrix}1\\2\end{pmatrix}$$

$$= \begin{pmatrix}1\cdot 2\\1\cdot 1\end{pmatrix} + \begin{pmatrix}2\cdot 0\\2\cdot 2\end{pmatrix} + \begin{pmatrix}0\cdot 1\\0\cdot 1\end{pmatrix} + \begin{pmatrix}2\cdot 1\\2\cdot 2\end{pmatrix}$$

$$= \begin{pmatrix}1\cdot 2 & + & 2\cdot 0 & + & 0\cdot 1 & + & 2\cdot 1\\1\cdot 1 & + & 2\cdot 2 & + & 0\cdot 1 & + & 2\cdot 2\end{pmatrix}$$

$$= \begin{pmatrix}1\cdot a_{11} & + & 2\cdot a_{12} & + & 0\cdot a_{13} & + & 2\cdot a_{14}\\1\cdot a_{21} & + & 2\cdot a_{22} & + & 0\cdot a_{23} & + & 2\cdot a_{24}\end{pmatrix}$$

$$[= \begin{pmatrix}1\\0\end{pmatrix}]$$

Das Zahlenschema $A = (a_{ij})_{1<i<3,1<j<5} = \begin{pmatrix}a_{11} & a_{12} & a_{13} & a_{14}\\a_{21} & a_{22} & a_{23} & a_{24}\end{pmatrix} = \begin{pmatrix}2 & 0 & 1 & 1\\1 & 2 & 1 & 2\end{pmatrix}$ ist eine 2×4-Matrix. Sie definiert dieselbe lineare Abbildung wie f. Wir sehen, dass die Spalten der Matrix denjenigen Vektoren $\begin{pmatrix}y_1\\y_2\end{pmatrix}$ aus $\mathbb{F}_3^2$ entsprechen, die f den Vektoren $\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}$ der kanonischen Basis aus $\mathbb{F}_3^4$ zuordnet (in der festgelegten Reihenfolge).

Mithilfe der gefundenen Matrix können wir nun für alle Vektoren $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$ des Vektorraums $\mathbb{F}_3^4$ das Bild aus $\mathbb{F}_3^2$ berechnen: $\begin{pmatrix} 2 & 0 & 1 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$. Beispielsweise haben wir $\begin{pmatrix} 2 & 0 & 1 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 2 \\ 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \cdot 2 & + & 2 \cdot 0 & + & 2 \cdot 1 & + & 2 \cdot 1 \\ 0 \cdot 1 & + & 2 \cdot 2 & + & 2 \cdot 1 & + & 2 \cdot 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$.

2.5.2 Lineare Gleichungen

Betrachten wir $\mathbb{F}_3$. Eine lineare Gleichung ist z.B. die Gleichung

$$2 \cdot x_1 + 2 \cdot x_2 + 1 \cdot x_3 = 1$$

Die x_i sind Unbekannte aus $\mathbb{F}_3$. Wir können die Unbekannten zu einem Vektor $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ zusammenfassen und definieren

$$g(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}) := x_1 \cdot \begin{pmatrix} 2 \end{pmatrix} + x_2 \cdot \begin{pmatrix} 2 \end{pmatrix} + x_3 \cdot \begin{pmatrix} 1 \end{pmatrix} = \begin{pmatrix} 2 \cdot x_1 & + & 2 \cdot x_2 & + & 1 \cdot x_3 \end{pmatrix}$$

Wir haben also eine lineare Abbildung g, die jedem Vektor $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ über $\mathbb{F}_3$ eine 1×1-Matrix $\begin{pmatrix} 2 \cdot x_1 + 2 \cdot x_2 + 1 \cdot x_3 \end{pmatrix}$ zuordnet. Also z.B.

$$g(\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}) = \begin{pmatrix} 2 \cdot 1 + 2 \cdot 2 + 1 \cdot 0 \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

$$g(\begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}) = \begin{pmatrix} 2 \cdot 0 + 2 \cdot 1 + 1 \cdot 2 \end{pmatrix} = \begin{pmatrix} 1 \end{pmatrix}$$

usw. Die lineare Abbildung ist also eine Abbildung $g : \mathbb{F}_3^3 \to \mathbb{F}_3$, gegeben durch die Matrix $\begin{pmatrix} 2 & 2 & 1 \end{pmatrix}$. Wir sehen, dass $\begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$ ein Vektor ist, dessen Bild unter g genau $\begin{pmatrix} 1 \end{pmatrix}$ ist.

Bei zwei Gleichungen, z.B.

$$2 \cdot x_1 + 2 \cdot x_2 + 1 \cdot x_3 = 1 \text{ und}$$

$$1 \cdot x_1 + 0 \cdot x_2 + 2 \cdot x_3 = 0$$

definieren wir:

$$h(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}) := x_1 \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} + x_2 \cdot \begin{pmatrix} 2 \\ 0 \end{pmatrix} + x_3 \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \cdot x_0 & + & 2 \cdot x_1 & + & 1 \cdot x_2 \\ 1 \cdot x_0 & + & 0 \cdot x_1 & + & 2 \cdot x_2 \end{pmatrix}$$

Also haben wir z.B.

$$h(\begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}) = \begin{pmatrix} 2 \cdot 1 & + & 2 \cdot 0 & + & 1 \cdot 2 \\ 1 \cdot 1 & + & 0 \cdot 0 & + & 2 \cdot 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

$$h(\begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}) = \begin{pmatrix} 2 \cdot 0 & + & 2 \cdot 2 & + & 1 \cdot 0 \\ 1 \cdot 0 & + & 0 \cdot 2 & + & 2 \cdot 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

usw. Die lineare Abbildung ist also eine Abbildung $h : \mathbb{F}_3^3 \to \mathbb{F}_3^2$. Wir sehen, dass $\begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}$ ein Vektor ist, dessen Bild unter h genau $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ist.

Eine n×m-Matrix definiert uns also eine lineare Abbildung von K^m nach K^n.

Im ersten Fall hatten wir die 1×3-Matrix $\begin{pmatrix} 2 & 2 & 1 \end{pmatrix}$, die uns eine Funktion $g : \mathbb{F}_3^3 \to \mathbb{F}_3^1$ definiert hat. Im zweiten Fall hatten wir eine 2×3-Matrix $\begin{pmatrix} 2 & 2 & 1 \\ 1 & 0 & 2 \end{pmatrix}$, die uns eine Funktion $h : \mathbb{F}_3^3 \to \mathbb{F}_3^2$ definiert hat.

2.5.3 Kerne

Betrachten wir die lineare Abbildung $i : \mathbb{F}_2^3 \to \mathbb{F}_2^2$ mit

$$i\left(\begin{pmatrix}1\\0\\0\end{pmatrix}\right)=\begin{pmatrix}1\\1\end{pmatrix},\ i\left(\begin{pmatrix}0\\1\\0\end{pmatrix}\right)=\begin{pmatrix}0\\1\end{pmatrix} \text{ und } i\left(\begin{pmatrix}0\\0\\1\end{pmatrix}\right)=\begin{pmatrix}0\\0\end{pmatrix}.$$

.

Die Vektoren v mit $i(v)=\begin{pmatrix}0\\0\end{pmatrix}$ bilden einen Unterraum von $\mathbb{F}_2^3$. Dieser Unterraum ist der *Kern* von i ($Ker(i)$). Wir suchen also alle Vektoren von $\mathbb{F}_2^3$, die unter der angegebenen Abbildung den Nullvektor von $\mathbb{F}_2^2$ ergeben. Gehen wir die Vektoren durch:

$$i\left(\begin{pmatrix}0\\0\\0\end{pmatrix}\right)=\begin{pmatrix}0\\0\end{pmatrix}$$

$$i\left(\begin{pmatrix}0\\0\\1\end{pmatrix}\right)=\begin{pmatrix}0\\0\end{pmatrix}$$

$$i\left(\begin{pmatrix}0\\1\\0\end{pmatrix}\right)=\begin{pmatrix}0\\1\end{pmatrix}$$

$$i\left(\begin{pmatrix}0\\1\\1\end{pmatrix}\right)=i\left(\begin{pmatrix}0\\0\\1\end{pmatrix}\right)+i\left(\begin{pmatrix}0\\1\\0\end{pmatrix}\right)=\begin{pmatrix}0\\0\end{pmatrix}+\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$$

$$i\left(\begin{pmatrix}1\\0\\0\end{pmatrix}\right)=\begin{pmatrix}1\\1\end{pmatrix}$$

$$i\left(\begin{pmatrix}1\\0\\1\end{pmatrix}\right)=i\left(\begin{pmatrix}0\\0\\1\end{pmatrix}\right)+i\left(\begin{pmatrix}1\\0\\0\end{pmatrix}\right)=\begin{pmatrix}0\\0\end{pmatrix}+\begin{pmatrix}1\\1\end{pmatrix}=\begin{pmatrix}1\\1\end{pmatrix}$$

$$i\left(\begin{pmatrix}1\\1\\0\end{pmatrix}\right)=i\left(\begin{pmatrix}1\\0\\0\end{pmatrix}\right)+i\left(\begin{pmatrix}0\\1\\0\end{pmatrix}\right)=\begin{pmatrix}1\\1\end{pmatrix}+\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$$

$$i\left(\begin{pmatrix}1\\1\\1\end{pmatrix}\right)=i\left(\begin{pmatrix}1\\0\\0\end{pmatrix}\right)+i\left(\begin{pmatrix}0\\1\\0\end{pmatrix}\right)+i\left(\begin{pmatrix}0\\0\\1\end{pmatrix}\right)=\begin{pmatrix}1\\1\end{pmatrix}+\begin{pmatrix}0\\1\end{pmatrix}+\begin{pmatrix}0\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$$

Die Vektoren aus $\mathbb{F}_2^3$, die den Kern der linearen Abbildung bilden, sind somit $\begin{pmatrix}0\\0\\0\end{pmatrix}$ und $\begin{pmatrix}0\\0\\1\end{pmatrix}$. D.h., $Ker(i) = \{\begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}\}$. $Ker(i)$ bildet einen Unterraum von $\mathbb{F}_2^3$.

2.5.4 Determinanten

Betrachten wir folgende Matrix über $\mathbb{F}_7$: $\begin{pmatrix}2&3&0&6&1\\1&1&1&5&0\\0&2&2&3&0\\0&1&6&5&4\\6&0&0&2&2\end{pmatrix}$

Diese Matrix nennen wir $A = (a_{i,j})_{i,j<5}$. Wir schreiben $A^{i,j}$ für diejenige Matrix, die aus A durch Streichen der i. Zeile und der j. Spalte entsteht. Also $A^{i,j} = (b_{k,l})_{k,l<4}$ mit

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

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

- für $m = 1$: $det(A) = a_{0,0}$
- für $m > 1$: $det(A) = a_{0,0} \cdot det(A^{0,0}) - a_{1,0} \cdot det(A^{1,0}) + a_{2,0} \cdot det(A^{2,0}) - \cdots + (-1)^{m-1} a_{m-1,0} \cdot det(A^{m-1,0})$

Schauen wir uns das am Beispiel unserer Matrix an: Wir haben $m = 5$. Also haben wir

$$\begin{aligned}
& det(\begin{pmatrix}2&3&0&6&1\\1&1&1&5&0\\0&2&2&3&0\\0&1&6&5&4\\6&0&0&2&2\end{pmatrix}) \\
= \; & 2 \cdot det(A^{0,0}) - 1 \cdot det(A^{1,0}) + 0 \cdot det(A^{2,0}) - 0 \cdot det(A^{3,0}) + 6 \cdot det(A^{4,0}) \\
= \; & 2 \cdot det(\begin{pmatrix}1&1&5&0\\2&2&3&0\\1&6&5&4\\0&0&2&2\end{pmatrix}) - 1 \cdot det(\begin{pmatrix}3&0&6&1\\2&2&3&0\\1&6&5&4\\0&0&2&2\end{pmatrix}) + 6 \cdot det(\begin{pmatrix}3&0&6&1\\1&1&5&0\\2&2&3&0\\1&6&5&4\end{pmatrix})
\end{aligned}$$

$$
\begin{aligned}
= \; & 2\cdot(1\cdot det(\begin{pmatrix}2&3&0\\6&5&4\\0&2&2\end{pmatrix}) - 2\cdot det(\begin{pmatrix}1&5&0\\6&5&4\\0&2&2\end{pmatrix}) + 1\cdot det(\begin{pmatrix}1&5&0\\2&3&0\\0&2&2\end{pmatrix}) - 0\cdot det(\begin{pmatrix}1&5&0\\2&3&0\\6&5&4\end{pmatrix}))\\
& -1\cdot(3\cdot det(\begin{pmatrix}2&3&0\\6&5&4\\0&2&2\end{pmatrix}) - 2\cdot det(\begin{pmatrix}0&6&1\\6&5&4\\0&2&2\end{pmatrix}) + 1\cdot det(\begin{pmatrix}0&6&1\\2&3&0\\0&2&2\end{pmatrix}) - 0\cdot det(\begin{pmatrix}0&6&1\\2&3&0\\6&5&4\end{pmatrix}))\\
& +6\cdot(3\cdot det(\begin{pmatrix}1&5&0\\2&3&0\\6&5&4\end{pmatrix}) - 1\cdot det(\begin{pmatrix}0&6&1\\2&3&0\\6&5&4\end{pmatrix}) + 2\cdot det(\begin{pmatrix}0&6&1\\1&5&0\\6&5&4\end{pmatrix}) - 1\cdot det(\begin{pmatrix}0&6&1\\1&5&0\\2&3&0\end{pmatrix}))
\end{aligned}
$$

$$
\begin{aligned}
= \; & 2\cdot(1\cdot(2\cdot det(\begin{pmatrix}5&4\\2&2\end{pmatrix}) - 6\cdot det(\begin{pmatrix}3&0\\2&2\end{pmatrix}) + 0\cdot det(\begin{pmatrix}3&0\\5&4\end{pmatrix}))\\
& -2\cdot(1\cdot det(\begin{pmatrix}5&4\\2&2\end{pmatrix}) - 6\cdot det(\begin{pmatrix}5&0\\2&2\end{pmatrix}) + 0\cdot det(\begin{pmatrix}5&0\\5&4\end{pmatrix}))\\
& +1\cdot(1\cdot det(\begin{pmatrix}3&0\\2&2\end{pmatrix}) - 2\cdot det(\begin{pmatrix}5&0\\2&2\end{pmatrix}) + 0\cdot det(\begin{pmatrix}5&0\\3&0\end{pmatrix})))\\
& -1\cdot(3\cdot(1\cdot det(\begin{pmatrix}5&4\\2&2\end{pmatrix}) - 6\cdot det(\begin{pmatrix}3&0\\2&2\end{pmatrix}) + 0\cdot det(\begin{pmatrix}3&0\\5&4\end{pmatrix}))\\
& -2\cdot(0\cdot det(\begin{pmatrix}5&4\\2&2\end{pmatrix}) - 6\cdot det(\begin{pmatrix}6&1\\2&2\end{pmatrix}) + 0\cdot det(\begin{pmatrix}6&1\\5&4\end{pmatrix}))\\
& +1\cdot(0\cdot det(\begin{pmatrix}3&0\\2&2\end{pmatrix}) - 2\cdot det(\begin{pmatrix}6&1\\2&2\end{pmatrix}) + 0\cdot det(\begin{pmatrix}6&1\\3&0\end{pmatrix})))\\
& +6\cdot(3\cdot(1\cdot det(\begin{pmatrix}3&0\\5&4\end{pmatrix}) - 2\cdot det(\begin{pmatrix}5&0\\5&4\end{pmatrix}) + 6\cdot det(\begin{pmatrix}5&0\\3&0\end{pmatrix}))\\
& -1\cdot(0\cdot det(\begin{pmatrix}3&0\\5&4\end{pmatrix}) - 2\cdot det(\begin{pmatrix}6&1\\5&4\end{pmatrix}) + 6\cdot det(\begin{pmatrix}6&1\\3&0\end{pmatrix}))\\
& +2\cdot(0\cdot det(\begin{pmatrix}5&0\\5&4\end{pmatrix}) - 1\cdot det(\begin{pmatrix}6&1\\5&4\end{pmatrix}) + 6\cdot det(\begin{pmatrix}6&1\\5&0\end{pmatrix}))\\
& -1\cdot(0\cdot det(\begin{pmatrix}5&0\\3&0\end{pmatrix}) - 1\cdot det(\begin{pmatrix}6&1\\3&0\end{pmatrix}) + 2\cdot det(\begin{pmatrix}6&1\\5&0\end{pmatrix})))
\end{aligned}
$$

$$
\begin{aligned}
= \; & 2\cdot(1\cdot(2\cdot(5\cdot 2-2\cdot 4) - 6\cdot(3\cdot 2-2\cdot 0))\\
& -2\cdot(1\cdot(5\cdot 2-2\cdot 4) - 6\cdot(5\cdot 2-2\cdot 0))\\
& +1\cdot(1\cdot(3\cdot 2-2\cdot 0) - 2\cdot(5\cdot 2-2\cdot 0)))\\
& -1\cdot(3\cdot(1\cdot(5\cdot 2-2\cdot 4) - 6\cdot(6\cdot 2-2\cdot 1))\\
& -2\cdot(-6\cdot(6\cdot 2-2\cdot 1))\\
& +1\cdot(-2\cdot(6\cdot 2-2\cdot 1)))\\
& +6\cdot(3\cdot(1\cdot(3\cdot 4-5\cdot 0) - 2\cdot(5\cdot 4-5\cdot 0) + 6\cdot(5\cdot 0-3\cdot 0))
\end{aligned}
$$

