Diskrete Strukturen

und

Lineare Algebra I für Informatiker

Skript zur Vorlesung

Dr. Timo Hanke
Prof. Dr. Gerhard Hiß
Lehrstuhl D für Mathematik
RWTH Aachen

Letzte Aktualisierung:
15. Januar 2019

Unter der freundlichen Mithilfe von:
Wolf-Daniel Andres, Grischa Studzinski und Florian Weingarten.

Inhaltsverzeichnis

Grundlagen

Kapitel 1

Mathematische Grundbegriffe

1.1 Aussagen

1.1.1 Definition und Beispiele

Definition. *Mathematische Aussagen* oder kurz *Aussagen* sind sprachliche Ausdrücke, die auch Formeln und Symbole enthalten können, und die einen eindeutigen *Wahrheitswert* besitzen, der entweder *wahr* oder *falsch* lautet.

Beispiel. Mathematische Aussagen sind:

(i) '$2 + 3 = 5$' (wahr)

(ii) 'Alle Punkte auf einem Kreis haben den gleichen Abstand zum Mittelpunkt' (wahr)

(iii) 'Jede ganze Zahl größer als 2 ist Summe zweier Primzahlen' (unbekannt)

(iv) 'Jede reelle Zahl ist ein Quadrat einer reellen Zahl' (falsch)

(v) 'Es gibt eine ganze Zahl, deren Quadrat gleich ihrem Doppelten ist' (wahr)

Die Aussage (iii) ist eine mathematische Aussage, denn sie besitzt einen Wahrheitswert, auch wenn uns dieser nicht bekannt ist. Die *Goldbach'sche Vermutung* besagt, dass der Wahrheitswert von (iii) wahr lautet. Keine mathematischen Aussagen sind dagegen 'Aachen ist schön' und 'Die Mensapreise sind zu hoch'.

1.1.2 Zusammensetzung und Verneinung

Definition a. Für beliebige Aussagen A und B definieren wir die Wahrheitswerte für folgende *zusammengesetzte Aussagen*:

(i) Die *Negation* (*Verneinung*) $\neg A$ ist genau dann wahr, wenn A falsch ist.

(ii) Die *Konjunktion* (*und*-Verknüpfung) $A \wedge B$ ist genau dann wahr, wenn sowohl A als auch B wahr ist.

(iii) Die *Disjunktion* (*oder*-Verknüpfung) $A \vee B$ ist genau dann wahr, wenn A oder B wahr ist oder beide wahr sind.

(iv) Das *exklusive oder* $A \operatorname{xor} B$ ist genau dann wahr, wenn A oder B wahr ist, aber nicht beide wahr sind.

(v) Die *Subjunktion* (*wenn-dann*-Verknüpfung) $A \to B$ ist genau dann falsch, wenn A wahr ist und B falsch ist.

(vi) Die *Bijunktion* (*genau-dann*-Verknüpfung) $A \leftrightarrow B$ ist genau dann wahr, wenn A und B den gleichen Wahrheitswert besitzen.

Sprechweise. Zu $\neg A$ sagt man „nicht A“, zu $A \wedge B$ „A und B“, zu $A \vee B$ „A oder B“, zu $A \operatorname{xor} B$ „A x-or B“ oder „entweder A oder B“, zu $A \to B$ „wenn A dann B“, zu $A \leftrightarrow B$ „A gilt genau dann, wenn B gilt“.

Wahrheitstafel. Die Wahrheitswerte der eingeführten zusammengesetzten Aussagen können in folgender Tabelle zusammengefasst werden. Dies ist ein Beispiel für eine *Wahrheitstafel*. Wir schreiben 1 bzw. 0 für die Wahrheitswerte *wahr* bzw. *falsch*.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \operatorname{xor} B$	$A \to B$	$A \leftrightarrow B$
1	1	0	1	1	0	1	1
1	0	0	0	1	1	0	0
0	1	1	0	1	1	1	0
0	0	1	0	0	0	1	1

Beispiel.

(i) Die Verneinung von ‘$2+3 = 5$’ lässt sich als ‘Es gilt nicht, dass $2+3 = 5$ ist’ oder kürzer als ‘$2 + 3$ ist ungleich 5’ formulieren.

(ii) Die Verneinung von 'Das Glas ist voll' lässt sich als 'Das Glas ist nicht voll' formulieren, nicht aber als 'Das Glas ist leer'.

(iii) Die Verneinung von 'Alle Gläser sind voll' lässt sich als 'Nicht alle Gläser sind voll', oder als 'Es gibt ein Glas, das nicht voll ist' formulieren.

(iv) 'Wenn $2+3=6$, dann ist $2+3=7$' ist wahr.

Definition b. Seien A und B Aussagen.

(i) Ist $A \to B$ wahr, dann schreiben wir $A \Rightarrow B$ und sagen: "*Aus A folgt B*" oder "*A impliziert B*" oder "*Wenn A, dann B*" oder "*A ist hinreichend für B*" oder "*B ist notwendig für A*".

(ii) Ist $A \leftrightarrow B$ wahr, dann schreiben wir $A \Leftrightarrow B$ und sagen: "*A genau dann, wenn B*" oder "*A dann und nur dann, wenn B*" oder "*A ist notwendig und hinreichend für B*".

1.1.3 Tautologien

Definition. (i) Ein *logischer Term* ist ein Ausdruck bestehend aus Variablen $A, B, \ldots$ und den Konstanten 1 und 0, die verknüpft sind mit den Symbolen $\neg, \wedge, \vee, \text{xor}, \to, \leftrightarrow$ (und Klammern). Durch Belegung der Variablen mit Wahrheitswerten bekommt der Term selbst einen Wahrheitswert.

(ii) Zwei logische Terme S und T, definiert auf derselben Variablenmenge, heißen *logisch äquivalent* oder *wertverlaufsgleich*, geschrieben $S \equiv T$, wenn S und T denselben Wahrheitswert haben für jede Belegung der Variablen.

(iii) Ein logischer Term T heißt *Tautologie*, wenn $T \equiv w$.

Beispiel a. Im Folgenden stellen wir einige einfachen logischen Äquivalenzen zusammen.

(i)
- $A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$
- $A \vee (B \vee C) \equiv (A \vee B) \vee C$

(ii)
- $A \wedge 1 \equiv A$
- $A \vee 0 \equiv A$

(iii)
- $A \wedge B \equiv B \wedge A$

- $A \vee B \equiv B \vee A$

(iv)
- $A \wedge A \equiv A$
- $A \vee A \equiv A$

(v)
- $A \wedge \neg A \equiv 0$
- $A \vee \neg A \equiv 1$

(vi)
- $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
- $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$

(vii)
- $A \wedge (A \vee B) \equiv A$
- $A \vee (A \wedge B) \equiv A$

Beispiel b. Durch logische Äquivalenzen lassen sich logische Symbole durch andere ersetzen.

(i) $A \operatorname{xor} B \equiv (A \wedge \neg B) \vee (\neg A \wedge B)$.

Wir sagen daher, dass xor durch $\neg, \wedge, \vee$ ausgedrückt werden kann.

(ii) $A \to B \equiv \neg(A \wedge \neg B)$.

(iii) $A \leftrightarrow B \equiv \neg(A \operatorname{xor} B)$.

Übung a. Man zeige, dass xor durch $\neg, \vee$ ausgedrückt werden kann.

Beispiel c. $A \wedge \neg B$ und $A \to ((B \to \neg C) \vee D)$ sind logische Terme, aber keine Tautologien. $(A \to B) \leftrightarrow \neg(A \wedge \neg B)$ ist eine Tautologie. Bedeutsame Tautologien sind:

(i) Modus Ponens:

$$(A \wedge (A \to B)) \to B$$

(ii) Tertium non datur (Gesetz des ausgeschlossenen Dritten):

$$A \vee \neg A$$

(iii) de Morgan-Gesetze:

$$\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B),$$
$$\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$$

(iv) Kontrapositionsgesetz:

$$(A \to B) \leftrightarrow (\neg B \to \neg A)$$

Bemerkung a. Es seien S, T logische Terme. Dann gilt $S \equiv T$ genau dann, $S \leftrightarrow T$ eine Tautologie ist.

Übung b.

(i) Man schreibe die Tautologien auf, die von Beispiel b geliefert werden.

(ii) Ist $(A \leftrightarrow B) \leftrightarrow ((A \to B) \wedge (B \to A))$ eine Tautologie?

(iii) Man folgere aus den Tautologien des Beispiels durch Einsetzen, dass auch $\neg(A \wedge \neg A)$ eine Tautologie ist.

(iv) Gelten die „Distributivgesetze“ $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$ und $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$?

Bemerkung b. Tautologien helfen bei Beweisen: Aus Modus Ponens folgt $(A \wedge (A \to B)) \Rightarrow B$; zeigt man also, dass A wahr ist und $A \Rightarrow B$ gilt (d.h. dass $A \to B$ wahr ist), so folgt, dass auch B wahr ist.

Möchte man $A \Rightarrow B$ zeigen, so kann man nach dem Kontrapositionsgesetz anstelle dessen auch $\neg B \Rightarrow \neg A$ zeigen (z.B. statt ‘Wenn x kein Quadrat ist, dann $x < 0$’ zeigt man ‘Wenn $x \geq 0$, dann x ein Quadrat’).

1.1.4 Aussageformen

Definition. Eine *Aussageform* ist ein sprachlicher Ausdruck, der Variablen enthält, und der für jede Belegung aller vorkommenden Variablen mit konkreten Objekten zu einer Aussage wird. (Diese letzte Bedingung führt dazu, dass die Auswahl der Objekte, mit denen die Variablen belegt werden können, i.A. eingeschränkt ist; siehe Beispiel (i) unten.)

Bemerkung. Eine Aussageform ist selbst keine Aussage. Die Zusammensetzung von Aussageformen mittels $\neg, \wedge, \vee, \to, \leftrightarrow$, etc. ist wieder eine Aussageform.

Beispiel.

(i) ‘Wenn $x > 0$, dann ist x ein Quadrat.’ ist eine Aussageform. Wird die Variable x mit einer beliebigen reellen Zahl belegt, so erhalten wir eine Aussage (einen eindeutigen Wahrheitswert).

Hier setzen wir implizit voraus, dass die Variable x nur mit Objekten belegt wird, für die die Aussage $x > 0$ Sinn ergibt (definiert ist).

(ii) ‘Person x hat mindestens 50% der Klausur-Punkte erzielt’ ist eine Aussageform. Wird die Variable x mit einer beliebigen Person belegt, so erhalten wir eine Aussage (einen eindeutigen Wahrheitswert).

(iii) Es sei $A(x)$ die Aussageform 'Person x hat in der Klausur volle Punktzahl erzielt' und $B(x)$ die Aussageform 'Person x hat das Modul bestanden'. Dann ist auch $A(x) \to B(x)$ eine Aussageform.

Für jede Belegung der Variable x mit einer Person ist $A(x) \to B(x)$ eine wahre Aussage. Es gilt also $A(x) \Rightarrow B(x)$. Das liegt daran, dass der Fall $A(x)$ wahr und $B(x)$ falsch (der einzige Fall in dem $A(x) \to B(x)$ falsch ist) nicht vorkommt.

(iv) Es sei $A(t)$ die Aussageform 'Der Projektor im Hörsaal ist zum Zeitpunkt t aus' und $B(t)$ die Aussageform 'Der Hörsaal ist zum Zeitpunkt t leer'.

Für jede Belegung der Variable t mit einem Zeitpunkt ist $A(t) \to B(t)$ eine Aussage. Deren Wahrheitswert hängt allerdings von t ab. Wann ist sie falsch?

Bemerkung. Wenn $A(x) \to B(x)$ unabhängig von x stets wahr ist (wie in Beispiel (iii)), gilt also $A(x) \Rightarrow B(x)$, dann drückt dies offensichtlich einen kausalen Zusammenhang aus.

1.1.5 Sprachliche Konventionen

Wir einigen uns auf folgende Konventionen

(i) Wir sagen: „Die Aussage A *gilt*“, falls A den Wahrheitswert 1 hat (also wahr ist).

(ii) $A := B$ bedeutet: Das Symbol A wird durch das Symbol B definiert.

(iii) $A :\Leftrightarrow B$ bedeutet: Die Aussage A wird durch die Aussage B definiert (A hat per Definition den gleichen Wahrheitswert wie B).

(iv) *Ein* bedeutet stets „mindestens ein“ und ist von „genau ein“ zu unterscheiden.

(v) In einer Aufzählung von Objekten $x_1, \ldots, x_n$ heißen $x_1, \ldots, x_n$ *paarweise verschieden*, wenn keine zwei Objekte der Aufzählung gleich sind (d.h. wenn in der Aufzählung keine Wiederholungen vorkommen). Davon zu unterscheiden ist „verschieden“ im Sinne von „nicht alle gleich“. Wenn wir von „n verschiedenen Objekten $x_1, \ldots, x_n$“ sprechen, impliziert das, dass $x_1, \ldots, x_n$ paarweise verschieden sind.

1.2 Mengen

1.2.1 Definition und Beispiele

> "Unter einer *Menge* verstehen wir jede Zusammenfassung M von bestimmten wohlunterscheidbaren Objekten unserer Anschauung oder unseres Denkens [welche die *Elemente* von M genannt werden] zu einem Ganzen."
>
> Georg Cantor, 1895

Bei der Auslegung von Cantor's Begriff einer „Zusammenfassung" ist allerdings Vorsicht geboten. Das wusste schon Cantor selbst und zeigte, dass die Betrachtung der „Menge aller Mengen" zu einem Widerspruch führt: nach der *Zweiten Cantor'schen Antinomie* wäre sie „größer" als sie selbst. Man kann auch ohne Betrachtung der „Größe" einer Menge einen rein logischen Widerspruch aus der „Menge aller Mengen" ableiten, die *Russel'sche Antinomie* (siehe Übung b unten). Wir einigen uns auf die folgende Definition des Mengenbegriffs.

Definition a. Eine *Menge* M ist etwas, zu dem jedes beliebige Objekt x entweder *Element* der Menge ist, geschrieben $x \in M$, oder nicht, geschrieben $x \notin M$.

Mengen sind also gerade dadurch gekennzeichnet, dass '$x \in M$' für jedes Objekt x eine Aussage ist (einen eindeutigen Wahrheitswert hat), also gerade dadurch, dass '$x \in M$' eine Aussageform ist. Umgekehrt ist für jede Aussageform $A(x)$ die Zusammenfassung aller x, für die $A(x)$ wahr ist, eine Menge (vgl. Schreibweise (iii) unten).

Bemerkung a. Mengen, die sich selbst enthalten führen nicht per se zu einem Widerspruch. In der weit verbreitetsten Mengenlehre (der *Zermelo-Fraenkel-Mengenlehre*), der wir uns anschließen wollen, sind Mengen, die sich selbst als Elemente enthalten, allerdings nicht erlaubt.

Definition b. Sind M, N zwei Mengen, so heißt N eine *Teilmenge* von M und M eine *Obermenge* von N, geschrieben $N \subseteq M$, wenn für alle $x \in N$ gilt: $x \in M$. Das Zeichen $\subseteq$ bzw. die Aussage $N \subseteq M$ heißt *Inklusion*.

Zwei Mengen M und N heißen *gleich*, geschrieben $M = N$, wenn $M \subseteq N$ und $N \subseteq M$.

Eine Menge M heißt *endlich*, wenn M nur endlich viele Elemente besitzt. Man schreibt in diesem Fall $|M|$ für die Anzahl der Elemente von M. Anderenfalls heißt M *unendlich* und man schreibt $|M| = \infty$.

Schreibweise. Es folgen die gebräuchlichsten Methoden, Mengen zu beschreiben.

(i) *Aufzählen.* Die Elemente werden aufgelistet und mit Mengenklammern eingeschlossen. Reihenfolge und Wiederholungen spielen bei der Mengenaufzählung keine Rolle, z.B.

$$\{1, 3, 17\} = \{3, 1, 17\} = \{1, 3, 17, 1, 3\}.$$

(ii) *Beschreiben.* Mengen können durch Worte beschrieben werden, etwa:

$$\begin{aligned}&\text{Menge der natürlichen Zahlen} = \{1, 2, 3, 4, 5, \ldots\}\\ &\text{Menge der ganzen Zahlen} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}\end{aligned}$$

(iii) *Aussondern.* Es sei M eine Menge. Ist $A(x)$ eine Aussageform, so bezeichnet

$$\{x \in M \mid A(x)\}$$

diejenige Teilmenge von M, die aus allen Elementen besteht, für die $A(x)$ wahr ist (gesprochen „Menge aller x aus M mit $A(x)$“). Benennen wir beispielsweise die Menge der natürlichen Zahlen mit $\mathbb{N}$, so ist $\{n \in \mathbb{N} \mid n \text{ ist ungerade}\}$ die Menge der ungeraden natürlichen Zahlen, also $\{1, 3, 5, 7, \ldots\}$.

(iv) *Abbilden.* Seien M und N Mengen und $e(x)$ für jedes $x \in M$ ein Element aus N. (Wir greifen hier dem Begriff der *Abbildung* vor.) Dann ist

$$\{e(x) \mid x \in M\}$$

eine Teilmenge von N (insbesondere eine Menge), die Menge aller Elemente der Form $e(x)$ von N, wobei x alle Elemente aus M durchläuft. Ist z.B. $\mathbb{N}$ die Menge der natürlichen Zahlen, dann ist $\{n^2 \mid n \in \mathbb{N}\}$ die Menge der Quadratzahlen (hier ist $M = N = \mathbb{N}$). Ist $\mathbb{R}$ die Menge der rellen Zahlen, dann ist $\{|x| \mid x \in \mathbb{R}\}$ die Menge der nicht-negativen rellen Zahlen. Abbilden und Aussondern können kombiniert werden, sodass z.B. $\{n^2 \mid n \in \mathbb{N}, n \text{ ungerade}\}$ die Menge aller Quadrate von ungeraden natürlichen Zahlen bezeichnet, also $\{1, 9, 25, 49, \ldots\}$.

Bemerkung b. In der Regel schreibt man die Menge $\{n^2 \mid n \in \mathbb{N}, n \text{ ungerade}\}$ auch kurz und intuitiv als $\{n^2 \mid n \in \mathbb{N} \text{ ungerade}\}$, ohne sich Gedanken über Abbilden und Aussondern zu machen. Man muss beide Schreibweisen aber penibel trennen, wenn man die Menge beispielsweise in ein Computeralgebra-System eingeben möchte.

Beispiel. Häufig auftretende Mengen sind:

Symbol	Beschreibung	Definition
$\emptyset$	leere Menge	$\{\}$
$\mathbb{N}$	natürliche Zahlen	$\{1, 2, 3, \ldots\}$
$\mathbb{N}_0$	natürliche Zahlen einschl. 0	$\{0, 1, 2, 3, \ldots\}$
$\underline{n}$	n-elementige Menge, $n \in \mathbb{N}_0$	$\{1, 2, \ldots, n\}$, $\underline{0} := \emptyset$
$\mathbb{P}$	Primzahlen	$\{2, 3, 5, 7, 11, 13, \ldots\}$
$\mathbb{Z}$	ganze Zahlen	$\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$\mathbb{Q}$	rationale Zahlen	$\{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}\}$
$\mathbb{R}$	reelle Zahlen	$\{a_1 a_2 \ldots a_r, b_1 b_2 \ldots : a_i, b_i \in \{0, 1, \ldots, 9\}\}$
$\mathbb{R}_{>0}$	positive reelle Zahlen	$\{x \in \mathbb{R} \mid x > 0\}$
$\mathbb{R}_{\geq 0}$	nicht-negative reelle Zahlen	$\{x \in \mathbb{R} \mid x \geq 0\}$
$\mathbb{C}$	komplexe Zahlen	$\{a + bi : a, b \in \mathbb{R}\}$

Nur die erste und vierte der Mengen der Tabelle sind endlich, nämlich $|\emptyset| = 0$ und $|\underline{n}| = n$ für alle $n \in \mathbb{N}_0$. Es gilt:

$$\emptyset = \underline{0} \subseteq \underline{1} \subseteq \underline{2} \subseteq \ldots \subseteq \mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

Übung a. Was gilt für eine Menge M:

(i) $x \in M$ xor $x \notin M$ für alle x?

(ii) $x \in M \Leftrightarrow \neg(x \notin M)$?

(iii) $\neg(x \in M) \Leftrightarrow x \notin M$?

Übung b (Russel's Antinomie). Die „Menge aller Mengen" würde als Teilmenge enthalten die „Menge" $\mathcal{M}$ aller Mengen, die sich nicht selbst als Element enthalten. Ist dann $\mathcal{M} \in \mathcal{M}$ oder $\mathcal{M} \notin \mathcal{M}$?

1.2.2 Quantifizierte Aussagen

Es sei $A(x)$ eine Aussageform. Nach Definition (1.1.4) ist $A(x)$ für jedes x eine Aussage. Setzt man in $A(x)$ für x in ein konkretes Objekt ein, so sagt man, x wird *spezifiziert*. Zwei weitere Möglichkeiten, aus $A(x)$ eine Aussage zu machen, bestehen darin, x zu *quantifizieren*:

'Für alle $x \in M$ gilt $A(x)$' und 'Es gibt ein $x \in M$, für das $A(x)$ gilt'.

Hierbei ist M eine Menge. Diese sprachlichen Ausdrücke sind Aussagen, denn x ist keine (freie) Variable mehr!

Beispiel.

(i) Sei $A(x)$ die Aussageform '$x > 5$'. Dann ist 'Es existiert ein $x \in \mathbb{N}$ mit $A(x)$' wahr, weil z.B. $A(7)$ wahr ist. Dagegen ist 'Für alle $x \in \mathbb{N}$ gilt $A(x)$' falsch, weil z.B. $A(2)$ falsch ist.

(ii) Sei $A(t)$ die Aussageform 'Zum Zeitpunkt t gilt: Projektor ist aus $\rightarrow$ Hörsaal ist leer'. Ist t ein konkreter Zeitpunkt, an dem der Projektor an ist oder der Hörsaal leer, so ist die Aussage $A(t)$ wahr. Da es solche Zeitpunkte gibt, ist 'Es gibt eine Zeit t mit $A(t)$' wahr. Ist t dagegen ein konkreter Zeitpunkt, an dem der Projektor aus ist und der Hörsaal nicht leer, so ist die Aussage $A(t)$ falsch. Da es auch solche Zeitpunkte gibt, ist auch 'Es gibt eine Zeit t mit $\neg A(t)$' wahr und 'Für alle Zeiten t gilt $A(t)$' falsch.

(iii) Die Verneinung von 'Für alle $x \in M$ gilt $A(x)$' lässt sich als 'Es existiert $x \in M$ mit $\neg A(x)$' bzw. 'Es existiert $x \in M$ für das $A(x)$ nicht gilt' formulieren. Die Verneinung von 'Für alle $x \in \mathbb{R}$ gilt $x^2 > 0$' lässt sich als 'Es existiert ein $x \in \mathbb{R}$ mit $x^2 \leq 0$' formulieren.

(iv) Die Verneinung von 'Es existiert ein $x \in M$ mit $A(x)$' lässt sich als 'Für alle $x \in M$ gilt $\neg A(x)$' formulieren. Die Verneinung von 'Es gibt eine Person im Hörsaal, die ihr Handy aus hat' lässt sich als 'Alle Personen im Hörsaal haben ihr Handy an' formulieren.

Bemerkung. Gelegentlich schreibt man (missbräuchlich) nur eine Aussageform $A(x)$ auf, meint damit aber die Aussage 'Für alle $x \in M$ gilt $A(x)$'. Das geht nur, wenn die Menge M aus dem Zusammenhang klar ist.

Übung. Wie lautet der Wahrheitswert der Aussagen 'Für alle $x \in \emptyset$ gilt $A(x)$' und 'Es gibt $x \in \emptyset$ mit $A(x)$'?

1.2.3 Konstruktion von Mengen

Definition (Mengenoperationen)**.** Es seien M, N beliebige Mengen.

(i) $M \cap N := \{x \in M \mid x \in N\}$ heißt *Durchschnitt* von M und N.

(ii) $M \cup N := \{x \mid x \in M \text{ oder } x \in N\}$ heißt *Vereinigung* von M und N.

(iii) $M \backslash N := \{x \in M \mid x \notin N\}$ heißt die *Differenzmenge*, gesprochen „M ohne N".

(iv) $M \times N := \{(x, y) \mid x \in M \text{ und } y \in N\}$ heißt *kartesisches Produkt* von M und N.
Hierbei ist (x, y) ein *geordnetes Paar*. Zwei geordnete Paare (x, y) und (x', y') sind genau dann gleich, wenn $x = x'$ und $y = y'$.

(v) $\mathrm{Pot}(M) := \{S \mid S \subseteq M\}$ heißt die *Potenzmenge* von M.

Beispiel.

(i) Die leere Menge ist Teilmenge jeder beliebigen Menge (auch von sich selbst).

(ii) Es gilt:

$$\begin{aligned} \mathrm{Pot}(\emptyset) &= \{\emptyset\}, \\ \mathrm{Pot}(\{1\}) &= \{\emptyset, \{1\}\}, \\ \mathrm{Pot}(\{1,2\}) &= \{\emptyset, \{1\}, \{2\}, \{1,2\}\}, \\ &\vdots \end{aligned}$$

(iii) Für Mengen M und N gilt:

- $M \cap N = N \Leftrightarrow N \subseteq M$.
- $M \cup N = N \Leftrightarrow M \subseteq N$.

Bemerkung. Für Mengen L, M, N gelten folgende Rechenregeln.