$$
\begin{aligned}
& - 1 \cdot (-2 \cdot (6 \cdot 4 - 5 \cdot 1) + 6 \cdot (6 \cdot 0 - 3 \cdot 1)) \\
& + 2 \cdot (-1 \cdot (6 \cdot 4 - 5 \cdot 1) + 6 \cdot (6 \cdot 0 - 5 \cdot 1)) \\
& - 1 \cdot (-1 \cdot (6 \cdot 0 - 3 \cdot 1) + 2 \cdot (6 \cdot 0 - 5 \cdot 1))) \\
= \ & 2 \cdot (1 \cdot (2 \cdot (3 - 1) - 6 \cdot (6 - 0)) \\
& - 2 \cdot (1 \cdot (3 - 1) - 6 \cdot (3 - 0)) \\
& + 1 \cdot (1 \cdot (6 - 0) - 2 \cdot (3 - 0))) \\
& - 1 \cdot (3 \cdot (1 \cdot (3 - 1) - 6 \cdot (5 - 2)) \\
& - 2 \cdot (-6 \cdot (5 - 2)) \\
& + 1 \cdot (-2 \cdot (5 - 2))) \\
& + 6 \cdot (3 \cdot (1 \cdot (5 - 0) - 2 \cdot (6 - 0) + 6 \cdot (0 - 0)) \\
& - 1 \cdot (-2 \cdot (3 - 5) + 6 \cdot (0 - 3)) \\
& + 2 \cdot (-1 \cdot (3 - 5) + 6 \cdot (0 - 5)) \\
& - 1 \cdot (-1 \cdot (0 - 3) + 2 \cdot (0 - 5))) \\
= \ & 2 \cdot (1 \cdot (2 \cdot 2 - 6 \cdot 6) \\
& - 2 \cdot (1 \cdot 2 - 6 \cdot 3) \\
& + 1 \cdot (1 \cdot 6 - 2 \cdot 3)) \\
& - 1 \cdot (3 \cdot (1 \cdot 2 - 6 \cdot 3) \\
& - 2 \cdot (-6 \cdot 3) \\
& + 1 \cdot (-2 \cdot 3)) \\
& + 6 \cdot (3 \cdot (1 \cdot 5 - 2 \cdot 6 + 6 \cdot 0) \\
& - 1 \cdot (-2 \cdot (-2) + 6 \cdot (-3)) \\
& + 2 \cdot (-1 \cdot (-2) + 6 \cdot (-5)) \\
& - 1 \cdot (-1 \cdot (-3) + 2 \cdot (-5))) \\
= \ & 2 \cdot (1 \cdot (4 - 1) \\
& - 2 \cdot (2 - 4) \\
& + 1 \cdot (6 - 6)) \\
& - 1 \cdot (3 \cdot (2 - 4) \\
& - 2 \cdot (1 \cdot 3) \\
& + 1 \cdot (5 \cdot 3)) \\
& + 6 \cdot (3 \cdot (5 - 5 + 0) \\
& - 1 \cdot (5 \cdot 5 + 6 \cdot 4) \\
& + 2 \cdot (6 \cdot 5 + 6 \cdot 2) \\
& - 1 \cdot (6 \cdot 4 + 2 \cdot 2)) \\
= \ & 2 \cdot (1 \cdot 3 \\
& - 2 \cdot (-2)
\end{aligned}
$$

$$
\begin{aligned}
&+ 1 \cdot 0) \\
&- 1 \cdot (3 \cdot (-2) \\
&- 2 \cdot 3 \\
&+ 1 \cdot 1) \\
&+ 6 \cdot (3 \cdot 0 \\
&- 1 \cdot (4 + 3) \\
&+ 2 \cdot (2 + 5) \\
&- 1 \cdot (3 + 4)) \\
= {} & 2 \cdot (3 - 2 \cdot 5 + 0) - 1 \cdot (3 \cdot 5 - 6 + 1) + 6 \cdot (0 - 1 \cdot 0 + 2 \cdot 0 - 1 \cdot 0) \\
= {} & 2 \cdot (3 - 3 + 0) - 1 \cdot (1 - 6 + 1) + 6 \cdot (0 - 0 + 0 - 0) \\
= {} & 2 \cdot 0 - 1 \cdot (-4) + 6 \cdot 0 \\
= {} & 0 - 1 \cdot 3 + 0 \\
= {} & 0 - 3 + 0 \\
= {} & -3 \\
= {} & 4
\end{aligned}
$$

2.6 Hilfe: Wie berechnet man den Kern einer linearen Abbildung?

Gegeben sei die Matrix $\begin{pmatrix} 2 & 3 & 0 & 6 \\ 1 & 1 & 2 & 5 \\ 0 & 2 & 2 & 3 \end{pmatrix}$ über $\mathbb{F}_7$.

Diese Matrix beschreibt eine lineare Abbildung $f : \mathbb{F}_7^4 \to \mathbb{F}_7^3$. Es soll der *Kern* berechnet werden. Dazu stellen wir zuerst folgende Gleichung auf:

$$
\begin{pmatrix} 2 & 3 & 0 & 6 \\ 1 & 1 & 2 & 5 \\ 0 & 2 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}
$$

Es ergibt sich ein lineares Gleichungssystem:

(1) $2 \cdot x_1 + 3 \cdot x_2 + 0 \cdot x_3 + 6 \cdot x_4 = 0$

(2) $1 \cdot x_1 + 1 \cdot x_2 + 2 \cdot x_3 + 5 \cdot x_4 = 0$

(3) $0 \cdot x_1 + 2 \cdot x_2 + 2 \cdot x_3 + 3 \cdot x_4 = 0$

Etwas verkürzt:

$$\begin{array}{c|ccccccccc|}
(1) & 2x_1 & + & 3x_2 & & & & 6x_4 & = & 0 \\
(2) & x_1 & + & x_2 & + & 2x_3 & + & 5x_4 & = & 0 \\
(3) & & & 2x_2 & + & 2x_3 & + & 3x_4 & = & 0
\end{array}$$

Nun können wir mit diesem LGS rechnen:

$$\begin{array}{c|ccccccccc|ll}
(1) & 2x_1 & + & 3x_2 & + & & + & 6x_4 & = & 0 & |-3x_2 & |-6x_4 \\
(2) & x_1 & + & x_2 & + & 2x_3 & + & 5x_4 & = & 0 & & \\
(3) & & & 2x_2 & + & 2x_3 & + & 3x_4 & = & 0 & |-2x_3 & |-3x_4
\end{array}$$

Wir erhalten (und rechnen immer weiter):

$$\begin{array}{c|cccccccccccc|l}
(1) & 2x_1 & & & & & & & = & 4x_2 & + & & x_4 & |:2 \\
(2) & x_1 & + & x_2 & + & 2x_3 & + & 5x_4 & = & 0 & & & & \\
(3) & & & 2x_2 & & & & & = & & & 5x_3 \; + & 4x_4 & |:2
\end{array}$$

$$\begin{array}{c|cccccccccccc|l}
(1) & x_1 & & & & & & & = & 2x_2 & + & & 4x_4 & |\text{ (1) in (2) einsetzen} \\
(2) & x_1 & + & x_2 & + & 2x_3 & + & 5x_4 & = & 0 & & & & \\
(3) & & & x_2 & & & & & = & & & 6x_3 \; + & 2x_4 & |\text{ (3) in (2) einsetzen}
\end{array}$$

$$\begin{array}{c|cccccccccc|l}
(1) & x_1 & & & & & = & 2x_2 & + & & 4x_4 & \\
(2) & & & 6x_3 & + & x_4 & = & 0 & & & & |-x_4 \\
(3) & & x_2 & & & & = & & & 6x_3 \; + & 2x_4 &
\end{array}$$

$$\begin{array}{c|cccccccc|l}
(1) & x_1 & & & = & 2x_2 & + & & 4x_4 & \\
(2) & & & 6x_3 & = & & & & 6x_4 & |:6 \\
(3) & & x_2 & & = & & & 6x_3 \; + & 2x_4 &
\end{array}$$

$$\begin{array}{c|ccccccc|l}
(1) & x_1 & & & = & 2x_2 & + & 4x_4 & \\
(2) & & & x_3 & = & & & x_4 & \mid (2) \text{ in } (3) \text{ einsetzen} \\
(3) & & x_2 & & = & & 6x_3 + & 2x_4 &
\end{array}$$

$$\begin{array}{c|cccccc|l}
(1) & x_1 & & & = & 2x_2 + & 4x_4 & \\
(2) & & & x_3 & = & & x_4 & \\
(3) & & x_2 & & = & & x_4 & \mid (3) \text{ in } (1) \text{ einsetzen}
\end{array}$$

$$\begin{array}{c|ccccc|}
(1) & x_1 & & & = & 6x_4 \\
(2) & & & x_3 & = & x_4 \\
(3) & & x_2 & & = & x_4
\end{array}$$

Nun können wir die Vektoren, die den Kern der Abbildung bilden, leicht ermitteln. Beginnen wir mit $x_1 = 0$. Dann ist 0 das 6-fache von x_4. Das 6-fache von 0 ist 0. Also ist $x_4 = 0$. Da $x_2 = x_3 = x_4$, ist auch $x_2 = 0$ und $x_3 = 0$. Der erste Vektor ist damit

$$v_1 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Weiter geht es mit $x_1 = 1$. Dann ist 1 das 6-fache von x_4. Das 6-fache von 6 ist 1. Also ist $x_4 = 6$. Da $x_2 = x_3 = x_4$, ist auch $x_2 = 6$ und $x_3 = 6$. Der zweite Vektor ist damit

$$v_2 = \begin{pmatrix} 1 \\ 6 \\ 6 \\ 6 \end{pmatrix}$$

Die anderen Vektoren des Kerns ergeben sich auf dieselbe Weise. Wir erhalten:

$$v_3 = \begin{pmatrix} 2 \\ 5 \\ 5 \\ 5 \end{pmatrix}$$

$$v_4 = \begin{pmatrix} 3 \\ 4 \\ 4 \\ 4 \end{pmatrix}$$

$$v_5 = \begin{pmatrix} 4 \\ 3 \\ 3 \\ 3 \end{pmatrix}$$

$$v_6 = \begin{pmatrix} 5 \\ 2 \\ 2 \\ 2 \end{pmatrix}$$

$$v_7 = \begin{pmatrix} 6 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Damit ist schließlich $Ker(f) = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$.

2.7 Hilfe: Wie berechnet man das Bild einer linearen Abbildung?

Gegeben sei die Matrix $\begin{pmatrix} 2 & 3 & 0 & 6 \\ 1 & 1 & 2 & 5 \\ 0 & 2 & 2 & 3 \end{pmatrix}$ über $\mathbb{F}_7$.

Diese Matrix beschreibt eine lineare Abbildung $f : \mathbb{F}_7^4 \to \mathbb{F}_7^3$. Es soll das *Bild* berechnet werden. Um das Bild schnell zu errechnen, kann man zuerst den *Kern* der linearen Abbildung berechnen. Für die obige Abbildung haben wir den folgenden Kern:

$$Ker(f) = \{\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 6 \\ 6 \\ 6 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \\ 5 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 4 \\ 4 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \\ 3 \\ 3 \end{pmatrix}, \begin{pmatrix} 5 \\ 2 \\ 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 6 \\ 1 \\ 1 \\ 1 \end{pmatrix}\}$$

Der Kern dieser linearen Abbildung bildet einen Unterraum von $\mathbb{F}_7^4$. Wir wissen, dass jeder Vektorraum eine Basis hat. Also hat auch $Ker(f)$ eine Basis. Die Basis eines Vektorraums liefert uns alle und nur die Vektoren des Vektorraums. Die Basis von $Ker(f)$ lautet:

$$B = \{\begin{pmatrix} 1 \\ 6 \\ 6 \\ 6 \end{pmatrix}\}$$

Um nun auf das Bild der linearen Abbildung zu kommen, gibt es zwei Möglichkeiten: eine sehr rechenintensive und eine, bei der man einen Satz geschickt verwendet.

2.7.1 Rechenintensiver Lösungsweg

Wir müssen die Basis des Kerns zuerst so vervollständigen, dass wir eine Basis von $\mathbb{F}_7^4$ erhalten. Dazu wählen wir drei weitere Vektoren:

$$C := \{\begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\end{pmatrix}\}$$

Anschließend berechnen wir $f[C] = \{f(c) : c \in C\}$. Wir berechnen also:

$$f(\begin{pmatrix}0\\1\\0\\0\end{pmatrix}) = \begin{pmatrix}2 & 3 & 0 & 6\\1 & 1 & 2 & 5\\0 & 2 & 2 & 3\end{pmatrix} \cdot \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}3\\1\\2\end{pmatrix}$$

$$f(\begin{pmatrix}0\\0\\1\\0\end{pmatrix}) = \begin{pmatrix}2 & 3 & 0 & 6\\1 & 1 & 2 & 5\\0 & 2 & 2 & 3\end{pmatrix} \cdot \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\2\\2\end{pmatrix}$$

$$f(\begin{pmatrix}0\\0\\0\\1\end{pmatrix}) = \begin{pmatrix}2 & 3 & 0 & 6\\1 & 1 & 2 & 5\\0 & 2 & 2 & 3\end{pmatrix} \cdot \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}6\\5\\3\end{pmatrix}$$

Wir stellen fest, dass diese drei Vektoren linear unabhängig voneinander sind. Außerden sind sie bezüglich Inklusion maximal. Würden wir einen einzigen Vektor hinzufügen, ließe sich dieser als Linearkombination der anderen Vektoren darstellen. Die Menge

$$f[C] = \{\begin{pmatrix}3\\1\\2\end{pmatrix}, \begin{pmatrix}0\\2\\2\end{pmatrix}, \begin{pmatrix}6\\5\\3\end{pmatrix}\}$$

bildet damit eine *Basis* der Dimension 3 über dem Körper $\mathbb{F}_7$. Das Bild von f ist damit die Vektormenge von $\mathbb{F}_7^3$.

2.7.2 Schneller Lösungsweg

Es gilt folgender Satz:

Satz: Sei $g : K^m \to K^n$. Dann ist m die Summe der Dimensionen von $Ker(g)$ und $Bild(g)$.

Die Basis des Kerns der obigen linearen Abbildung enthält einen Vektor. Damit beträgt die Dimension des Kerns 1. Nun war unsere lineare Abbildung eine Abbildung mit $f : \mathbb{F}_7^4 \to \mathbb{F}_7^3$. Dem Satz zufolge muss nun gelten: 4 ist die Summe der Dimensionen von $Ker(f)$ (also 1) und $Bild(f)$. Damit hat das Bild von f die Dimension 3. Die Basis vom Bild von f enthält damit 3 linear unabhängige Vektoren. Das Bild von f ist damit die Vektormenge von $\mathbb{F}_7^3$.

2.7.3 Weiterer Lösungsweg

Es folgt eine weitere Lösungsstrategie, um das Bild einer linearen Abbildung zu ermitteln. Für diese Lösungsstrategie ist es nicht erforderlich, zuerst den Kern der Abbildung zu bestimmen.

Gegeben sei wieder die Matrix $\begin{pmatrix} 2 & 3 & 0 & 6 \\ 1 & 1 & 2 & 5 \\ 0 & 2 & 2 & 3 \end{pmatrix}$ über $\mathbb{F}_7$.

Diese Matrix beschreibt eine lineare Abbildung $f : \mathbb{F}_7^4 \to \mathbb{F}_7^3$. Eine Möglichkeit, das Bild dieser linearen Abbildung zu berechnen, besteht darin, zu überprüfen, welche Funktionswerte die Vektoren der *kanonischen Basis* des Ausgangsvektorraums einnehmen. Die kanonische Basis des Vektorraums $\mathbb{F}_7^4$ enthält folgende Vektoren:

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \text{ und } \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Nun können wir die Funktionswerte für die Vektoren der kanonischen Basis ausrechnen:

$$f(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}) = \begin{pmatrix} 2 & 3 & 0 & 6 \\ 1 & 1 & 2 & 5 \\ 0 & 2 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$$

$$f\begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}2&3&0&6\\1&1&2&5\\0&2&2&3\end{pmatrix}\cdot\begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}3\\1\\2\end{pmatrix}$$

$$f\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}2&3&0&6\\1&1&2&5\\0&2&2&3\end{pmatrix}\cdot\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\2\\2\end{pmatrix}$$

$$f\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}2&3&0&6\\1&1&2&5\\0&2&2&3\end{pmatrix}\cdot\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}6\\5\\3\end{pmatrix}$$

Wir erhalten somit einfach die *Spalten* der obigen Matrix. Mindestens einer dieser Vektoren muss sich als Linearkombination der anderen Vektoren darstellen lassen [warum?]. So gilt z.B.

$$\begin{pmatrix}6\\5\\3\end{pmatrix} = 1\cdot\begin{pmatrix}2\\1\\0\end{pmatrix} + 6\cdot\begin{pmatrix}3\\1\\2\end{pmatrix} + 6\cdot\begin{pmatrix}0\\2\\2\end{pmatrix}$$

Damit bleiben die Vektoren $\begin{pmatrix}2\\1\\0\end{pmatrix}, \begin{pmatrix}3\\1\\2\end{pmatrix}$ und $\begin{pmatrix}0\\2\\2\end{pmatrix}$. Diese bilden eine linear unabhängige Menge. Damit handelt es sich bei $\{\begin{pmatrix}2\\1\\0\end{pmatrix}, \begin{pmatrix}3\\1\\2\end{pmatrix}, \begin{pmatrix}0\\2\\2\end{pmatrix}\}$ um eine *Basis* des Vektorraums $\mathbb{F}_7^3$. Und das ist unser Zielvektorraum. Also ist das Bild der linearen Abbildung $\mathbb{F}_7^3$.

2.8 Übungen: Eigenwerte

1. Berechne

   (a) $\begin{pmatrix}1&2\\0&1\end{pmatrix}\begin{pmatrix}2&2\\1&1\end{pmatrix}$ über $\mathbb{F}_3$

   (b) $\begin{pmatrix}2&3&0&6\\1&1&2&5\\0&2&2&3\end{pmatrix}\begin{pmatrix}1&2&0\\1&1&4\\2&2&2\\3&5&7\end{pmatrix}$ über $\mathbb{F}_7$

2. Gegeben sei folgendes Gleichungssystem.

$$\begin{array}{c|rcrcrcr|} (1) & 2x_1 & + & 3x_2 & + & 4x_3 & = & 0 \\ (2) & x_1 & - & x_2 & + & 2x_3 & = & 0 \\ (3) & -2x_1 & + & 2x_2 & + & 4x_3 & = & 1 \end{array}$$

   (a) Gib dieses Gleichungssystem als Gleichung über einem Produkt einer Matrix A mit dem Vektor $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ wieder.