(i)
- $L \cap (M \cap N) = (L \cap M) \cap N$
- $L \cup (M \cup N) = (L \cup M) \cup N$

(ii)
- $L \cap M = M \cap L$
- $L \cup M = M \cup L$

(iii)
- $L \cap L = L$
- $L \cup L = L$

(iv)
- $L \cap (M \cup N) = (L \cap M) \cup (L \cap N)$
- $L \cup (M \cap N) = (L \cup M) \cap (L \cup N)$

(v)
- $L \cap (L \cup M) = L$
- $L \cup (L \cap M) = L$

Übung.

(i) Wie viele Elemente hat $\mathrm{Pot}(\underline{n})$ für $n \in \mathbb{N}_0$?

1.2.4 Indexmengen

Definition a. Es sei $n \in \mathbb{N}$. Für Zahlen $a_1, \ldots, a_n$, Mengen $M_1, \ldots, M_n$ und Aussagen $A_1, \ldots, A_n$ definieren wir:

(i) $\sum_{i=1}^{n} a_i := a_1 + \ldots + a_n$

(ii) $\prod_{i=1}^{n} a_i := a_1 \cdot \ldots \cdot a_n$

(iii) $\bigcup_{i=1}^{n} M_i := M_1 \cup \ldots \cup M_n$

(iv) $\bigcap_{i=1}^{n} M_i := M_1 \cap \ldots \cap M_n$

(v) $\bigvee_{i=1}^{n} A_i := A_1 \vee \ldots \vee A_n$

(vi) $\bigwedge_{i=1}^{n} A_i := A_1 \wedge \ldots \wedge A_n$

Diese *Aufzählschreibweisen* können teilweise auf beliebige *Indexmengen* I verallgemeinert werden, die auch unendlich sein dürfen:

Definition b. Für jedes $i \in I$ sei M_i eine Menge.

(i) Wir definieren $\bigcup_{i \in I} M_i$ durch

$$x \in \bigcup_{i \in I} M_i :\Leftrightarrow \text{ es gibt } i \in I \text{ mit } x \in M_i$$

(ii) Wir definieren $\bigcap_{i \in I} M_i$ durch

$$x \in \bigcap_{i \in I} M_i :\Leftrightarrow \text{ für alle } i \in I \text{ gilt } x \in M_i$$

Es ist auch sinnvoll, den Begriff „paarweise verschieden“ für beliebig indizierte Objekte auszudehnen:

Definition c. Für jedes $i \in I$ sei x_i ein Objekt. Die Objekte $x_i, i \in I$, heißen *paarweise verschieden*, wenn für alle $i, j \in I$ gilt: $x_i = x_j \Rightarrow i = j$.

Beispiel. (i) Die Zahlen $n^2, n \in \mathbb{N}$, sind paarweise verschieden.

(ii) Die Zahlen $n^2, n \in \mathbb{Z}$, sind nicht paarweise verschieden.

1.2.5 Mengenpartitionen

Definition.

(i) Zwei Mengen A, B heißen *disjunkt*, wenn $A \cap B = \emptyset$.

(ii) Mengen $M_i, i \in I$, heißen *paarweise disjunkt*, wenn für alle $i, j \in I$ mit $i \neq j$ gilt: $M_i \cap M_j = \emptyset$.

(iii) Es sei $\mathcal{M}$ eine Menge von Mengen ($\mathcal{M}$ darf hier unendlich sein). Die Elemente von $\mathcal{M}$ heißen *paarweise disjunkt*, wenn je zwei davon disjunkt sind, d.h. wenn für alle $M, M' \in \mathcal{M}$ mit $M \neq M'$ gilt: $M \cap M' = \emptyset$.

(iv) Es sei M eine Menge. Eine *Partition* von M ist eine Menge $\mathcal{P}$ nichtleerer, paarweise disjunkter Teilmengen von M mit $M = \bigcup_{C \in \mathcal{P}} C$. Die Elemente $C \in \mathcal{P}$ heißen *Teile* der Partition.

Bemerkung. Für jede Partition $\mathcal{P}$ von M ist $\mathcal{P} \subseteq \mathrm{Pot}(M) \setminus \{\emptyset\}$.

Beispiel.

(i) $\mathcal{P} = \{\{n \in \mathbb{N} \mid n \text{ gerade}\}, \{n \in \mathbb{N} \mid n \text{ ungerade}\}\}$ stellt eine Partition von $\mathbb{N}$ mit zwei Teilen dar.

(ii) $\mathcal{P} = \{\{n \in \mathbb{N} \mid n \text{ hat } k \text{ Dezimalstellen}\} \mid k \in \mathbb{N}\}$ stellt eine Partition von $\mathbb{N}$ mit unendlich vielen Teilen dar.

(iii) Die einzige Partition von $\emptyset$ ist $\mathcal{P} = \emptyset$.

Übung. Man mache sich klar:

(i) Sind M, N endliche, disjunkte Mengen, so gilt $|M \cup N| = |M| + |N|$.

(ii) Sind $M_1, \ldots, M_n$ endliche, paarweise disjunkte Mengen, so gilt

$$|\bigcup_{i=1}^{n} M_i| = \sum_{i=1}^{n} |M_i|.$$

1.3 Beweisprinzipien

1.3.1 Direkter Beweis

Prinzip. Ziel: $A \Rightarrow B$ (d.h. $A \to B$ ist wahr).

Um das Ziel zu zeigen, nehmen wir an, dass A wahr ist und folgern daraus mittels logischer Schlüsse, dass B wahr ist. Wenn das gelungen ist, ist $A \Rightarrow B$ bewiesen.

Beispiel. Für alle $n \in \mathbb{N}$ gilt: n ungerade $\Rightarrow n^2$ ungerade.

Beweis. Sei $n \in \mathbb{N}$ beliebig, sei A die Aussage 'n ist ungerade' und B die Aussage 'n^2 ist ungerade'. Wir nehmen an, A ist wahr, d.h. n ist ungerade. Wir folgern, dass B wahr ist: Da n ungerade ist, existiert ein $k \in \mathbb{N}$ mit $n = 2k - 1$. Dann ist $n^2 = (2k-1)^2 = 4k^2 - 4k + 1 = 2(2k^2 - 2k) + 1$, eine ungerade Zahl. Damit ist gefolgert, dass B wahr ist. Nach dem Beweisprinzip des direkten Beweises ist also $A \Rightarrow B$ wahr. Da $n \in \mathbb{N}$ beliebig gewählt war, gilt dies für alle $n \in \mathbb{N}$. □

Übung. Was passiert, wenn sich aus A ein Widerspruch folgern lässt, A also falsch ist?

1.3.2 Beweis durch Kontraposition

Prinzip. Ziel: $A \Rightarrow B$.

Stattdessen zeigen wir, $\neg B \Rightarrow \neg A$. Wenn das gelungen ist, ist $A \Rightarrow B$ bewiesen.

Beweis des Prinzips. Dieses Prinzip beruht auf der bekannten Tautologie $(A \to B) \Leftrightarrow (\neg B \to \neg A)$ aus Beispiel (1.1.3). □

Beispiel. Für alle $n \in \mathbb{N}$ gilt: n^2 gerade $\Rightarrow n$ gerade.

Beweis. Sei $n \in \mathbb{N}$ beliebig, sei A die Aussage 'n^2 ist gerade' und B die Aussage 'n ist gerade'. Wir zeigen $\neg B \Rightarrow \neg A$: Dies ist gleichbedeutend mit 'n ist ungerade $\Rightarrow n^2$ ist ungerade' und wurde schon in (1.3.1) gezeigt. Damit gilt nach dem Beweisprinzip der Kontraposition auch $A \Rightarrow B$. Da $n \in \mathbb{N}$ beliebig gewählt war, gilt dies für alle $n \in \mathbb{N}$. □

1.3.3 Beweis durch Widerspruch

Prinzip. Ziel: A ist wahr.

Wir zeigen, dass $\neg A \Rightarrow (B \wedge \neg B)$ gilt. Wenn das gelungen ist, ist auch A wahr. ($B \wedge \neg B$ ist hier der Widerspruch und die Aussage B kann frei gewählt werden.)

Beweis des Prinzips. $B \wedge \neg B$ ist stets falsch (vgl. Übung 1.1.3). Wenn $\neg A \Rightarrow (B \wedge \neg B)$ gilt, ist also $\neg A \to (B \wedge \neg B)$ wahr. Das kann nur der Fall sein, wenn $\neg A$ falsch ist (vgl. Definition von $\to$), d.h. A wahr ist. □

Beispiel. Es sei A die Aussage $\sqrt{2} \notin \mathbb{Q}$.

Beweis. Wir nehmen an, $\neg A$ ist wahr, d.h. $\sqrt{2} \in \mathbb{Q}$. Dann gibt es $n, m \in \mathbb{N}$, die nicht beide gerade sind und $\sqrt{2} = m/n$ erfüllen ($\sqrt{2}$ wird als Bruch geschrieben und dieser gekürzt). Seien solche n, m gewählt. Durch Quadrieren folgt $2n^2 = m^2$, d.h. m^2 ist gerade. Also ist m gerade nach Beispiel (1.3.2). Sei $k \in \mathbb{N}$ mit $m = 2k$. Dann gilt $2n^2 = m^2 = 4k^2$, also $n^2 = 2k^2$, d.h. n^2 ist gerade. Also ist n gerade nach Beispiel (1.3.2). Insgesamt wurde gezeigt, dass sowohl n als auch m gerade sind. Das ist ein Widerspruch (die Aussage B kann hier 'n und m sind nicht beide gerade' gewählt werden). Also ist die Annahme $\sqrt{2} \in \mathbb{Q}$ falsch, und damit ist die Behauptung $\sqrt{2} \notin \mathbb{Q}$ wahr. □

1.3.4 Vollständige Induktion

Prinzip. Ziel: Für alle $n \in \mathbb{N}$ gilt $A(n)$.
Wir zeigen als *Induktionsanfang*, dass $A(1)$ wahr ist, und als *Induktionsschritt* die Implikation $A(n) \Rightarrow A(n+1)$ für alle $n \in \mathbb{N}$. Dann ist $A(n)$ für alle $n \in \mathbb{N}$ wahr. Man spricht präziser von einer vollständigen Induktion *über* n. Im Induktionsschritt nennt man die Aussage $A(n)$ die *Induktionsvoraussetzung*.

Beweis des Prinzips. Das Prinzip beruht auf der folgenden Eigenschaft von $\mathbb{N}$, die wir als gegeben annehmen:

> Für jede Teilmenge $A \subseteq \mathbb{N}$ gilt: Ist $1 \in A$ und ist für jedes $n \in A$ auch $n + 1 \in A$, dann ist $A = \mathbb{N}$.

Bei der vollständigen Induktion zeigen wir gerade, dass die Menge $A := \{n \in \mathbb{N} \mid A(n) \text{ ist wahr}\}$ diese Bedingung erfüllt, also gleich $\mathbb{N}$ ist. □

Bemerkung. Eine alternative Möglichkeit, die Aussage 'Für alle $n \in \mathbb{N}$ gilt $A(n)$' zu zeigen, wäre, ein *beliebiges* $n \in \mathbb{N}$ zu wählen und dann $A(n)$ mit einem der Prinzipien (1.3.1)–(1.3.3) zu beweisen. (Genau so wurde in Beispiel (1.3.1) und (1.3.2) vorgegangen.) Da vollständige Induktion nur für $\mathbb{N}$ möglich ist, ist diese Alternative sogar der einzige Weg, um Aussagen 'Für alle $x \in M$ gilt $A(x)$' zu zeigen, bei denen die Menge M „größer" als $\mathbb{N}$ ist.

Beispiel. Für alle $n \in \mathbb{N}$ gilt $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Beweis. Wir führen eine vollständige Induktion über n. Sei also $A(n)$ die Aussageform $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Induktionsanfang: Es ist $\sum_{i=1}^{1} i = 1 = \frac{1 \cdot 2}{2}$, d.h. $A(1)$ ist wahr.

Induktionsschritt: Sei jetzt $n \in \mathbb{N}$ beliebig. Wir zeigen $A(n) \Rightarrow A(n+1)$ mittels eines direkten Beweises. Wir nehmen an, dass $A(n)$ wahr ist, d.h.

dass $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ gilt. Dieses ist die Induktionsvoraussetzung (kurz IV). Dann ist

$$\sum_{i=1}^{n+1} i = (\sum_{i=1}^{n} i) + (n+1) \overset{IV}{=} \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2}$$
$$= \frac{(n+1)(n+2)}{2}.$$

Der Induktionsschritt ist damit erledigt, weil dies genau die Aussage $A(n+1)$ ist. □

Bemerkung. Es gibt verschiedene Varianten der Induktion, z.B.

(i) Der Induktionsanfang kann bei $n_0 \in \mathbb{N}$ statt bei 1 gemacht werden. Damit wird die Aussage $A(n)$ für alle $n \geq n_0$ gezeigt.

(ii) Als Induktionsvoraussetzung kann $A(1) \wedge \ldots \wedge A(n)$ anstelle von $A(n)$ verwendet werden, was unter Umständen stärker ist.

(iii) Es gibt die vollständige Induktion nicht nur für $\mathbb{N}$ sondern auch eine sog. *strukturelle Induktion*, die z.B. über einen „Termaufbau“ geführt werden kann. Dies spielt in der Logik und bei formalen Sprachen eine Rolle.

(iv) In der Informatik beweist man die Korrektheit von Algorithmen häufig mit sog. *Schleifeninvarianten*. Im Prinzip beweist man damit die Korrektheit des Algorithmus durch Induktion über die Anzahl der Schleifendurchläufe, und die Schleifeninvariante hat die Rolle der Induktionsvoraussetzung.

Übung. Man zeige mittels vollständiger Induktion, dass sich eine Tafel Schokolade mit n Stücken stets durch $(n-1)$-maliges Durchbrechen in Einzelstücke zerlegen lässt. Hier wird vorausgesetzt, dass einmaliges Durchbrechen ein einzelnes Stück in genau zwei Teile zerlegt. Hinweis: Verwenden Sie als Induktionsvoraussetzung $A(1) \wedge \ldots \wedge A(n)$.

1.4 Abbildungen

1.4.1 Definition und Beispiele

Definition a. Seien M, N Mengen. Eine *Abbildung f von M nach N* ist eine „Vorschrift“ (z.B. eine Formel), die jedem $x \in M$ genau ein Element $f(x) \in N$ zuordnet, geschrieben

$$f : M \to N, \quad x \mapsto f(x).$$

Es heißen: M der *Definitionsbereich* von f, N der *Zielbereich* oder *Wertebereich* von f, $f(x)$ das *Bild* von x unter f, x ein *Urbild* von $f(x)$ unter f.

Zur Angabe einer Abbildung gehört die Angabe von Definitions- und Zielbereich dazu, d.h. zwei Abbildungen $f : M \to N$ und $g : M' \to N'$ sind nur dann gleich, wenn $M = M', N = N'$ und $f(x) = g(x)$ für alle $x \in M$.

Die Menge aller Abbildungen von M nach N wird mit $\mathrm{Abb}(M, N)$ oder mit N^M bezeichnet.

Beispiel a.

(i) $f : \mathbb{N} \to \mathbb{R}, i \mapsto i^2$.

(ii) Es sei M eine Menge von Glasperlen , und sei F die Menge aller Farben. Dann gibt es die Abbildung $f : M \to F, x \mapsto$ Farbe von x.

(iii) Für jede Menge A von Personen gibt es die Abbildung $J : A \to \mathbb{Z}, p \mapsto$ Geburtsjahr von p.

(iv) Die Addition in $\mathbb{Z}$ kann als die Abbildung

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (x, y) \mapsto x + y$$

aufgefasst werden.

(v) Für jede Menge M gibt es die *Identitätsabbildung*

$$\mathrm{id}_M : M \to M, x \mapsto x.$$

(vi) Betrachten wir die Abbildungen

$$\begin{aligned} f &: \mathbb{R} \to \mathbb{R}, \quad x \mapsto \sqrt{x^2}, \\ g &: \mathbb{R} \to \mathbb{R}, \quad x \mapsto |x|, \\ h &: \mathbb{R} \to \mathbb{R}_{\geq 0}, \quad x \mapsto |x|, \end{aligned}$$

so ist $f = g \neq h$.

(vii) $\mathrm{Abb}(\mathbb{R}, \mathbb{R}) = \{\mathbb{R} \to \mathbb{R}\} =$ Menge aller reellen Funktionen.

(viii) Für jede Menge N existiert genau eine Abbildung $\emptyset \to N$.

(ix) Für jede nicht-leere Menge M existiert keine Abbildung $M \to \emptyset$.

Bemerkung. Eine Abbildung $f : \mathbb{N} \to N$ wird auch *Folge in* N genannt. Oft benutzt man für Folgen die Schreibweise $a_1, a_2, a_3, \ldots$ oder $(a_i)_{i\in\mathbb{N}}$, wobei a_i für das Bild $f(i) \in N$ steht. Die Folge aus Beispiel a.(i) würde also auch geschrieben als $1, 4, 9, 16, \ldots$ oder als $(i^2)_{i\in\mathbb{N}}$.

Die Menge aller Folgen in N wird daher auch als $\mathrm{Abb}(\mathbb{N}, N)$ oder $N^{\mathbb{N}}$ geschrieben. Beispielsweise ist $\{0, 1\}^{\mathbb{N}}$ die Menge der Binärfolgen (manchmal auch geschrieben als $2^{\mathbb{N}}$), $\mathbb{R}^{\mathbb{N}}$ die Menge der reellen Folgen, usw.

Definition b. Es sei M eine Menge und $n \in \mathbb{N}$. Ein n-Tupel über M ist eine Abbildung $t : \underline{n} \to M$. Wie bei Folgen schreiben wir $(x_1, \ldots, x_n)$ oder $(x_i)_{i\in\underline{n}}$ für t, wobei $x_i := t(i)$ ist für $i \in \underline{n}$. Wir setzen $M^n := M^{\underline{n}} = \mathrm{Abb}(\underline{n}, M)$.

Beispiel b. (i) Das 5-Tupel $(1, -3, 0, 0, 27)$ über $\mathbb{Z}$ ist z.B. die Abbildung $t : \underline{5} \to \mathbb{Z}$ mit $t(1) = 1, t(2) = -3, t(3) = t(4) = 0, t(5) = 27$.

(ii) Für jede Menge N kann N^2 mit $N \times N$ identifiziert werden. (Hier wird das 2-**Tupel** $(x, y) \in N^2$, d.i. die Abbildung $\{1, 2\} \to N$, $1 \mapsto x$, $2 \mapsto y$, mit dem **geordneten Paar** $(x, y) \in N \times N$ identifiziert.)

Schließlich können wir mit dem Abbildungsbegriff auch kartesische Produkte von mehr als zwei Mengen definieren.

Definition c. Es sei $n \in \mathbb{N}$ und M_i eine Menge für alle $i \in \underline{n}$. Wir setzen

$$M := \bigcup_{i\in\underline{n}} M_i$$

und definieren

$$M_1 \times \cdots \times M_n := \{f : \underline{n} \to M \mid f(i) \in M_i \text{ für alle } i \in \underline{n}\},$$

und nennen $M_1 \times \cdots \times M_n$ das *kartesische Produkt* der Mengen $M_1, \ldots, M_n$.

Wie bei Folgen schreiben wir $(x_1, \ldots, x_n)$ oder $(x_i)_{i\in\underline{n}}$ für $f \in M_1 \times \cdots \times M_n$, wobei $x_i := f(i)$ ist für $1 \le i \le n$.

Es ist also $M_1 \times \cdots \times M_n$ die Menge aller n-Tupel $(x_1, \ldots, x_n) = (x_i)_{i\in\underline{n}} \in M^n$ mit $x_i \in M_i$ für $i \in \underline{n}$.

Beispiel c. Für jede Menge M und jede natürliche Zahl $n \ge 2$ kann M^n mit dem n-fachen kartesischen Produkt $M \times \cdots \times M$ (mit n Faktoren) identifiziert werden.

Ersetzt man in Definition c die Menge $\underline{n}$ durch eine beliebige Indexmenge I, erhält man das kartesische Produkt über I.

Definition d. (i) Es seien I und M Mengen. Eine Abbildung $f : I \to M$ wird gelegentlich auch mit $(x_i)_{i\in I}$ notiert, wobei $x_i := f(i)$ ist für $i \in I$. In diesem Fall nennen wir $(x_i)_{i\in I}$ eine durch I indizierte *Familie* in M.

(ii) Es sei I eine Menge und M_i eine Menge für alle $i \in I$. Wir setzen

$$M := \bigcup_{i\in \underline{n}} M_i$$

und definieren

$$\prod_{i\in I} M_i := \{f : \underline{n} \to M \mid f(i) \in M_i \text{ für alle } i \in I\},$$

und nennen $\prod_{i\in I} M_i$ das *kartesische Produkt* der Mengen $M_i, i \in I$.

In der oben eingeführten Schreibweise gilt also

$$\prod_{i\in I} M_i := \{(x_i)_{i\in I} \mid x_i \in M_i \text{ für alle } i \in I\}.$$

Übung.

(i) Bestimmen Sie $|\operatorname{Abb}(N, M)|$ für endliche Mengen N und M.

(ii) Wie viele Elemente hat $M_1 \times \cdots \times M_n$ für $n \in \mathbb{N}$ und endliche Mengen $M_1, \ldots, M_n$?

(iii) Wie viele Elemente hat M^n für $n \in \mathbb{N}$ und eine endlichen Menge M?

1.4.2 Definition durch Rekursion

Folgen auf einer Menge können *rekursiv* definiert werden.

Beispiel. (i) Auf $\mathbb{R}_{>0}$ existiert genau eine Folge $(a_n)_{n\in\mathbb{N}}$ mit

$$a_1 := 1 \text{ und } a_{n+1} := 1 + \frac{1}{a_n} \text{ für } n \geq 1.$$

(ii) Es sei $a \in \mathbb{R}$. Es gibt genau eine Folge $x = (x_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ mit

$$x_1 = a \text{ und } x_{n+1} = a \cdot x_n \text{ für } n \geq 1.$$

Wir schreiben: $a^n := x_n$ für das n-te Glied dieser Folge.

Alternativ verwenden wir für dieses Vorgehen oft auch die Sprechweise:

Für $a \in \mathbb{R}$ definieren wir die *Potenzen* a^n für $n \in \mathbb{N}$ *rekursiv* durch:

$$a^1 := a \text{ und } a^{n+1} := a \cdot a^n \text{ für } n \geq 1.$$

Die Definition durch Rekursion beruht auf dem folgenden Satz.

Satz. *Es sei N eine Menge, $f\colon N \to N$ Abbildung und $a \in N$.*
Dann gibt es genau eine Folge $(a_n)_{n\in\mathbb{N}}$ in N mit:

- $a_1 = a$
- $a_{n+1} = f(a_n)$ *für* $n \in \mathbb{N}$.

Dieser *Rekursionssatz von Dedekind* kann durch vollständige Induktion bewiesen werden. Wir verzichten hier auf einen Beweis.

Bemerkung. Wir erhalten die Folgen aus Beispiel 1.4.2 mittels der folgenden Abbildungen.

(i) $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$, $x \mapsto 1 + 1/x$.

(ii) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto ax$.

1.4.3 Bild und Urbild

Definition. Es sei $f : M \to N$ eine Abbildung.

(i) Für jede Teilmenge $X \subseteq M$ heißt $f(X) := \{f(x) \mid x \in X\}$ das *Bild von X* unter f.

(ii) Das Bild $f(M)$ von M unter f wird schlicht das *Bild* von f genannt.

(iii) Für jede Teilmenge $Y \subseteq N$ heißt $f^{-1}(Y) := \{x \in M \mid f(x) \in Y\}$ das *Urbild von Y* unter f.

(iv) Die Mengen $f^{-1}(\{y\})$ mit $y \in N$ heißen die *Fasern von f*.

Die Schreibweise f^{-1} für das Urbild hat im Allgemeinen nichts mit Umkehrabbildungen zu tun.

Beispiel. Die Faser der Abbildung J aus Beispiel (1.4.1)a.(i) zu 2000 ist die Menge aller Personen, die im Jahr 2000 geboren sind.

Bemerkung a. Die nicht-leeren Fasern einer Abbildung bilden eine Partition des Definitionsbereichs.

1.4.4 Injektive und surjektive Abbildungen

Definition. Es sei $f : M \to N$ eine Abbildung.

(i) f heißt *surjektiv*, falls $f(M) = N$.

(ii) f heißt *injektiv*, falls für alle $x, x' \in M$ gilt: $f(x) = f(x') \Rightarrow x = x'$.

(iii) f heißt *bijektiv*, falls f injektiv und surjektiv ist.

Bemerkung a. Eine Abbildung $f : M \to N$ ist per Definition injektiv, surjektiv bzw. bijektiv, wenn jedes Element $y \in N$ höchstens ein, mindestens ein bzw. genau ein Urbild hat. Das ist genau dann der Fall, wenn alle Fasern von f höchstens ein, mindestens ein bzw. genau ein Element besitzen, also genau dann, wenn für jedes $y \in N$ die Gleichung $f(x) = y$ höchstens eine, mindestens eine bzw. genau eine Lösung $x \in M$ hat.

Beispiel.

(i) $f : \mathbb{Z} \to \mathbb{Z}, z \mapsto 2z$ ist injektiv, aber nicht surjektiv.

(ii) $f : \mathbb{R} \to \mathbb{R}, x \mapsto 2x$ ist bijektiv.

(iii) $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ ist weder injektiv noch surjektiv. In der Tat ist $f(\mathbb{R}) = \mathbb{R}_{\geq 0}$, also f nicht surjektiv. Weiter ist z.B. $f(2) = 4 = f(-2)$ aber $2 \neq -2$, folglich ist f nicht injektiv.