   (b) Wie lautet das homogene Gleichungssystem?

   (c) Die Matrix A bestimmt eine lineare Abbildung $f : \mathbb{F}_5^3 \to \mathbb{F}_5^3$. Bestimme Kern und Bild dieser Abbildung.

3. Bestimme das charakteristische Polynom und die Eigenwerte der folgenden Abbildungen über $\mathbb{F}_5$.

   (a) $\begin{pmatrix} 2 & 4 \\ 1 & 1 \end{pmatrix}$

   (b) $\begin{pmatrix} 2 & 3 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 2 \end{pmatrix}$

2.9 Hilfe: Fragen und Antworten

Frage: Was ist ein Unterraum?

Antwort: Angenommen, wir haben einen Vektorraum $\langle V, +, -, 0, \circ \rangle$ über einem Körper K. Wir betrachten eine Teilmenge W von V (also eine Menge von Vektoren). Wenn die Menge W unter den Operationen $+$, $-$ und $\circ$ abgeschlossen ist (wenn man also, wie beim Ausgangsvektorraum, durch Anwendung dieser Operationen auf Vektoren der Menge W nicht aus dieser Menge "herauskommt"), dann ist $\langle W, +_W, -_W, 0, \circ_W \rangle$ ein Unterraum von $\langle V, +, -, 0, \circ \rangle$.

Frage: Was genau ist die *lineare Fortsetzung*?

Antwort: Angenommen, wir haben zwei Vektorräume V und W über einem Körper K. Sagen wir, V enthält die Vektormenge (über $\mathbb{F}_3$):

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

B soll eine Basis des Vektorraums V sein, also z.B.

- $B = \{\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}\}$

Nun ist $u : B \to W$ eine beliebige Abbildung, also eine Abbildung, die jedem Vektor aus B einen Vektor des Vektorraums W (ebenfalls über $\mathbb{F}_3$) zuordnet, z.B.

- $u(\begin{pmatrix}1\\0\end{pmatrix}) = \begin{pmatrix}2\\1\\1\end{pmatrix}$
- $u(\begin{pmatrix}0\\1\end{pmatrix}) = \begin{pmatrix}0\\2\\0\end{pmatrix}$

Nun gibt es genau eine lineare Abbildung $f : V \to W$, die jedem Vektor aus B *denselben Vektor* aus W zuordnet wie die Abbildung u. Für diese lineare Abbildung f muss also gelten:

- $f(\begin{pmatrix}1\\0\end{pmatrix}) = u(\begin{pmatrix}1\\0\end{pmatrix}) = \begin{pmatrix}2\\1\\1\end{pmatrix}$
- $f(\begin{pmatrix}0\\1\end{pmatrix}) = u(\begin{pmatrix}1\\0\end{pmatrix}) = \begin{pmatrix}0\\2\\0\end{pmatrix}$

Für das Beispiel ist das die folgende lineare Abbildung:

- $f(\begin{pmatrix}0\\0\end{pmatrix}) = \begin{pmatrix}0\\0\\0\end{pmatrix}$
- $f(\begin{pmatrix}1\\0\end{pmatrix}) = \begin{pmatrix}0\\2\\0\end{pmatrix}$
- $f(\begin{pmatrix}2\\0\end{pmatrix}) = \begin{pmatrix}0\\1\\0\end{pmatrix}$
- $f(\begin{pmatrix}0\\1\end{pmatrix}) = \begin{pmatrix}2\\1\\1\end{pmatrix}$

- $f(\begin{pmatrix}1\\1\end{pmatrix}) = \begin{pmatrix}2\\0\\1\end{pmatrix}$
- $f(\begin{pmatrix}2\\1\end{pmatrix}) = \begin{pmatrix}2\\2\\1\end{pmatrix}$
- $f(\begin{pmatrix}0\\2\end{pmatrix}) = \begin{pmatrix}1\\2\\2\end{pmatrix}$
- $f(\begin{pmatrix}1\\2\end{pmatrix}) = \begin{pmatrix}1\\1\\2\end{pmatrix}$
- $f(\begin{pmatrix}2\\2\end{pmatrix}) = \begin{pmatrix}1\\0\\2\end{pmatrix}$

Diese lineare Abbildung f nennt man die *lineare Fortsetzung* der Abbildung u. Die Abbildung u ordnet nur den Basisvektoren von V etwas aus W zu. Die Abbildung f setzt diese Abbildung linear fort, indem sie auch allen *Linearkombinationen der Basisvektoren* etwas zuordnet. (Alle Linearkombinationen der Basisvektoren eines Vektorraums V ergeben gerade die Vektormenge des Vektorraums V. Also haben wir eine lineare Abbildung.)

Frage: Was genau ist die *Koordinatenfunktion*?

Antwort: Sei $f : V \to K^B$ eine Funktion, wobei V die Vektormenge eines Vektorraums, K eine Menge von Körperelementen und B eine Basis des Vektorraums ist. Diese Funktion ordnet jedem Vektor v die Faktoren aus K zu, die man benötigt, um v als Linearkombination der Basisvektoren aus B darzustellen. Angenommen, wir haben einen Vektorraum mit der Vektormenge

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

Dann ist eine Basis dieses Vektorraums:

- $B = \{\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}\}$

Dann lässt sich z.B. der Vektor $\begin{pmatrix}2\\1\end{pmatrix}$ als Linearkombination der Basisvektoren so darstellen: $2 \circ \begin{pmatrix}1\\0\end{pmatrix} + 1 \circ \begin{pmatrix}0\\1\end{pmatrix}$. Die Koordinatenfunktion liefert uns damit die Werte 2 und 1. Genau sieht das so aus:

- $f(\begin{pmatrix}2\\1\end{pmatrix}) = \{\langle\begin{pmatrix}1\\0\end{pmatrix}, 2\rangle, \langle\begin{pmatrix}0\\1\end{pmatrix}, 1\rangle\}$

Die *Koordinatenfunktion* liefert uns also für jeden Vektor v eine Funktion, nämlich die Funktion, die jedem Basisvektor b den Koeffizienten zuordnet, den man benötigt, um v als Linearkombination der Basisvektoren darzustellen.

Frage: Könntest du noch einmal kurz erklären, was genau die *kanonische Basis* ist und wie man sie bekommt?

Antwort: Eine kanonische Basis eines Vektorraums ist einfach eine Basis, deren Vektoren eine bestimmte Gestalt haben: Jeder Vektor einer kanonischen Basis enthält in genau einer Zeile eine 1 und in jeder anderen Zeile eine 0.

Frage: Sind im Folgenden alle Zwischenschritte notwendig?

$$\begin{aligned}&f(z)\\&= f(1x + 1y)\\&= f(1x) + f(1y)\\&= f(x) + f(y)\end{aligned}$$

Antwort: Es fehlt sogar noch einer, nämlich $1 \cdot f(x) + 1 \cdot f(y)$! ;) Aber nein, wenn ein Faktor 0 beträgt, kann man den Summanden ganz weglassen. Wenn ein Faktor 1 beträgt (im unteren Beispiel, entsprechend dem obigen Beispiel, vor den Vektoren x und y), reicht es so:

$$\begin{aligned}&f(z)\\&= f(x + y)\\&= f(x) + f(y)\end{aligned}$$

Frage: Könntest Du noch einmal eine Kurzdefinition oder Ähnliches für Ker(Matrix) und $Bild$(Matrix) geben?

Antwort: Der *Kern* einer linearen Abbildung $f : V \to W$ besteht aus den Vektoren des Ausgangsvektorraums V, die von f auf den Nullvektor des Zielvektorraums W der linearen Abbildung abgebildet werden. Eine $n \times m$-Matrix definiert eine lineare Abbildung von einem m-dimensionalen Vektorraum in einen n-dimensionalen Vektorraum. Gesucht werden dann die m-dimensionalen Vektoren v, sodass "$n \times m$-Matrix $\cdot\, v$" den n-dimensionalen Nullvektor ergibt. Diese Vektoren kann man mithilfe eines linearen Gleichungssystems ermitteln.

Das *Bild* einer linearen Abbildung $f : V \to W$ besteht aus den Vektoren des Zielvektorraums W, auf die die Vektoren des Ausgangsvektorraums V der linearen Abbildung abgebildet werden. Eine $n \times m$-Matrix definiert eine lineare Abbildung von einem m-dimensionalen Vektorraum in einen n-dimensionalen Vektorraum. Gesucht werden dann alle n-dimensionalen Vektoren w, sodass irgendein m-dimensionaler Vektor v mit "$n \times m$-Matrix $\cdot\, v$" auf w abgebildet wird. Am einfachsten kann man dies berechnen, indem man zuerst die kanonische Basis des Ausgangsvektorraums bestimmt und dann die lineare Abbildung (Matrix) auf alle Vektoren der kanonischen Basis anwendet. Die linear unabhängigen Vektoren, die sich daraus ergeben, bilden das Bild der linearen Abbildung.

3 Verbände

3.1 Übungen: Partielle Ordnungen und Verbandsordnungen

1. Es sei $A := \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}$. Bei welchen der folgenden Relationen handelt es sich um partielle Ordnungen? Zeichne die Relationen.

   (a) $R_1 := \{\langle\diamondsuit,\heartsuit\rangle, \langle\heartsuit,\clubsuit\rangle, \langle\heartsuit,\spadesuit\rangle, \langle\diamondsuit,\clubsuit\rangle, \langle\diamondsuit,\spadesuit\rangle\}$

   (b) $R_2 := \{\langle\diamondsuit,\diamondsuit\rangle, \langle\diamondsuit,\heartsuit\rangle, \langle\heartsuit,\heartsuit\rangle, \langle\heartsuit,\spadesuit\rangle, \langle\spadesuit,\spadesuit\rangle, \langle\diamondsuit,\spadesuit\rangle, \langle\diamondsuit,\clubsuit\rangle, \langle\clubsuit,\clubsuit\rangle, \langle\clubsuit,\diamondsuit\rangle\}$

   (c) $R_3 := \{\langle\diamondsuit,\diamondsuit\rangle, \langle\diamondsuit,\heartsuit\rangle, \langle\heartsuit,\heartsuit\rangle, \langle\heartsuit,\spadesuit\rangle, \langle\spadesuit,\spadesuit\rangle, \langle\diamondsuit,\spadesuit\rangle, \langle\clubsuit,\clubsuit\rangle\}$

   (d) $R_4 := \{\langle\diamondsuit,\diamondsuit\rangle, \langle\heartsuit,\heartsuit\rangle, \langle\spadesuit,\spadesuit\rangle, \langle\clubsuit,\clubsuit\rangle\}$

   Bestimme eine weitere partielle Ordnung auf A.

2. Betrachte folgende partiell geordnete Mengen.

   (a) $\langle D, \leq\rangle$ mit $D := \{a, b, c, d, e\}$ und
   $\leq\, := \{\langle a,a\rangle, \langle b,b\rangle, \langle c,c\rangle, \langle d,d\rangle, \langle e,e\rangle, \langle a,b\rangle, \langle a,c\rangle, \langle c,d\rangle, \langle a,d\rangle, \langle a,e\rangle\}$

   (b) $\langle E, \leq\rangle$ mit $E := \{1, 2, 3, 4, 5\}$ und
   $\leq\, := \{\langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle, \langle 4,4\rangle, \langle 5,5\rangle, \langle 1,2\rangle, \langle 1,5\rangle, \langle 1,3\rangle, \langle 1,4\rangle, \langle 2,4\rangle, \langle 3,5\rangle\}$

(c) $\langle F, \leq\rangle$ mit $F := \{f, g, h, i, j, k\}$ und
$\leq := \{\langle f, f\rangle, \langle g, g\rangle, \langle h, h\rangle, \langle i, i\rangle, \langle j, j\rangle, \langle k, k\rangle, \langle f, g\rangle, \langle g, h\rangle, \langle f, h\rangle, \langle h, i\rangle, \langle g, i\rangle, \langle f, i\rangle, \langle f, j\rangle, \langle j, k\rangle, \langle f, k\rangle, \langle k, i\rangle, \langle j, i\rangle\}$

(d) $\langle G, \leq\rangle$ mit $M := \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit, \square\}$ und
$\leq := \{\langle\heartsuit, \heartsuit\rangle, \langle\spadesuit, \spadesuit\rangle, \langle\clubsuit, \clubsuit\rangle, \langle\square, \square\rangle, \langle\diamondsuit, \diamondsuit\rangle, \langle\heartsuit, \spadesuit\rangle, \langle\spadesuit, \clubsuit\rangle, \langle\heartsuit, \clubsuit\rangle, \langle\clubsuit, \square\rangle, \langle\heartsuit, \square\rangle, \langle\spadesuit, \square\rangle, \langle\heartsuit, \diamondsuit\rangle, \langle\diamondsuit, \square\rangle\}$

Bearbeite die folgenden Aufgaben für jede der partiellen Ordnungen.

(i) Zeichne sie.

(ii) Betrachte alle Teilmengen der Grundmenge. Gibt es obere/untere Schranken irgendwelcher Teilmengen? Falls ja: welche?

(iii) Betrachte alle Teilmengen der Grundmenge. Gibt es Suprema/Infima irgendwelcher Teilmengen? Falls ja: welche?

(iv) Handelt es sich um eine Verbandsordnung?

3. Sei $H := \{a, b, c\}$. Bestimme (zeichne) die Verbandsordnung, die durch $\subseteq$ auf $\wp(H)$ definiert wird. Was sind jeweils die Suprema und Infima der Teilmengen?

4. Sei $I := \{1, 2, 3, 4, 5, 6, 7, 8\}$. Bestimme (zeichne) die Verbandsordnung, die durch $| := \{\langle x, y\rangle : \text{x teilt y}\}$ definiert wird. Was sind jeweils die Suprema und Infima der Teilmengen?

5. Es sei $X \subseteq Y$. Zeige, dass $inf_{\leq}X \geq inf_{\leq}Y$.

3.2 LÖSUNG: Aufgabe 5

Es sei $X \subseteq Y$.

Zu zeigen: $inf_{\leq}X \geq inf_{\leq}Y$.

Zuerst einmal muss man für einen Beweis genau gucken, was einem zur Verfügung steht. In diesem Fall steht uns die Behauptung zur Verfügung, dass X eine Teilmenge von Y ist. Das bedeutet, dass es (evtl.) Elemente gibt, die zwar in Y sind, aber nicht in X. Diese Elemente können wir zu einer Menge Z zusammenfassen. Wir haben also:

- Da $X \subseteq Y$, gilt: Es gibt ein Z mit $X \cap Z = \varnothing$ und $Y = X \cup Z$.

Nun können wir die Behauptung, die bewiesen werden soll, ein wenig umformulieren:

- Zu zeigen ist, dass $inf_{\leq}X \geq inf_{\leq}X \cup Z$, wobei $X \cap Z = \varnothing$.

Die Menge Z hat ein Infimum $inf_{\leq}Z$. Nun können wir uns überlegen, wo sich das Infimum aus Z relativ zum Infimum von X befinden kann. Es gibt vier Möglichkeiten:

1. $inf_{\leq}Z = inf_{\leq}X$ [$inf_{\leq}Z \geq inf_{\leq}X$ und $inf_{\leq}Z \leq inf_{\leq}X$]: Wenn wir nun die Elemente von X und Z zusammenpacken, ändert sich nichts am Infimum der Vereinigung. Damit ist $inf_{\leq}X \geq inf_{\leq}X \cup Z$.

2. $inf_{\leq}Z > inf_{\leq}X$ [$inf_{\leq}Z \geq inf_{\leq}X$ und $inf_{\leq}Z \nleq inf_{\leq}X$]: Wenn wir nun die Elemente von X und Z zusammenpacken, gibt es entweder ein neues Infimum der Vereinigung, das unterhalb der beiden Infima liegt (damit wäre $inf_{\leq}X > inf_{\leq}X \cup Z$), oder das Infimum von X ist das Infimum der Vereinigung (damit wäre $inf_{\leq}X = inf_{\leq}X \cup Z$). In beiden Fällen wäre $inf_{\leq}X \geq inf_{\leq}X \cup Z$. Damit ist $inf_{\leq}X \geq inf_{\leq}X \cup Z$.

3. $inf_{\leq}Z < inf_{\leq}X$ [$inf_{\leq}Z \ngeq inf_{\leq}X$ und $inf_{\leq}Z \leq inf_{\leq}X$]: Wenn wir nun die Elemente von X und Z zusammenpacken, gibt es entweder ein neues Infimum der Vereinigung, das unterhalb der beiden Infima liegt (damit wäre $inf_{\leq}X > inf_{\leq}X \cup Z$), oder das Infimum von Z ist das Infimum der Vereinigung (damit wäre $inf_{\leq}Z = inf_{\leq}X \cup Z$). In beiden Fällen wäre $inf_{\leq}X \geq inf_{\leq}X \cup Z$. Damit ist $inf_{\leq}X \geq inf_{\leq}X \cup Z$.

4. $inf_{\leq}Z \ngeq inf_{\leq}X$ und $inf_{\leq}Z \nleq inf_{\leq}X$: Wenn wir nun die Elemente von X und Z zusammenpacken, dann gibt es unter den beiden Infima ein Element, das das Infimum der Vereinigung darstellt. Damit ist $inf_{\leq}X \geq inf_{\leq}X \cup Z$.

Damit wäre $inf_{\leq}X \geq inf_{\leq}X \cup Z$ für alle 4 Möglichkeiten. Damit ist $inf_{\leq}X \geq inf_{\leq}X \cup Z$. Damit ist schließlich $inf_{\leq}X \geq inf_{\leq}Y$, falls $X \subseteq Y$.

Eine ähnliche Argumentation kann man für die Behauptung, dass $sup_{\leq}X \leq sup_{\leq}Y$ (falls $X \subseteq Y$) durchführen. Probiert es aus!

3.3 Hilfe: Kommentierte Definitionen

Im Folgenden sollen ein paar der zentralen Definitionen für die Verbandstheorie aufgeführt und ein wenig erläutert werden.

3.3.1 Partielle Ordnung

Es sei M eine nichtleere Menge und $\leq \subseteq M \times M$. $\leq$ ist eine **partielle Ordnung** gdw. $\leq$ reflexiv, transitiv und antisymmetrisch ist. Das Paar $\langle M, \leq \rangle$ ist dann eine **partiell geordnete Menge**.

- Dass eine Relation **antisymmetrisch** ist, heißt nicht, dass sie **nicht symmetrisch** ist. Eine Relation R ist genau dann nicht symmetrisch, wenn es mindestens ein $\langle x, y\rangle$ in R gibt, sodass $\langle y, x\rangle$ nicht in R ist. Eine Relation R ist hingegen antisymmetrisch genau dann, wenn für keine *zwei verschiedenen* Elemente der Grundmenge x und y sowohl $\langle x, y\rangle$ als auch $\langle y, x\rangle$ in R sind.

3.3.2 Schranken

Es sei $\langle M, \leq\rangle$ eine partiell geordnete Menge und $X \subseteq M$.

- y ist eine **obere Schranke** von X, falls $x \leq y$ für alle $x \in X$.
  - y muss kein Element von X sein.
  - Wenn alle Elemente *innerhalb* von X in der Ordnung "unter" y liegen (oder y selbst sind), dann ist y eine obere Schranke von X.
  - Es kann mehrere obere Schranken einer Menge geben.
  - Es kann auch eine obere Schranke innerhalb einer Menge geben.
  - Alle Elemente "über" allen Elementen einer Menge X sind obere Schranken von X. Wenn wir beispielsweise die natürlichen Zahlen und die normale "größer oder gleich"-Relation betrachten, und uns die Teilmenge $\{1, 2\}$ herausnehmen, dann sind z.B. 2, 3, aber auch 100 und 3.567.345 obere Schranken von $\{1, 2\}$.
- Falls ein eindeutig bestimmtes $y \in M$ existiert, sodass $y \leq z$ für jede obere Schranke z von X gilt, so ist y das **Supremum** (kleinste obere Schranke) von X ($sup_{\leq}X$).
  - Das Supremum ist eine besondere obere Schranke, nämlich die kleinste (oder unterste) Schranke aller oberen Schranken einer Menge.
  - Wenn es ein Supremum einer Menge gibt, dann ist dieses auch eindeutig. Eine Menge kann nicht mehrere Suprema haben (anders als obere Schranken).
  - Ein Supremum kann innerhalb oder außerhalb einer Menge liegen.
- y ist eine **untere Schranke** von X, falls $y \leq x$ für alle $x \in X$.
  - y muss kein Element von X sein.
  - Wenn alle Elemente *innerhalb* von X in der Ordnung "über" y liegen (oder y selbst sind), dann ist y eine untere Schranke von X.
  - Es kann mehrere untere Schranken einer Menge geben.
  - Es kann auch eine untere Schranke innerhalb einer Menge geben.

- Alle Elemente "unter" allen Elementen eine Menge X sind untere Schranken von X. Wenn wir beispielsweise die natürlichen Zahlen und die normale "kleiner oder gleich"-Relation betrachten, und uns die Teilmenge $\{100, 50\}$ herausnehmen, dann sind z.B. 50, 49, aber auch 0 und 1 untere Schranken von $\{100, 50\}$.

- Falls ein eindeutig bestimmtes $y \in M$ existiert, sodass $z \leq y$ für jede obere Schranke z von X gilt, so ist y das **Infimum** (größte untere Schranke) von X ($inf_{\leq}X$).
  - Das Infimum ist eine besondere untere Schranke, nämlich die größte (oder oberste) Schranke aller unteren Schranken einer Menge.
  - Wenn es ein Infimum einer Menge gibt, dann ist dieses auch eindeutig. Eine Menge kann nicht mehrere Infima haben (anders als untere Schranken).
  - Ein Infimum kann innerhalb oder außerhalb einer Menge liegen.

3.3.3 Verbandsordung

$\leq$ ist genau dann eine **Verbandsordnung**, wenn $sup_{\leq}X$ und $inf_{\leq}X$ für alle endlichen $X \subseteq M$ existieren.

- Wenn es immer ein Supremum und ein Infimum gibt, egal welche Teilmenge der Ausgangsmenge wir herausnehmen, dann handelt es sich bei der dazugehörigen partiellen Ordnung um eine Verbandsordnung.

3.3.4 Verband

Es sei M eine nichtleere Menge und $\sqcap : M \times M \to M$ und $\sqcup : M \times M \to M$ zweistellige Funktionen. $\langle M, \sqcap, \sqcup \rangle$ ist ein **Verband**, falls folgende Gesetze gelten für alle $x, y, z \in M$:

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

- $\sqcup$ und $\sqcap$ sind Funktionen, die den beiden Elementen, auf die sie angewendet werden, jeweils ihr Supremum bzw. ihr Infimum zuordnen.

- Jede Verbandsordnung lässt sich damit auch als Verband verstehen und umgekehrt. Dabei gilt $x \leq y$ gdw. $x \sqcap y = x$ gdw. $x \sqcup y = y$, sowie $sup_{\leq}\{x, y\} = x \sqcup y$ und $inf_{\leq}\{x, y\} = x \sqcap y$.

3.4 Hilfe: Ein Verband

Es sei folgende partiell geordnete Menge gegeben:

$$M = \langle \{a, b, c, d\}, \leq \rangle \text{ mit}$$

$$\leq\ = \{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle, \langle d, d\rangle, \langle a, b\rangle, \langle a, c\rangle, \langle b, d\rangle, \langle a, d\rangle, \langle c, d\rangle\}$$

Wie stellt man nun fest, ob es sich bei der partiellen Ordnung um eine **Verbandsordnung** handelt? Nun, damit es sich bei einer partiellen Ordnung um eine Verbandsordnung handelt, muss folgende Bedingung erfüllt sein:

- Jede Teilmenge der Ausgangsmenge besitzt ein Supremum und ein Infimum.

In unserer Ausgangsmenge befinden sich 4 Elemente. D.h. wir erhalten $2^4 = 16$ verschiedene Teilmengen. Falls jede Teilmenge ein Supremum und ein Infomum besitzt, handelt es sich bei der gegebenen partiellen Ordnung um eine Verbandsordnung. Gehen wir die Teilmengen durch:

$$\begin{array}{ll}
sup\{a\} = a & inf\{a\} = a \\
sup\{b\} = b & inf\{b\} = b \\
sup\{c\} = c & inf\{c\} = c \\
sup\{d\} = d & inf\{d\} = b \\
sup\{a, b\} = b & inf\{a, b\} = a \\
sup\{a, c\} = c & inf\{a, c\} = a \\
sup\{a, d\} = d & inf\{a, d\} = a \\
sup\{b, c\} = d & inf\{b, c\} = a \\
sup\{b, d\} = d & inf\{b, d\} = b \\
sup\{c, d\} = d & inf\{c, d\} = c \\
sup\{a, b, c\} = d & inf\{a, b, c\} = a \\
sup\{a, b, d\} = d & inf\{a, b, d\} = a \\
sup\{a, c, d\} = d & inf\{a, c, d\} = a \\
sup\{b, c, d\} = d & inf\{b, c, d\} = a \\
sup\{a, b, c, d\} = d & inf\{a, b, c, d\} = a
\end{array}$$

Diese Teilmengen haben somit jeweils schon mal ein Infimum und ein Supremum. Wenn wir die Teilmengen allerdings durchzählen, stellen wir fest, dass eine fehlt: Die leere Menge. Damit es sich bei der partiellen Ordnung um eine Verbandsordnung handelt, müssen aber *alle* Teilmengen ein Supremum und ein Infimum besitzen, also auch die leere Menge (da die leere Menge eine Teilmenge jeder Menge ist). Doch welche Elemente könnten wir der leeren Menge als Supremum oder Infimum zuordnen? Um diese Frage zu beantworten, müssen wir uns noch einmal anschauen, was das Supremum bzw. das Infimum einer gegebenen Menge ist.

- Das **Supremum** einer Menge M ist die "kleinste" obere Schranke von M.
- Das **Infimum** einer Menge M ist die "größte" untere Schranke von M.

Was sind nun noch einmal obere bzw. untere Schranken?

- y ist eine **obere Schranke** von M, falls $x \leq y$ für alle $x \in M$.
- y ist eine **untere Schranke** von M, falls $y \leq x$ für alle $x \in M$.

Damit wir sofort sehen, was das für die leere Menge bedeutet, können wir diese beiden Bedingungen ein wenig umformen:

- y ist eine **obere Schranke** von M, falls es kein $x \in M$ gibt, sodass $x \nleq y$.
- y ist eine **untere Schranke** von M, falls es kein $x \in M$ gibt, sodass $y \nleq x$.

Die erste Bedingung sagt, dass y eine obere Schranke von M ist, falls kein x aus der Menge M "über" y ist. Die zweite Bedingung sagt, dass y eine untere Schranke von M ist, falls kein x aus der Menge M "unter" y ist. Wenn wir diese Bedingungen auf die leere Menge anwenden, ergibt sich folgendes Ergebnis: Da die leere Menge *gar kein* Element enthält, gilt für alle Elemente x der Grundmenge, dass die leere Menge *insbesondere* kein Elemente enthält, welches "über" oder "unter" x ist. Damit ist *jedes* Element der Ausgangsmenge *obere und untere Schranke der leeren Menge.*

Wenn nun alle Elemente der Ausgangsmenge *obere* Schranken der leeren Menge sind, dann ist die *kleinste* obere Schranke (also das Supremum) offenbar das Element a. Und wenn alle Elemente der Ausgangsmenge *untere* Schranken der leeren Menge sind, dann ist die *größte* untere Schranke (also das Infimum) offenbar das Element d. Das mag etwas merkwürdig sein, aber die Definitionen legen diese Elemente eindeutig als Supremum bzw. Infimum der leeren Menge fest. Wir haben also:

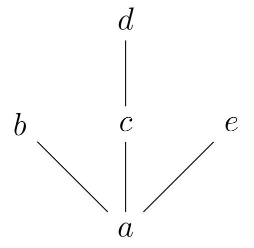
$$sup\varnothing = a \quad inf\varnothing = d$$

Damit sind alle Teilmengen mit Suprema und Infima versorgt. Bei der obigen partiellen Ordnung handelt es sich somit um eine Verbandsordnung. Die obige partiell geordnete Menge $\langle\{a,b,c,d\},\leq\rangle$ lässt sich damit als Verband $\langle\{a,b,c,d\},\sqcap,\sqcup\rangle$ mit entsprechenden Funktionen $\sqcap$ und $\sqcup$ verstehen.

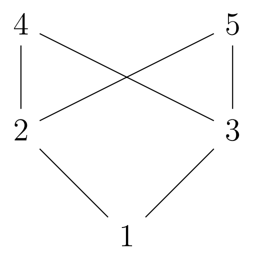
3.5 Übungen: Distributive Verbände

1. Betrachte folgende partiell geordnete Mengen.

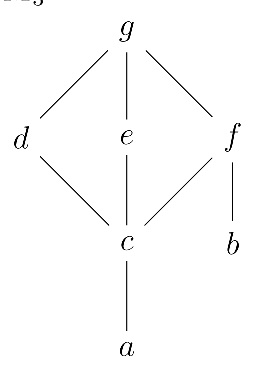
   (a) M_1 :

   (b) M_2 :

   (c) M_3 :

   (i) Warum handelt es sich bei den Ordnungen *nicht* um Verbandsordnungen?

   (ii) Sind die Ordnungen linear?

2. Betrachte folgende Verbände.

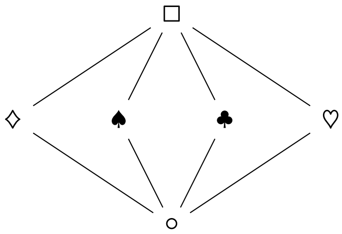
   (a) $\mathfrak{V}_1 = \langle T(18), \text{ggT}, \text{kgV} \rangle$

   (b) $\mathfrak{V}_2 = \langle T(28), \text{ggT}, \text{kgV} \rangle$

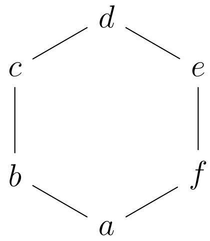
   (c) $\mathfrak{V}_3 = \langle T(25), \text{ggT}, \text{kgV} \rangle$

   (d) $\mathfrak{V}_4 = \langle T(60), \text{ggT}, \text{kgV} \rangle$

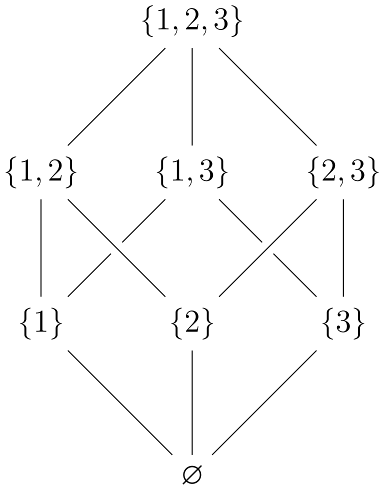
(e) $\mathfrak{V}_5$:



(f) $\mathfrak{V}_6$:



(g) $\mathfrak{V}_7$:



(i) Zeichne die Verbände $\mathfrak{V}_1$, $\mathfrak{V}_2$, $\mathfrak{V}_3$ und $\mathfrak{V}_4$.

(ii) Gib für jeden Verband $\mathfrak{V}_n$ die Null ($\bot$) und die Eins ($\top$) an.

(iii) Gib für jeden Verband $\mathfrak{V}_n$ die Menge $\mathrm{Irr}_{\sqcup}\mathfrak{V}_n$ der $\sqcup$-irreduziblen Elemente (und die Menge $\mathrm{Irr}_{\sqcap}\mathfrak{V}_n$ der $\sqcap$-irreduziblen Elemente) an.

(iv) Bilde jeweils für jede Teilmenge $T_{\mathfrak{V}_n}$ von $\mathrm{Irr}_{\sqcup}\mathfrak{V}_n$ die nach unten abgeschlossene Menge $\downarrow T_{\mathfrak{V}_n} = \{y \in \mathrm{Irr}_{\sqcup}\mathfrak{V}_n : \text{es gibt ein } x \in T_{\mathfrak{V}_n} \text{ mit } y \leq x\}$.

(v) Lassen sich die Mengen $\downarrow T_{\mathfrak{V}_n}$ unter den Operationen $\cup$ und $\cap$ genauso anordnen wie die Elemente von $\mathfrak{V}_n$ unter den Operationen $\sqcup$ und $\sqcap$?

(vi) Welche der Verbände $\mathfrak{V}_n$ sind distributiv?

3. Zeige, dass jeder lineare Verband distributiv ist.

4. Zeige, dass für jeden endlichen Verband gilt, dass ein Element genau dann $\sqcup$-irreduzibel ist, wenn es genau einen unteren Nachbarn hat.

3.6 Lösungen: Distributive Verbände

3.6.1 Aufgabe 3

Zu zeigen: Jeder lineare Verband ist distributiv.

Für einen Beweis ist es zuerst einmal wichtig, genau zu gucken, was alles gegeben ist und was genau man daraus ableiten soll. Es soll gezeigt werden, dass jeder lineare Verband distributiv ist.

Die Eigenschaft, linear zu sein, haben nur Relationen.

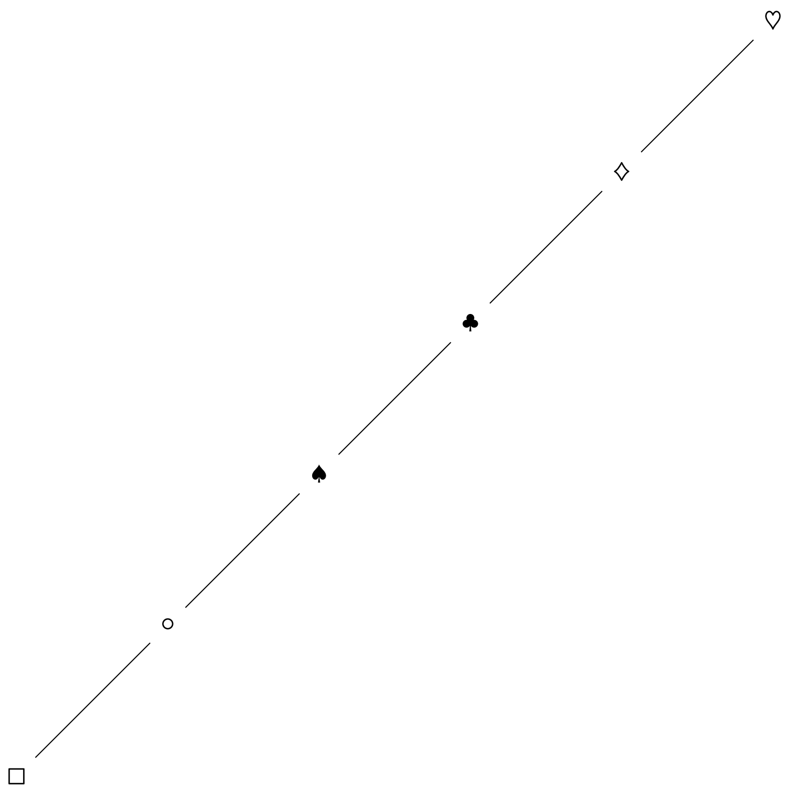
- Eine Relation $R \subseteq M \times M$ ist genau dann **linear**, wenn für alle $x, y \in M$, wobei $x \neq y$, gilt: entweder $\langle x, y\rangle \in R$ oder $\langle y, x\rangle \in R$.

Man kann sich das so vorstellen: Eine Relation ist genau dann linear, wenn sich jedes Element mit jedem anderen Element vergleichen lässt, und sich alle Elemente somit auf einer Linie anordnen lassen.