(iv) Es sei $f : M \to F$ die Abbildung aus Beispiel (1.4.1)a.(ii). Die Faser $f^{-1}(\{\text{rot}\})$ ist die Menge der roten Perlen in M. Es ist f genau dann injektiv, wenn von jeder Farbe höchstens eine Perle in M vorkommt, wenn also keine zwei Perlen aus M die gleiche Farbe haben. Weiter ist f genau dann surjektiv, wenn von jeder Farbe (mindestens) eine Perle in M vorkommt.

(v) Die Abbildung $\emptyset \to N$ ist injektiv. Sie ist genau dann surjektiv, wenn $N = \emptyset$.

(vi) Hashfunktionen (bzw. „Checksummen“ oder „Fingerprints“), z.B. die bekannte md5 : $\{\text{Texte}\} \to \{0,1\}^{128}$, die einen 128-bit Hashwert produziert, sind nicht injektiv (da verschiedene Texte gleichen Hashwert haben können), sind surjektiv (um alle Hashwerte auszunutzen), und haben „gleich große“ Fasern (das macht gerade eine gute Hashfunktion aus!).

(vii) Verschlüsselungsfunktionen, etwa crypt : $\{0,1\}^k \to \{0,1\}^k$, sind injektiv, damit eine eindeutige Entschlüsselung möglich ist.

Übung. Man mache sich klar, dass eine Abbildung $f : M \to N$ genau dann injektiv ist, wenn für alle $x_1, \ldots, x_r \in M$ gilt:

$$x_1, \ldots, x_r \text{ paarweise verschieden} \Leftrightarrow f(x_1), \ldots, f(x_r) \text{ paarweise verschieden.}$$

1.4.5 Einschränkung

Definition. Es sei $f : M \to N$ eine Abbildung und $M' \subseteq M$. Dann heißt die Abbildung

$$f|_{M'} : M' \to N, \quad x \mapsto f(x)$$

die *Einschränkung* von f auf M'.

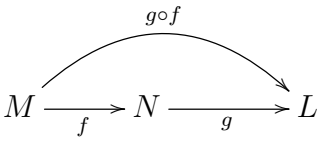
Bemerkung. Jede Abbildung kann durch Einschränkung auf eine geeignete Teilmenge des Definitionsbereichs injektiv gemacht werden. Z.B. ist für f aus Beispiel (1.4.4)(iii) die Einschränkung $f|_{\mathbb{R}_{\geq 0}}$ injektiv, ebenso wie die Einschränkung $f|_{\mathbb{R}_{\leq 0}}$.

1.4.6 Komposition

Definition. Es seien M, N, L Mengen. Weiter seien $f : M \to N$ und $g : N \to L$ zwei Abbildungen. Dann heißt die Abbildung

$$g \circ f : M \to L, \quad x \mapsto (g \circ f)(x) := g(f(x))$$

die *Komposition von g mit f.*



$$x \overset{f}{\longmapsto} f(x) \overset{g}{\longmapsto} g(f(x))$$

Beispiel. Für die Abbildungen

$$f : \mathbb{R} \to \mathbb{R}_{\geq 0}, \quad x \mapsto (x-3)^2,$$
$$g : \mathbb{R}_{\geq 0} \to \mathbb{R}, \quad x \mapsto \sqrt{x}$$

ergeben sich die Kompositionen

$$g \circ f : \mathbb{R} \to \mathbb{R}, x \mapsto \sqrt{(x-3)^2} = |x-3|,$$
$$f \circ g : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, \quad x \mapsto (\sqrt{x}-3)^2$$

Bemerkung. Es seien f, g, h Abbildungen.

(i) Es gilt $(h \circ g) \circ f = h \circ (g \circ f)$, sofern beide Seiten der Gleichung definiert sind. Daher kann die Komposition auch ohne Klammern kurz als $h \circ g \circ f$ geschrieben werden.

1.4.7 Umkehrabbildungen

Definition. Es seien $f : M \to N$ und $g : N \to M$ Abbildungen. Dann heißt g eine *linksseitige (rechtsseitige) Umkehrabbildung von* f, wenn $g \circ f = \mathrm{id}_M$ (wenn $f \circ g = \mathrm{id}_N$). Wir sprechen schlicht von einer *Umkehrabbildung von* f, wenn g sowohl links- als auch rechtsseitige Umkehrabbildung von f ist.

Satz a. *Sei $f : M \to N$ eine Abbildung und sei M nicht leer.*

(i) f besitzt genau dann eine linksseitige Umkehrabbildung, wenn f injektiv ist.

(ii) f besitzt genau dann eine rechtsseitige Umkehrabbildung, wenn f surjektiv ist.

(iii) f besitzt genau dann eine Umkehrabbildung, wenn f bijektiv ist.

Bemerkung. Existiert eine Umkehrabbildung, so ist sie eindeutig bestimmt (Übung). Links- und rechtsseitige Umkehrabbildungen sind im Allgemeinen nicht eindeutig (Beispiel unten).

Schreibweise. Falls f bijektiv ist, so wird die eindeutige Umkehrabbildung mit f^{-1} bezeichnet. Die ist nicht zu verwechseln mit dem Urbild, das ebenfalls mit f^{-1} bezeichnet wird. Was gemeint ist, ergibt sich aus dem Zusammenhang.

Beweis. (i) Es sind zwei Richtungen zu zeigen, wir zeigen zuerst den „wenn“-Teil. Dazu nehmen wir an, f sei injektiv und konstruieren eine linksseitige Umkehrabbildung g. Wähle $x_0 \in M$ beliebig ($M \neq \emptyset$) und definiere $g : N \to M$ durch

$$g(y) := \begin{cases} x & \text{falls } y = f(x) \text{ für ein } x \in M, \\ x_0 & \text{falls } y \notin f(M), \end{cases}$$

Das x in der ersten Zeile ist eindeutig, da f injektiv ist, also ist g wohldefiniert. Damit gilt $(g \circ f)(x) = g(f(x)) = x$ für alle $x \in M$, d.h. $g \circ f = \mathrm{id}_M$ wie gewünscht.

Wir zeigen jetzt die andere Richtung, den „genau dann“-Teil. Dazu nehmen wir an, $g : N \to M$ sei eine linksseitige Umkehrabbildung und folgern, dass f injektiv ist. Aus $g \circ f = \mathrm{id}_M$ folgt, dass für alle $x, x' \in N$ gilt:

$$f(x) = f(x') \Rightarrow g(f(x)) = g(f(x')) \Rightarrow \underbrace{(g \circ f)}_{=\mathrm{id}_N}(x) = \underbrace{(g \circ f)}_{=\mathrm{id}_N}(x') \Rightarrow x = x'.$$

Also ist f tatsächlich injektiv und der Beweis beendet.
(ii), (iii) siehe Vorlesung. □

Beispiel.

(i) $f : \mathbb{R} \to \mathbb{R}, x \mapsto 2x$ ist bijektiv mit der Umkehrabbildung

$$f^{-1} : \mathbb{R} \to \mathbb{R}, \quad x \mapsto \frac{1}{2}x$$

(ii) $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 1}, x \mapsto x^2 + 1$ ist bijektiv mit der Umkehrabbildung

$$f^{-1} : \mathbb{R}_{\geq 1} \to \mathbb{R}_{\geq 0}, \quad x \mapsto \sqrt{x - 1}$$

(iii) $f : \mathbb{Z} \to \mathbb{Q}, a \mapsto a$ ist injektiv, aber nicht surjektiv.

$$\begin{aligned} g \circ f = \mathrm{id}_{\mathbb{Z}} &: \text{z.B. } g(x) := \lfloor x \rfloor \text{ oder } g(x) := \lceil x \rceil \\ f \circ g = \mathrm{id}_{\mathbb{Q}} &: \text{nicht möglich} \end{aligned}$$

(Hier bezeichnet $\lfloor x \rfloor$ die größte ganze Zahl $\leq x$, und $\lceil x \rceil$ die kleinste ganze Zahl $\geq x$.)

(iv) $f : \mathbb{R} \to \mathbb{R}_{\geq 0}, x \mapsto |x|$ ist surjektiv, aber nicht injektiv.

$$\begin{aligned} g \circ f = \mathrm{id}_{\mathbb{R}} &: \text{nicht möglich} \\ f \circ g = \mathrm{id}_{\mathbb{R}_{\geq 0}} &: \text{z.B. } g(x) := x \text{ oder } g(x) := -x \end{aligned}$$

Satz b. *Es seien $f : M \to N$ und $g : N \to L$ zwei bijektive Abbildungen. Wenn $g \circ f$ definiert ist, so ist $g \circ f$ ebenfalls bijektiv und es gilt:*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Beweis. als Übung. □

Übung.

(i) Zeigen Sie die restlichen Teile der Bemerkung.

(ii) Zeigen Sie den Satz.

(iii) Gilt der Satz auch, wenn man bijektiv durch injektiv ersetzt?

(iv) Gilt der Satz auch, wenn man bijektiv durch surjektiv ersetzt?

1.4.8 Abbildungen einer Menge in sich

Sind $f, g : M \to M$ zwei Abbildungen einer Menge M in sich, so kann man stets die Kompositionen $f \circ g$ und $g \circ f$ bilden.

Definition. Es sei $f : M \to M$ eine Abbildung und es sei $n \in \mathbb{N}$. Dann setzen wir

$$f^n := \underbrace{f \circ \ldots \circ f}_{n\text{-mal}}, \quad f^0 := \mathrm{id}_M.$$

Falls f bijektiv ist, so definieren wir auch $f^{-n} := (f^{-1})^n$.

Bemerkung.

(i) Es gilt $f^n(x) = f(f(\cdots f(x)))$.

(ii) Für bijektive Abbildungen einer Menge in sich selbst haben wir die üblichen Potenzrechenregeln:

$$f^{a+b} = f^a \circ f^b \quad \text{und} \quad f^{ab} = (f^a)^b \quad \text{für alle } a, b \in \mathbb{Z}.$$

1.4.9 Die Mächtigkeit von Mengen

Definition a. Zwei Mengen M und N heißen *gleichmächtig*, wenn eine bijektive Abbildung $M \to N$ existiert.

Übung a. $\mathbb{N}, \mathbb{Z}$ und $\mathbb{Q}$ sind gleichmächtig.

Satz a (Cantor)**.** *Für jede Menge M sind M und* $\mathrm{Pot}(M)$ *nicht gleichmächtig.*

Beweis. Sei f eine beliebige Abbildung $f : M \to \mathrm{Pot}(M)$. Definiere $A_f := \{x \in M \mid x \notin f(x)\} \in \mathrm{Pot}(M)$. Angenommen, es gibt $m \in M$ mit $f(m) = A_f$. Falls $m \in A_f$, so folgt $m \notin f(m) = A_f$ (Widerspruch). Falls $m \notin A_f = f(m)$, so folgt $m \in A_f$ (Widerspruch). Also ist f nicht surjektiv. □

Übung b. Man folgere aus dem Satz:

(i) $\mathbb{N}$ und $\mathbb{R}$ sind nicht gleichmächtig.

(ii) Die Zusammenfassung aller Mengen ist keine Menge.

Nun können wir eine exakte Definition der Endlichkeit einer Menge geben.

Definition b. Es sei M eine Menge.

(i) M heißt *endlich*, wenn M gleichmächtig zu $\underline{n}$ für ein $n \in \mathbb{N}_0$ ist (Erinnerung: $\underline{0} = \emptyset$).

In diesem Fall definieren wir $|M| := n$, und nennen $|M|$ die *Mächtigkeit* von M (oder die *Anzahl der Elemente* von M).

(ii) M heißt *unendlich*, wenn M nicht endlich ist.

Für Abbildungen zwischen endlichen Mengen gibt es Beziehungen zwischen deren Mächtigkeit.

Bemerkung a. Es seien M, N endliche Mengen und $f : M \to N$ eine Abbildung. Dann gelten $|f(M)| \leq |M|$ und $|f(M)| \leq |N|$.

Übung c. Man folgere aus Bemerkung a, dass für eine injektive Abbildung $f : M \to N$ stets $|M| \leq |N|$ ist, und für eine surjektive Abbildung $f : M \to N$ stets $|M| \geq |N|$ ist.

Genauer kann man bei Abbildungen zwischen endlichen Mengen Injektivität, Surjektivität und Bijektivität wie folgt charakterisieren.

Satz b. *Es sei $f : M \to N$ eine Abbildung und M, N endlich.*

(i) *f injektiv* $\Leftrightarrow |f(M)| = |M|$.

(ii) *f surjektiv* $\Leftrightarrow |f(M)| = |N|$.

(iii) *Ist $|M| = |N|$, dann sind äquivalent:*

- *f injektiv*
- *f surjektiv*
- *f bijektiv*

Darauf beruht das berühmte Dedekind'sche Schubfachprinzip:

Bemerkung b. Werden m Objekte auf n Schubfächer verteilt, und ist $m > n$, dann gibt es ein Schubfach, welches mindestens zwei Objekte enthält.

Dies ist genau die Aussage: Sind M, N endliche Mengen mit $|M| > |N|$, und $f : M \to N$ eine Abbildung, dann ist f nicht injektiv.

Übung. Bestimmen Sie die Anzahl injektiver Abbildungen von $\underline{m}$ nach $\underline{n}$.

Übung. Es sei $f : M \to N$ eine Abbildung zwischen endlichen Mengen. Dann gilt

$$|M| < |N| \Rightarrow f \text{ nicht surjektiv.}$$

1.4.10 Kombinatorische Strukturen als Abbildungen

Tupel, Permutationen, Kombinationen und Multimengen (Definition erst in späterem Kapitel) können mit Abbildungen bestimmter Art identifiziert werden.

Beispiel. Es sei A eine Menge und $k \in \mathbb{N}$.

(i) Eine *k-Permutation* aus A ist eine injektive Abbildung $\underline{k} \to A$. Die Permutation $(a_1, \ldots, a_k)$ entspricht der Abbildung $f : \underline{k} \to A, i \mapsto a_i$.

(ii) Ist $|A| = n \in \mathbb{N}$, so ist eine Permutation aus A eine bijektive Abbildung $\underline{n} \to A$. Die Permutation $(a_1, \ldots, a_n)$ entspricht der Abbildung $f : \underline{n} \to A, i \mapsto a_i$.

(iii) Eine *k-Kombination* aus A ist eine Abbildung $A \to \{0, 1\}$ mit $|f^{-1}(\{1\})| = k$ (die Faser zu 1 hat k Elemente). Die Kombination $M \subseteq A$ entspricht der Abbildung $f : A \to \{0, 1\}$ mit $f(a) = 0$ falls $a \notin M$ und $f(a) = 1$ falls $a \in M$. Die Abbildung f bezeichnet man auch als *charakteristische Funktion* von M.

(iv) Eine *k-Multimenge* ist eine Abbildung $A \to \mathbb{N}_0$ mit $\sum_{a \in A} f(a) = k$. Die Multimenge $M \subseteq A$ entspricht der Abbildung $f : A \to \mathbb{N}_0$, wobei $f(a)$ angibt, wie oft a in M vorkommt. Die Abbildung f wird als *Häufigkeitsfunktion* von M bezeichnet.

Übung. Eine k-elementige Teilmenge M von A kann als k-Kombination oder als k-Multimenge aufgefasst werden. Vergleichen Sie die charakteristische Funktion von M mit der Häufigkeitsfunktion von M.

1.5 Relationen

1.5.1 Definition und Beispiele

Relationen drücken Beziehungen zwischen Elementen von zwei Mengen aus, z.B. wäre „liegt in“ eine Relation zwischen {Städte} und {Länder}. In der Informatik werden Relationen z.B. in relationalen Datenbanken verwendet.

Definition. Es seien M und N zwei Mengen.

(i) Eine Teilmenge $R \subseteq M \times N$ heißt *Relation zwischen M und N*, oder kürzer *Relation auf M* falls $M = N$. Für $(x, y) \in R$ schreiben wir auch xRy und sagen „x steht in Relation zu y bzgl. R“.

(ii) Eine Relation $R \subseteq M \times M$ auf M heißt

(R) *reflexiv*, falls xRx für alle $x \in M$,

(R') *antireflexiv*, falls nicht xRx für alle $x \in M$,

(S) *symmetrisch*, falls $xRy \Rightarrow yRx$ für alle $x, y \in M$,

(A) *antisymmetrisch*, falls $(xRy \wedge yRx) \Rightarrow x = y$ für alle $x, y \in M$,

(T) *transitiv*, falls $(xRy \wedge yRz) \Rightarrow xRz$ für alle $x, y, z \in M$.

(iii) Eine Relation, die (R), (S) und (T) erfüllt, heißt *Äquivalenzrelation.*

(iv) Eine Relation, die (R), (A) und (T) erfüllt, heißt *(partielle) Ordnung.*

(v) Eine Relation, die (R) und (T) erfüllt, heißt *Präordnung.*

(vi) Eine Ordnung heißt *Totalordnung*, wenn $xRy \vee yRx$ für alle $x, y \in M$.

Beispiel.

(i) $M = \mathbb{R}$ und $R =$„$\leq$“, d.h. $(x, y) \in R$ genau dann, wenn $x \leq y$.
„$\leq$“ ist reflexiv, antisymmetrisch und transitiv, also eine Ordnung.
„$\leq$“ ist sogar eine Totalordnung.

(ii) $M = \mathbb{R}$ und $R =$„$<$“, d.h. $(x, y) \in R \Leftrightarrow x < y$.
„$<$“ ist antisymmetrisch(!) und transitiv, aber weder reflexiv noch symmetrisch.

(iii) $M = \mathrm{Pot}(N)$ und $R =$„$\subseteq$“.
„$\subseteq$“ ist eine Ordnung. Falls $|N| \geq 2$, so ist „$\subseteq$“ jedoch keine Totalordnung, da z.B. für $\{1\}, \{2\} \in \mathrm{Pot}\,\{1, 2\}$ weder $\{1\} \subseteq \{2\}$ noch $\{2\} \subseteq \{1\}$ gilt.

(iv) $M = \mathbb{Z}$. Die *Teilbarkeitsrelation* „$|$“ ist erklärt durch $x \mid y$ genau dann, wenn ein $z \in \mathbb{Z}$ existiert mit $xz = y$. Sie ist reflexiv und transitiv, also eine Präordnung. Sie ist nicht antisymmetrisch, denn $1 \mid -1$ und $-1 \mid 1$ obwohl $1 \neq -1$. Also ist „$|$“ keine Ordnung auf $\mathbb{Z}$.

(v) Die *Teilbarkeitsrelation* „$|$“ ist eine Ordnung auf $\mathbb{N}$, aber keine Totalordnung.

(vi) Auf jeder Menge M stellt die *Gleichheit* „$=$“ eine Äquivalenzrelation dar mit $R = \{(x, x) \mid x \in M\}$.

(vii) Auf einer Menge M von Personen können zwei Relationen V und G erklärt werden durch:

$xVy :\Leftrightarrow x$ ist verwandt mit y,
$xGy :\Leftrightarrow x$ hat das gleiche Geburtsdatum (Tag und Monat) wie y.

Beide sind Äquivalenzrelationen. Ersetzt man „verwandt“ durch „erstgradig verwandt“, so ist V nicht mehr transitiv.

(viii) Jede Abbildung $f : M \to N$ kann als Relation zwischen M und N aufgefasst werden:

$$f = \{(x, f(x)) \mid x \in M\}.$$

Abbildungen sind also eine spezielle Art von Relationen.

(ix) Für jede Abbildung $f : M \to N$ kann man eine Relation R_f auf M erklären durch

$xR_fy :\Leftrightarrow f(x) = f(y)$ (d.h. x und y liegen in derselben Faser von f).

R_f ist eine Äquivalenzrelation.

(x) $M = \mathbb{Z}$. Die *Paritätsrelation* „$\equiv_2$“, definiert durch

$$x \equiv_2 y :\Leftrightarrow x - y \text{ gerade}$$

ist eine Äquivalenzrelation auf $\mathbb{Z}$.

(xi) Sei M eine Menge und $\leq$ eine Präordnung auf M. Definiere Relation $\diamond$ auf M durch

$$x \diamond y :\Leftrightarrow x \leq y \text{ und } y \leq x.$$

Dann ist $\diamond$ eine Äquivalenzrelation auf M.

Übung. Durch welche Datenstruktur würden Sie eine Relation auf einer endlichen Menge in einem Computerprogramm repräsentieren? Wie prüfen Sie anhand dieser Datenstruktur, ob die Relation reflexiv, symmetrisch bzw. antisymmetrisch ist?

Übung. Es seien R eine Relation auf A und $A' \subseteq A$. Dann ist $R' := R \cap (A' \times A')$ eine Relation auf A'. Man mache sich klar, dass jede der Eigenschaften aus Teil (ii) der Definition beim Übergang von R zu R' erhalten bleibt.

Übung. Welche Bedingung muss eine Relation $R \subseteq N \times M$ erfüllen, damit sie im Sinne von Beispiel (ix) als eine Abbildung von N nach M aufgefasst werden kann? Unter welcher Bedingung ist diese Abbildung injektiv, surjektiv bzw. bijektiv? Welche Relation gehört im bijektiven Fall zur Umkehrabbildung?

1.5.2 Äquivalenzrelationen

Definition. Es sei $\sim$ eine Äquivalenzrelation auf M. Für $x \in M$ heißt

$$[x] := [x]_\sim := \{y \in M \mid x \sim y\}$$

die *Äquivalenzklasse von* $\sim$ *zu* x. Die Menge aller Äquivalenzklassen von $\sim$ wird mit $M/_\sim$ bezeichnet.

Bemerkung. Es sei $\sim$ eine Äquivalenzrelation auf M. Dann gilt für alle $x, y \in M$:

(i) $x \in [x]_\sim$,

(ii) $y \in [x]_\sim \Leftrightarrow x \in [y]_\sim$,

(iii) $y \in [x]_\sim \Rightarrow [y]_\sim = [x]_\sim$.

Wegen (iii) bezeichnet man jedes Element einer Äquivalenzklasse als ein *Repräsentant* derselben.

Beweis. als Übung. □

Beispiel.

(i) Für die Gleichheitsrelation auf einer Menge M ist $[x]_= = \{x\}$ und $M/_= = \{\{x\} \mid x \in M\}$.

(ii) Für die Äquivalenzrelationen V und G aus Beispiel (1.5.1)(vii) gilt für jede Person P der Menge:

$$[P]_V = \{\text{Verwandte von } P\},$$
$$[P]_G = \{\text{Personen, die am gleichen Tag Geburtstag feiern wie } P\}.$$

(iii) Es sei $f : N \to M$ eine Abbildung und R_f die Äquivalenzrelation aus Beispiel (1.5.1)(ix). Dann ist

$$[x]_{R_f} = \{x' \in N \mid f(x) = f(x')\} = f^{-1}(\{x\}),$$

für jedes $x \in N$, und $M/_{R_f}$ ist die Menge der nicht-leeren Fasern von f.

(iv) Für die Paritätsrelation aus Beispiel (1.5.1)(x) ist

$$[0]_{\equiv_2} = \{a \in \mathbb{Z} \mid a \text{ gerade}\},$$
$$[1]_{\equiv_2} = \{a \in \mathbb{Z} \mid a \text{ ungerade}\},$$

und $M/_{\equiv_2} = \{[0]_{\equiv_2}, [1]_{\equiv_2}\}$.

(v) Betrachte die Teilbarkeitsrelation „|“ auf $\mathbb{Z}$. Dies ist eine Präordnung. Sei $\diamond$ die daraus gemäß Beispiel (1.5.1)(xi) gebildete Äquivalenzrelation (d.h. $z \diamond z' \Leftrightarrow z \mid z'$ und $z' \mid z$). Dann ist $[z]_\diamond = \{z, -z\}$.

Offensichtlich „partitioniert“ eine Äquivalenzrelation die Menge.

Satz. *Es sei M eine Menge.*

(i) Ist $\sim$ eine Äquivalenzrelation auf M, so ist $M/_\sim$ eine Partition von M.

(ii) Ist $\mathcal{P}$ eine Partition von M, so existiert eine Äquivalenzrelation $\sim$ auf M mit $M/_\sim = \mathcal{P}$.

Die Äquivalenzrelationen auf M entsprechen also den Partitionen von M.

Beweis.

(i) Sei $\sim$ eine Äquivalenzrelation auf M und setze $\mathcal{P} := M/_\sim$. Wegen $x \in [x]_\sim$ sind alle Äquivalenzklassen nicht leer und ihre Vereinigung ist ganz M. Es bleibt zu zeigen, dass die Äquivalenzklassen paarweise disjunkt sind (vgl. Definition (1.2.5)(iv)). Betrachte also zwei beliebige Klassen $[x]_\sim, [y]_\sim$ mit $x, y \in M$. Zu zeigen ist:

$$[x]_\sim \neq [y]_\sim \Rightarrow [x]_\sim \cap [y]_\sim = \emptyset,$$

bzw. die Kontraposition

$$[x]_\sim \cap [y]_\sim \neq \emptyset \Rightarrow [x]_\sim = [y]_\sim.$$

Ist aber $z \in [x]_\sim \cap [y]_\sim$, so folgt daraus nach Teil (iii) der Bemerkung $[x]_\sim = [z]_\sim = [y]_\sim$.

(ii) Durch die Vorschrift

$$x \sim y :\Leftrightarrow \ x \text{ und } y \text{ liegen in demselben Teil der Partition}$$

wird eine Äquivalenzrelation definiert. (Man überprüfe das!)
Die Äquivalenzklassen sind offensichtlich genau die Teile von $\mathcal{P}$.