Da wir die Eigenschaft, linear zu sein, nur Relationen zuschreiben können, betrachten wir nicht direkt Verbände, sondern Verbandsordnungen. Das ist kein Problem: Wir wissen, dass eine eineindeutige Korrespondenz zwischen Verbänden und Verbandsordnungen besteht. Verbandsordnungen sind besondere partielle Ordnungen und damit reflexiv, transitiv und antisymmetrisch. Somit haben wir:

- Eine Verbandsordnung $\leq \subseteq M \times M$ ist genau dann **linear**, wenn für alle $x, y \in M$, wobei $x \neq y$, gilt: entweder $x < y$ oder $y > x$.

Diese Eigenschaft besagt, dass je zwei Elemente der Grundmenge der Verbandsordnung auf genau eine Weise miteinander verbunden sind. D.h. egal, welche zwei Elemente der Grundordnung wir betrachten, entweder ist das eine Element über dem anderen, oder umgekehrt. Es gibt also keine zwei Elemente, die auf zwei Weisen miteinander verbunden sind (aber das geht bei Verbandsordnungen ohnehin nicht, wegen ihrer wesentlichen Antisymmetrie), und keine zwei Elemente, die auf gar keine Weise miteinander verbunden sind (das ist eine neue und durch die Linearität geforderte Eigenschaft). Ein linearer Verband sieht z.B. so aus:



Da die eine von der Linearität geforderte Eigenschaft (dass es keine zwei Elemente gibt, die auf zwei Weisen miteinander verbunden sind) von allen Verbandsordnungen geteilt wird, kommt es für uns nur auf die zweite Eigenschaft an (dass jedes Element mit jedem anderen Element verbunden ist). Es ist also zu zeigen, dass jede Verbandsordnung, die *diese* Eigenschaft hat, auch die Eigenschaft der Distributivität hat.

Zu zeigen: Jede Verbandsordnung, in der jedes Element mit jedem anderen Element verbunden ist, ist distributiv.

Wir müssen dazu noch aufschreiben, was es heißt, dass ein Verband distributiv ist. Wir verwenden folgende Bestimmung:

- Ein Verband $\langle V, \sqcap, \sqcup \rangle$ ist genau dann **distributiv**, wenn sich alle $x \in V$ eindeutig als nach unten abgeschlossene Mengen irreduzibler Elemente aus V (die Menge all dieser Mengen sei U) darstellen lassen, sodass $\langle U, \cap, \cup \rangle$ zum Ausgangsverband isomorph ist.

Nun haben wir die Vorarbeit geleistet. Wir sind uns über die relevanten Begriffe klar geworden und haben verstanden, was einen linearen Verband eigentlich auszeichnet. Tatsächlich steckt in dieser Vorarbeit häufig die eigentliche (und schwierigste) Arbeit für einen Beweis. Der Beweis für die obige Behauptung sieht nämlich so aus (man könnte ihn glatt verpassen!):

Beweis: Da in einem linearen Verband jedes Element mit jedem anderen verbunden ist, gilt für beliebige Elemente $x, y, z \in M$: Aus $x = y \sqcup z$ folgt $x = y$ oder $x = z$. Damit ist jedes Element (bis auf die Null) eines linearen Verbands irreduzibel. Damit lässt sich jedes Element eines linearen Verbands eindeutig durch eine nach unten abgeschlossene Menge irreduzibler Elemente darstellen, sodass der Verband dieser Mengen zusammen mit $\cap$ und $\cup$ isomorph zum Ausgangsverband ist. Damit ist der Verband distributiv.

3.6.2 Aufgabe 4

Für die folgenden Definitionen, Behauptungen und Beweise sei $\mathfrak{V} = \langle V, \sqcap, \sqcup \rangle$ ein endlicher Verband. Die genannten Elemente seien stets in V.

Zu zeigen: In jedem endlichen Verband gilt, dass ein Element x genau dann $\sqcup$-irreduzibel ist, wenn es genau einen unteren Nachbarn hat.

Es folgen die relevanten Definitionen:

- x ist genau dann **$\sqcup$-irreduzibel**, wenn $x \neq \bot$ und aus $x = y \sqcup z$ folgt, dass $x = y$ oder $x = z$ (für alle y, z).
- y ist ein **unterer Nachbar von** x genau dann, wenn $y < x$ und es kein z gibt mit $y < z < x$.

Wir zerlegen die obige Behauptung in zwei Teilbehauptungen, die zu beweisen sind:

Zu zeigen$_{\rightarrow}$: Wenn x $\sqcup$-irreduzibel ist, dann hat x genau einen unteren Nachbarn.

Beweis$_{\rightarrow}$: Wir beweisen die Kontraposition. Angenommen, es ist nicht der Fall, dass x genau einen unteren Nachbarn hat. Dann hat x keinen oder mehr als einen unteren Nachbarn. Im ersten Fall ist $x = \bot$ und damit nicht $\sqcup$-irreduzibel. Im zweiten Fall seien a und b untere Nachbarn von x. Dann ist $a \sqcup b = x$, aber $x \neq a$ und $x \neq b$. Damit ist x ebenfalls nicht $\sqcup$-irreduzibel.

Zu zeigen$_{\leftarrow}$: Wenn x genau einen unteren Nachbarn hat, dann ist x $\sqcup$-irreduzibel.

Beweis$_{\leftarrow}$: Wir beweisen die Kontraposition. Angenommen, es ist nicht der Fall, dass x $\sqcup$-irreduzibel ist. Dann ist $x = \bot$ oder es gibt y und x mit $x = y \sqcup z$, aber $x \neq y$ und $x \neq z$. Im ersten Fall hat x keinen unteren Nachbarn. Im zweiten Fall gibt es Elemente u und v mit $y \sqcup u = u$ und $z \sqcup v = v$, sodass u und v untere Nachbarn von x sind. Damit hat x ebenfalls mehr als einen unteren Nachbarn.

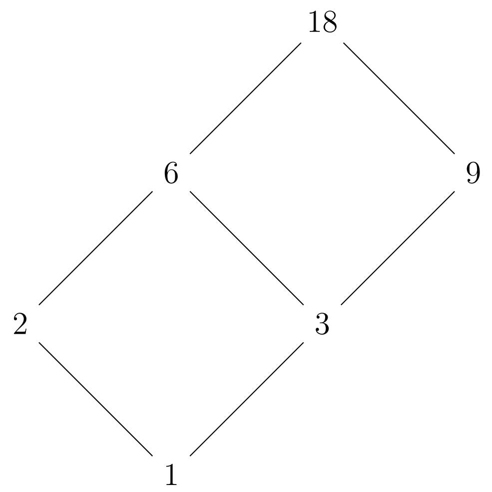
Beide Behauptungen wurden bewiesen. Damit wurde die Ausgangsbehauptung bewiesen.

3.7 Hilfe: Ein distributiver Verband

Es sei folgender Verband gegeben:

$$\mathfrak{T} = \langle T(18), \text{ggT}, \text{kgV} \rangle$$

Dies ist der Teilerverband von 18, mit $T(18) = \{1, 2, 3, 6, 9, 18\}$. Die Operation ggT liefert den größten gemeinsamen Teiler zweier Elemente. Die Operation kgV liefert das kleinste gemeinsame Vielfache zweier Elemente. Die Verbandsordnung des Verbands ist die x-teilt-y-Relation. Als Diagramm lässt sich der Verband folgendermaßen darstellen:



Das **minimale Element** (die **Null**) des Verbands ist 1 ($\bot = 1$). Das **maximale Element** (die **Eins**) ist 18 ($\top = 18$). 1 ist ein neutrales Element für ggT (in diesem Verband) und 18 ein neutrales Element für kgV (in diesem Verband).

Wir wollen nun herausfinden, ob der Verband $\mathfrak{T}$ **distributiv** ist. Dafür gehen wir folgendermaßen vor:

Schritt 1: Im Verband $\mathfrak{T}$ haben wir kgV-irreduzible Elemente. Das sind alle Elemente $x \neq 1$ für die gilt: Wenn $x = \text{kgV}(y,z)$, dann $x = y$ oder $x = z$ für alle $x, y \in T(18)$. Gehen wir die Elemente durch:

- $2 = \text{kgV}(\mathbf{2}, 1) = \text{kgV}(1, \mathbf{2}) = \text{kgV}(\mathbf{2}, \mathbf{2})$
  - In allen Fällen ist 2 mit mindestens einem der Teiler identisch.
  - Damit ist 2 kgV-irreduzibel.
- $3 = \text{kgV}(\mathbf{3}, 1) = \text{kgV}(1, \mathbf{3}) = \text{kgV}(\mathbf{3}, \mathbf{3})$

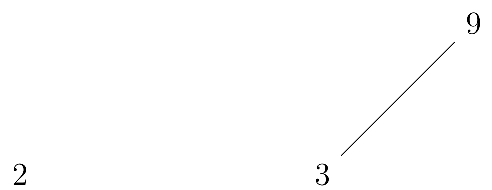
  - In allen Fällen ist 3 mit mindestens einem der Teiler identisch.
  - Damit ist 3 kgV-irreduzibel.

- $6 = \text{kgV}(2, 3)$ oder ...
  - Es gibt Elemente $x, y \in T(18)$, sodass zwar $6 = \text{kgV}(x, y)$, aber $6 \neq x$ und $6 \neq y$.
  - Damit ist 6 *nicht* kgV-irreduzibel.

- $9 = \text{kgV}(\mathbf{9}, 3) = \text{kgV}(3, \mathbf{9}) = \text{kgV}(\mathbf{9}, \mathbf{9}) = \text{kgV}(1, \mathbf{9}) = \text{kgV}(\mathbf{9}, 1)$
  - In allen Fällen ist 9 mit mindestens einem der Teiler identisch.
  - Damit ist 9 kgV-irreduzibel.

- $18 = \text{kgV}(6, 9)$ oder ...
  - Es gibt Elemente $x, y \in T(18)$, sodass zwar $18 = \text{kgV}(x, y)$, aber $18 \neq x$ und $18 \neq y$.
  - Damit ist 18 *nicht* kgV-irreduzibel.

Die kgV-irreduziblen Elemente von $\mathfrak{T}$ sind 2, 3 und 9. Damit ist $\text{Irr}_{kgV}\mathfrak{T} = \{2, 3, 9\}$. (Wir haben auch ggT-irreduzible Elemente. Diese sind 2, 6 und 9.) $\langle \text{Irr}_{kgV}\mathfrak{T}, \leq \rangle$ ist eine partiell geordnete Menge:



Schritt 2: Die Teilmengen von $\text{Irr}_{kgV}\mathfrak{T} = \{2, 3, 9\}$ sind $\varnothing, \{2\}, \{3\}, \{9\}, \{2, 3\}, \{2, 9\}, \{3, 9\}$ und $\{2, 3, 9\}$. Für jede dieser Teilmengen S können wir eine **nach unten abgeschlossene Menge** kgV-irreduzibler Elemente $\downarrow S = \{y \in \text{Irr}_{kgV}\mathfrak{T} : (\exists x \in S)(y \leq x)\}$ bilden:

- $\downarrow \varnothing = \{y \in \text{Irr}_{kgV}\mathfrak{T} : (\exists x \in \varnothing)(y \leq x)\} = \varnothing$
- $\downarrow \{2\} = \{y \in \text{Irr}_{kgV}\mathfrak{T} : (\exists x \in \{2\})(y \leq x)\} = \{2\}$
- $\downarrow \{3\} = \{y \in \text{Irr}_{kgV}\mathfrak{T} : (\exists x \in \{3\})(y \leq x)\} = \{3\}$
- $\downarrow \{9\} = \{y \in \text{Irr}_{kgV}\mathfrak{T} : (\exists x \in \{9\})(y \leq x)\} = \{3, 9\}$
- $\downarrow \{2, 3\} = \{y \in \text{Irr}_{kgV}\mathfrak{T} : (\exists x \in \{2, 3\})(y \leq x)\} = \{2, 3\}$

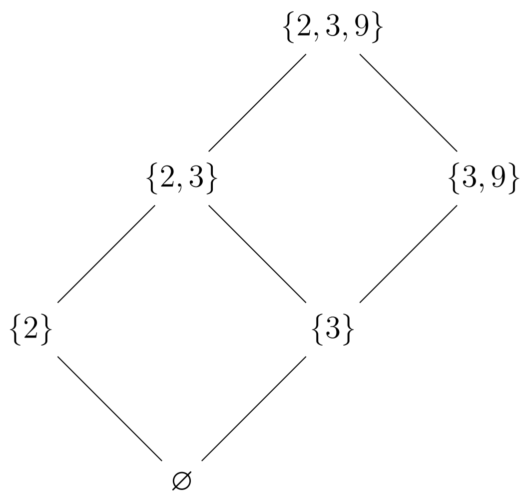
- $\downarrow \{2,9\} = \{y \in \mathrm{Irr}_{kgV}\mathfrak{T} : (\exists x \in \{2,9\})(y \leq x)\} = \{2,3,9\}$
- $\downarrow \{3,9\} = \{y \in \mathrm{Irr}_{kgV}\mathfrak{T} : (\exists x \in \{2,3\})(y \leq x)\} = \{3,9\}$
- $\downarrow \{2,3,9\} = \{y \in \mathrm{Irr}_{kgV}\mathfrak{T} : (\exists x \in \{2,3,9\})(y \leq x)\} = \{2,3,9\}$

Damit haben wir 6 verschiedene nach unten abgeschlossene Mengen kgV-irreduzibler Elemente: $\varnothing, \{2\}, \{3\}, \{3,9\}, \{2,3\}, \{2,3,9\}$.

Schritt 3: Nun können wir diese 6 Elemente so anordnen, wie die Elemente des Ausgangsverbands $\mathfrak{T}$ angeordnet sind, sodass die Struktur, die im Ausgangsverband durch die Operationen ggT und kgV gegeben ist, durch die Operationen $\cap$ und $\cup$ übernommen wird. Wir ordnen dazu jedem Element des Ausgangsverbands eine der 6 ermittelten nach unten abgeschlossenen Mengen kgV-irreduzibler Elemente zu:

- $1 \mapsto \varnothing$
- $2 \mapsto \{2\}$
- $3 \mapsto \{3\}$
- $6 \mapsto \{2,3\}$
- $9 \mapsto \{3,9\}$
- $18 \mapsto \{2,3,9\}$

Wir sehen, dass die nicht-kgV-irreduziblen Elemente des Ausgangsverbands (1, 6 und 18) eindeutig durch nach unten abgeschlossene Mengen kgV-irreduzibler Elemente dargestellt werden können. Der resultierende Verband sieht dann so aus:



Der Operation ggT entspricht die Operation $\cap$ im neuen Verband. Der Operation kgV entspricht die Operation $\cup$ im neuen Verband.

Ergebnis: Der obige Verband

$$\mathfrak{U} = \langle \{\varnothing, \{2\}, \{3\}, \{3,9\}, \{2,3\}, \{2,3,9\}\}, \cap, \cup \rangle$$

ist **isomorph** zum Ausgangsverband

$$\mathfrak{T} = \langle T(18), \text{ggT}, \text{kgV} \rangle$$

Damit handelt es sich beim Ausgangsverband $\mathfrak{T}$ um einen **distributiven Verband.** (Verwendet wurde für diesen Nachweis der **Darstellungssatz für endliche distributive Verbände**.)

3.8 Übungen: Boolesche Algebren

1. Warum sind folgende Verbände keine booleschen Algebren?
   (a) Der Teilerverband von 20
   (b) Ein beliebiger linearer Verband mit mehr als zwei Elementen
2. Es sei $\mathfrak{B}$ ein distributiver Verband mit Null und Eins. Sind y_1 und y_2 Komplemente von x, so ist $y_y = y_2$. Im Skript wurde bereits gezeigt, dass $y_1 \leq y_2$. Zeige, dass $y_2 \leq y_1$.
3. Zeichne die Hasse-Diagramme für die folgenden booleschen Algebren und gib die Komplementfunktionen explizit an.
   (a) Die boolesche Algebra $\mathfrak{B}_1$ der Wahrheitswerte **t** und **f**
   (b) Die boolesche Algebra $\mathfrak{B}_2$ der Teiler von 30
4. Bestimme Homomorphismen f_i mit:
   (a) $f_1 : \mathfrak{B}_1 \to \mathfrak{B}_2$
   (b) $f_2 : \mathfrak{B}_2 \to \mathfrak{B}_1$
   (c) $f_3 : \mathfrak{B}_2 \to \mathfrak{B}_2$

   Bestimme auch jeweils $f_i^{-1}(1)$.
5. Bestimme:

(a) Die Potenzmengenalgebra der Atome von $\mathfrak{B}_1$ und zeige, dass sie zu $\mathfrak{B}_1$ isomorph ist.

(b) Die Potenzmengenalgebra der Atome von $\mathfrak{B}_2$ und zeige, dass sie zu $\mathfrak{B}_2$ isomorph ist.

6. Zeichne die Hasse-Diagramme für die folgenden booleschen Algebren. Gib für (a) und (b) auch die Operationen an.

   (a) $\mathbf{2}$

   (b) $\mathbf{2}^2 = \langle 2^2, \vec{0}, \vec{1}, -, \cap, \cup \rangle$

   (c) $\mathbf{2}^3 = \langle 2^3, \vec{0}, \vec{1}, -, \cap, \cup \rangle$

   (d) $\mathbf{2}^4 = \langle 2^4, \vec{0}, \vec{1}, -, \cap, \cup \rangle$

7. Bestimme Homomorphismen g_i mit:

   (a) $g_1 : \mathbf{2}^3 \to \mathbf{2}^4$

   (b) $g_2 : \mathbf{2}^4 \to \mathbf{2}^2$

   (c) $g_5 : \mathbf{2}^2 \to \mathbf{2}^2$

   Bestimme auch jeweils $g_i^{-1}(1)$.

8. Bestimme:

   (a) $d_H(010, 110)$

   (b) $d_H(101, 010)$

   (c) $d_H(011, 001)$

   (d) $d_H(100, 100)$

9. Zeige für $\mathbf{2}$, $\mathbf{2}^2$, $\mathbf{2}^3$ und $\mathbf{2}^4$, dass jedes $\vec{x}$ die Dimension $d_H(\vec{0}, \vec{x})$ hat.

3.9 Hilfe: Dimensionen und Hamming-Abstände

Es sei 2^n die Menge aller Folgen der Länge n von Elementen aus $\{0, 1\}$.

- Beispiel: $2^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$.

Für $\vec{x}, \vec{y} \in 2^n$ ist der **Hamming-Abstand** von $\vec{x}$ und $\vec{y}$, $d_H(\vec{x}, \vec{y})$, die Anzahl aller $i \leq n$ mit $x_i \neq y_i$.

- Beispiel: $d_H(011, 110) = 2$, da sich die Folgen an zwei Positionen unterscheiden.

Der Hamming-Abstand einer Folge $\vec{x}$ zu einer gleich langen 0-Folge $\vec{0}$, $d_H(\vec{0}, \vec{x})$, ist damit die Anzahl der Vorkommen von 1 in $\vec{x}$.

- Beispiel: $d_H(000, 110) = 2$, da 110 zwei Vorkommen von 1 enthält.

Die **Dimension** einer Folge $\vec{x}$ von Elementen aus $\{0, 1\}$ in einer booleschen Algebra, $dim(\vec{x})$, ist die Länge m einer beliebigen Kette $\vec{f_0} = \vec{0} < \vec{f_1} < \cdots < \vec{f_m} = \vec{x}$, wobei $\vec{f_i}$ jeweils unterer Nachbar von $\vec{f_{i+1}}$ ist (für alle $i < m$).

- Beispiel: $dim(110) = 2$, da $\vec{f_0} = 000 < 100 < 110 = \vec{f_2}$.

Für $\vec{x}, \vec{y} \in 2^n$ ist $\vec{x} < \vec{y}$ genau dann, wenn $x_i < y_i$ für mindestens ein $i \leq n$ und $x_i = y_i$ für alle anderen $i \leq n$.

- Beispiel: 010 < 111, da die zweite Folge an zwei Positionen größere Einträge hat und der Eintrag an einer Position gleich bleibt.

$\vec{x}$ ist **unterer Nachbar** von $\vec{y}$ genau dann, wenn es kein $\vec{z}$ gibt, sodass $\vec{x} < \vec{z} < \vec{y}$. Das ist genau dann der Fall, wenn $x_i < y_i$ für *genau* ein $i \leq n$ und $x_i = y_i$ für alle anderen $i \leq n$. Damit ist $\vec{x}$ genau dann unterer Nachbar von $\vec{y}$, wenn $\vec{y}$ genau ein Vorkommen von 1 mehr enthält als $\vec{x}$ und alle anderen Positionen gleich bleiben.

- Beispiel: 010 ist unterer Nachbar von 011, da 011 genau ein Vorkommen von 1 mehr enthält als 010 und alle anderen Positionen gleich bleiben.

Damit kommt bei allen $\vec{f_i} > \vec{0}$ der Kette der Länge m mit $\vec{f_0} = \vec{0} < \vec{f_1} < \cdots < \vec{f_m} = \vec{x}$, wobei $\vec{f_i}$ jeweils unterer Nachbar von $\vec{f_{i+1}}$ ist (für alle $i < m$), ein Vorkommen von 1 hinzu, während alle anderen Positionen gleich bleiben.

- Beispiel: In der Kette 000 < 100 < 110 kommt bei jedem $\vec{f_i} > 000$ ein Vorkommen von 1 hinzu, während alle anderen Positionen gleich bleiben.

Damit ist die Dimension einer Folge $\vec{x}$ von Elementen aus $\{0, 1\}$ in einer booleschen Algebra, $dim(\vec{x})$, die Anzahl der Vorkommen von 1 in $\vec{x}$. Damit gilt: $dim(\vec{x}) = d_H(\vec{0}, \vec{x})$.

3.10 Hilfe: Fragen und Antworten

Frage: Sind irreduzible Elemente immer die, die nur einen unteren Nachbarn haben?

Antwort: Ja.

Frage: Und kann man einen distributiven Verband beschreiben, ohne diese ganzen x, y, z Formeln auswendig zu lernen?

Antwort: Ja, z.B. so: Ein Verband $\langle V, \sqcap, \sqcup \rangle$ ist genau dann **distributiv**, wenn sich alle $x \in V$ eindeutig als nach unten abgeschlossene Mengen irreduzibler Elemente aus V (die Menge all dieser Mengen sei U) darstellen lassen, sodass $\langle U, \cap, \cup \rangle$ zum Ausgangsverband isomorph ist.

Frage: Was besagt das Dualitätsprinzip?

Antwort: Im Wesentlichen nur, dass man partielle Ordnungen, Verbandsordnungen und Verbände allesamt "umdrehen" oder von oben nach unten "spiegeln" kann und das Resultat wieder eine partielle Ordnung, eine Verbandsordnung bzw. ein Verband ist. Das, was vorher *kleiner-oder-gleich* war, ist in der dualen Ordnung *größer-oder-gleich* (und umgekehrt). Und das, was vorher das *Infimum* einer Menge war, ist im dualen Verband das *Supremum* derselben Menge (und umgekehrt).

4 Kombinatorik und Wahrscheinlichkeitsrechnung

4.1 Übungen: Binomialkoeffizienten

1. Bestimme
   (a) $\#\{a, b, c\}$; $\#\varnothing$
   (b) $\#(\{2,4,5\} \cup \{1,2,3,4\})$; $\#(\{\heartsuit, \diamondsuit\} \cup \{\spadesuit, \clubsuit\})$
   (c) $\#(\{a,b\} \times \{a,b,c\} \times \{d,e\})$; $\#(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \times \varnothing)$
   (d) $\#\{1,2,3\}^{\{1,2\}}$; $\#\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}^{(\{\triangledown, \vartriangle\}^{\{\circ, \star, \bullet\}})}$
2. Gib $\#\{1,2,3\}^{\{1,2\}}$ explizit an.
3. Bestimme
   (a) $\binom{\{1,2,3\}}{2}$; $\binom{\{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}}{2}$
   (b) $\binom{\{a,b\}}{3}$
   (c) $\binom{\{A,B\}}{0}$; $\binom{\{\circ, \bullet, \diamond, \star, \triangledown\}}{5}$
4. Sei $\mathfrak{B} = \langle\{\triangledown, \vartriangle, \diamond, \times, \star, \bullet, \circ, \bigcirc\}, \triangledown, \vartriangle, -, \cap, \cup\rangle$ eine boolesche Algebra.
   (a) Zeichne ein Hasse-Diagramm, sodass $-$, $\cap$ und $\cup$ vollständig bestimmt sind.
   (b) Bestimme die Atome von $\mathfrak{B}$.

(c) Bestimme die Potenzmengenalgebra $\mathfrak{B}'$ über der Menge der Atome von $\mathfrak{B}$.

(d) Bestimme die Elemente der Dimension 2 in $\mathfrak{B}'$.

(e) Warum gilt, dass die Anzahl der Elemente der Dimension k in $\mathfrak{B}$ gleich $\begin{pmatrix} n \\ k \end{pmatrix}$ ist (wobei n die Anzahl der Atome von $\mathfrak{B}$ ist)?

5. Betrachte den Term $(x + y)^3$.

(a) Zerlege den Term in eine Summe aus Elementarsummanden.

(b) Schreibe alle Elementarsummanden um in Terme der Form $x^k y^{3-k}$, wobei $k \leq 3$ die Anzahl der x-Vorkommen im jeweiligen Elementarsummanden ist.

(c) Fasse die neuen Terme zu einer Summe von Termen der Form $a(3, k)x^k y^{3-k}$ $(0 \leq k \leq 3)$ zusammen.

(d) Wie lauten die Koeffizienten $a(3, k)$?

(e) Warum gilt, dass die $a(n, k)$ gleich $\begin{pmatrix} n \\ k \end{pmatrix}$ sind?

6. Sei die Menge der $\langle i, j\rangle$ mit $0 \leq i \leq 3$ und $0 \leq j \leq 4$ ein Punkte-Gitter.

(a) Zeichne das Gitter.

(b) Gib drei verschieden lange Wege von $\langle 1, 1\rangle$ nach $\langle 2, 4\rangle$ an.

(c) Gib das kleinste k an, sodass ein Weg der Länge k von $\langle 1, 1\rangle$ nach $\langle 2, 4\rangle$ existiert?

(d) Wie viele verschiedene Wege der kürzesten Länge gibt es von $\langle 1, 1\rangle$ nach $\langle 2, 4\rangle$?

(e) Welcher Punkt $P_{m+n} = \langle m, n\rangle$ ist mit genau so vielen Wegen der Länge k von $P_0 = \langle 0, 0\rangle$ zu erreichen wie $\langle 2, 4\rangle$ von $\langle 1, 1\rangle$?

(f) Gib alle Wege $W = \langle P_0, \ldots, P_{m+n}\rangle$ der Länge k explizit an.

(g) Ordne jedem Weg W eine Folge $O(W) = \langle \mu_i : 1 \leq i \leq m + n\rangle$ zu, wobei $\mu_i = o$, falls $P_i = \langle p_{i-1} + 1, q_{i-1}\rangle$ und $\mu_i = r$, falls $P_i = \langle p_{i-1}, q_{i-1} + 1\rangle$.

(h) Warum gilt, dass die Anzahl der kürzesten Wege zwischen zwei Punkten $\begin{pmatrix} m + n \\ n \end{pmatrix}$ ist?

7. Betrachte die Menge $M := \{p, q, r, s, t, u\}$.

(a) Gib drei verschiedene Partitionen Π von M an und verifiziere jeweils, dass die Summe der Mächtigkeiten der Partitionsmengen von Π gleich $\#M$ ist.

(b) Gib zwei verschiedene Partitionen Π von M an, sodass die Partitionsmengen von Π alle dieselbe Mächtigkeit p haben, und verifiziere jeweils, dass $\#M = p \cdot \#\Pi$.

8. Sei $N := \{a, b, c, d\}$.

   (a) Bestimme die Menge M, bestehend aus den Folgen F der Länge 2 von verschiedenen Elementen aus N. Wie groß ist $\#M$?

   (b) Verifiziere, dass $(\#N)^{\underline{2}} = \#N \cdot (\#N - 1) = \#M$

   (c) Bestimme zu jeder Folge F die Menge $\mu(F)$ der in der Folge enthaltenen Elemente. Wie groß ist $\#\mu(F)$?

   (d) Bestimme für eine 3-elementige Teilmenge X von N die Menge $\Phi(X) := \{G : \mu(G) = X\}$.

   (e) Bestimme $\{\Phi(X) : X \subseteq N, \#X = 3\}$ und verifiziere, dass es sich dabei um eine Partition der Menge aller Folgen der Länge 3 von Elementen aus N handelt.

   (f) Wie viele Elemente hat jedes $\Phi(X)$?

   (g) Verifiziere, dass die Menge der 3-elementigen Teilmengen der Menge N gleich $\frac{(\#N)^{\underline{3}}}{3!} = \frac{(\#N)!}{3!(\#N-3)!}$ ist.

9. 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?

10. Die Bewohner eines Hauses besitzen zusammen x Fahrräder, und es gibt genau y Fahrradständer vor dem Haus. Auf wie viele Weisen können die Fahrräder an die Fahrradständer gekettet werden? (Wir nehmen an, dass die größtmögliche Anzahl Fahrräder an die Fahrradständer gekettet wird. Ist $y \geq x$, so werden alle Fahrräder angekettet. Falls aber $y < x$, so müssen einige Fahrräder woanders angekettet werden.)

4.2 Übungen: Verteilungen

1. Eine Tüte Gummibären enthalte stets genau 9 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? Gib zunächst eine Benennung der Zahl in Form einer Formel an (welcher Typ von Zählkoeffizient) und berechne seinen Wert.

2. Wie in der vorigen Aufgabe. Nun seien aber die Farben konkret gegeben: rot, gelb und grün. Bestimmen also die Farbmischungsverhältnisse rot:gelb:grün mit und ohne die Bedingung, dass eine Farbe mindestens einmal vertreten sein muss.

4.3 Hilfe: Von Bällen und Fächern

Im Wesentlichen lassen sich Verteilungsprobleme immer als Varianten der Frage: "Wir wollen m Bälle auf n Fächer verteilen. Wie viele Möglichkeiten gibt es?" verstehen. Egal, was wir verteilen wollen (ob Gummibären, Autos, Eiskugeln), und egal, worauf wir diese Dinge verteilen wollen (auf Farben, Parkplätze, Eiswaffeln) – immer müssen wir herausfinden, was den Bällen entspricht und was den Fächern, bevor wir uns überhaupt daran machen können, auszurechnen, wie viele Verteilungen es denn nun gibt. Wir kümmern uns also zuerst um:

Schritt 1: Überlege dir, was in der gegebenen Aufgabe den Bällen und was den Fächern entspricht.

Wenn das erledigt ist, kann man sich überlegen, ob die Bälle (oder das, was den Bällen entspricht; im Folgenden soll einfach von "Bällen" die Rede sein) voneinander unterschieden werden oder nicht. Haben die Bälle z.B. Namen? Oder sind sie nummeriert? Wenn für jeden Ball irgendeine Eigenschaft explizit angegeben ist, die nur dieser und kein anderer Ball hat, dann werden die Bälle voneinander unterschieden. Einen bestimmten Namen zu haben, ist z.B. eine solche Eigenschaft. Genau dasselbe kann man sich in Bezug auf die Fächer (oder das, was den Fächern entspricht; im Folgenden soll einfach von "Fächern" die Rede sein) fragen. Werden sie voneinander unterschieden oder nicht? Ist für jedes Fach explizit eine Eigenschaft angegeben, die nur dieses Fach hat? Wir kümmern uns also um:

Schritt 2: Finde heraus, ob die Bälle (explizit) voneinander unterschieden werden. Finde heraus, ob die Fächer (explizit) voneinander unterschieden werden.

Bälle können unterschieden werden oder nicht. Ebenso können Fächer unterschieden werden oder nicht. Insgesamt gibt es damit vier verschiedene Kombinationen. Für jede dieser vier Kombinationen gibt es eine passende Rechenregel, um die Anzahl der möglichen Verteilungen zu berechnen. Im Folgenden sei die Anzahl der Bälle jeweils b und die Anzahl der Fächer jeweils f.

(1) Sowohl Bälle als auch Fächer werden unterschieden.

Verteilungen: f^b

(2) Bälle werden nicht unterschieden, Fächer aber schon.

Verteilungen: $\binom{f+b-1}{b}$

(3) Bälle werden unterschieden, Fächer aber nicht.

Verteilungen: $\sum_{i\leq f} S_{b,i} = S_{b,0} + S_{b,1} + \cdots + S_{b,f}$ ("$S_{n,r}$" bezeichnet die Anzahl der Partitionen einer n-elementigen Menge in r nichtleere Teilmengen).

(4) Weder Bälle noch Fächer werden unterschieden.

Verteilungen: $\sum_{i\leq f} P_{b,i} = P_{b,0} + P_{b,1} + \cdots + P_{b,f}$ ("$P_{n,r}$" bezeichnet die Anzahl der Möglichkeiten, die Zahl n in r von Null verschiedene Summanden zu zerlegen).

Für die einzelnen $S_{n,r}$ und $P_{n,r}$ der Möglichkeiten (3) und (4) gibt es keine einfachen Rechenregeln. Am besten, man schreibt alle Kombinationen auf. Zuletzt kümmern wir uns also um:

Schritt 3: Wenn du erkannt hast, welche der vier Kombinationsmöglichkeiten (die sich aus der (Nicht-)Unterscheidung von Bällen und Fächern ergeben) vorliegt, wende die passende Rechenregel an.

4.4 Übungen: Bedingte Wahrscheinlichkeiten

1. Hans wirft mit einer gezinkten Münze. Die Wahrscheinlichkeit, dass die Münze *Kopf* zeigt, beträgt nur 0,3. Hans wirft die Münze fünf Mal.

   (a) Wie hoch ist die Wahrscheinlichkeit, dass Hans fünf Mal hintereinander *Kopf* wirft?

   (b) Wie hoch ist die Wahrscheinlichkeit, dass Hans drei Mal *Zahl* wirft?

   (c) Wie hoch ist die Wahrscheinlichkeit, dass Hans mindestens drei Mal *Zahl* wirft?

   (d) Wie hoch ist die Wahrscheinlichkeit, dass Hans die Folge *Zahl, Kopf, Zahl, Kopf, Zahl* wirft?

   (e) Wie hoch ist die Wahrscheinlichkeit, dass Hans Kopf wirft, gegeben, dass er bereits vier Mal *Kopf* geworfen hat?

2. Gegeben sind zwei Urnen A und B mit folgenden Inhalten:

   - Urne A: 14 Kunststoffkugeln, 6 Holzkugeln
   - Urne B: 4 Kunststoffkugeln, 16 Holzkugeln.

Nehmen wir an, wir wählen eine der Urnen durch einen Münzwurf aus und ziehen zwei Mal aus dieser Urne. Wie hoch ist dann die Wahrscheinlichkeit, ...

(a) ... 2 Kunststoffkugeln zu ziehen, mit Zurücklegen?

(b) ... 1 Holz- und 1 Kunststoffkugel zu ziehen, ohne Zurücklegen?

(c) ... 2 Kugeln aus gleichem Material zu ziehen, mit Zurücklegen?

(d) ... 2 Kugeln aus gleichem Material zu ziehen, ohne zurücklegen?

3. Wir verfahren genauso wie in der vorigen Aufgabe, nur dass wir jetzt nicht mehr wissen, welches Urne A und welches Urne B ist. Wie hoch ist die Wahrscheinlichkeit, ...

   (a) ... aus Urne A gezogen zu haben, gegeben, dass wir eine Kunststoffkugel gezogen haben?

   (b) ... aus Urne B gezogen zu haben, gegeben, dass wir eine Holzkugel gezogen haben?

   (c) ... aus Urne A gezogen zu haben, gegeben, dass wir 2 Kunststoffkugeln nacheinander gezogen haben (mit Zurücklegen)?

   (d) ... aus Urne A gezogen zu haben, gegeben, dass wir 2 Holzkugeln nacheinander gezogen haben (mit Zurücklegen)?