□

1.5.3 Partielle Ordnungen

Es sei $\trianglelefteq$ eine partielle Ordnung auf M.

Definition. Ein Element $m \in M$ heißt *minimal* in M, falls kein $m' \in M$ existiert mit $m' \neq m$ und $m' \trianglelefteq m$. Ein Element $m \in M$ wird ein *Minimum* von M genannt, falls für alle $m' \in M$ gilt: $m \trianglelefteq m'$.

Analog definiert man *maximal* und *Maximum* (Übung).

Bemerkung a. Nach Definition bedeutet

$$\begin{aligned} m \text{ Minimum von } M: &\quad \text{für alle } x \in M \text{ gilt } m \trianglelefteq x. \\ m \text{ minimal in } M: &\quad \text{für alle } x \in M \text{ gilt } x \trianglelefteq m \Rightarrow x = m. \end{aligned}$$

Minimal zu sein ist also zu verstehen als „kein anderes ist kleiner“. Minimum zu sein ist also zu verstehen als „alle anderen sind größer“.

Beispiel. Wir betrachten die Teilbarkeitsrelation „|“ auf $\mathbb{N}$. Minimal zu sein bzgl. „|“ bedeutet „kein anderes ist Teiler“. Minimum zu sein bzgl. „|“ bedeutet „alle anderen sind Vielfache“.

(i) Die Menge $\{2, 3, 4, 6\}$ besitzt kein Minimum, hat aber die minimalen Elemente 2 und 3.

(ii) Die Menge $\{2, 3, 5\}$ besitzt kein Minimum, und jedes Element ist minimal.

(iii) Die Menge $\{2, 4, 6\}$ besitzt das Minimum 2, und 2 ist das einzige minimale Element.

Satz. *Es sei $\trianglelefteq$ eine partielle Ordnung auf M.*

(i) Jedes Minimum von M ist minimal in M.

(ii) Existiert ein Minimum von M, so ist es das einzige minimale Element in M. Insbesondere ist das Minimum eindeutig.

(iii) Bei einer Totalordnung ist jedes minimale Element in M auch Minimum von M (die Begriffe minimal und Minimum sind bei Totalordnungen also identisch).

Beweis. (i) Ist m ein Minimum und $x \trianglelefteq m$, so folgt $x = m$ wegen der Antisymmetrie ($m \trianglelefteq x \wedge x \trianglelefteq m \Rightarrow x = m$).

(ii) Sei m ein Minimum und sei m' minimal. Da m Minimum ist, gilt $m \trianglelefteq m'$. Da m' minimal ist, folgt daraus $m = m'$.

(iii) Sei $\trianglelefteq$ eine Totalordnung auf M und sei $m \in M$ minimal. Zu zeigen ist $m \trianglelefteq x$ für alle $x \in M$. Sei also $x \in M$ beliebig. Bei einer Totalordnung ist $m \trianglelefteq x$ oder $x \trianglelefteq m$. Im ersten Fall sind wir fertig. Im zweiten Fall folgt $x = m$, da m minimal ist, also $x \trianglelefteq m$ wegen der Reflexivität. □

Bemerkung b. Jede nicht-leere Teilmenge von $\mathbb{N}$ hat bzgl. der Ordnung $\leq$ ein Minimum. (Ohne Beweis; das ist ein Axiom der Mengenlehre.)

Übung. Jede endliche Menge mit partieller Ordnung hat ein minimales Element.

Übung. Formuliere Definition, Bemerkung a und Satz für *maximal* und *Maximum* aus.

Übung. Wir können die Begriffe minimal und Minimum auch definieren, wenn die Relation keine Ordnung ist. Zeigen Sie am Beispiel der Teilbarkeitsrelation auf $\mathbb{Z}$ (die keine Ordnung ist), dass dann der Satz nicht mehr gilt.

Kapitel 2

Algebraische Strukturen

2.1 Gruppen

2.1.1 Strukturen und Verknüpfungen

Definition. Eine *Verknüpfung* auf einer Menge M ist eine Abbildung

$$M \times M \to M.$$

Eine *algebraische Struktur* ist eine Menge mit ein oder mehreren Verknüpfungen.

Beispiel a.

(i) $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (x, y) \mapsto x - y$ ist eine Verknüpfung auf $\mathbb{Z}$.

(ii) Für jede Menge N ist $\circ$ eine Verknüpfung auf $\mathrm{Abb}(N, N)$.

(iii) $\wedge$ ist eine Verknüpfung auf $B = \{0, 1\}$ (wenn wir 0 und 1 als Wahrheitswerte definieren, und $\wedge$ durch die zugehörige Wahrheitstafel definiert ist).

(iv) Es sei A eine beliebige Menge und $n \in \mathbb{N}_0$. Sind $a_1, \ldots, a_n \in A$, so nennen wir $a_1 \cdots a_n$ ein *Wort* der Länge n über dem Alphabet A (formal ist $a_1 \cdots a_n$ das n-Tupel $(a_1, \ldots, a_n)$, wobei wir in diesem Kontext die Klammern und Kommas in der Notation der Tupel weglassen).

Es bezeichne ϵ das Wort der Länge 0 (das leere Wort oder leere Tupel), und A^* die Menge aller Wörter über A (beliebiger Länge) einschließlich ϵ. Dann wird durch

$$a_1 \cdots a_n * b_1 \cdots b_m := a_1 \cdots a_n b_1 \cdots b_m$$

eine Verknüpfung auf A^* definiert, die *Verkettung* oder *Konkatenation*.

Schreibweise. Es seien M eine Menge, $\bullet$ eine Verknüpfung auf M, $m \in M$, und $A, B \subseteq M$.

(i) $m \bullet A := \{m \bullet a \mid a \in A\} \subseteq M$

(ii) $A \bullet m := \{a \bullet m \mid a \in A\} \subseteq M$

(iii) $A \bullet B := \{a \bullet b \mid a \in A, b \in B\} \subseteq M$

Beispiel b.

$$7\mathbb{Z} = \{7a \,|\, a \in \mathbb{Z}\} = \{\ldots, -14, -7, 0, 7, 14, \ldots\},$$
$$2 + 7\mathbb{Z} = \{2 + 7a \mid a \in \mathbb{Z}\} = \{\ldots - 12, -5, 2, 9, 16, \ldots\}.$$

2.1.2 Monoide

Definition a. Es sei M eine Menge mit einer Verknüpfung

$$\bullet : M \times M \to M, (x, y) \mapsto x \bullet y.$$

Wir nennen $(M, \bullet)$ ein *Monoid*, wenn folgende Axiome gelten:

(G1) $(x \bullet y) \bullet z = x \bullet (y \bullet z)$ für alle $x, y, z \in M$.

(G2) Es existiert $e \in M$ mit $e \bullet x = x = x \bullet e$ für alle $x \in M$.

Das Monoid heißt *abelsch* oder *kommutativ*, wenn zusätzlich gilt:

(G4) $x \bullet y = y \bullet x$ für alle $x, y \in G$.

Man nennt (G1) das Assoziativgesetz und (G4) das Kommutativgesetz.

Bemerkung. Das Element e in (G2) ist eindeutig und wird das *neutrale Element* von M genannt.

Beweis. Sind $e, e' \in M$ zwei Elemente wie in (G2), so gilt einerseits $e \bullet e' = e$ und andererseits $e \bullet e' = e'$, also $e = e'$. □

Schreibweise.

(i) In einem Monoid $(M, \bullet)$ gilt $a_1 \bullet a_2 \bullet \cdots \bullet a_n := (\cdots((a_1 \bullet a_2) \bullet a_3) \bullet \cdots a_n)$ (oder jede andere Klammerung).

(ii) In einem abelschen Monoid benutzt man häufig $+$ als Verknüpfungszeichen, schreibt 0 statt e und na ($n \in \mathbb{N}$) als Abkürzung für $\underbrace{a + a + \cdots + a}_{n\text{-mal}}$.

(iii) Falls $\cdot$ als Verknüpfungszeichen benutzt wird, schreibt man häufig 1 statt e und a^n ($n \in \mathbb{N}$) als Abkürzung für $\underbrace{a \cdot a \cdot \ldots \cdot a}_{n\text{-mal}}$.

Beispiel a. Es sei A eine beliebige Menge, $B := \{0, 1\}$.

(i) $(\mathbb{N}, +)$ ist kein Monoid, da (G2) nicht gilt.

(ii) $(\mathbb{Z}, -)$ ist kein Monoid, da (G1) nicht gilt.

(iii) $(\mathbb{N}_0, +)$ ist ein abelsches Monoid mit neutralem Element 0.

(iv) $(\mathbb{R}, \cdot)$ ist ein abelsches Monoid mit neutralem Element 1.

(v) Für jede nicht-leere Menge A ist $(\mathrm{Abb}(A, A), \circ)$ ein Monoid mit neutralem Element id_A.

(vi) $(B, \wedge)$ ist ein abelsches Monoid mit neutralem Element 1.

(vii) $(B, \vee), (B, \mathrm{xor})$ sind abelsche Monoide mit neutralem Element 0.

(viii) $(B, \Rightarrow)$ ist kein Monoid, da (G1) nicht gilt. (man prüfe nach, dass z.B. $(0 \Rightarrow 0) \Rightarrow 0$ ungleich $0 \Rightarrow (0 \Rightarrow 0)$ ist).

(ix) $(A^*, *)$ ist Monoid mit neutralem Element ϵ.

Übung. Es sei A eine nicht-leere Menge. Man zeige, dass $(\mathrm{Abb}(A, A), \circ)$ genau dann abelsch ist wenn $|A| = 1$ ist.

2.1.3 Inverse und Einheiten

Definition. Es seien $(M, \bullet)$ ein Monoid mit neutralem Element e und $a \in M$.

(i) Gibt es $b \in M$ mit $a \bullet b = e$, so heißt a *rechtsinvertierbar* und b *rechtsinvers* zu a bzw. b ein *Rechtsinverses* von a.

(ii) Gibt es $b \in M$ mit $b \bullet a = e$, so heißt a *linksinvertierbar* und b *linksinvers* zu a bzw. b ein *Linksinverses* von a.

(iii) Ist a sowohl links- als auch rechtsinvertierbar, so heißt a eine *Einheit.*

(iv) Gibt es $b \in M$ mit $b \bullet a = e = a \bullet b$, so heißt a *invertierbar* und b *invers* zu a bzw. b ein *Inverses* von a.

Bemerkung. Es seien $(M, \bullet)$ ein Monoid und $a \in M$. Dann ist a genau dann eine Einheit, wenn a invertierbar ist. In diesem Fall ist jedes Linksinverse von a auch Rechtsinverses, und umgekehrt. Weiter ist das Inverse von a eindeutig durch a bestimmt und wird mit a^{-1} bezeichnet. Wir bezeichnen die Menge der Einheiten von M mit $M^\times$.

Beweis. Per Definition ist jedes invertierbare Element eine Einheit. Sei umgekehrt a eine Einheit, etwa $b, b' \in M$ mit $b \bullet a = e$ und $a \bullet b' = e$. Dann folgt $b = b \bullet e = b \bullet (a \bullet b') = (b \bullet a) \bullet b' = e \bullet b' = b'$. Also ist $b = b'$ und somit a invertierbar. Mit $b = b'$ sind auch alle weiteren Aussagen der Bemerkung gezeigt. □

Beispiel. Es sei A eine nicht-leere Menge. Wir betrachten ein Element $f : A \to A$ des Monoids $(\mathrm{Abb}(A, A), \circ)$.

(i) f ist genau dann rechtsinvertierbar, wenn f surjektiv ist.

(ii) f ist genau dann linksinvertierbar, wenn f injektiv ist.

(iii) f ist genau dann invertierbar, wenn f bijektiv ist.

Übung a. Es seien $(M, \bullet)$ ein Monoid, $a \in M$, und m_a die Abbildung

$$m_a : M \to M, x \mapsto a \bullet x.$$

Man zeige:

(i) m_a ist genau dann surjektiv, wenn a rechtsinvertierbar ist.

(ii) Ist a linksinvertierbar, so ist m_a injektiv.

Man gebe ein Beispiel dafür an, dass die Umkehrung von (ii) nicht gilt.

Übung b. Es seien $(M, \bullet)$ ein Monoid, $a, a' \in M^\times$ und $c \in M$. Man zeige:

(i) Es gilt $a^{-1} \in M^\times$ und $(a^{-1})^{-1} = a$.

(ii) Es gilt $a \bullet a' \in M^\times$ und $(a \bullet a')^{-1} = a'^{-1} \bullet a^{-1}$.

(iii) Die Gleichung $a \bullet x = c$ hat eine eindeutige Lösung $x \in M$.

(iv) Die Gleichung $x \bullet a = c$ hat eine eindeutige Lösung $x \in M$.

(v) Aus $a \bullet c = e$ folgt $c = a^{-1}$.

(vi) Aus $c \bullet a = e$ folgt $c = a^{-1}$.

2.1.4 Gruppen

Definition a. Ein Monoid $(G, \bullet)$, in dem alle Elemente invertierbar sind, heißt *Gruppe*. D.h. in einer Gruppe gilt:

(G3) Für alle $x \in G$ existiert $x' \in G$ mit $x \bullet x' = e = x' \bullet x$.

Beispiel a.

(i) $(\mathbb{Z}, +)$ ist eine abelsche Gruppe.

(ii) $(\mathbb{N}_0, +)$ ist keine Gruppe, da (G3) nicht gilt.

(iii) $(\mathbb{R}, \cdot)$ ist keine Gruppe, da (G3) nicht gilt.

(iv) $(\mathbb{R}\backslash\{0\}, \cdot)$ und $(\mathbb{R}_{>0}, \cdot)$ sind abelsche Gruppen.

(v) $(\mathbb{Z}\backslash\{0\}, \cdot)$ und $(\mathbb{N}, \cdot)$ sind keine Gruppen.

(vi) Sei A eine nicht-leere Menge und

$$S_A := \{f \in \mathrm{Abb}(A, A) \mid f \text{ ist invertierbar}\}.$$

Dann ist $(S_A, \circ)$ eine Gruppe, die *symmetrische Gruppe auf* A. Ist $A = \underline{n}$ für ein $n \in \mathbb{N}$, dann schreiben wir $S_n := S_{\underline{n}}$ und nennen S_n die *symmetrische Gruppe* auf n Ziffern.

(vii) $(B, \wedge), (B, \vee)$ sind keine Gruppen.

(viii) (B, xor) ist eine Gruppe.

(ix) $(A^*, *)$ ist keine Gruppe, da (G3) nicht gilt.

Schreibweise.

(i) In einer abelschen Gruppe benutzt man häufig $+$ als Verknüpfungszeichen, schreibt $-a$ für das Inverse von a, und benutzt die Abkürzungen: $a - b := a + (-b), (-n)a := n(-a)$ für $n \in \mathbb{N}$, $0a := 0$.

(ii) Falls $\cdot$ als Verknüpfungszeichen benutzt wird, schreibt man a^{-1} für das Inverse von a, 1 statt e, lässt $\cdot$ einfach weg, und benutzt die Abkürzungen: $a^{-n} := (a^{-1})^n$ für $n \in \mathbb{N}$, $a^0 := 1$. Falls die Gruppe abelsch ist, kann man auch a/b für ab^{-1} schreiben.

Bemerkung. Ist $(M, \bullet)$ ein Monoid, so ist $(M^\times, \bullet)$ eine Gruppe. Die Gruppe $(M^\times, \bullet)$ wird *Einheitengruppe* von M genannt.

Beweis. Zu zeigen ist, dass $\bullet$ eine Verknüpfung auf $M^\times$ ist, und dass für $a \in M^\times$ auch das Inverse von a in $M^\times$ liegt. Beides wurde in Übung 2.1.3b gezeigt. □

Satz. *Es sei $(G, \cdot)$ eine Gruppe und $a, b \in G$.*

(i) Für alle $c \in G$ gilt: $a = b \Leftrightarrow a \cdot c = b \cdot c$ und $a = b \Leftrightarrow c \cdot a = c \cdot b$. („Multiplikation" von links oder rechts in einer Gruppe ist eine Äquivalenzumformung*.)*

(ii) Die Gleichung $a \cdot x = b$ hat eine eindeutige Lösung $x \in G$ (ebenso die Gleichung $x \cdot a = b$).

Beweis.

(i) Die Implikation $a = b \Rightarrow a \cdot c = b \cdot c$ ist trivial. Damit folgt aber auch $a \cdot c = b \cdot c \Rightarrow (a \cdot c) \cdot c^{-1} = (b \cdot c) \cdot c^{-1}$, und die rechte Seite lautet $a = b$. Die Äquivalenz $a = b \Leftrightarrow c \cdot a = c \cdot b$ verläuft entsprechend mit Multiplikation von c^{-1} auf der linken Seite.

(ii) Nach (i) gilt $a \cdot x = b$ genau dann, wenn $x = a^{-1} \cdot (a \cdot x) = a^{-1} \cdot b$ ist. Entsprechend gilt $x \cdot a = b$ genau dann, wenn $x = (x \cdot a) \cdot a^{-1} = b \cdot a^{-1}$ ist.

□

Übung a. Bestimmen Sie zu allen Beispielen von Monoiden und Gruppen die neutralen bzw. inversen Elemente.

Übung b. Es sei A eine nicht-leere endliche Menge. Man zeige, dass S_A genau dann abelsch ist, wenn $|A| \leq 2$.

Übung c. Es seien $(G, \cdot)$ eine Gruppe und $a \in G$. Ist die Abbildung $\lambda_a : G \to G, x \mapsto a \cdot x$ injektiv, surjektiv, bijektiv?

2.1.5 Untergruppen

Definition. Es sei $(G, \cdot)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt *Untergruppe von G*, geschrieben $H \leq G$, wenn gilt:

(U1) $e \in H$.

(U2) Für alle $x, y \in H$ ist auch $x \cdot y^{-1} \in H$. (Wir sagen: H ist *abgeschlossen* bzgl. $\cdot$ und Invertieren.)

In diesem Fall ist H selbst eine Gruppe bzgl. der Verknüpfung $\cdot$ aus G.

Beispiel.

(i) Für jedes $n \in \mathbb{N}_0$ ist $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$ eine Untergruppe von $(\mathbb{Z}, +)$ (z.B. $3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$).

(ii) $\mathbb{N}$ ist keine Untergruppe von $(\mathbb{Z}, +)$.

(iii) $H := \{\pi \in S_n \mid \pi(n) = n\}$ ist eine Untergruppe von $(S_n, \circ)$.

(iv) $\mathbb{Q}_{>0}$ ist eine Untergruppe von $(\mathbb{R}_{>0}, \cdot)$.

(v) $\mathbb{N}$ ist keine Untergruppe von $(\mathbb{R}_{>0}, \cdot)$.

Beweis.

(i) (U1): $e = 0 = n \cdot 0 \in n\mathbb{Z}$.
(U2): $nx - ny = n(x - y) \in n\mathbb{Z}$.

(ii) (U1) gilt nicht, denn $e = 0 \notin \mathbb{N}$.

(iii) (U1): $e = \mathrm{id}_{\underline{n}}$ lässt n fest, also $\mathrm{id}_{\underline{n}} \in H$.
(U2): Seien $\sigma, \pi \in H$, d.h. $\sigma(n) = n$ und $\pi(n) = n$. Aus $\pi(n) = n$ folgt $\pi^{-1}(n) = n$. Weiter ergibt sich $\sigma \circ \pi^{-1}(n) = \sigma(\pi^{-1}(n)) = \sigma(n) = n$, d.h. $\sigma \circ \pi^{-1} \in H$.

(iv) (U1): $e = 1 \in \mathbb{Q}_{>0}$.
(U2): Sind $x, y \in \mathbb{Q}_{>0}$, so ist auch $xy^{-1} \in \mathbb{Q}_{>0}$.

(v) (U2) gilt nicht, da z.B. $2^{-1} \notin \mathbb{N}$.

□

2.1.6 Kartesische Produkte

Satz. *Es seien $(G, \cdot)$ eine Gruppe und M eine Menge. Die Menge $\mathrm{Abb}(M, G) = \{f : M \to G\}$ wird zu einer Gruppe $(\mathrm{Abb}(M, G), \bullet)$, wenn man die Verknüpfung*

$$\bullet : \mathrm{Abb}(M, G) \times \mathrm{Abb}(M, G) \to \mathrm{Abb}(M, G), (f, g) \mapsto f \bullet g$$

durch

$$(f \bullet g)(x) := f(x) \cdot g(x) \text{ für alle } x \in M$$

definiert. Da $\bullet$ durch $\cdot$ definiert ist schreibt man in der Regel $(\mathrm{Abb}(M, G), \cdot)$. Ist $(G, \cdot)$ abelsch, so ist auch $(\mathrm{Abb}(M, G), \cdot)$ abelsch.

Beispiel. Es sei $(G, \cdot)$ eine Gruppe. Die Gruppe $(G^{\underline{n}}, \cdot)$ ist dann die Menge

$$G^n = \{n\text{-Tupel über } G\} = \{(a_1, \ldots, a_n) \mid a_i \in G\}$$

mit *komponentenweiser* Verknüpfung, d.h.

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) := (a_1 \cdot b_1, \ldots, a_n \cdot b_n).$$

G^n wird das *n-fache kartesische Produkt* von G genannt.

Übung. Es seien $(G, \bullet)$ und $(G', \circ)$ zwei Gruppen. Man zeige, dass die Menge $G \times G'$ mit der Verknüpfung

$$(g_1, g_1') \cdot (g_2, g_2') := (g_1 \bullet g_2, g_1' \circ g_2')$$

wieder eine Gruppe ist.

2.2 Ringe

2.2.1 Definition und Beispiele

In $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ gibt es zwei Verknüpfungen $+$ und $\cdot$, die mittels der Distributivgesetze miteinander verbunden sind. Die entsprechende Abstraktion der Rechenregeln führt zu den Begriffen Ring und Körper.

Definition. Eine Menge R mit zwei Verknüpfungen

$$+ : R \times R \to R, \quad \text{und} \quad \cdot : R \times R \to R$$

heißt *Ring*, wenn folgende Bedingungen erfüllt sind:

(R1) $(R, +)$ ist eine abelsche Gruppe.

(R2) $(R, \cdot)$ ist ein Monoid.

(R3) $x \cdot (y + z) = x \cdot y + x \cdot z$ und $(x + y) \cdot z = x \cdot z + y \cdot z$ für alle $x, y, z \in R$.

Der Ring heißt *kommutativ*, wenn zusätzlich gilt:

(R4) $x \cdot y = y \cdot x$ für alle $x, y \in R$.

Beispiel.

(i) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring.

(ii) $R = \{0\}$ mit $0 + 0 := 0$ und $0 \cdot 0 := 0$ bildet den trivialen Ring.

(iii) Nicht-kommutative Ringe begegnen uns in der Linearen Algebra, z.B. der „Matrizenring“ und der „Endomorphismenring“.

Bemerkung. Die Gleichungen aus (R3) heißen *Distributivgesetze*. Man vereinbart in einem Ring, dass $\cdot$ stärker bindet als $+$, d.h. $a \cdot b + c$ steht für $(a \cdot b) + c$, und $a + b \cdot c$ für $a + (b \cdot c)$. (Punktrechnung geht vor Strichrechnung.) Dies spart Klammern und wurde in obiger Formulierung von (R3) bereits benutzt! Ferner wird vereinbart, dass $\cdot$ weggelassen werden kann, d.h. ab steht für $a \cdot b$. Das neutrale Element der Gruppe $(R, +)$ wird mit 0 bezeichnet und *Nullelement* bzw. kurz *Null* von R genannt. Das neutrale Element des Monoids $(R, \cdot)$ wird mit 1 bezeichnet und *Einselement* bzw. kurz *Eins* von R genannt. Wir nennen $-a$ das *additive Inverse* oder *negative* Element von a.

Übung a. Es sei R ein Ring. Man zeige:

(i) $0 \cdot a = a \cdot 0 = 0$ für alle $a \in R$.

(ii) $-a = (-1) \cdot a$ und $a = (-1) \cdot (-a)$ für alle $a \in R$.

(iii) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ für alle $a, b \in R$.

Beweis. Aus $0 = 0 + 0$ und dem Distributivgesetz folgt $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$. Addition von $-(0 \cdot a)$ auf beiden Seiten liefert $0 = 0 \cdot a$.
$a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = (1 + (-1)) \cdot a = 0 \cdot a = 0$. □

Übung b. Es sei R ein Ring. Für jedes $n \in \mathbb{N}$ und $a \in R$ definieren wir

$$na := \underbrace{a + \ldots + a}_{n\text{-mal}}.$$

Man zeige: $-(na) = n(-a)$. Wie definiert man sinnvoll na für alle $n \in \mathbb{Z}$?

Übung c. Man zeige: Ist R ein Ring mit $1 = 0$, so ist $R = \{0\}$.

Übung d. Es seien R, S zwei Ringe, $n \in \mathbb{N}$ und M eine Menge. Wie sind die Verknüpfungen zu definieren, mit denen auch $R \times S, R^n$ und $\mathrm{Abb}(M, R)$ zu einem Ring werden?

2.2.2 Einheitengruppe

Definition. Es sei R ein Ring. Die Begriffe *invertierbar*, *Einheit*, *Einheitengruppe* und die Notation $R^\times$ beziehen sich auf das Monoid $(R, \cdot)$.

Beispiel.

(i) $\mathbb{Z}^\times = \{1, -1\}$.

(ii) In jedem Ring R ist $1, -1 \in R^\times$. (1 und -1 können aber gleich sein, wie wir an den Beispielen $\mathbb{F}_2$ und $\mathbb{F}_4$ unten sehen werden.)