4. Otto besitzt ein 2-Eurostück, das so gezinkt ist, dass es bei 7 von 10 Würfen *Kopf* zeigt, und ein ungezinktes 2-Eurostück. Leider kann er sie nicht mehr auseinander halten. Er wirft eines der beiden 2-Eurostücke zwei Mal und erhält beide Male *Kopf*. Wie hoch ist die Wahrscheinlichkeit, dass es sich um das gezinkte 2-Eurostück handelt?

5. Eine kleine Firma arbeitet mit den Betriebssystemen Windows, Linux und Mac OS. Windows stürzt an durchschnittlich drei von zehn Arbeitstagen ab, Linux an durchschnittlich zwei von zehn und Mac OS an durchschnittlich einem von zehn. Von zehn Mitarbeiter/innen benutzen sechs Mac OS, drei Linux und eine/r Windows. Sophia wurde irgendein Rechner zugeteilt. Er stürzte gleich an ihren ersten beiden Arbeitstagen ab. Wie hoch ist die Wahrscheinlichkeit, dass Sophia ein Windows-Rechner zugeteilt wurde?

6. Im Frankfurter Zoo gibt es einen Kragenbären und drei Malaienbären. Eines Morgens ist der Honigbaum im Bärengehege umgeworfen. Bärenpfleger Udo behauptet, gesehen zu haben, dass es der Kragenbär war. Allerdings ist Udo machmal etwas verwirrt und seine Aussage kann nur zu 90 Prozent als gesichert angesehen werden, falls

es tatsächlich der Kragenbär war. Er verwechselt Malaienbären außerdem so häufig mit Kragenbären, dass er auch mit 80-prozentiger Wahrscheinlichkeit behaupten würde, einen Kragenbären gesehen zu haben, falls der Honigbaum tatsächlich von einem Malaienbären umgestoßen wurde. Wie hoch ist nun die Wahrscheinlichkeit, dass der Kragenbär den Honigbaum umgestoßen hat?

7. In einem See gibt es zwei Arten Fische, nennen wir sie A und B. Hypothese H_0 besagt, dass es genauso viele Fische gibt von der Art A wie von der Art B. Hypothese H_1 besagt, dass es doppelt so viele Fische der Art A gibt wie von der Art B. Ein Forscher fängt 10 Fische, wovon 7 von der Art A sind. Sollen wir nach diesem Fang eher H_0 oder H_1 bevorzugen? (Beginne mit einer Vermutung, ohne dass du die Berechnung ausgeführt hast und mach dich dann an die Rechnung.) Hinweis: Berechne zunächst aus den Hypothesen die Wahrscheinlichkeiten dafür, dass ein beliebiger Fisch von der Art A bzw. B ist. Der See soll großsein, sodass sich diese Wahrscheinlichkeiten nicht wesentlich ändern, wenn man 10 Fische fängt. Daraus bekommen wir Wahrscheinlichkeiten für den Fang unter der Hypothese H_0 bzw. H_1. Gehe Sie jetzt davon aus, dass a priori beide Hypothesen dieselbe Wahrscheinlichkeit haben und bestimme die a posteriori Wahrscheinlichkeiten.

4.5 Lösung: Aufgabe 7

Wir haben folgende Ereignisse/Hypothesen:

- "A" repräsentiert das Ereignis, dass ein Fisch von Art A gefangen wurde.
- "B" repräsentiert das Ereignis, dass ein Fisch von Art B gefangen wurde.
- "H_0" repräsentiert die Hypothese, dass es genauso viele Fische von der Art A gibt wie von der Art B.
- "H_1" repräsentiert die Hypothese, dass es doppelt so viele Fische von der Art A gibt wie von der Art B.

Es ergeben sich folgende Wahrscheinlichkeiten:

- $P(A|H_0) = \frac{1}{2}$
- $P(B|H_0) = \frac{1}{2}$
- $P(A|H_1) = \frac{2}{3}$
- $P(B|H_2) = \frac{1}{3}$

- $P(H_0) = \frac{1}{2}$
- $P(H_1) = \frac{1}{2}$

Gesucht ist:

- $P(H_0|A_7)$, wobei "A_7" das Ereignis repräsentiert, dass 7 von 10 gefangenen Fischen von der Art A sind.

Die Formel, die wir benötigen, um dies zu berechnen, ist diese:

- **Umgekehrung:** Sei $P(A), P(B) > 0$. Dann gilt: $P(B|A) = \frac{P(A|B) \cdot P(B)}{P(A)}$

Wir bekommen:

- $P(H_0|A_7) = \frac{P(A_7|H_0) \cdot P(H_0)}{P(A_7)}$

Um die obige Formel anwenden zu können, müssen wir zuerst folgende Wahrscheinlichkeiten berechnen:

- $P(A_7|H_0)$
- $P(A_7)$

Die erste Wahrscheinlichkeit berechnet sich folgendermaßen: Es gibt

- $\binom{10}{7} = \frac{10!}{7! \cdot (10-7)!} = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2} = 120$

verschiedene Möglichkeiten, 7 Fische der Art A von insgesamt 10 Fischen zu fangen. Jede dieser Möglichkeiten hat eine Wahrscheinlichkeit von

- $(\frac{1}{2})^7 \cdot (\frac{1}{2})^3 = \frac{1}{1.024}$

Damit gilt:

- $P(A_7|H_0) = 120 \cdot \frac{1}{1.024} = \frac{15}{128}$

Die zweite noch fehlende Wahrscheinlichkeit können wir mithilfe der folgenden Formel berechnen:

- **Totale Wahrscheinlichkeit:** $P(A) = P(B) \cdot P(A|B) \ + P(-B) \cdot P(A|-B)$

Wir bekommen:

- $P(A_7) = P(H_0) \cdot P(A_7|H_0) \ + P(H_1) \cdot P(A_7|H_1)$

Zu berechnen ist somit vorerst:

- $P(A_7|H_1) = 120 \cdot (\frac{2}{3})^7 \cdot (\frac{1}{3})^3 = 120 \cdot \frac{2^7}{3^{10}} = \frac{15.360}{59.049}$

Damit gilt:

- $P(A_7) = \frac{1}{2} \cdot \frac{15}{128} + \frac{1}{2} \cdot \frac{15.360}{59.049} = \frac{15}{256} + \frac{15.360}{118.098} = \frac{950.605}{5.038.848}$

Wir bekommen schließlich:

- $P(H_0|A_7) = \frac{\frac{15.360}{59.049} \cdot \frac{1}{2}}{\frac{950.605}{5.038.848}} = \frac{131.072}{19.0121} \approx 0,689$

Dementsprechend erhalten wir:

- $P(H_1|A_7) = 1 - P(H_0|A_7) = 1 - \frac{131.072}{190.121} = \frac{59.049}{190.121} \approx 0,311$

Damit ist die Hypothese H_0 zu bevorzugen.

4.6 Hilfe: Wichtige Formeln der Wahrscheinlichkeitsrechnung

4.6.1 Gesamt- und Ereigniswahrscheinlichkeit

Sei Ω ein Ergebnisraum und p eine Funktion mit $p : \Omega \to [0,1]$ (p ist also eine Funktion, die jedem Ergebnis $\omega \in \Omega$ einen Wert zwischen 0 und 1 zuordnet). Dann gilt:

Gesamtwahrscheinlichkeit: $\sum_{\omega \in \Omega} p(\omega) = 1$

Die Summe aller Ergebnisse im Ergebnisraum beträgt damit 1.

Ein *Ereignis* ist eine Teilmenge des Ergebnisraumes. Die Wahrscheinlichkeit eines solchen Ereignisses ist die Summe aller Ergebnisse, die Elemente des Ereignisses sind:

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

4.6.2 Leeres und sicheres Ereignis

Zwei Ereignisse sind besonders: Da die leere Menge eine Teilmenge eines Ergebnisraumes bildet, ist die leere Menge ein Ereignis, das *leere Ereignis*. Genauso bildet der Ergebnisraum selbst eine Teilmenge des Ergebnisraumes. Dieses ist das *sichere Ereignis*. Die Wahrscheinlichkeiten dieser Ereignisse sind die folgenden:

Leeres Ereignis: $P(\emptyset) = 0$

Sicheres Ereignis: $P(\Omega) = 1$

4.6.3 Addition

Wir können die Wahrscheinlichkeiten von Ereignissen auch addieren:

Ereigniswahrscheinlichkeiten addieren: $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

Sind die Ereignisse disjunkt (d.h., sind keine Ergebnisse in beiden Ereignissen enthalten), so können wir auch einfach folgendermaßen rechnen:

Disjunkte Ereigniswahrscheinlichkeiten addieren: $P(A \cup B) = P(A) + P(B)$

Beide Rechnungen lassen sich auch für mehr als zwei Ereignisse verallgemeinern: Wir addieren entweder die Wahrscheinlichkeiten aller Ereignisse, falls die Ereignisse paarweise disjunkt sind, oder wir addieren die Wahrscheinlichkeiten aller Ereignisse und ziehen jeweils die Wahrscheinlichkeiten der Schnitte aller nicht-disjunkten Ereignispaare wieder ab.

4.6.4 Bedingte und totale Wahrscheinlichkeiten, Multiplikation

Eine weitere wichtige Rechenregel ist die Regel für sogenannte *bedingte Wahrscheinlichkeiten*. Als "bedingte Wahrscheinlichkeit $P(A|B)$" bezeichnet man die Wahrscheinlichkeit eines Ereignisses A *unter der Bedingung*, dass ein Ereignis B eingetreten ist.

Bedingte Wahrscheinlichkeit: Sei $P(B) > 0$. Dann gilt: $P(A|B) = \frac{P(A \cap B)}{P(B)}$

Aus dieser Regel ergibt sich ganz einfach eine weitere:

Ereigniswahrscheinlichkeiten multiplizieren: $P(A \cap B) = P(A|B) \cdot P(B)$

Wenn zwei Ereignisse A und B völlig unabhängig voneinander sind (d.h., wenn $P(A|B) = P(A)$ und $P(B|A) = P(B)$), dann können wir die Wahrscheinlichkeiten der Ereignisse auch einfach so mulitplizieren:

Unabhängige Ereigniswahrscheinlichkeiten multiplizieren: $P(A \cap B) = P(A) \cdot P(B)$

Manchmal wollen wir die totale Wahrscheinlichkeit eines Ereignisses berechnen, welches auf verschiedenen Ereignispfaden erreicht werden kann. Das bedeutet, dass ein Ereignis A auftreten kann, nachdem ein Ereignis B aufgetreten ist *oder* nachdem ein von B disjunktes Ereignis $-B$ aufgetreten ist. Wir müssen dann einfach die Wahrscheinlichkeiten beider Pfade, die zum Ereignis führen, von dem wir die totale Wahrscheinlichkeit ausrechnen wollen, addieren:

Totale Wahrscheinlichkeit: $P(A) = P(B) \cdot P(A|B) + P(-B) \cdot P(A|-B)$

Auch diese Rechnung lässt sich für mehr als zwei disjunkte Ereignisse, die zum Ereignis A führen können, verallgemeinern: Wenn es mehr als zwei disjunkte Ereignisse gibt, die zum Ereignis A führen können, müssen wir lediglich die Wahrscheinlichkeiten *aller* möglichen Ereignispfade addieren.

Eine weitere wichtige Rechenregel ist die Regel der Umkehrung. Manchmal haben wir eine bestimmte bedingte Wahrscheinlichkeit gegeben, wollen aber gerade die *umgekehrte* bedingte Wahrscheinlichkeit haben. Diese können wir folgendermaßen berechnen:

Umgekehrung: Sei $P(A), P(B) > 0$. Dann gilt: $P(B|A) = \frac{P(A|B) \cdot P(B)}{P(A)}$

4.7 Hilfe: Lottozahlen

Angenommen, wir spielen Lotto mit einer Ziehung von 6 aus 49 Zahlen. Wie hoch ist die Wahrscheinlichkeit, auf 6 richtige Zahlen zu tippen, wenn wir auf 6 Zahlen tippen? Dazu müssen wir erst einmal wissen, wie viele Ziehungen es überhaupt gibt. Das sind:

- $\binom{49}{6} = \frac{49!}{43! \cdot 6!} = 13.983.816$

Nun tippen wir auf 6 Zahlen. Wir wollen wissen, wie viele Möglichkeiten es gibt, dass diese 6 getippten Zahlen auch allen 6 der 6 gezogenen Zahlen entsprechen. Von den anderen 43 Zahlen, die auf die wir nicht getippt haben, interessiert uns also keine einzige. Offenbar gibt es nur eine Möglichkeit, und diese lässt sich so berechnen. (Hierbei steht "`TIPP`" für die Anzahl der getippten Zahlen, "`YEAH`" für die Anzahl der gezogenen Zahlen, die den getippten Zahlen entsprechen, "`NICHT-TIPP`" für die Anzahl der nicht getippten Zahlen und "`BUUH`" für die Anzahl der gezogenen Zahlen, die nicht den getippten Zahlen entsprechen.)

- $\binom{\texttt{TIPP}}{\texttt{YEAH}} \cdot \binom{\texttt{NICHT-TIPP}}{\texttt{BUUH}} = \binom{6}{6} \cdot \binom{43}{0} = 1 \cdot 1 = 1$

Die Wahrscheinlichkeit, bei einem Tipp auf 6 Zahlen auch auf 6 zu tippen, beträgt damit $\frac{1}{13.983.816}$.

Als Nächstes können wir uns fragen, wie hoch die Wahrscheinlichkeit ist, bei einem Tipp auf 6 Zahlen nicht auf 6 richtige, sondern nur auf 5 richtige zu tippen. Insgesamt gibt es natürlich immer noch 13.983.816 Ziehungen. Nun wollen wir aber wissen, wie viele Möglichkeiten es gibt, dass von den 6 getippten Zahlen nur 5 Zahlen jeweils einer Zahl der 6 gezogenen Zahlen entsprechen. Diesmal interessiert uns also auch die Menge der Zahlen, auf die wir nicht getippt haben. Davon soll nämlich genau eine gezogen werden. Damit haben wir:

- $\binom{\texttt{TIPP}}{\texttt{YEAH}} \cdot \binom{\texttt{NICHT-TIPP}}{\texttt{BUUH}} = \binom{6}{5} \cdot \binom{43}{1} = 6 \cdot 43 = 258$

Die Wahrscheinlichkeit, bei einem Tipp auf 6 Zahlen auf genau 5 richtige zu tippen, beträgt damit $\frac{258}{13.983.816}$. Die Wahrscheinlichkeit, bei einem Tipp auf 6 Zahlen auf mindestens 5 richtige zu tippen, beträgt damit $\frac{1}{13.983.816} + \frac{258}{13.983.816} = \frac{259}{13.983.816}$.

Und so geht es weiter. Wie hoch ist die Wahrscheinlichkeit, bei einem Tipp auf 6 Zahlen auf genau 4 richtige zu tippen? Dazu müssen wir berechnen, wie viele Möglichkeiten es gibt, dass von den 6 getippten Zahlen nur genau 4 Zahlen jeweils einer 6 gezogenen Zahlen entsprechen. Von den Zahlen, auf die wir nicht getippt haben, sollen also diesmal genau 2 gezogen werden. Damit haben wir:

- $\binom{\texttt{TIPP}}{\texttt{YEAH}} \cdot \binom{\texttt{NICHT-TIPP}}{\texttt{BUUH}} = \binom{6}{4} \cdot \binom{43}{2} = 15 \cdot 903 = 13.545$

Die Wahrscheinlichkeit, bei einem Tipp auf 6 Zahlen auf genau 4 richtige zu tippen, beträgt damit $\frac{13.545}{13.983.816}$. Die Wahrscheinlichkeit, bei einem Tipp auf 6 Zahlen auf mindestens 4 richtige zu tippen, beträgt damit $\frac{1}{13.983.816} + \frac{258}{13.983.816} + \frac{13.545}{13.983.816} = \frac{13.804}{13.983.816}$.

Aufgabe: Wie hoch ist die Wahrscheinlichkeit, bei einem Tipp auf 6 Zahlen

(a) auf genau 3 richtige zu tippen?

(b) auf genau 2 richtige zu tippen?

(c) auf mindestens 3 richtige zu tippen?

(d) auf mindestens 2 richtige zu tippen?

Die obigen Rechnungen können wir uns auch anhand eines einfacheren Beispiels klar machen. Angenommen, wir haben nur 5 Zahlen: ①, ②, ③, ④, ⑤. Von diesen Zahlen tippen wir auf 3. Wir haben folgende 10 (= $\binom{5}{3}$) mögliche Ziehungen:

1.	①	②	③		
2.	①	②		④	
3.	①	②			⑤
4.	①		③	④	
5.	①		③		⑤
6.	①			④	⑤
7.		②	③	④	
8.		②	③		⑤
9.		②		④	⑤
10.			③	④	⑤

Nun wollen wir wissen, wie hoch die Wahrscheinlichkeit ist, bei einem Tipp auf 3 Zahlen auf genau 3 richtige zu tippen. Dazu müssen wir berechnen, wie viele Möglichkeiten es gibt, dass diese 3 getippten Zahlen auch allen 3 gezogenen Zahlen entsprechen. Von den anderen 2 Zahlen, auf die wir nicht getippt haben, interessiert uns also keine einzige. Angenommen, wir tippen auf folgende Zahlen: ②, ③ und ⑤. Offenbar gibt es nur eine mögliche Ziehung, sodass diese 3 Zahlen auch den 3 gezogenen Zahlen entsprechen, nämlich Ziehung 8. Also beträgt die Wahrscheinlichkeit dafür, bei einem Tipp auf diese 3 (oder irgendwelchen anderen 3) Zahlen mit allen 3 Zahlen richtig zu liegen, $\frac{1}{10}$.