Übung a. Es seien R kommutativ, $a \in R$, und m_a bezeichne die Abbildung $m_a : R \to R, x \mapsto ax$. Man zeige die Äquivalenz folgender Aussagen:

(i) a ist Einheit.

(ii) m_a ist bijektiv.

(iii) Die Gleichung $ax = b$ ist für alle $b \in R$ eindeutig lösbar.

Insbesondere gilt für jedes $a \in R^\times$: $ax = 0 \Rightarrow x = 0$.

Übung b. Es seien R kommutativ, $a, b \in R$. Man zeige: $ab \in R^\times \Leftrightarrow a \in R^\times \wedge b \in R^\times$. Hieraus folgt, dass auch $R \setminus R^\times$ unter der Multiplikation abgeschlossen ist.

2.2.3 Nullteiler

Es sei R ein kommutativer Ring.

Definition. Ein Element $a \in R$ heißt *Nullteiler* von R, wenn $b \in R\setminus\{0\}$ existiert mit $ab = 0$. Der Ring R heißt *nullteilerfrei*, wenn er keine Nullteiler außer 0 enthält. Der Ring R heißt *Integritätsbereich*, wenn $1 \neq 0$ und R nullteilerfrei ist.

Bemerkung. Sei $a \in R$ und bezeichne m_a die Abbildung $m_a : R \to R, x \mapsto ax$. Dann sind äquivalent:

(i) a ist kein Nullteiler von R.

(ii) Für alle $x \in R$ gilt: $ax = 0 \Rightarrow x = 0$.

(iii) Für alle $x, x' \in R$ gilt: $ax = ax' \Rightarrow x = x'$. (Kürzungsregel)

(iv) Für alle $b \in R$ hat die Gleichung $ax = b$ höchstens eine Lösung.

(v) m_a ist injektiv.

Insbesondere sind Einheiten keine Nullteiler (nach Übung 2.2.2 ist m_a für Einheiten bijektiv). Weiter ist R genau dann nullteilerfrei, wenn für alle $a, b \in R$ gilt:

$$ab = 0 \Rightarrow (a = 0 \vee b = 0).$$

Beweis. Übung. □

Beispiel. $\mathbb{Z}$, alle Körper sowie der triviale Ring sind nullteilerfrei.

Beweis. als Übung. □

Übung a. Man zeige: 0 ist genau dann kein Nullteiler, wenn R der triviale Ring ist.

Übung b. Man zeige für alle $a, b \in R$: Ist a ein Nullteiler, so auch ab. Gilt auch die Umkehrung?

2.2.4 Körper

Definition. Ein kommutativer Ring R heißt *Körper*, wenn $1 \neq 0$ und $R^\times = R\backslash\{0\}$ gilt.

Ein Körper ist also ein nicht-trivialer Ring, in dem jedes von 0 verschiedene Element invertierbar ist.

Beispiel a. $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind Körper. Im Unterschied zu $\mathbb{Q}$ erfüllt $\mathbb{R}$ noch die „Vollständigkeitsaxiome“ und die „Anordnungsaxiome“, die man in der Analysis-Vorlesung lernt. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.

Es gibt aber auch endliche Körper.

Beispiel b. Definiert man auf der Menge $\{0, 1\}$ zwei Abbildungen $+, \cdot$ durch die *Verknüpfungstafeln*

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

so entsteht ein Körper (man prüfe alle Axiome nach!). Wir bezeichnen diesen Körper mit $\mathbb{F}_2$.

Identifiziert man 0 mit „falsch“ und 1 mit „wahr“, dann stellt man außerdem fest, dass $+$ gerade der Verknüpfung xor entspricht, und $\cdot$ der Verknüpfung $\wedge$.

Beispiel c. Die Menge $\mathbb{F}_4 := \{0, 1, a, b\}$ mit den Verknüpfungstafeln

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

bildet einen Körper.

Beweis. Übung. □

Bemerkung.

(i) Die Tafeln in Beispiel c sind bis auf Benennung der Elemente a, b eindeutig, d.h. es gibt genau einen Körper mit 4 Elementen (siehe Vorlesung oder vgl. [3], §2.2, 37-38, leicht lesbar).

(ii) Es gibt für jede Primzahlpotenz p^n genau einen Körper mit p^n Elementen (ohne Beweis). Dieser wird mit $\mathbb{F}_{p^n}$ bezeichnet (das $\mathbb{F}$ steht hier für „field“, engl. für Körper). Für $n = 1$ werden diese Körper weiter unten konstruiert: $\mathbb{F}_p$ ist identisch mit dem dort eingeführten „Restklassenring“ $\mathbb{Z}_p$.
Achtung: $\mathbb{F}_{p^n}$ für $n > 1$ wird in dieser Vorlesung nicht behandelt und ist insbesondere nicht identisch mit $\mathbb{Z}_{p^n}$, denn $\mathbb{Z}_{p^n}$ ist für $n > 1$ kein Körper.

(iii) Endliche Körper sind für die Informatik von besonderer Bedeutung, etwa in der Kodierungstheorie. Es sei daran erinnert, dass man ein Bit als Element des Körper $\mathbb{F}_2$ auffassen kann, ein Byte als Element des Körpers $\mathbb{F}_{256}$, usw.

Übung. Sind K, L zwei Körper, so ist der Ring $K \times L$ (mit komponentenweisen Operationen) *kein* Körper.

Beweis. Es gilt $(1, 0) \cdot (0, 1) = (0, 0)$. Nach Übung 2.2.2a ist $(1, 0)$ keine Einheit in $K \times L$. □

2.3 Polynome

In diesem Abschnitt sei K ein Körper. Der hier eingeführte Polynomring über K ist ein besonders wichtiges Beispiel für einen Integritätsbereich.

2.3.1 Definition und Beispiele

Definition.

(i) Ein *Polynom* über K in der *Unbestimmten* X ist ein Ausdruck der Form

$$f = \sum_{i=0}^{n} a_i X^i$$

mit $a_i \in K$ für alle $i = 0, \ldots, n$. Die a_i heißen die *Koeffizienten* des Polynoms, insbesondere heißt a_0 der *konstante* oder *absolute Koeffizient*.

(Koeffizienten, die gleich 0 sind können beliebig hinzugefügt oder weggelassen werden, ohne den Ausdruck zu verändern.)

(ii) Zwei Polynome $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{i=0}^{n} b_i X^i$ sind genau dann *gleich*, wenn $a_i = b_i$ für alle $i = 0, \ldots, n$.

(iii) Die Menge aller Polynome über K wird mit $K[X]$ bezeichnet.

(iv) Sind alle Koeffizienten von $f \in K[X]$ gleich 0, so heißt f das *Nullpolynom*, geschrieben $f = 0$.

(v) Ist $f \in K[X]$ nicht das Nullpolynom, dann wird das größte $i \in \mathbb{N}_0$, für das $a_i \neq 0$ ist, der *Grad* von f genannt und mit $\deg f$ bezeichnet. Für das Nullpolynom setzen wir $\deg 0 := -\infty$.

(vi) Ist $\deg f = n \geq 0$, so heißt a_n der *Leitkoeffizient* oder *Hauptkoeffizient* von f.

(vii) Ein Polynom heißt *normiert*, wenn der Hauptkoeffizient gleich 1 ist.

(viii) Ein Polynom f heißt *linear*, wenn $\deg f = 1$.

(ix) Ein Polynom f heißt *konstant*, wenn $\deg f \leq 0$ ist.

Schreibweise. Der Kürze halber schreibt man X^i statt $1X^i$, X statt X^1, a_0 statt a_0X^0, und $0X^i$ lässt man weg.

Beispiel.

(i) $f = 1X^4 + 0X^3 - \frac{1}{3}X^2 + 1X^1 - 2X^0 = X^4 - \frac{1}{3}X^2 + X - 2 \in \mathbb{R}[X]$.

(ii) $g = 1X^2 + 1X^1 + 0X^0 = X^2 + X \in \mathbb{F}_2[X]$.

Bemerkung a. Jedes Polynom $f \in K[X]$ definiert eine Abbildung $K \to K$ dadurch, dass man das „Einsetzen“ in die Unbestimmte als Zuordnungsvorschrift wählt. Diese Abbildung bezeichnen wir ebenfalls mit f, sprechen aber zur Unterscheidung von der *Polynomfunktion* zu f. Für jedes $a \in K$ nennen wir $f(a)$ den *Wert von* f an der Stelle a.

Die Polynome f und g aus dem Beispiel haben die Polynomfunktionen

$$f : \mathbb{R} \to \mathbb{R}, \quad a \mapsto f(a) = a^4 - \frac{1}{3}a^2 + a^1 - 2a^0 = a^4 - \frac{1}{3}a^2 + a - 2.$$

$$g : \mathbb{F}_2 \to \mathbb{F}_2, \quad a \mapsto g(a) = a^2 - a = 0.$$

(Man beachte, dass $a^2 - a = 0$ für alle $a \in \mathbb{F}_2$.)

Verschiedene Polynome können dieselbe Polynomfunktion haben (z.B. g und das Nullpolynom). Aus diesem Grund sind Polynomfunktionen und Polynome zu unterscheiden.

Bemerkung b. Jedes $a \in K$ kann als konstantes Polynom aX^0 aufgefasst werden. Auf diese Weise wird K zu einer Teilmenge von $K[X]$.

Bemerkung c. Für eine mathematisch präzise Definition des Polynombegriffs betrachtet man

$$K^{(\mathbb{N}_0)} := \{(a_i)_{i\in\mathbb{N}_0} \in K^{\mathbb{N}_0} \mid a_i = 0 \text{ für fast alle } i \in \mathbb{N}_0\}.$$

Hier bedeutet *fast alle*, wie in der Analysis, *alle, bis auf endlich viele*. Eine Folge $(a_i)_{i\in\mathbb{N}_0}$ liegt also genau dann in $K^{(\mathbb{N}_0)}$, wenn ein $N \in \mathbb{N}_0$ existiert mit $a_i = 0$ für alle $i \geq N$.

Das Polynom $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ kann durch die Folge seiner Koeffizienten

$$(a_0, a_1, a_2, \ldots, a_n, 0, 0, 0, \ldots) \in K^{(\mathbb{N}_0)}$$

definiert werden. Dies führt zu der Definition $K[X] := K^{(\mathbb{N}_0)}$.

In dieser Formulierung gilt dann für die Unbestimmte:

$$X = 1X = 1X^1 = (0, 1, 0, 0, 0, \ldots).$$

Konstante Polynome entsprechen den Folgen

$$a_0X^0 = (a_0, 0, 0, 0, \ldots), \quad a_0 \in K.$$

2.3.2 Der Polynomring

Für Polynome gibt es eine natürliche Addition und Multiplikation, die aus der Menge $K[X]$ einen Ring macht.

Definition. Für beliebige Polynome $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{i=0}^{m} b_i X^i$ aus $K[X]$ wird deren Summe und Produkt definiert als:

$$f + g := \sum_{i=0}^{\max\{n,m\}} (a_i + b_i)X^i,$$

$$f \cdot g := \sum_{i=0}^{n+m} c_i X^i \text{ mit } c_i := \sum_{k=0}^{i} a_k b_{i-k}.$$

Bemerkung.

(i) Mit dieser Addition und Multiplikation wird $K[X]$ ein kommutativer Ring. (Man prüfe die Ringaxiome nach!) Das neutrale Element der Addition ist das Nullpolynom, und das neutrale Element der Multiplikation ist das konstante Polynom $1 = 1X^0$.

(ii) Man kann Polynome auch als endliche Folgen auffassen, etwa das Polynom $-3X^2 + X + 2$ als die Folge $(2, 1, -3, 0, 0, \ldots)$. Somit haben wir die Inklusion $K[X] \subseteq \mathrm{Abb}(\mathbb{N}, K)$. Dabei stimmt die Addition in $K[X]$ mit der punktweisen Addition in $\mathrm{Abb}(\mathbb{N}, K)$ überein, nicht aber die Multiplikation.

(iii) K ist ein „Teilring“ von $K[X]$.

(iv) Für jedes $a \in K$ ist die Abbildung

(v) Es gelten die Gradformeln

$$\deg(f + g) \leq \max\{\deg f, \deg g\},$$
$$\deg(f \cdot g) = \deg f + \deg g.$$

(vi) $K[X]$ ist nullteilerfrei.

(vii) In $K[X]$ gilt die Kürzungsregel, d.h. für alle $f, g, h \in K[X]$ mit $f \neq 0$ gilt:

$$fg = fh \Rightarrow g = h.$$

(viii) Die Einheitengruppe des Ringes $K[X]$ lautet

$$K[X]^\times = \{f \in K[X] \mid \deg f = 0\} = \{\text{konstante Polynome} \neq 0\}$$
$$= K^\times = K \backslash \{0\}.$$

Beweis. Übung. □

2.4 Teilbarkeitslehre in kommutativen Ringen

Hier definieren wir die Teilbarkeitsrelation in kommutativen Ringen und leiten einige Eigenschaften davon her. Wir werden die Ergebnisse hauptsächlich auf den Ring $\mathbb{Z}$ der ganzen Zahlen und den Polynomring $K[X]$ über dem Körper K anwenden.

2.4.1 Teilbarkeitsrelation

Es sei R ein kommutativer Ring.

Definition a. Es seien $a, b \in R$. Wir sagen *a teilt b* bzw. *b ist Vielfaches von a*, geschrieben $a \mid b$, wenn ein $x \in R$ existiert mit $ax = b$.

Bemerkung a. Die Relation $\mid$ auf R ist reflexiv und transitiv. Für alle $a, b, c \in R$ und alle $u, v \in R^\times$ gelten:

(i) $a \mid b \Rightarrow a \mid bc$,

(ii) $(a \mid b \wedge a \mid c) \Rightarrow a \mid b + c$,

(iii) $a \mid 0$,

(iv) $0 \mid a \Leftrightarrow a = 0$,

(v) $a \mid b \Leftrightarrow ua \mid vb$.

Beweis. Siehe Vorlesung. □

Übung a. Es seien $a, b, c \in R$. Man zeige, dass aus zwei der folgenden Aussagen die dritte folgt:

(i) $a \mid b$

(ii) $a \mid c$

(iii) $a \mid b + c$

Definition b. Wir nennen $a, b \in R$ *assoziiert*, geschrieben $a \sim b$, wenn ein $u \in R^\times$ existiert mit $au = b$. Aus $a \sim b$ folgt offensichtlich $a \mid b$ und $b \mid a$.

Erinnerung (vgl. Abschnitt 2.2.3): R heißt Integritätsbereich, wenn $1 \neq 0$ ist und aus $ab = 0$ für $a, b \in R$ folgt: $a = 0$ oder $b = 0$.

Bemerkung b. Es sei R ein Integritätsbereich und $a, b \in R$. Dann sind äquivalent:

(i) $a \mid b$ und $b \mid a$,

(ii) $a \sim b$.

Beweis. (i) $\Rightarrow$ (ii): Es seien $x, y \in R$ mit $b = ax$ und $a = by$. Dann ist $b = ax = byx$. Ausklammern von b liefert $b(1 - yx) = 0$. Ist $b = 0$, dann auch $a = by = 0$ und es gilt $a \sim b$. Sei nun $b \neq 0$. Da R ein Integritätsbereich ist folgt $1 - yx = 0$, also $yx = 1$. Damit ist $x \in R^\times$ und somit $a \sim b$.
(ii) $\Rightarrow$ (i): Das ist Bemerkung b. □

Beispiel. (i) In $\mathbb{Z}$ gilt: $a \sim b \Leftrightarrow |a| = |b|$. Die Relation $\mid$ auf $\mathbb{Z}$ ist also nicht antisymmetrisch.

(ii) Die Relation $\mid$ auf $\mathbb{N}$ ist eine partielle Ordnung.

(iii) Es sei K ein Körper und $R = K[X]$ der Polynomring über K in der Unbestimmten X. Auf der Menge der normierten Polynome aus $K[X]$ bildet $\mid$ eine partielle Ordnung. Aus $f \mid g$ folgt offensichtlich $\deg f \leq \deg g$.

Übung b. (i) Man zeige, dass $\sim$ eine Äquivalenzrelation auf R ist. Die Äquivalenzklassen $[a]_\sim$ bzgl. $\sim$ heißen die *Assoziiertenklassen* von R.

(ii) Wie sehen die Assoziiertenklassen von $\mathbb{Z}$ aus?

(iii) Wie sehen die Assoziiertenklassen von $K[X]$ aus?

(iv) Die Assoziiertenklasse von 1 ist $R^\times$.

(v) Nach Teil (v) von Bemerkung a hängt die Relation $a \mid b$ nur von den Assoziiertenklassen von a und b ab. Die Relation $\mid$ lässt sich also als eine Relation $|_\sim$ auf der Menge $R/_\sim$ der Assoziiertenklassen von R auffassen. Man zeige, dass $|_\sim$ reflexiv und transitiv ist.

Übung c. Man zeige: Ist b eine Einheit in R und $a \mid b$, so ist auch a eine Einheit.

2.4.2 Ideale

Es sei R ein kommutativer Ring.

Definition. Eine Teilmenge $I \subseteq R$ von R heißt *Ideal* von R, falls gilt:

(i) I ist Untergruppe der additiven Gruppe $(R, +)$.

(ii) $RI \subseteq I$, das heißt $ra \in I$ für alle $r \in R$ und $a \in I$.

Bemerkung. Für Elemente $a_1, \ldots, a_k \in R$ definieren wir

$$(a_1, \ldots, a_k) = \{r_1 a_1 + \ldots + r_k a_k \mid \ r_1, \ldots, r_k \in R\}.$$

Dann ist $(a_1, \ldots, a_k)$ das kleinste Ideal, das $a_1, \ldots, a_k$ enthält, und wird *das von $a_1, \ldots, a_r$ erzeugte Ideal* genannt. Ideale, die von einem Element erzeugt werden, d.h. Ideale von der Form (a), heißen *Hauptideale*. Für alle $a, b \in R$ gelten:

(i) $a \mid b \Leftrightarrow (a) \supseteq (b)$

(ii) $a \sim b \Rightarrow (a) = (b)$

Beweis. Als Übung. □

Übung a. Man zeige, dass mit zwei Idealen $I, J \subseteq R$ auch $I \cap J$ ein Ideal von R ist.

Übung b. Es sei R ein Integritätsbereich. Man zeige, dass für alle $a, b \in R$ gilt:

$$(a) = (b) \Leftrightarrow a \sim b.$$

Es gibt also eine Bijektion zwischen $R/_\sim$ (die Menge der Assoziiertenklassen) und der Menge der Hauptideale $\mathcal{P}$ von R, die die Relation $|_\sim$ in die partielle Ordnung $\supseteq$ auf $\mathcal{P}$ überführt. Insbesondere ist $|_\sim$ eine partielle Ordnung.

Frage: Gibt es einen nicht nullteilerfreien Ring, der dies erfüllt?

2.4.3 Division mit Rest in $\mathbb{Z}$

Satz. *Für alle $a, b \in \mathbb{Z}$ mit $b \neq 0$ existieren eindeutig bestimmte $q, r \in \mathbb{Z}$ mit $a = qb + r$ und $0 \leq r < |b|$.*

Beweis. Wegen $a = qb + r \Leftrightarrow a = (-q)(-b) + r$ können wir oBdA $b \geq 0$ annehmen. Eindeutigkeit: Angenommen, wir haben $q, q', r, r' \in \mathbb{Z}$ mit $qb+r = q'b + r'$ und $0 \leq r, r' < b$. Nach Annahme ist $(q - q')b = r' - r$, also $b \mid r' - r$. Ebenfalls nach Annahme ist $0 \leq r' - r < b$. Es folgt $r' - r = 0$ bzw. $r' = r$. Da $\mathbb{Z}$ nullteilerfrei ist und $b \neq 0$, folgt aus $(q - q')b = 0$ auch $q = q'$.

Existenz: Wähle q maximal mit $qb \leq a$ und setze $r := a - qb$. (Die Wahl von q bedeutet $q := \lfloor a/b \rfloor$.) Damit ist $r \geq 0$ klar. Wir zeigen $r < b$ mit einem Widerspruchsbeweis. Angenommen $r \geq b$. Dann ist $a = r + qb \geq (q + 1)b$. Das steht im Widerspruch zur Maximalität von q, also ist die Annahme $r \geq b$ falsch und die Behauptung $r < b$ bewiesen. □

Beispiel. $-237 = (-12) \cdot 21 + 15, 0 \leq 15 < 21$.
Man beachte $(-11) \cdot 21 = -231 > -237$ und $(-12) \cdot 21 = -252 \leq -237$.

2.4.4 Division mit Rest in $K[X]$

In diesem Abschnitt sei K ein Körper. wir haben in $K[X]$ ein analoges Ergebnis zur Division mit Rest in $\mathbb{Z}$, die *Polynomdivision*.

Satz. *Es seien $f, g \in K[X]$ mit $g \neq 0$. Dann existieren eindeutige $q, r \in K[X]$ mit $f = qg + r$ und $\deg r < \deg g$.*

Beweis. Eindeutigkeit: Angenommen, wir haben $q, q', r, r' \in K[X]$ mit $qg + r = q'g + r'$ und $\deg r, r' < \deg g$. Dann ist $(q - q')g = r' - r$, also

$$\deg(q - q') + \deg g = \deg(r' - r) \leq \max\{\deg r', \deg r\} < \deg g.$$

Es folgt $\deg(q-q') < 0$, d.h. $q-q' = 0$. Somit ist $q = q'$ und $r = r'$.

Existenz: Wir können $\deg f \geq \deg g$ annehmen, denn sonst ist $f = 0 \cdot g + f$ und $\deg f < \deg g$. Zusammen mit der Voraussetzung $g \neq 0$ haben wir $\deg f \geq \deg g \geq 0$ und können somit eine vollständige Induktion nach $\deg f$ führen.
Induktionsanfang ($\deg f = 0$): Dann ist auch $\deg g = 0$, d.h. f und g sind beide konstant und ungleich 0. Für $f = a_0$ und $g = b_0$ mit $a_0, b_0 \in K\backslash\{0\}$ gilt aber $f = \frac{a_0}{b_0} \cdot g + 0$ und $\deg 0 = -\infty < 0 = \deg g$. Damit ist der Induktionsanfang erledigt.
Induktionsschritt: Sei jetzt $\deg f = n > 0$ und sei die Existenz von q und r für alle f mit $\deg f < n$ bereits bewiesen (Ind.Vor.). Es seien $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{i=0}^{m} b_i X^i$ mit $a_n, b_m \neq 0$ und $m \leq n$. Setzt man

$$f' := f - \frac{a_n}{b_m} X^{n-m} g,$$

so ist $\deg f' < n$. Nach Induktionsvoraussetzung gibt es $q', r \in K[X]$ mit $f' = q'g + r$ und $\deg r < \deg g$. Es folgt $f = (\frac{a_n}{b_m} X^{n-m} + q')g + r$, d.h. $q := \frac{a_n}{b_m} X^{n-m} + q'$ und r sind wie gewünscht. □

Bemerkung. In der Formulierung und im Beweis des Satzes benutzen wir die Konvention $-\infty = \deg 0 < \deg h$ für alle $0 \neq h \in K[X]$. Wem diese Konvention missfällt, darf stattdessen die Aussage wie folgt lesen: *Dann existieren eindeutig bestimmte $q, r \in K[X]$ mit $f = qg + r$ und $r = 0$ oder $r \neq 0$ und $\deg r < \deg g$.*

Beispiel. $f = 2X^3 - 9X^2 + 4X, g = X^2 - 3X - 4 \in \mathbb{Q}[X]$. Wir dividieren f durch g mit Rest:

$$\begin{array}{rrl} (2X^3 & -9X^2+ & 4X) : (X^2 - 3X - 4) = 2X - 3 \\ -(2X^3 & -6X^2- & 8X) \\ \hline & -3X^2+ & 12X \\ & -(-3X^2+ & 9X + 12) \\ \hline & & 3X - 12 \end{array}$$

Also

$$f = \underbrace{(2X-3)}_{q} \cdot g + \underbrace{3X - 12}_{r}, \quad \deg r = 1 < 2 = \deg g.$$

2.4.5 Nullstellen

Wie im vorigen Abschnitt sei K ein Körper. Bevor wir die Theorie weiterentwickeln, führen wir den wichtigen Begriff des Ringhomomorphismus ein.

Definition a. Es seien R und S zwei kommutative Ringe. Eine Abbildung $\varphi : R \to S$ heißt *Ringhomomorphismus*, wenn gilt:

(i) $\varphi(r + r') = \varphi(r) + \varphi(r')$ für alle $r, r' \in R$;

(ii) $\varphi(rr') = \varphi(r)\varphi(r')$ für alle $r, r' \in R$;

(iii) $\varphi(1) = 1$.

Ein wichtiger Ringhomomorphismus ist das Einsetzen eines Körperelements in Polynome.

Bemerkung a. Es sei $x \in K$ fest. Wir betrachten die Abbildung

$$\tau_x : K[X] \to K, \quad f \mapsto f(x).$$

Jedem Polynom $f \in K$ wird also der Wert der durch f definierten Polynomfunktion an der Stelle x zugeordnet. Dann ist τ_x eine Ringhomomorphismus, der *Einsetzungshomomorphismus* zu x.

Beweis. Wir weisen die Bedingungen aus Definition a für τ_x nach. Dazu seien $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{i=0}^{n} b_i X^i$ in $K[X]$.

(i) Es ist zu zeigen: $\tau_x(f + g) = \tau_x(f) + \tau_x(g)$. Dies ist äquivalent zu $(f + g)(x) = f(x) + g(x)$. Es ist $f + g = \sum_{i=0}^{n}(a_i + b_i)X^i$, also

$$\begin{aligned}(f+g)(x) &= \sum_{i=0}^{n}(a_i + b_i)x^i \\ &= \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i \\ &= f(x) + g(x).\end{aligned}$$

(ii) Es ist zu zeigen: $\tau_x(fg) = \tau_x(f)\tau_x(g)$. Dies ist äquivalent zu $(fg)(x) = f(x)g(x)$. Es ist $fg = \sum_{i=0}^{2n} c_i X^i$, mit $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. Es gilt:

$$\begin{aligned}f(x)g(x) &= \left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{i=0}^{n} b_i x^i\right) \\ &= \sum_{i=0}^{2n} c_i x^i \\ &= fg(x),\end{aligned}$$

wobei die zweite Gleichung aus dem Distributivgesetz in K folgt.

(iii) Das Einselement in $K[X]$ ist das konstante Polynom $1 = 1X^0$, also ist $\tau_x(1) = 1$.

□

Definition b. Wir sagen $a \in K$ ist *Nullstelle* eines Polynoms $f \in K[X]$, wenn $f(a) = 0$ gilt, d.h. wenn die durch f definierte Polynomfunktion an der Stelle a den Wert 0 hat.

Satz. *Es seien $f \in K[X]$ und $a \in K$. Dann gilt:*

$$f(a) = 0 \Leftrightarrow X - a \text{ teilt } f.$$

Beweis. $\Leftarrow$: Es sei $f = (X - a) \cdot g$ mit $g \in K[X]$. Da τ_a (das Einsetzen von a) ein Homomorphismus ist, folgt $f(a) = (a - a) \cdot g(a) = 0$.

$\Rightarrow$: Es sei $f(a) = 0$. Nach Polynomdivision gibt es eindeutig bestimmte $q, r \in K[X]$ mit $f = q \cdot (X - a) + r$ und $\deg r < \deg(X - a) = 1$. Das bedeutet, dass r konstant ist, also $r = r_0 \in K$. Da τ_a ein Homomorphismus ist, folgt $0 = f(a) = q(a)(a - a) + r(a) = q(a) \cdot 0 + r(a) = r_0$. Somit ist r das Nullpolynom und $f = (X - a) \cdot q$. □

Definition c. Es seien $0 \neq f \in K[X]$ und $a \in K$. Die Teiler von f der Form $X - a$ werden *Linearfaktoren* von f genannt. Weiter heißt

$$\max\{n \in \mathbb{N}_0 \mid (X - a)^n \text{ teilt } f\}$$

die *Vielfachheit von a* als Nullstelle von f.

Bemerkung b. Wegen der Gradformel aus Bemerkung (2.3.2) ist die Vielfachheit stets $\leq \deg f$, also insbesondere endlich. Der Satz besagt, dass a genau dann Nullstelle von $f \neq 0$ ist, wenn a Vielfachheit ≥ 1 hat.

2.4.6 Zerlegung in Linearfaktoren

Weiterhin sei K ein Körper.

Satz. *Es sei $0 \neq f \in K[X]$. Sind $a_1, \ldots, a_l$ paarweise verschiedene Nullstellen von f mit den Vielfachheiten $n_1, \ldots, n_l$, so gilt*

$$f = (X - a_1)^{n_1} \cdots (X - a_l)^{n_l} \cdot g \tag{2.1}$$

für ein $0 \neq g \in K[X]$ mit $g(a_1), \ldots, g(a_l) \neq 0$.

Beweis. Wenn f die Zerlegung (2.1) hat, dann folgt $g(a_i) \neq 0$ aus der Maximalität der n_i. In der Tat, falls $g(a_i) = 0$ dann würde g nach Satz 2.4.5 von $X - a_i$ geteilt werden, woraus $(X - a_i)^{n_i+1} \mid f$ folgt.

Wir zeigen nun per Induktion nach l, dass die Zerlegung (2.1) existiert. Für $l = 1$ folgt das aus der Definition der Vielfachheit. Sei also $l > 1$ und die Behauptung für $l - 1$ bereits bewiesen. Dann gibt es $0 \neq g \in K[X]$ mit $f = (X - a_1)^{n_1} \cdots (X - a_{l-1})^{n_{l-1}} \cdot g$. Setzen wir $h := (X - a_1)^{n_1} \cdots (X - a_{l-1})^{n_{l-1}}$, so erhalten wir $f = hg$. Da die $a_1, \ldots, a_l$ paarweise verschieden sind, ist $h(a_l) = (a_l - a_1)^{n_1} \cdots (a_l - a_{l-1})^{n_{l-1}} \neq 0$. Nach Voraussetzung gilt $(X - a_l)^{n_l} \mid f = hg$. Das folgende Lemma zeigt, dass dann g von $(X - a_l)^{n_l}$ geteilt wird. Damit ist die Behauptung bewiesen. □

Lemma. *Es seien $g, h \in K[X], a \in K$ und $n \in \mathbb{N}$. Aus $(X - a)^n \mid hg$ und $h(a) \neq 0$ folgt $(X - a)^n \mid g$.*

Beweis. Induktion nach n. Sei $n = 1$: Wegen $X - a \mid hg$ gilt $h(a)g(a) = (hg)(a) = 0$, also $g(a) = 0$ denn $h(a) \neq 0$. Nach Satz 2.4.5 bedeutet das $X - a \mid g$.

Sei nun $n > 1$ und die Behauptung für $n-1$ bereits bewiesen. Sei $(X-a)^n \mid hg$. Da insbesondere $X - a \mid hg$, so folgt nach der Überlegung für $n = 1$, dass $X - a \mid g$. Sei $g = (X - a) \cdot g'$, also $(X - a)^n \mid hg = (X - a)hg'$. Mit der Kürzungsregel in $K[X]$ folgt $(X - a)^{n-1} \mid hg'$, und daraus nach Induktionsvoraussetzung $(X - a)^{n-1} \mid g'$. Insgesamt also $(X - a)^n \mid g$. □

Folgerung. *Es sei $0 \neq f \in K[X]$. Sind $a_1, \ldots, a_l$ paarweise verschiedene Nullstellen von f mit den Vielfachheiten $n_1, \ldots, n_l$, so gilt $\sum_{i=1}^{l} n_i \leq \deg f$.*

Das heißt, jedes Polynom f hat höchstens $\deg f$ viele Nullstellen, wenn jede Nullstelle mit ihrer Vielfachheit gezählt wird.

Beweis. Folgt sofort aus dem Satz. □

Definition. Es sei $0 \neq f \in K[X]$. Wir sagen *f zerfällt vollständig in Linearfaktoren* (über K), wenn es paarweise verschiedenen Nullstellen $a_1, \ldots, a_l$ gibt, deren Vielfachheiten $\sum_{i=1}^{l} n_i = \deg f$ erfüllen. Das ist genau dann der Fall, wenn es eine Zerlegung

$$f = c(X - a_1)^{n_1} \cdots (X - a_l)^{n_l}$$

gibt mit $c \in K$ konstant.

2.4.7 Fundamentalsatz der Algebra

Satz. *Jedes Polynom $f \in \mathbb{C}[X]$ zerfällt vollständig in Linearfaktoren.*

Beispiel.

$$\begin{aligned} f(X) &= X^4 - 1 = (X^2 - 1)(X^2 + 1) \\ &= (X + 1)(X - 1)(X^2 + 1) \\ &= (X + 1)(X - 1)(X - i)(X + i) \end{aligned}$$

Folgerung. *Jedes Polynom $f \in \mathbb{R}[X]$ besitzt eine Zerlegung $f = f_1 \dots f_l$ mit allen $f_i \in \mathbb{R}[X]$ und $\deg f_i \leq 2$.*

Beweis. Für $z = a + bi \in \mathbb{C}$ mit $a, b \in \mathbb{R}$ heißt $\overline{z} = a - bi$ das *konjugierte Element* zu z. Offensichtlich gilt $\overline{z} = z$ genau dann, wenn $z \in \mathbb{R}$. Da die Abbildung $\mathbb{C} \to \mathbb{C}, z \mapsto \overline{z}$ ein Ringisomorphismus ist (man prüfe das nach!), gilt $f(\overline{z}) = \overline{f(z)}$. Folglich ist $f(z) = 0 \Leftrightarrow f(\overline{z}) = 0$. Die komplexen (nicht-reellen) Nullstellen treten also in Paaren, bestehend aus z und $\overline{z}$, auf. Somit hat f nach dem Fundamentalsatz eine Zerlegung der Form

$$f = c(X - a_1) \cdots (X - a_r)(X - z_1)(X - \overline{z_1}) \cdots (X - z_s)(X - \overline{z_s})$$

mit $a_1, \dots, a_r \in \mathbb{R}, z_1, \dots, z_s \in \mathbb{C} \backslash \mathbb{R}, c \in \mathbb{C}$ und $r + 2s = \deg f$. Man sagt, das Polynom f hat r reelle Nullstellen und s Paare komplex-konjugierter Nullstellen. Die Behauptung folgt nun, weil

$$(X - z)(X - \overline{z}) = X^2 - (z + \overline{z})X + z\overline{z} \in \mathbb{R}[X].$$

(Man prüfe nach, dass $z + \overline{z}$ und $z\overline{z}$ tatsächlich reell sind!) □

2.5 Der Euklidische Algorithmus

In diesem Abschnitt sei K ein Körper und R einer der beiden folgenden Ringe: $R = \mathbb{Z}$, der Ring der ganzen Zahlen, oder $R = K[X]$, der Polynomring in der Unbestimmten X über dem Körper K. Der Ring R ist kommutativ und nullteilerfrei, also ein Integritätsbereich.

2.5.1 Der ggT

Wir ziehen eine erste Folgerung aus der Division mit Rest. Dazu führen wir die folgende Notation ein.

Notation. Sei $R = \mathbb{Z}$ oder $R = K[X]$. Für $0 \neq a \in R$ setzen wir

$$\nu(a) := \begin{cases} |a|, & \text{falls } R = \mathbb{Z} \\ \deg a, & \text{falls } R = K[X] \end{cases}$$

Bemerkung a. Sei I ein Ideal in R. Dann existiert $g \in R$ mit $I = (g) = gR$.

Beweis. Ist $I = \{0\}$, nehme $g = 0$. Sei also $I \neq \{0\}$ und $g \in I \setminus \{0\}$ mit $\nu(g)$ minimal unter allen Elementen aus $I \setminus \{0\}$. Sei $f \in I$. Wir müssen zeigen: $f \in (g)$, d.h. $g \mid f$. Dazu dividieren wir f durch g mit Rest. Aus den Sätzen 2.4.3 und 2.4.4 erhalten wir $q, r \in R$ mit $f = qg + r$ und $r = 0$ oder $\nu(r) < \nu(g)$. Angenommen, $r \neq 0$. Dann ist $r = f - qg \in I \setminus \{0\}$ und $\nu(r) < \nu(g)$, im Widerspruch zur Wahl von g. □

Bemerkung b. Integritätsbereiche, in denen jedes Ideal ein Hauptideal ist, werden *Hauptidealringe* genannt. Die Ringe $\mathbb{Z}$ und $K[X]$ sind also Hauptidealringe.

Bemerkung c. Es seien $f, g \in R$ mit $g \neq 0$. Betrachte die Menge D der positiven bzw. normierten gemeinsamen Teiler von f und g, d.h.

$$D := \{d \in \mathbb{N} \mid d \text{ teilt } f \text{ und } d \text{ teilt } g\}$$

falls $R = \mathbb{Z}$ bzw.

$$D := \{d \in K[X] \mid d \text{ teilt } f, d \text{ teilt } g \text{ und } d \text{ normiert}\}$$

falls $R = K[X]$. Dann hat D bzgl. der Ordnung $\mid$ ein Maximum.

Beweis. Betrachte das Ideal $(f, g) = \{\lambda f + \mu g \text{ mit } \lambda, \mu \in R\}$ (siehe Bemerkung 2.4.2). Nach Bemerkung a existiert ein $d \in R$ mit $(f, g) = (d)$. Insbesondere ist $d = \lambda f + \mu g$ mit geeigneten $\lambda, \mu \in R$. Wir können oBdA d als positiv bzw. normiert annehmen. Dann ist $d \in D$ wegen $(f) \subseteq (f, g) = (d)$ und $(g) \subseteq (f, g) = (d)$ (siehe Bemerkung 2.4.2). Sei nun $d' \in D$. Aus $d' \mid f$ und $d' \mid g$ folgt $d' \mid \lambda f + \mu g = d$ nach Bemerkung 2.4.1 a. Damit ist d das Maximum von D. □

Notation. Sei $0 \neq f \in K[X]$. Wir schreiben $|f|$ für das eindeutig bestimmte normierte Polynom in der Assoziiertenklasse von f, d.h. $|f| = a_n^{-1} f$, falls a_n den Leitkoeffizienten von f bezeichnet. Für $f = 0$ sei $|f| = 0$.

Definition. Seien $f, g \in R$. Der *größte gemeinsame Teiler*, geschrieben $\mathrm{ggT}(f, g)$ von f und g ist definiert durch

$$\mathrm{ggT}(f, g) := \max D$$

mit D wie in Bemerkung c, falls $g \neq 0$, und

$$\mathrm{ggT}(f, 0) := |f|,$$

falls $g = 0$. Wir nennen f und g *teilerfremd*, wenn $\mathrm{ggT}(f, g) = 1$ ist.

Bemerkung d. Für alle $a, b \in R$ gilt:

(i) $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a)$,

(ii) $\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|)$,

(iii) $\mathrm{ggT}(a, 0) = |a|$,

(iv) $a = qb + r \Rightarrow \mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$.

Beweis. Sei $a = qb + r$ bzw. $r = a - qb$. Nach Bemerkung 2.4.1 a gilt sowohl $d \mid a, b \Rightarrow d \mid r$ und $d \mid b, r \Rightarrow d \mid a$. Die gemeinsamen Teiler von a, b sind also identisch mit den gemeinsamen Teilern von b, r. □

2.5.2 Das kgV

Bemerkung a. Es seien $f, g \in R$, $f, g \neq 0$. Betrachte die Menge V der positiven bzw. normierten gemeinsamen Vielfachen von f und g, d.h.

$$V := \{v \in \mathbb{N} \mid f \text{ teilt } v \text{ und } g \text{ teilt } v\}$$

falls $R = \mathbb{Z}$ bzw.

$$V := \{v \in K[X] \setminus \{0\} \mid f \text{ teilt } v, g \text{ teilt } v \text{ und } v \text{ normiert}\}$$

falls $R = K[X]$. Dann hat V bzgl. der Ordnung $\mid$ ein Minimum.

Beweis. Betrachte das Ideal $(f) \cap (g)$ (siehe Übung 2.4.2 a). Nach Bemerkung 2.5.1 a existiert ein $v \in R$ mit $(f) \cap (g) = (v)$. Wir können oBdA v als positiv bzw. normiert annehmen. Dann ist $v \in V$ wegen $(v) \subseteq (f)$ und $(v) \subseteq (g)$ (siehe Bemerkung 2.4.2). Sei nun $v' \in V$. Aus $f \mid v'$ und $g \mid v'$ folgt $v' \in (f) \cap (g) = (v)$ nach Bemerkung 2.4.1 a. Damit gilt $v \mid v'$ und v ist das Minimum von V. □

Definition. Seien $f, g \in R$. Das *kleinste gemeinsame Vielfache*, geschrieben $\mathrm{kgV}(f, g)$ von f und g ist definiert durch

$$\mathrm{kgV}(f, g) := \min V$$

mit V wie Bemerkung a, falls $f, g \neq 0$ sind, und

$$\mathrm{kgV}(f, g) = 0,$$

falls $f = 0$ oder $g = 0$ ist.

Bemerkung b. Mit der Notation aus Abschnitt 2.5.1 gilt für alle $a, b \in R$:

(i) $\mathrm{kgV}(a,b) = \mathrm{kgV}(b,a)$,

(ii) $\mathrm{kgV}(a,b) = \mathrm{kgV}(|a|,|b|)$,

(iii) $\mathrm{kgV}(a,0) = 0$.

Übung. Es seien $a, b \in R$ nicht beide gleich 0. Man zeige

$$\mathrm{kgV}(a,b) = \frac{|ab|}{\mathrm{ggT}(a,b)}.$$

2.5.3 Der Euklidische Algorithmus

Hier stellen wir den Euklidische Algorithmus vor. Dieser berechnet nicht nur $\mathrm{ggT}(a,b)$ für $a, b \in R$, sondern auch eine Darstellung $\mathrm{ggT}(a,b) = \lambda a + \mu b$ mit $\lambda, \mu \in R$.

Beispiel. Wie lautet $\mathrm{ggT}(91, 168)$?
Rechnung:

$$\begin{aligned} 168 &= 1 \cdot 91 + 77 \\ 91 &= 1 \cdot 77 + 14 \\ 77 &= 5 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0. \end{aligned}$$

Nach Bemerkung (2.5.1)(d) gilt somit

$$\mathrm{ggT}(168,91) = \mathrm{ggT}(91,77) = \mathrm{ggT}(77,14) = \mathrm{ggT}(14,7) = \mathrm{ggT}(7,0) = 7.$$

Rückwärts Einsetzen:

$$\begin{aligned} 7 &= 77 - 5 \cdot 14 \\ &= 77 - 5 \cdot (91 - 1 \cdot 77) = -5 \cdot 91 + 6 \cdot 77 \\ &= -5 \cdot 91 + 6 \cdot (168 - 1 \cdot 91) = 6 \cdot 168 - 11 \cdot 91. \end{aligned}$$

Somit gilt $\mathrm{ggT}(91, 168) = (-11) \cdot 91 + 6 \cdot 168$.

Beispiel (Fortsetzung von Beispiel (2.4.4))**.** Wir dividieren g durch r mit Rest:

$$\begin{array}{rrr} (X^2 & -3X & -4) : (3X - 12) = \frac{1}{3}X + \frac{1}{3} = \frac{1}{3}(X+1) \\ -(X^2 & -4X) & \\ \hline & X & -4 \\ & -(X & -4) \\ \hline & & 0 \end{array}$$

D.h. $g = \frac{1}{3}(X+1)\cdot r + 0$. Damit ist r bis auf Normierung der ggT von f und g, also $\mathrm{ggT}(f,g) = X-4$. Rückwärtseinsetzen liefert weiterhin die Darstellung:

$$\begin{aligned}\mathrm{ggT}(f,g) = X-4 = \frac{1}{3}(3X-12) &= \frac{1}{3}(f-(2X-3)g)\\ &= \frac{1}{3}\cdot f - \frac{1}{3}(2X-3)\cdot g.\end{aligned}$$

Im folgenden Algorithmus benutzen wir die Notation ν aus (2.5.1).

Algorithmus. *Es seien $a, b \in R$ mit $b \neq 0$. Die folgende Prozedur liefert $d, \lambda, \mu \in R$ mit $d = \mathrm{ggT}(a,b) = \lambda a + \mu b$.*

EUKLID(a,b)
1 Bestimme q, r mit $a = qb + r$ und $\nu(r) < \nu(b)$.
2 **if** $r = 0$
3 **then return** $(|b|, 0, |b|/b)$
4 **else** $(d, \lambda, \mu) \leftarrow$ EUKLID(b, r)
5 **return** $(d, \mu, \lambda - q\mu)$

Beweis. 1. Es sei $a = qb + r$.
3. Falls $r = 0$, dann $b \mid a$, also $\mathrm{ggT}(a,b) = |b| = 0\cdot a + |b|/b \cdot b$.
4. Sei $r > 0$ und $d = \mathrm{ggT}(b,r) = \lambda b + \mu r$.
5. Nach Bemerkung (2.5.1)(d) ist $d = \mathrm{ggT}(a,b)$. Außerdem gilt $d = \lambda b + \mu(a - qb) = \mu a + (\lambda - q\mu)b$. □

Bemerkung. Der größte gemeinsame Teiler wurde ohne Verwendung des Begriffs „Primzahl“ definiert und kann mit dem Euklidischen Algorithmus ohne Kenntnis der Primfaktorzerlegung berechnet werden.

Übung a. Es seien $a, b \in \mathbb{N}$. Die Koeffizienten λ, μ in der Darstellung

$$\mathrm{ggT}(a,b) = \lambda a + \mu b$$

sind nicht eindeutig. Geben Sie ein Beispiel an. Zeigen Sie weiter, dass λ, μ unter der Zusatzbedingung $-b/d < \lambda \leq 0$ und $0 < \mu \leq a/d$ eindeutig werden.

2.6 Restklassenringe

In diesem Abschnitt führen wir die wichtigsten Konstruktionen von kommutativen Ringen und Körpern ein. Dies sind Restklassenringe von ganzen Zahlen bzw. Polynomringen.

2.6.1 Kongruenz modulo n

Definition. Für jedes $n \in \mathbb{N}$ definieren wir auf $\mathbb{Z}$ eine Relation $\equiv_n$ durch

$$a \equiv_n b :\Leftrightarrow n \mid a - b.$$

Statt $a \equiv_n b$ schreibt man auch $a \equiv b \pmod{n}$ und sagt „*a kongruent b modulo n*“.

Bemerkung. Es gilt $a \equiv_n b$ genau dann, wenn a und b bei Division durch n denselben Rest lassen.

Beweis. Seien $a = qn + r$ und $b = q'n + r'$ mit $0 \leq r, r' < n$. Dann ist $a - b = (q - q')n + (r - r')$ und $|r - r'| < n$. Nach Bemerkung (2.4.1) gilt $n \mid a - b$ genau dann, wenn $n \mid r - r'$. Wegen $|r - r'| < n$ ist das genau dann der Fall, wenn $r - r' = 0$. □

Beispiel. Ist 14 kongruent 23 modulo 3 ($14 \equiv_3 23$)? Ja, weil $14 - 23 = -9$ Vielfaches von 3 ist. Alternativ kann man die Reste bei Division durch 3 vergleichen: $14 = 4 \cdot 3 + 2$ und $23 = 7 \cdot 4 + 2$. Sie stimmen überein (beide $= 2$).

Satz. *Für jedes $n \in \mathbb{N}$ ist die Relation $\equiv_n$ eine Äquivalenzrelation.*

Beweis. Klar aus der Bemerkung. □

2.6.2 Restklassen modulo n

Es sei $n \in \mathbb{N}$ in diesem Abschnitt fest gewählt.

Definition a. Es sei $a \in \mathbb{Z}$. Wir setzen

$$a \bmod n := r,$$

für den eindeutig bestimmten Rest $r \in \mathbb{Z}$ bei der Division mit Rest von a durch n. Es ist also $a \bmod n = r$ genau dann, wenn $a = qn + r$ mit $0 \leq r < n$ ist.

Definition b. Die Äquivalenzklasse von $a \in \mathbb{Z}$ bzgl. $\equiv_n$ wird mit $\overline{a}$ bezeichnet und wird die *Restklasse von a modulo n* genannt.

Bemerkung. Die Restklasse $\overline{a}$ besteht aus allen ganzen Zahlen, die bei Division durch n denselben Rest lassen wie a. Es gilt

$$\overline{a} = a + n\mathbb{Z} = \{\ldots, a - 2n, a - n, a, a + n, a + 2n, \ldots\}.$$

Dividiert man a durch n mit Rest, etwa $a = qn + r$ mit $0 \leq r < n$, so ist $\overline{a} = \overline{r}$. Mit Definition a gilt also

$$\overline{a} = \overline{a \bmod n}.$$

Der Rest $a \bmod n$ ist weiterhin der kleinste nicht-negative Repräsentant von $\overline{a}$. Folglich hat jede Restklasse modulo n genau einen Repräsentanten zwischen 0 und $n-1$ (nämlich $a \bmod n$ für die Restklasse, die a enthält). Es gibt also genau n verschiedene Restklassen modulo n: $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.

Beispiel a. Für $n = 3$ ist $\overline{14} = \{\ldots, 5, 8, 11, 14, 17, 20, 23, \ldots\} = \overline{23}$. Wegen $14 = 4 \cdot 3 + 2$ ist $\overline{14} = \overline{2}$, und 2 ist der kleinste nicht-negative Repräsentant von $\overline{14}$.

Definition c. Die Menge der Restklassen modulo n wird mit $\mathbb{Z}_n$ (oder $\mathbb{Z}/(n)$) bezeichnet, also $\mathbb{Z}_n := \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Es gilt $|\mathbb{Z}_n| = n$.

Beispiel b. $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$.

2.6.3 Rechnen mit Restklassen

Wir möchten auf der Menge der Restklassen modulo n zwei Verknüpfungen $+$ und $\cdot$ einführen mittels der Definition

$$\overline{a} + \overline{b} := \overline{a + b} \quad \text{und} \quad \overline{a} \cdot \overline{b} := \overline{a \cdot b}. \tag{$*$}$$

Das Problem in dieser Definition ist, dass sie – auf den ersten Blick – von der Wahl der Repräsentanten a und b abzuhängen scheint. Der folgende Satz zeigt, dass dem nicht so ist. Nur aufgrund des Satzes handelt es sich bei ($*$) überhaupt um eine gültige Definition.

Satz. *Sei $n \in \mathbb{N}$ fest. Sind $a, a', b, b' \in \mathbb{Z}$ mit $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$, so gilt:*

(i) $\overline{a + b} = \overline{a' + b'}$,

(ii) $\overline{a \cdot b} = \overline{a' \cdot b'}$.