Als Nächstes können wir uns fragen, wie hoch die Wahrscheinlichkeit ist, bei einem Tipp auf 3 Zahlen auf genau 2 richtige zu tippen. Angenommen, wir tippen wieder auf die Zahlen ②, ③ und ⑤. Dann erfüllen folgende mögliche Ziehungen (etwas anders sortiert) unsere Bedingung, mit genau 2 Zahlen richtig zu liegen:

1.	①	②	③		
7.		②	③	④	
3.	①	②			⑤
9.		②		④	⑤
5.	①		③		⑤
10.			③	④	⑤

Wir sehen, dass es von den übrigen, nicht getippten Zahlen, entweder die ① oder die ④ gezogen werden kann. Das entspricht genau den 1-elementigen Teilmengen der Menge der nicht getippten Zahlen. Die Anzahl der 2-elementigen Teilmengen der Menge der getippten Zahlen ($\binom{3}{2} = 3$) müssen wir also noch mit der Anzahl der 1-elementigen Teilmengen der Menge der nicht getippten Zahlen ($\binom{2}{1} = 2$) mutliplizieren, weil es immer zwei Möglichkeiten gibt, die gewünschten Zahlen "aufzufüllen". Wir haben also:

- $\binom{\texttt{TIPP}}{\texttt{YEAH}} \cdot \binom{\texttt{NICHT-TIPP}}{\texttt{BUUH}} = \binom{3}{2} \cdot \binom{2}{1} = 3 \cdot 2 = 6$

Und da wir insgesamt 10 mögliche Ziehungen haben, beträgt die Wahrscheinlichkeit, bei einem Tipp auf 3 Zahlen auf genau 2 richtige zu tippen, $\frac{6}{10}$. Die Wahrscheinlichkeit, bei einem Tipp auf 3 Zahlen auf mindestens 2 richtige zu tippen, beträgt damit $\frac{1}{10} + \frac{6}{10} = \frac{7}{10}$.

Zuletzt fragen wir uns, wie hoch die Wahrscheinlichkeit ist, bei einem Tipp auf 3 Zahlen auf genau eine richtige zu tippen. Wir tippen wieder beispielhaft auf ②, ③ und ⑤. Dann erfüllen folgende Ziehungen die Bedingung:

2. ① <u>②</u> ④
4. ① <u>③</u> ④
6. ① ④ <u>⑤</u>

Wir sehen, dass von den übrigen, nicht getippten Zahlen, ① und ④ gezogen werden müssen. Das entspricht genau den 2-elementigen Teilmengen der Menge der nicht getippten Zahlen. Wenn wir die Anzahl der 1-elementigen Teilmengen der Menge der getippten Zahlen ($\binom{3}{1} = 3$) also mit der Anzahl der 2-elementigen Teilmengen der Menge der nicht getippten Zahlen ($\binom{2}{2} = 1$) mutliplizieren, ändert sich nichts, weil es nur eine Möglichkeit gibt, die gewünschten Zahlen "aufzufüllen". Wir haben also:

- $\binom{\texttt{TIPP}}{\texttt{YEAH}} \cdot \binom{\texttt{NICHT-TIPP}}{\texttt{BUUH}} = \binom{3}{1} \cdot \binom{2}{2} = 3 \cdot 1 = 3$

Die Wahrscheinlichkeit, bei einem Tipp auf 3 Zahlen auf genau eine richtige Zahl zu tippen, beträgt damit $\frac{3}{10}$. Die Wahrscheinlichkeit, bei einem Tipp auf 3 Zahlen auf mindestens eine richtige getippt zu haben, beträgt damit $\frac{1}{10} + \frac{6}{10} + \frac{3}{10} = \frac{10}{10} = 1$.

Aufgabe: Angenommen, wir haben 6 Zahlen. Wie hoch ist die Wahrscheinlichkeit,

(a) bei einem Tipp auf 4 Zahlen auf genau 4 richtige zu tippen?
(b) bei einem Tipp auf 4 Zahlen auf genau 3 richtige zu tippen?
(c) bei einem Tipp auf 4 Zahlen auf genau 2 richtige zu tippen?
(d) bei einem Tipp auf 4 Zahlen auf mindestens 2 richtige zu tippen?
(e) bei einem Tipp auf 3 Zahlen auf genau 3 richtige zu tippen?
(f) bei einem Tipp auf 3 Zahlen auf genau 2 richtige zu tippen?
(g) bei einem Tipp auf 3 Zahlen auf mindestens 2 richtige zu tippen?

4.8 Übungen: Zufallsvariablen

1. Gegeben sei ein normaler, fairer, sechsseitiger Würfel. Er wird zwei Mal gewürfelt.
   (a) Bestimme den Ergebnisraum.
   (b) Wie wahrscheinlich sind die einzelnen Ergebnisse?
   (c) Bestimme die Wahrscheinlichkeitsverteilung der Zufallsvariablen X: Anzahl der gewürfelten Sechsen.
   (d) Berechne den Erwartungswert von X.
   (e) Berechne die Varianz von X.

(f) Berechne die Standardabweichung von X.

2. Hans sucht sich aus einer Palette von Überraschungseiern nacheinander drei Stück aus. Er weiß, dass sich in jedem siebten Ei eine Figur befindet.

   (a) Bestimme die Wahrscheinlichkeitsverteilung der Zufallsvariablen X: Anzahl der Figuren aus den drei ausgesuchten Überraschungseiern.

   (b) Berechne den Erwartungswert von X.

   (c) Berechne die Varianz von X.

   (d) Berechne die Standardabweichung von X.

3. Eine Münze wird so lange geworfen, bis *Kopf* oder neun Mal *Zahl* geworfen wurde.

   (a) Bestimme den Ergebnisraum.

   (b) Wie wahrscheinlich sind die einzelnen Ergebnisse?

   (c) Man gewinnt bei n Würfen 2^n Euro. Welchen Gewinn kann man erwarten?

4. Du hast gerade ein altes Fahrrad für 70 Euro gekauft. Du kannst nun entweder ein unzerstörbares Kryptonit-Schloss für 15 Euro oder ein billiges Schloss für 6 Euro kaufen oder du benutzt das Schloss, das der Verkäufer dir geschenkt hat. Du gehst davon aus, dass niemand versuchen wird, dein Fahrrad zu stehlen, wenn es mit dem Kryptonit-Schloss gesichert ist. Die Wahrscheinlichkeit, dass das Schloss geknackt wird, beträgt beim billigen 10 Prozent und beim geschenkten 25 Prozent. Für welches Schloss solltest du dich entscheiden?

4.9 Lösungen: Zufallsvariablen

4.9.1 Aufgabe 1

Gegeben sei ein normaler, fairer, sechsseitiger Würfel. Er wird zwei Mal gewürfelt.

1. Bestimme den Ergebnisraum.

   Lösung: $\Omega = \{1, 2, 3, 4, 5, 6\}^2$

2. Wie wahrscheinlich sind die einzelnen Ergebnisse?

   Lösung: $p(\omega) = \frac{1}{36}$ für alle $\omega \in \Omega$

3. Bestimme die Wahrscheinlichkeitsverteilung der Zufallsvariablen X: Anzahl der gewürfelten Sechsen.

Lösung:

- $X(\langle i,j\rangle) = 0$ für $1 \leq i,j \leq 5$
- $X(\langle 6,j\rangle) = 1$ für $0 \leq j \leq 5$
- $X(\langle i,6\rangle) = 1$ für $0 \leq i \leq 5$
- $X(\langle 6,6\rangle) = 2$

4. Berechne den Erwartungswert von X.

   Lösung: $E(X) = 25 \cdot (\frac{1}{36} \cdot 0) + 10 \cdot (\frac{1}{36} \cdot 1) + 1 \cdot (\frac{1}{36} \cdot 2) = \frac{10}{36} + \frac{2}{36} = \frac{1}{3}$

5. Berechne die Varianz von X.

   Lösung: $V(X) = E(X^2) - (E(X))^2 = 25 \cdot (\frac{1}{36} \cdot 0^2) + 10 \cdot (\frac{1}{36} \cdot 1^2) + 1 \cdot (\frac{1}{36} \cdot 2^2) - \frac{1}{9} = \frac{10}{36} + \frac{4}{36} - \frac{1}{9} = \frac{14}{36} - \frac{1}{9} = \frac{5}{18}$

6. Berechne die Standardabweichung von X.

   Lösung: $\sigma(X) = \sqrt{V(X)} = \sqrt{\frac{5}{18}} = \frac{\sqrt{10}}{6} \approx 0,527$

4.9.2 Aufgabe 2

Hans sucht sich aus einer Palette von Überraschungseiern nacheinander drei Stück aus. Er weiß, dass sich in jedem siebten Ei eine Figur befindet.

1. Bestimme die Wahrscheinlichkeitsverteilung der Zufallsvariablen X: Anzahl der Figuren aus den drei ausgesuchten Überraschungseiern.
2. Berechne den Erwartungswert von X.
3. Berechne die Varianz von X.
4. Berechne die Standardabweichung von X.

4.9.3 Aufgabe 3

Eine Münze wird so lange geworfen, bis *Kopf* oder neun Mal *Zahl* geworfen wurde.

1. Bestimme den Ergebnisraum.

   Lösung: $\Omega = \{\langle K\rangle, \langle Z,K\rangle, \langle Z,Z,K\rangle, \langle Z,Z,Z,K\rangle, \langle Z,Z,Z,Z,K\rangle,$
   $\langle Z,Z,Z,Z,Z,K\rangle, \langle Z,Z,Z,Z,Z,Z,K\rangle, \langle Z,Z,Z,Z,Z,Z,Z,K\rangle,$
   $\langle Z,Z,Z,Z,Z,Z,Z,Z,K\rangle, \langle Z,Z,Z,Z,Z,Z,Z,Z,Z\rangle\}$

2. Wie wahrscheinlich sind die einzelnen Ergebnisse?

Lösung: $p(\omega) = (\frac{1}{2})^n$, wobei $n = |\omega|$ (die Länge des n-Tupels), also z.B.

- $p(\langle K\rangle) = (\frac{1}{2})^1 = \frac{1}{2}$
- $p(\langle Z,Z,Z,Z,K\rangle) = (\frac{1}{2})^5 = \frac{1}{32}$
- $p(\langle Z,Z,Z,Z,Z,Z,Z,Z,K\rangle) = p(\langle Z,Z,Z,Z,Z,Z,Z,Z,Z\rangle) = (\frac{1}{2})^9 = \frac{1}{512}$

3. Man gewinnt bei n Würfen 2^n Euro. Welchen Gewinn kann man erwarten?

Lösung: $E(X) = (\frac{1}{2})^1 \cdot 2^1 + (\frac{1}{2})^2 \cdot 2^2 + (\frac{1}{2})^3 \cdot 2^3 + (\frac{1}{2})^4 \cdot 2^4 + (\frac{1}{2})^5 \cdot 2^5 + (\frac{1}{2})^6 \cdot 2^6 + (\frac{1}{2})^7 \cdot 2^7 + (\frac{1}{2})^8 \cdot 2^8 + (\frac{1}{2})^9 \cdot 2^9 + (\frac{1}{2})^9 \cdot 2^9 = 1+1+1+1+1+1+1+1+1+1 = 10$

4.9.4 Aufgabe 4

Du hast gerade ein altes Fahrrad für 70 Euro gekauft. Du kannst nun entweder ein unzerstörbares Kryptonit-Schloss für 15 Euro oder ein billiges Schloss für 6 Euro kaufen oder du benutzt das Schloss, das der Verkäufer dir geschenkt hat. Du gehst davon aus, dass niemand versuchen wird, dein Fahrrad zu stehlen, wenn es mit dem Kryptonit-Schloss gesichert ist. Die Wahrscheinlichkeit, dass das Schloss geknackt wird, beträgt beim billigen 10 Prozent und beim geschenkten 25 Prozent. Für welches Schloss solltest du dich entscheiden?

Lösung: Wir haben folgende Ereignisse:

- "K" repräsentiert das Ereignis, dass du dir das Kryptonit-Schloss kaufst.
- "B" repräsentiert das Ereignis, dass du dir das billige Schloss kaufst.
- "G" repräsentiert das Ereignis, dass du das geschenkte Schloss verwendest.
- "S" repräsentiert das Ereignis, dass das Fahrrad gestohlen wird.
- "$-S$" repräsentiert das Ereignis, dass das Fahrrad nicht gestohlen wird.

Die folgenden Wahrscheinlichkeiten sind relevant:

- $P(S|K) = 0$
- $P(-S|K) = 1$
- $P(S|B) = \frac{1}{10}$
- $P(-S|B) = \frac{9}{10}$
- $P(S|G) = \frac{1}{4}$
- $P(-S|G) = \frac{3}{4}$

Nun brauchen wir noch die Werte der Zufallsvariablen X mit X: Verlust in Euro:

- Für Ereignis K:
  - $X(S) = 85$
  - $X(-S) = 15$
- Für Ereignis B:
  - $X(S) = 76$
  - $X(-S) = 6$
- Für Ereignis G:
  - $X(S) = 70$
  - $X(-S) = 0$

Nun können wir die Erwartungswerte berechnen:

- $E(K) = P(S|K) \cdot X(S) + P(-S|K) \cdot X(-S) = 0 \cdot 85 + 1 \cdot 15 = 15$
- $E(B) = P(S|B) \cdot X(S) + P(-S|B) \cdot X(-S) = \frac{1}{10} \cdot 76 + \frac{9}{10} \cdot 6 = \frac{76}{10} + \frac{54}{10} = 13$
- $E(G) = P(S|G) \cdot X(S) + P(-S|G) \cdot X(-S) = \frac{1}{4} \cdot 70 + \frac{3}{4} \cdot 0 = \frac{70}{4} = 17\frac{1}{2}$

Du solltest also das billige Schloss kaufen, da du dabei den niedrigsten Verlust erwarten kannst.

4.10 Hilfe: Fragen und Antworten

Frage: Zu der Gummibärenaufgabe: Kannst du eine kurze Erklärung geben, warum in der Aufgabe Fächer = Farben und Bälle = Bären sind?

Antwort: Verteilungsprobleme lassen sich immer als Varianten der Frage: "Wir wollen m Bälle auf n Fächer verteilen. Wie viele Möglichkeiten gibt es?" verstehen. Also entsprechen, so aufgefasst, auf jeden Fall entweder die Bären den Bällen oder den Fächern (es handelt sich schließlich um ein Verteilungsproblem). Angenommen, wir sagen, dass die Bären den Fächern entsprechen. Dann entsprechen die Farben den Bällen. Dann müssen wir die 3 Farben (Bälle) auf 9 Bären (Fächer) verteilen. Aber dann erhalten ja mindestens 6 Bären keine Farbe. So war die Aufgabe aber nicht gemeint. (Die Anzahl der Farben ist hier wörtlich zu nehmen. Es gibt sozusagen wirklich nur 3 Dinge, die nicht von mehreren Dinge "gehabt" werden können oder Ähnliches. Farben sind hier also nicht ihrem Wesen nach, also als abstrakte Eigenschaften, zu verstehen. Wenn wir das aber in etwa so verstehen wollen, müssen wir die Farben eben als Fächer verstehen, und die Bären dementsprechend als Bälle. Dann passt alles.)

Frage: Kannst du vielleicht noch einmal erklären, wie man die Varianz berechnet (z.B. bezogen auf die Aufgabe 1e) der Übungen zu Zufallsvariablen'?

Antwort: Wir haben von 36 Ergebnissen 25 Ergebnisse, für die die Anzahl der gewürfelten Sechsen 0 beträgt, 10 Ergebnisse, für die die Anzahl der gewürfelten Ergebnisse 1 beträgt und 1 Ergebnis, für die die Anzahl der gewürfelten Sechsen 2 beträgt. Jedes Ergebnis hat eine Wahrscheinlichkeit von $\frac{1}{36}$. Der Erwartungswert der Zufallsvariablen X beträgt damit: $E(X) = 25 \cdot (\frac{1}{36} \cdot 0) + 10 \cdot (\frac{1}{36} \cdot 1) + 1 \cdot (\frac{1}{36} \cdot 2) = \frac{10}{36} + \frac{2}{36} = \frac{1}{3}$.

Die Varianz berechnet sich nun folgendermaßen:

Die Formel, die wir benötigen, ist $V(X) = E(X - E(X))^2$. (Die "^{2}" bezieht sich hier nur auf "$(X - E(X))$".)

$X - E(X)$ ist eine Funktion (genauer: eine Zufallsvariable), die für jedes Ergebnis ω die Differenz $X(\omega) - E(X)$ liefert. $E(X)$ ist für alle Ergebnisse gleich, nämlich $\frac{1}{3}$, wie bereits ausgerechnet. Damit ist z.B. $(E - E(X))(\langle 1, 6 \rangle) = X(\langle 1, 6 \rangle) - \frac{1}{3} = 1 - \frac{1}{3} = \frac{2}{3}$.

Damit ist $(X - E(X))$ für die 25 Ergebnisse, für die die Anzahl der gewürfelten Sechsen 0 beträgt, gleich $-\frac{1}{3}$, für die 10 Ergebnisse, für die die Anzahl der gewürfelten Sechsen 1 beträgt, gleich $\frac{2}{3}$ und für das 1 Ergebnis, für die die Anzahl der gewürfelten Sechsen 2 beträgt, gleich $\frac{5}{3}$.

Nun müssen wir diese Werte quadrieren und *daraus* schließlich erneut den Erwartungswert berechnen. Wir haben also $V(X) = E(X - E(X))^2 = 25 \cdot (\frac{1}{36} \cdot \frac{1}{9}) + 10 \cdot (\frac{1}{36} \cdot \frac{4}{9}) + 1 \cdot (\frac{1}{36} \cdot \frac{25}{9}) = \frac{25}{324} + \frac{40}{324} + \frac{25}{324} = \frac{90}{324} = \frac{5}{18}$.

Die Varianz kann auch mithilfe folgender Formel berechnet werden: $V(X) = E(X^2) - (E(X))^2$. $(E(X))^2$ ist einfach $(\frac{1}{3})^2 = \frac{1}{9}$. $E(X^2)$ ist der Erwartungswert von X^2, also $E(X^2) = 25 \cdot (\frac{1}{36} \cdot 0^2) + 10 \cdot (\frac{1}{36} \cdot 1^2) + 1 \cdot (\frac{1}{36} \cdot 2^2) = \frac{10}{36} + \frac{4}{36} = \frac{14}{36}$. Damit ist $V(X) = E(X^2) - (E(X))^2 = \frac{14}{36} - \frac{1}{9} = \frac{5}{18}$.