Beweis. Nach Voraussetzung ist $n \mid a - a'$ und $n \mid b - b'$. Nach Bemerkung (2.4.1) (ii) teilt n auch $(a-a')+(b-b') = (a+b)-(a'+b')$, also gilt (i). Nach Bemerkung (2.4.1) (i) und (ii) teilt n auch $(a-a')b'+(b-b')a = (a \cdot b - a' \cdot b')$, also gilt (ii). □

Folgerung. *Die Menge $\mathbb{Z}_n$ bildet bzgl. der Verknüpfungen aus ($*$) einen kommutativen Ring.*

Beweis. Addition und Multiplikation in $\mathbb{Z}_n$ sind über die entsprechenden Operationen aus $\mathbb{Z}$ definiert. Daher werde Assoziativ-, Kommutativ- und Distributivgesetze von $\mathbb{Z}$ „geerbt“. Weiter ist die 0 in $\mathbb{Z}_n$ die Restklasse $\overline{0}$, das negative Element zu $\overline{a}$ ist $\overline{-a}$, und die 1 in $\mathbb{Z}_n$ ist die Restklasse $\overline{1}$. Damit prüft man alle Axiome leicht nach. □

Definition. Der Ring $(\mathbb{Z}_n, +, \cdot)$ mit den Verknüpfungen aus (∗) wird *Restklassenring modulo n* genannt.

Bemerkung. Das praktische Rechnen mit Restklassen geschieht am besten auf die folgende Weise. Es seien $0 \leq i, j < n$ Elemente aus $\mathbb{Z}$, die die Restklassen $\overline{i}$ und $\overline{j}$ repräsentieren.

(i) Zur Addition von $\overline{i}$ und $\overline{j}$, addiere i und j in $\mathbb{Z}$ und dividiere das Ergebnis mit Rest durch n. Der Rest ist der Repräsentant der Restklasse $\overline{i} + \overline{j}$. In Formeln:

$$\overline{i} + \overline{j} = \overline{(i + j) \bmod n}.$$

Diese Rechnung wird noch durch folgende Überlegung vereinfacht. Ist $i+j < n$, dann ist $(i+j) \bmod n = i+j$. Andernfalls ist $(i+j) \bmod n = n - (i + j)$. Ist $i > 0$, dann ist $\overline{n - i}$ das Additive Inverse von $\overline{i}$.

(ii) Zur Multiplikation von $\overline{i}$ und $\overline{j}$, multipliziere i und j in $\mathbb{Z}$ und dividiere das Ergebnis mit Rest durch n. Der Rest ist der Repräsentant der Restklasse $\overline{i} \cdot \overline{j}$. In Formeln:

$$\overline{i} \cdot \overline{j} = \overline{(i \cdot j) \bmod n}.$$

Bei dieser Rechnung müssen nur nicht-negative ganze Zahlen kleiner als $n(n-1)$ betrachtet werden.

Beispiel.

(i) $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, wobei

$$\overline{0} = 2\mathbb{Z} = \{\text{gerade ganze Zahlen}\},$$
$$\overline{1} = 1 + 2\mathbb{Z} = \{\text{ungerade ganze Zahlen}\}.$$

Die Verknüpfungstafeln von $\mathbb{Z}_2$ lauten (beachte $\overline{1}+\overline{1} = \overline{1+1} = \overline{2} = \overline{0}$):

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

und

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Aus der Tabelle für + liest man z.B. ab, dass „gerade+ungerade immer ungerade ergibt“ und dass „ungerade+ungerade immer gerade ergibt“. Diese Aussagen sind hiermit auch bewiesen (genauer durch obigen Satz)!

Identifiziert man $\overline{0}$ mit falsch und $\overline{1}$ mit wahr, so entspricht + gerade xor und $\cdot$ entspricht $\wedge$. Damit ist gezeigt, dass auch $(B, \text{xor}, \wedge)$ einen kommutativen Ring bildet, und dass dieser als identisch mit dem Ring $(\mathbb{Z}_2, +, \cdot)$ angesehen werden kann.

(ii) Die Verknüpfungstafeln von $\mathbb{Z}_4$ lauten

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

und

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

(iii) In $\mathbb{Z}_7$ gilt:

$$\begin{aligned}
\overline{3} + \overline{5} &= \overline{8} = \overline{1}, \\
\overline{3} - \overline{5} &= \overline{3} + (\overline{-5}) = \overline{3} + \overline{-5} = \overline{3 - 5} = \overline{-2} = \overline{5}, \\
\overline{6} \cdot \overline{5} &= \overline{30} = \overline{2}, \\
\overline{6} \cdot \overline{5} &= \overline{-1} \cdot \overline{5} = \overline{-5} = \overline{2}, \\
\overline{6}^{100000} &= \overline{-1}^{100000} = \overline{(-1)^{100000}} = \overline{1}.
\end{aligned}$$

(iv) In $\mathbb{Z}_6$ gilt $\overline{3} \cdot \overline{2} = \overline{6} = \overline{0}$, aber $\overline{3} \neq \overline{0}$ und $\overline{2} \neq \overline{0}$. Die Restklasse $\overline{0}$ ist aber die 0 in $\mathbb{Z}_6$, d.h. $\mathbb{Z}_6$ ist nicht nullteilerfrei! $\mathbb{Z}_6$ ist auch ein Gegenbeispiel zur Kürzungsregel (vgl. Bemerkung 2.2.3): $\overline{2} \cdot \overline{3} = \overline{4} \cdot \overline{3}$, aber $\overline{2} \neq \overline{4}$.

(v) In $\mathbb{Z}_6$ ist $\overline{5}$ eine Einheit, denn $\overline{5} \cdot \overline{5} = \overline{1}$ und $\overline{1}$ ist die 1. Neben $\overline{1}$ ist $\overline{5}$ sogar die einzige Einheit (man prüfe das nach!), also $\mathbb{Z}_6^\times = \{\overline{1}, \overline{5}\}$. Man beachte $\overline{5} = -\overline{1}$.

Übung. Was für ein Ring ist $\mathbb{Z}_1$?

2.6.4 Gleichungen in $\mathbb{Z}_n$

Beispiel a. Für welche $b \in \mathbb{Z}$ ist $\overline{9} \cdot x = \overline{b}$ in $\mathbb{Z}_{15}$ lösbar?

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{13}$	$\overline{14}$
$\overline{9} \cdot x$	$\overline{0}$	$\overline{9}$	$\overline{3}$	$\overline{12}$	$\overline{6}$	$\overline{0}$	$\overline{9}$	$\overline{3}$	$\overline{12}$	$\overline{6}$	$\overline{0}$	$\overline{9}$	$\overline{3}$	$\overline{12}$	$\overline{6}$

Antwort: Es gibt genau dann eine Lösung, wenn $\overline{b} = \overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}$. Für $b = 3$ gibt es z.B. die Lösungen $x = \overline{2}, \overline{7}, \overline{12}$.

Satz. *Es seien $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$ gegeben. Die Gleichung $\overline{a} \cdot x = \overline{b}$ in $\mathbb{Z}_n$ ist genau dann lösbar, wenn* $\mathrm{ggT}(a, n) \mid b$.

Beweis. Sei $\overline{a} \cdot x = \overline{b}$ lösbar, etwa $\lambda \in \mathbb{Z}$ mit $\overline{a} \cdot \overline{\lambda} = \overline{b}$. D.h. $n \mid \lambda a - b$. Aus $\mathrm{ggT}(a, n) \mid \lambda a$ und $\mathrm{ggT}(a, n) \mid \lambda a - b$ folgt $\mathrm{ggT}(a, n) \mid b$ (vgl. Übung 2.4.1a).

Sei umgekehrt $\mathrm{ggT}(a, n) \mid b$, etwa $c \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) \cdot c = b$. Nach Algorithmus 2.5.3 gibt es $\lambda, \mu \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = \lambda a + \mu n$. Multiplikation mit c liefert $b = (c\lambda)a + (c\mu)n$. In $\mathbb{Z}_n$ bedeutet das $\overline{b} = \overline{c\lambda} \cdot \overline{a}$, d.h. $x = c\lambda$ ist eine Lösung. □

Beispiel b. Löse $\overline{6} \cdot x = \overline{9}$ in $\mathbb{Z}_{15}$. Rechnung: Mit dem euklidischen Algorithmus berechnet man $\mathrm{ggT}(6, 15) = 3 = 1 \cdot 15 - 2 \cdot 6$. Multiplikation mit 3 liefert $9 = 3 \cdot 15 - 6 \cdot 6$. Modulo 15 ergibt sich $\overline{9} = \overline{0} - \overline{6} \cdot \overline{6}$. Folglich ist $x = -\overline{6} = \overline{-6} = \overline{9}$ eine Lösung. Die Lösung ist nicht eindeutig, z.B. ist auch $\overline{6} \cdot \overline{4} = \overline{24} = \overline{9}$ oder $\overline{6} \cdot \overline{14} = \overline{6} \cdot \overline{-1} = \overline{-6} = \overline{9}$.

Definition. Ein Element $p \in \mathbb{N}$ heißt *Primzahl*, wenn $p > 1$ ist und 1 und p die einzigen Teiler von p in $\mathbb{N}$ sind.

Folgerung. *Es seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$.*

(i) $\overline{a} \in \mathbb{Z}_n^\times \Leftrightarrow \mathrm{ggT}(a, n) = 1$.

(ii) $\mathbb{Z}_n$ ist genau dann ein Körper, wenn n eine Primzahl ist.

Beweis. Übung unter Verwendung des Satzes. □

Beispiel c. $\mathbb{Z}_9^\times = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$. Es gilt:

$$\overline{1}^{-1} = \overline{1}, \qquad \overline{8}^{-1} = \overline{8},$$
$$\overline{2}^{-1} = \overline{5}, \qquad \overline{7}^{-1} = \overline{4},$$
$$\overline{4}^{-1} = \overline{7}, \qquad \overline{5}^{-1} = \overline{2}.$$

Übung a. Wie lauten alle Einheiten von $\mathbb{Z}_{11}$ und ihre Inversen? Ist $\mathbb{Z}_{11}$ ein Körper?

Übung b. Man zeige, dass für teilerfremde $a, b \in \mathbb{Z}$ stets gilt: $a \mid bc \Rightarrow a \mid c$. *Hinweis: Man rechne in $\mathbb{Z}_a$.*

Übung c. Wie viele Einheiten hat $\mathbb{Z}_{p^n}$, wenn p eine Primzahl ist?

Übung d. Es sei $n > 1$. Man zeige, dass $\overline{a} \in \mathbb{Z}_n$ genau dann Nullteiler ist, wenn $\mathrm{ggT}(a, n) \neq 1$.

Übung e. Man zeige, dass in $\mathbb{Z}_n$ jedes Element entweder Einheit oder Nullteiler ist.
Übung f. Man prüfe folgende Aussage aus Übung 2.2.3b in verschiedenen $\mathbb{Z}_n$ nach: $(a) = (b) \Leftrightarrow a \sim b$?

2.6.5 Die Euler'sche Funktion

Definition. Für $n \in \mathbb{N}$ definiere

$$\varphi(n) := |\mathbb{Z}_n^\times| = |\{a \in \mathbb{Z} \mid 0 \leq a < n, \mathrm{ggT}(a,n) = 1\}.$$

Die Abbildung $\varphi : \mathbb{N} \to \mathbb{N}$ heißt die *Euler'sche φ-Funktion.*

Bemerkung a. (i) Für alle $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$ gilt $\varphi(mn) = \varphi(m)\varphi(n)$.

(ii) Für alle Primzahlen p gilt $\varphi(p^k) = p^{k-1}(p-1)$.

Beweis. (i) Ohne Beweis. (ii) Als Übung. (Kombinatorik!) □

Beispiel. $\varphi(9) = \varphi(3^2) = 3^1(3-1) = 3 \cdot 2 = 6$.
$\varphi(20) = \varphi(4) \cdot \varphi(5) = 2^1(2-1) \cdot 5^0(5-1) = 2 \cdot 4 = 8$.

Bemerkung b. Es sei G eine endliche abelsche Gruppe und $x \in G$. Dann ist $x^{|G|} = 1$.

Beweis. Es sei $|G| = m$ und $G = \{g_1, g_2, \ldots, g_m\}$. Dann ist auch $G = \{xg_1, xg_2, \ldots, xg_m\}$. Wir setzen $a := \prod_{i=1}^m g_i \in G$ und erhalten

$$a = \prod_{i=1}^m g_i = \prod_{i=1}^m (xg_i) = x^{|G|} \prod_{i=1}^m g_i = x^{|G|} a,$$

wobei beide mittlere Gleichungen benutzen, dass G abelsch ist. Multiplikation mit a^{-1} liefert die Behauptung. □

Daraus ergeben sich zwei wichtige Resultate der elementaren Zahlentheorie.

Satz a. (Satz von Euler) *Es seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$. Dann ist*

$$a^{\varphi(n)} \equiv_n 1.$$

Beweis. Wegen $\mathrm{ggT}(a,n) = 1$ ist $\overline{a} \in (Z_n)^\times$. Aus Bemerkung b ergibt sich mit $\varphi(n) = |(Z_n)^\times|$, dass $\overline{a}^{\varphi(nl} = \overline{1}$ ist in $(Z_n)^\times$. Daraus folgt die Behauptung. □

Wir spezialisieren noch auf den Fall, dass n eine Primzahl ist.

Satz b. (Kleiner Satz von Fermat) *Es seien $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann ist*

$$a^{p-1} \equiv_p 1.$$

2.6.6 Restklassenringe von $K[X]$

In diesem Abschnitt sei K ein Körper. Die Konstruktionen und Aussagen aus den Abschnitten 2.6.1 – 2.6.3 lassen sich auf den Fall des Ringes $K[X]$ übertragen. Wir geben die wichtigsten Resultate ohne Beweise an. Diese lassen sich wie beim Ring der ganzen Zahlen führen.

Definition. Für jedes $g \in K[X] \setminus \{0\}$ definieren wir auf $K[X]$ eine Relation $\equiv_g$ durch

$$f \equiv_g h :\Leftrightarrow g \mid f - h.$$

Statt $f \equiv_g h$ schreibt man auch $f \equiv h \pmod{g}$ und sagt „*f kongruent h modulo g*“.

Bemerkung. Es gilt $f \equiv_g h$ genau dann, wenn f und h bei Division durch g denselben Rest lassen.

Beispiel. (i) $X^2 - 1 \equiv_{X^2-1} 0$

(ii) $X^2 \equiv_{X^2-1} 1$

(iii) $X^4 - X^2 + 1 \equiv_{X^2-1} 1$

Satz. *Für jedes $g \in K[X] \setminus \{0\}$ ist die Relation $\equiv_g$ eine Äquivalenzrelation.*

Definition a. Es sei $g \in K[X] \setminus \{0\}$. Die Äquivalenzklasse von $f \in K[X]$ bzgl. $\equiv_g$ wird die *Restklasse von f modulo g* genannt und mit $\overline{f}$ bezeichnet. Wir schreiben

$$K[X]/(g) := \{\overline{f} \mid f \in K[X]\}$$

für die Menge der Restklassen modulo g.

Definition b. Es sei $d \in \mathbb{N}_0$. Wir setzen

$$K[X]_{<d} := \{f \in K[X] \mid \deg f < d\}.$$

Insbesondere ist $K[X]_{<0} = \{0\}$ und $K[X]_{<1}$ die Menge der konstanten Polynome.

Definition c. Es seien $g \in K[X] \setminus \{0\}$ und $f \in K[X]$. Wir setzen

$$f \bmod g := r,$$

für den eindeutig bestimmten Rest $r \in K[X]$ bei der Division mit Rest von f durch g. Es ist also $f \bmod g = r$ genau dann, wenn $f = qg + r$ mit $\deg r < \deg g$ ist.

Bemerkung. Es seien $g \in K[X] \setminus \{0\}$ und $n := \deg g$.

Die Restklasse $\overline{f}$ von $f \in K[X]$ modulo g besteht aus den Polynomen, die bei Division durch g denselben Rest lassen wie f. Dies ist die Menge

$$\overline{f} = f + gK[X] := \{f + gh \mid h \in K[X]\}.$$

Dividiert man f durch g mit Rest, etwa $f = qg + r$ mit $\deg r < \deg g$, so ist $f \equiv_g r$. Mit Definition c gilt also

$$\overline{f} = \overline{f \bmod n}.$$

Der Rest $f \bmod n$ ist weiterhin der Repräsentant der Restklasse $\overline{f}$ von kleinstem Grad. Folglich hat jede Restklasse modulo g genau einen Repräsentanten aus $K[X]_{<n}$ (nämlich $f \bmod g$ für die Restklasse, die f enthält). Es gibt also eine Bijektion zwischen der Menge der Restklassen modulo g und $K[X]_{<n}$.

Satz. *Es sei $g \in K[X] \setminus \{0\}$. Sind $f, f', h, h' \in K[X]$ mit $f \equiv_g f'$ und $h \equiv_g h'$, so gilt:*

(i) $f + h \equiv_g f' + h'$,

(ii) $f \cdot h \equiv_g f' \cdot h'$.

Folgerung. *Es sei $g \in K[X] \setminus \{0\}$. Die Menge $K[X]/(g)$ bildet bzgl. der folgenden Verknüpfungen einen kommutativen Ring.*

(i) $\overline{f} + \overline{h} := \overline{f + h}, \quad f, h \in K[X]$;

(ii) $\overline{f} \cdot \overline{h} := \overline{f \cdot h}, \quad f, h \in K[X]$;

Definition. Es sei $g \in K[X] \setminus \{0\}$. Der Ring $(K[X]/(g), +, \cdot)$ mit den obigen Verknüpfungen wird *Restklassenring von $K[X]$ modulo g* genannt.

Bemerkung. Es sei $g \in K[X] \setminus \{0\}$ und $n := \deg g$. Das praktische Rechnen in $K[X]/(g)$ geschieht am besten auf die folgende Weise. Seien f, h Elemente aus $K[X]_{<n}$, die die Restklassen $\overline{f}$ und $\overline{h}$ repräsentieren.

(i) Zur Addition von $\overline{f}$ und $\overline{h}$, addiere f und h in $K[X]$. Die Summe ist Repräsentant der Restklasse $\overline{f} + \overline{h}$. In Formeln:

$$\overline{f} + \overline{h} = \overline{f + h}.$$

Das Additive Inverse von $\overline{f}$ ist $\overline{-f}$.

(ii) Zur Multiplikation von $\overline{f}$ und $\overline{h}$, multipliziere f und h in $K[X]$ und dividiere das Ergebnis mit Rest durch g. Der Rest ist der Repräsentant der Restklasse $\overline{f} \cdot \overline{h}$. In Formeln:

$$\overline{f} \cdot \overline{h} = \overline{(f \cdot h) \bmod g}.$$

Bei dieser Rechnung müssen nur Polynome vom Grad höchstens $2(n-1)$ betrachtet werden.

Was sind die Einheiten in $K[X]/(g)$?

Satz. *Es sei $g \in K[X] \setminus \{0\}$ und $f \in K[X]$. Dann gilt:*

$$\overline{f} \text{ ist Einheit in } K[X]/(g) \Leftrightarrow \mathrm{ggT}(f, g) = 1.$$

Definition. Ein Element $g \in K[X]$ heißt *irreduzibel*, wenn $g \neq 0$ ist, $\deg g \geq 1$ ist und es gilt: die einzigen Teiler von g sind Einheiten oder assoziiert zu g. Mit anderen Worten: Ist $g = fh$ mit $f, h \in K[X]$, dann ist $f \in K^\times$ oder $h \in K^\times$.

Folgerung. *Es sei $g \in K[X] \setminus \{0\}$. Dann gilt:*
$K[X]/(g)$ ist genau dann ein Körper, wenn g irreduzibel ist.

Mithilfe dieser Folgerung können wir weitere Körper definieren.

Beispiel. (i) $\mathbb{F}_4 := \mathbb{F}_2[X]/(X^2+X+1)$ ist ein Körper mit vier Elementen. Wir setzen $\alpha := \overline{X} \in \mathbb{F}_4$. Die Elemente von $\mathbb{F}_4$ sind $0, 1, \alpha, 1+\alpha$. Es bestehen folgende Verknüpfungstafeln.

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Vergleiche diese Tafeln mit Beispiel 2.2.4 c.

(ii) $\mathbb{C} := \mathbb{R}[X]/(X^2+1)$ ist ein Körper, der Körper der komplexen Zahlen. Wir setzen $\mathrm{i} := \overline{X} \in \mathbb{C}$ und identifizieren $\overline{r}$ mit r für $r \in \mathbb{R}$. Dann ist $\mathrm{i}^2 = -1$, und jedes Element $z \in \mathbb{C}$ hat eine eindeutige Darstellung als

$$z := a + b\mathrm{i}$$

mit $a, b \in \mathbb{R}$. Wir nennen a den *Realteil* von z und b den *Imaginärteil* von z. Die Abbildung

$$\mathbb{C} \to \mathbb{C}, \quad a + b\mathrm{i} \mapsto a - b\mathrm{i}$$

heißt *komplexe Konjugation*.

2.7 Permutationen

2.7.1 Definition und Beispiele

Es sei A eine endliche Menge und $|A| = n$. Wir nummerieren die Elemente von A und schreiben $A = \{a_1, a_2, \ldots, a_n\}$.

Definition. Eine bijektive Abbildung $\pi : A \to A$ heißt *Permutation von A*. Wir verwenden für Permutationen die Schreibweise

$$\pi = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \pi(a_1) & \pi(a_2) & \cdots & \pi(a_n) \end{pmatrix}.$$

Die Menge aller Permutationen von A wird mit S_A bezeichnet, also

$$S_A := \{\pi : A \to A \,|\, \pi \text{ bijektiv}\}.$$

In dem wichtigen Spezialfall $A = \underline{n}$ schreiben wir kurz S_n statt $S_{\underline{n}}$.

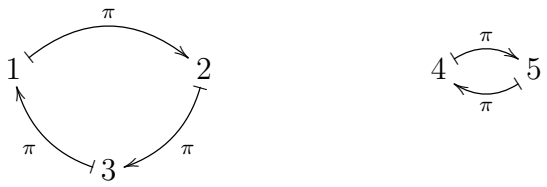
Bemerkung.

(i) Wenn $|A| = n$, dann $|S_A| = n!$. Das gilt auch für $n = 0$, denn $S_\emptyset$ hat genau ein Element (nach Beispiel 1.4.1viii existiert genau eine Abbildung $\emptyset \to \emptyset$ und die ist bijektiv).

(ii) Die Komposition von Permutationen von A ist wieder eine Permutation von A. Bei Permutationen sagt man statt Komposition auch *Produkt* und lässt das Zeichen $\circ$ einfach weg.

Beispiel.

(i) Die Permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \in S_5$ lässt sich so veranschaulichen:



(ii) Ist $\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}$ und π wie oben dann ergeben sich als Kompositionen

$$\pi \circ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} \quad \text{und} \quad \psi \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix}.$$

2.7.2 Der Träger einer Permutation

Definition. Für $\pi \in S_A$ heißt

$$T_\pi := \{a \in A \,|\, \pi(a) \neq a\} \subseteq A$$

der *Träger* von π.

Beispiel.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 8 & 3 & 6 & 2 & 7 & 4 & 1 & 9 & 11 & 10 \end{pmatrix}, \quad T_\pi = \{1, 2, 4, 5, 6, 7, 8, 10, 11\}.$$

Bemerkung. Es seien $\pi, \psi \in S_A$.

(i) $\pi(T_\pi) = T_\pi$.

(ii) Gilt $T_\pi \subseteq B$, so kann π auch als Element von S_B aufgefasst werden.

(iii) Haben π und ψ disjunkte Träger, so gilt $\pi \circ \psi = \psi \circ \pi$.

Beweis.

(i) Es reicht, die Inklusion $\pi(T_\pi) \subseteq T_\pi$ zu zeigen. Daraus folgt schon die Gleichheit, da es sich um endliche Mengen handelt und da $|\pi(T_\pi)| = |T_\pi|$ wegen der Injektivität von π gilt (vgl. Bem. 1.4.4a). Sei also a ein beliebiges Element aus T_π. Da $\pi(a) \neq a$ und π injektiv, folgt $\pi(\pi(a)) \neq \pi(a)$. Das bedeutet gerade $\pi(a) \in T_\pi$. Da $a \in T_\pi$ beliebig war, ist $\pi(T_\pi) \subseteq T_\pi$ gezeigt.

(ii) klar.

(iii) als Übung.

□

2.7.3 Zykel und Transpositionen

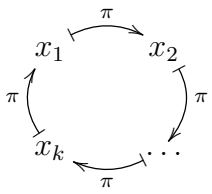
Definition. Es seien $x_1, x_2, \ldots, x_k \in A$ paarweise verschieden. Die Permutation $\sigma \in S_A$ mit

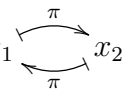
$$\sigma(x) = \begin{cases} x_{i+1} & \text{falls } x = x_i \text{ und } i < k, \\ x_1 & \text{falls } x = x_k, \\ x & \text{falls } x \neq x_1, x_2, \ldots, x_k, \end{cases}$$

heißt *Zykel der Länge k* oder kurz *k-Zykel* von S_A. Wir verwenden für σ die Schreibweise

$$\sigma = (x_1, x_2, \ldots, x_k).$$

Die 2-Zykel heißen auch *Transpositionen* von S_A.

k-Zykel: 

Transposition: 

Bemerkung.

(i) Es gilt stets $(x_1, x_2, \ldots, x_k)^k = \mathrm{id}$.

(ii) Es gilt stets $(x_1, x_2, \ldots, x_k)^{-1} = (x_k, x_{k-1}, \ldots, x_1)$.

(iii) Für Transpositionen τ gilt $\tau^{-1} = \tau$.

(iv) Jeder 1-Zykel ist die Identität.

(v) Jeder k-Zykel lässt sich als Produkt von $k-1$ Transpositionen schreiben:

$$(x_1, x_2, \ldots, x_k) = (x_1, x_2)(x_2, x_3) \cdots (x_{k-1}, x_k).$$

Eine solche Zerlegung ist im Allgemeinen nicht eindeutig (vgl. Beispiel a unten).

Beispiel a. Der 4-Zykel $\sigma := (1,5,2,4) \in S_5$ ist die Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}.$$

Es gilt

$$\begin{aligned}
\sigma^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix} = (4,2,5,1), \\
\sigma^{2} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} = (1,2)(5,4), \\
\sigma^{3} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix} = (1,4,2,5), \\
\sigma^{4} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \mathrm{id}.
\end{aligned}$$

Es gilt

$$\sigma = (1,5)(5,2)(2,4) = (1,4)(1,2)(1,5).$$

Beispiel b. Möchte man eine Liste von n Elementen ordnen (z.B. eine Liste von Wörtern nach alphabetischer Reihenfolge), so ist eine Permutation $\pi \in S_n$ zu finden, die die (ungeordnete) Liste in ihre geordnete Reihenfolge überführt. Das i-te Wort der ungeordneten Liste steht in der geordneten Liste dann an $\pi(i)$-ter Stelle. Ein Sortieralgorithmus findet π im Allgemeinen nicht in einem Schritt, sondern nimmt nacheinander eine Reihe von Vertauschungen vor; er konstruiert somit π als ein Produkt $\pi_1 \circ \ldots \circ \pi_r$ einzelner (einfacherer) Umordnungen π_i. Der *Bubblesort*-Algorithmus kommt dabei z.B. mit Transpositionen π_i aus. Damit das immer funktioniert muss sich jede Permutation als Produkt von Transpositionen schreiben lassen. Davon überzeugen wir uns mit Hilfe von Satz 2.7.4 unten.

2.7.4 Zerlegung in Zykel

Satz. *Jede Permutation $\pi \in S_A$ lässt sich als Produkt von Zykeln schreiben, deren Träger paarweise disjunkt sind. Bis auf Reihenfolge und bis auf Erwähnung von 1-Zykeln ist diese Zerlegung eindeutig.*

Beweis. Siehe Beispiel. □

Man spricht kurz von einer Zerlegung von π in *paarweise disjunkte Zykeln*.

Beispiel a. Für π aus Beispiel (2.7.2) haben wir die Zerlegung

$$\begin{aligned}\pi &= (1,5,2,8)(3)(4,6,7)(9)(10,11)\\ &= (1,5,2,8)(4,6,7)(10,11).\end{aligned}$$

Die Träger der drei Zykeln lauten $\{1,5,2,8\}, \{4,6,7\}, \{10,11\}$ und sind paarweise disjunkt. Die einzelnen Zykeln zerlegen sich weiter in Produkte von Transpositionen, z.B. $(1,5,2,8) = (1,5)(5,2)(2,8)$ und $(4,6,7) = (4,6)(6,7)$, also

$$\pi = (1,5)(5,2)(2,8)(4,6)(6,7)(10,11).$$

Die Zykelschreibweise lässt sich besonders leicht „potenzieren“:

$$\begin{aligned}\pi &= (10,11)(7,6,4)(8,2,5,1),\\ \pi^2 &= (1,2)(5,8)(4,6,7),\\ \pi^3 &= (1,5,2,8)(10,11),\\ \pi^4 &= (4,7,6)\\ &\vdots\\ \pi^{11} &= (1,5,2,8)(4,6,7)(10,11) = \pi^{-1}\\ \pi^{12} &= \mathrm{id}.\end{aligned}$$

Definition. Es sei $\pi \in S_A$. Die *Zykelzahl* von $\pi \in S_A$ ist die Anzahl der Zykeln inklusive aller 1-Zykeln, die bei einer Zerlegung von π in paarweise disjunkte Zykeln auftreten.

Die Zykelzahl ist gemäß obigem Satz eindeutig bestimmt. Sie hängt allerdings nicht nur von π sondern auch von A ab!

Beispiel b. Die Zykelzahl von π aus Beispiel a ist 5. Da sich die Identität $\mathrm{id} \in S_n$ in lauter 1-Zykeln zerlegt, hat sie die Zykelzahl n. Die Zykelzahl der (einzigen) Permutation $\emptyset \to \emptyset$ wird als 0 definiert.

2.7.5 Das Signum

Wir bezeichnen hier mit I_A die Menge der 2-elementigen Teilmengen einer Menge A, d.h. $I_A = \{\{i,j\} \subseteq A \,|\, i \neq j\}$. Wir schreiben I_n für $I_{\underline{n}}$. (In der Kombinatorik lernen wir, dass $|I_n| = \frac{n(n-1)}{2}$.)

Definition. Sei $\pi \in S_n$. Das *Signum* von π ist definiert als

$$\operatorname{sgn}\pi := \prod_{\{i,j\}\in I_n} \frac{\pi(i)-\pi(j)}{i-j}.$$

Man beachte, dass $\operatorname{sgn}\pi$ wohldefiniert ist, weil sich jeder einzelne Quotient nicht ändert, wenn man i und j vertauscht.

Beispiel a. Für $\pi = \mathrm{id} \in S_n$ sind alle Faktoren des Produktes gleich 1, also $\operatorname{sgn}\mathrm{id} = 1$. Für $n = 2$ und $\pi = (1,2)$ ist $I_n = \{\{1,2\}\}$, also $\operatorname{sgn}(1,2) = \frac{2-1}{1-2} = -1$.

Bemerkung a.

(i) Es gilt stets $\operatorname{sgn}\pi = \pm 1$.

(ii) Wir nennen π *gerade*, falls $\operatorname{sgn}\pi = 1$ und *ungerade* falls $\operatorname{sgn}\pi = -1$.

(iii) Es gilt $\operatorname{sgn}\pi = \operatorname{sgn}\pi'$ wobei $\pi' := \pi|_{T_\pi} \in S_{T_\pi}$.

Beweis. (i) Da π bijektiv ist, gilt $\{\{\pi(i), \pi(j)\} \subseteq \underline{n} \,|\, i \neq j\} = I_n$. D.h. wenn $\{i,j\}$ die Menge I_n durchläuft, so durchläuft auch $\{\pi(i), \pi(j)\}$ genau die Menge I_n. Folglich sind $\prod_{\{i,j\}\in I_n}(\pi(i) - \pi(j))$ und $\prod_{\{i,j\}\in I_n}(i-j)|$ (Zähler und Nenner) bis auf Vorzeichen gleich, und somit $|\operatorname{sgn}\pi| = 1$.

(iii) Es sei $T = T_\pi$ (der Träger von π) und $F = \underline{n} \setminus T$ (die Fixpunkte von π). Die Menge I_n partitioniert sich in $I_n = I_T \cup I_F \cup \{\{i,j\} \,|\, i \in T, j \in F\}$. Folglich zerlegt sich das Produkt aus der Definition von $\operatorname{sgn}\pi$ in die drei Teilprodukte

$$\begin{aligned}
\prod_{\{i,j\}\in I_T} \frac{\pi(i)-\pi(j)}{i-j} &= \operatorname{sgn}\pi', \\
\prod_{\{i,j\}\in I_F} \frac{\pi(i)-\pi(j)}{i-j} &= \prod_{\{i,j\}\in I_F} \frac{i-j}{i-j} = 1, \\
\prod_{i\in T, j\in F} \frac{\pi(i)-\pi(j)}{i-j} &= \prod_{j\in F} \underbrace{\prod_{i\in T} \frac{\pi(i)-j}{i-j}}_{=1} = 1.
\end{aligned}$$

Man beachte in der letzten Gleichung, dass wenn i die Menge T durchläuft, dann auch $\pi(i)$ genau die Menge T durchläuft. Damit ist $\operatorname{sgn}\pi = \operatorname{sgn}\pi'$ gezeigt. □

Beispiel b. Für jede Transposition $\pi = (a,b) \in S_n$ ist $\operatorname{sgn}\pi = -1$.

Beweis. Es ist $T_\pi = \{a,b\}$ und $\pi' = \pi|_{\{a,b\}} \in S_{\{a,b\}}$. Somit gilt

$$\operatorname{sgn}\pi = \operatorname{sgn}\pi' = \frac{\pi(a)-\pi(b)}{a-b} = \frac{b-a}{a-b} = -1.$$

□

Satz. *Für alle* $\pi, \psi \in S_n$ *gilt* $\operatorname{sgn}(\pi \circ \psi) = \operatorname{sgn}\pi \cdot \operatorname{sgn}\psi$.

Beweis. Es gilt

$$\begin{aligned}\operatorname{sgn}(\pi\circ\psi) &= \prod_{\{i,j\}\in I_n} \frac{(\pi\circ\psi)(i)-(\pi\circ\psi)(j)}{i-j}\\ &= \prod_{\{i,j\}\in I_n} \left(\frac{\pi(\psi(i))-\pi(\psi(j))}{\psi(i)-\psi(j)}\cdot\frac{\psi(i)-\psi(j)}{i-j}\right)\end{aligned}$$

Da mit $\{i,j\}$ auch $\{\psi(i),\psi(j)\}$ genau die Menge I_n durchläuft ist dieses Produkt gleich $\operatorname{sgn}\pi \cdot \operatorname{sgn}\psi$. □

Folgerung a. *Für alle* $\pi, \psi \in S_n$ *gelten:*

(i) $\operatorname{sgn}\pi^{-1} = \operatorname{sgn}\pi$.

(ii) $\operatorname{sgn}(\psi^{-1}\pi\psi) = \operatorname{sgn}\pi$.

Beweis. Der Satz und die Tatsache $\operatorname{sgn}\mathrm{id} = 1$. □

Bemerkung b. Aus Folgerung a(ii) geht hervor, dass eine Umbenennung der Elemente von $\underline{n}$ (hier vorgenommen durch ψ) das Signum von π nicht ändert. Die Definition des Signum stellt sich deshalb (nachträglich) als unabhängig von der Nummerierung innerhalb der Menge $\underline{n}$ heraus.

Diese Tatsache kann man ausnutzen, um die Definition des Signum auf Permutationen $\pi \in S_A$ (anstatt nur $\pi \in S_n$) auszudehnen: wähle eine beliebige Bijektion $\varphi : A \to \underline{n}$ und setze $\operatorname{sgn}\pi := \operatorname{sgn}(\varphi \circ \pi \circ \varphi^{-1})$ (beachte $\varphi \circ \pi \circ \varphi^{-1} \in S_n$).

Folgerung b. *Es sei* $\pi \in S_A$.

(i) Ist $\pi = \tau_1 \circ \cdots \circ \tau_r$ *mit Transpositionen* τ_i, *so gilt* $\operatorname{sgn}\pi = (-1)^r$.

(ii) Ist π *ein* k*-Zykel so gilt* $\operatorname{sgn}\pi = (-1)^{k-1}$.

(iii) π *ist genau dann gerade, wenn in jeder Darstellung von* π *als Produkt von Transpositionen die Anzahl der Transpositionen gerade ist.*

Beweis. (i) folgt aus dem Satz und Beispiel b. (ii) folgt aus (i) und Bemerkung 2.7.3(v). (iii) folgt aus (i). □

Beispiel c. Um das Signum der Permutation π aus Beispiel (2.7.2) zu berechnen, benutzen wir die Zerlegung $\pi = (1,5,2,8)(4,6,7)(10,11)$ aus Beispiel (2.7.3). Dann ergibt sich aus dem Satz und Folgerung b(ii):

$$\operatorname{sgn}\pi = \operatorname{sgn}(1,5,2,8)\cdot\operatorname{sgn}(4,6,7)\cdot\operatorname{sgn}(10,11) = (-1)^3\cdot(-1)^2\cdot(-1)^1 = (-1)^6 = 1.$$

Übung. (i) Es seien $\pi \in S_A$ und $\varphi : A \to \underline{n}$ eine Bijektion. Man zeige, dass $\operatorname{sgn}(\varphi \circ \pi \circ \varphi^{-1})$ unabhängig von der Wahl der Bijektion φ ist.

(ii) Es seien $\pi \in S_n$ und $n \leq m$. Fasse π als Element von S_m auf. Hängt $\operatorname{sgn} \pi$ von m ab?

(iii) Man zeige: Hat $\pi \in S_n$ die Zykelzahl z, so gilt $\operatorname{sgn} \pi = (-1)^{n-z}$.

Kapitel 3

Lineare Gleichungssysteme und Matrizen

3.1 Matrizen

Es sei R ein kommutativer Ring mit $1 \neq 0$.

Definition.

(i) Eine $(m \times n)$-Matrix A über R ist ein rechteckiges „Schema“ von $m \cdot n$ Elementen $a_{ij} \in R$ der Form

$$A = (a_{ij})_{\substack{1 \leq i \leq m, \\ 1 \leq j \leq n}} := \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Die $a_{ij} \in R$, $1 \leq i \leq m$, $1 \leq j \leq n$, heißen die *Koeffizienten* oder *Einträge* von A.

(ii) Zwei $(m \times n)$-Matrizen $A = (a_{ij})$ und $B = (b_{ij})$ über R heißen *gleich*, geschrieben $A = B$, wenn $a_{ij} = b_{ij}$ für alle $1 \leq i \leq m$ und alle $1 \leq j \leq n$. Die Menge aller $(m \times n)$-Matrizen über R wird mit $R^{m \times n}$ bezeichnet.

(iii) Es sei $A = (a_{ij}) \in R^{m \times n}$.

Die $(1 \times n)$-Matrix $z_i := \begin{pmatrix} a_{i1} & a_{i2} & \dots & a_{in} \end{pmatrix}$ heißt i-te *Zeile* von A.

Die $(m \times 1)$-Matrix $s_j := \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$ heißt j-te *Spalte* von A.

(iv) Eine $(1\times n)$-Matrix wird auch (Zeilen-)n-Tupel und eine $(m\times 1)$-Matrix wird (Spalten-)m-Tupel genannt. Wir setzen (vgl. Definition 1.4.1b):

$$R^n := R^{n\times 1} = \text{Menge aller Spalten-}n\text{-Tupel über } R.$$

(v) Eine $(m \times n)$-Matrix $A = (a_{ij})$ mit allen $a_{ij} = 0$ wird *Nullmatrix* genannt, geschrieben $A = 0$.

Bemerkung.

(i) Im Index gilt „Zeile vor Spalte“, d.h. a_{ij} steht in der i-ten Zeile und j-ten Spalte.

(ii) Eine $(m \times n)$-Matrix $A = (a_{ij})$ über R kann als Abbildung

$$a : \underline{m} \times \underline{n} \to R, (i, j) \mapsto a(i, j) := a_{ij}$$

aufgefasst werden. Das steht in Analogie zu den n-Tupeln, die man ebenfalls als Abbildung auffassen kann (vgl. Definition 1.4.1b).

Schreibweise. Sind $z_1, \ldots, z_m$ die Zeilen und $s_1, \ldots, s_n$ die Spalten von A, so schreiben wir auch:

$$A = \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{pmatrix} = \begin{pmatrix} s_1 & s_2 & \ldots & s_n \end{pmatrix} = (s_1, s_2, \ldots, s_n).$$

Diese Vereinbarung ist Teil einer flexiblen Schreibweise, nach der eine Matrix aus Blöcken, die selbst Matrizen sind, zusammengebaut werden kann. Man kann z.B.

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

bilden, wenn A und B ebenso wie C und D jeweils gleich viele Zeilen haben, und A und C ebenso wie B und D jeweils gleich viele Spalten.

Beispiel.

(i) $\begin{pmatrix} 2 & -1 \\ 4 & 0 \\ 5 & 3 \end{pmatrix}$ ist eine (3×2)-Matrix.

(ii) $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ ist die (2×3)-Nullmatrix.

(iii) $\underbrace{\begin{pmatrix} 2 \\ 4 \\ 5 \end{pmatrix}}_{(3\times 1)} \neq \underbrace{\begin{pmatrix} 2 & 4 & 5 \end{pmatrix}}_{(1\times 3)}$.

3.2 Matrix-Arithmetik

In dem ganzen Abschnitt ist R ein kommutativer Ring mit $1 \neq 0$ und $R^{m\times n}$ die Menge der $m \times n$-Matrizen über R.

3.2.1 Die Grundrechenarten

Schreibweise. Es sei $A \in R^{m\times n}$. Für $1 \leq i \leq m$ und $1 \leq j \leq n$ bezeichnen wir – wie üblich – mit a_{ij} den (i,j)-*Eintrag* von A, d.h. den Eintrag in der i-ten Zeile und j-ten Spalte. (Merke: „Zeile vor Spalte“).

Sei umgekehrt a eine Abbildung $a : \underline{m} \times \underline{n} \to R, (i,j) \mapsto a(i,j)$. Dann bezeichnen wir mit

$$(a(i,j)) := (a(i,j))_{ij} := (a(i,j))_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}$$

diejenige Matrix $A \in R^{m\times n}$ mit $a_{ij} = a(i,j)$ für alle $1 \leq i \leq m, 1 \leq j \leq n$.

Definition. Es seien $A \in R^{m\times n}$ und $r \in R$.

(i) $A^t := (a_{ji})_{\substack{1\leq i\leq n\\ 1\leq j\leq m}} \in R^{n\times m}$ heißt die *Transponierte von A*.

(ii) $r \cdot A := (r \cdot a_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} \in R^{m\times n}$ heißt *(skalares) Vielfaches* von A.

(iii) Für jedes $B = (b_{ij}) \in R^{m\times n}$ definieren wir die *Summe* $A + B := (a_{ij} + b_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} \in R^{m\times n}$.

(iv) Für jedes $B = (b_{ij}) \in R^{n\times l}, l \in \mathbb{N}$, definieren wir das *Produkt* $A \cdot B := (c_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq l}} \in R^{m\times l}$ durch

$$c_{ij} := \sum_{k=1}^{n} a_{ik}b_{kj} \text{ für alle } i,j.$$

Beispiel a.

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

$$\begin{pmatrix} 2 & 3 & 0 \\ -1 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & -1 & 0 & 3 \\ 0 & 2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 8 & -3 & 2 & 9 \\ -1 & 4 & -1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 3 & 0 \\ -1 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 1 \\ 2 & -1 & 0 \end{pmatrix} \text{ nicht definiert}$$

Bemerkung a.

(i) Die Zeilen von A^t erhält man aus den Spalten von A (in gleicher Reihenfolge), und umgekehrt. Spalten addiert haben in der Schreibweise $\mathbb{L}(A, b) = s + \mathbb{L}(A, 0)$.

(ii) Wir identifizieren $R^{1\times 1}$ mit R, also die 1×1-Matrix (a) über R mit dem Ringelement $a \in R$.

(iii) Das Produkt $A \cdot B$ ist nur definiert, wenn Spaltenzahl von A gleich Zeilenzahl von B ist.

$$\cdot : R^{m\times n} \times R^{n\times l} \to R^{m\times l}$$

Spezialfälle:

$\cdot : R^{m\times n} \times R^{n} \to R^{m}$	$l = 1$ (Matrix·Spalte=Spalte)
$\cdot : R^{1\times n} \times R^{n\times l} \to R^{1\times l}$	$m = 1$ (Zeile·Matrix=Zeile)
$\cdot : R^{1\times n} \times R^{n} \to R = R^{1\times 1}$	$l = m = 1$ (Skalarprodukt)
$\cdot : R^{m} \times R^{1\times l} \to R^{m\times l}$	$n = 1$ (Spalte·Zeile=Matrix)

Der Fall $l = m = 1$ ist das Skalarprodukt aus der Schule, nur dass hier einer der Vektoren als Zeile geschrieben wird.

(iv) Es seien $A \in R^{m\times n}$ und $B \in R^{n\times l}$. Bezeichnet z_i die i-te Zeile von A und s_j die j-te Spalte von B, so gilt

$$A \cdot B = (z_i \cdot s_j)_{\substack{1\le i\le m,\\ 1\le j\le l}} \in R^{m\times l}.$$

Hier bezeichnet $\cdot$ in $z_i \cdot s_j$ die Matrixmultiplikation (also das Skalarprodukt), und die (1×1)-Matrix $z_i \cdot s_j$ wird ihrem Eintrag identifiziert.

Beispiel b.

(i) $l = 1$: $\begin{pmatrix} 1 & 0 & -2 \\ 3 & 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 11 \end{pmatrix}$

(ii) $m = 1$: $\begin{pmatrix} 1 & 0 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -2 & -1 \end{pmatrix}$

(iii) $l = m = 1$ (Skalarprodukt): $\begin{pmatrix} 1 & 0 & -2 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix} = 3 + 0 + 0 = 3$

(iv) $n = 1$: $\begin{pmatrix}3\\1\\0\end{pmatrix} \cdot \begin{pmatrix}1 & 0 & -2\end{pmatrix} = \begin{pmatrix}3 & 0 & -6\\1 & 0 & -2\\0 & 0 & 0\end{pmatrix}$

3.2.2 Quadratische Matrizen

Definition. Es sei $n \in \mathbb{N}$.

(i) Eine $n \times n$-Matrix heißt *quadratisch*.

(ii) Die n-reihige *Einheitsmatrix* ist definiert als $E_n := (\delta_{ij})_{1 \le i,j \le n}$ mit

$$\delta_{ij} := \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{falls } i \neq j. \end{cases}$$

Es gilt $E_n = \begin{pmatrix}1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & 1\end{pmatrix} \in R^{n\times n}$, z.B. $E_3 = \begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix}$.

(iii) Quadratische Matrizen der Formen

$$\begin{pmatrix}\star & & 0\\ & \ddots & \\ 0 & & \star\end{pmatrix}, \quad \begin{pmatrix}\star & \cdots & \star\\ & \ddots & \vdots\\ 0 & & \star\end{pmatrix}, \quad \text{bzw.} \quad \begin{pmatrix}\star & & 0\\ \vdots & \ddots & \\ \star & \cdots & \star\end{pmatrix}$$

mit beliebigen Einträgen $\star \in R$ heißen *Diagonalmatrix*, *obere Dreiecksmatrix*, bzw. *untere Dreiecksmatrix*.

3.2.3 Der Matrizenring

Satz. *Es seien $n, m, l, p \in \mathbb{N}$. Es bezeichne 0 die $m \times n$-Nullmatrix. Für alle $A, A' \in R^{m\times n}, B, B' \in R^{n\times l}, C \in R^{l\times p}$ und $r \in R$ gilt:*

(i) $(R^{m\times n}, +)$ *ist abelsche Gruppe mit neutralem Element* 0.

(ii) $(A \cdot B) \cdot C = A \cdot (B \cdot C)$

(iii) $E_m \cdot A = A = A \cdot E_n$

(iv) $(A + A') \cdot B = A \cdot B + A' \cdot B$

(v) $A \cdot (B + B') = A \cdot B + A \cdot B'$

(vi) $r \cdot (A \cdot B) = (r \cdot A) \cdot B = A \cdot (r \cdot B)$

(vii) $(A^t)^t = A$

(viii) $(A + A')^t = A^t + (A')^t$

(ix) $(A \cdot B)^t = B^t \cdot A^t$

Beweis. (i) ist klar, weil + einträgeweise definiert ist (vgl. §2.1.6).
(ii) Auf beiden Seiten ergibt sich der (i,j)-Eintrag $\sum_{\alpha=1}^{n}\sum_{\beta=1}^{l} a_{i\alpha}b_{\alpha\beta}c_{\beta j}$ (Rechnung als Übung).
(iii) Nach Bemerkung 3.2.1iv ist $E_m \cdot A = (z_i \cdot s_j)_{ij}$, wobei z_i die i-te Zeile von E_m ist und s_j die j-te Spalte von A. Es gilt

$$z_i = (0 \cdots 0 \underbrace{1}_{\text{Pos. } i} 0 \cdots 0) \quad \text{und} \quad s_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix},$$

also

$$z_i \cdot s_j = 0 \cdot a_{1j} + \cdots + 1 \cdot a_{ij} + 0 + \cdots + 0 = a_{ij}.$$

Damit ist $E_m \cdot A = (a_{ij}) = A$ gezeigt. Genauso verfährt man mit $A \cdot E_n = A$.
(iv)

$$\begin{aligned} (A+B)\cdot C &= \left(\sum_{k=1}^{n}(a_{ik}+b_{ik})c_{kj}\right)_{ij} \\ &= \left(\sum_{k=1}^{n} a_{ik}c_{kj} + \sum_{k=1}^{n} b_{ik}c_{kj}\right)_{ij} \\ &= \left(\sum_{k=1}^{n} a_{ik}c_{kj}\right)_{ij} + \left(\sum_{k=1}^{n} b_{ik}c_{kj}\right)_{ij} = AC + BC. \end{aligned}$$

(v) genauso wie (iv).
(vi) Übung (Ansatz wie in (iv)).
(vii) und (viii) sind klar.
(ix)

$$\begin{aligned} (A\cdot B)^t &= \left(\sum_{k=1}^{n} a_{ik}b_{kj}\right)^t_{ij} = \left(\sum_{k=1}^{n} a_{ik}b_{kj}\right)_{ji} \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \| \\ B^t \cdot A^t &= (b_{ji})_{ij}\cdot(a_{ji})_{ij} = \left(\sum_{k=1}^{n} b_{ki}a_{jk}\right)_{ij} \end{aligned}$$

□

Übung. Für welche Teile des Satzes braucht man, dass R kommutativ ist?

Folgerung. *Es sei $n \in \mathbb{N}$. Dann wird $R^{n\times n}$ mit der Matrix-Addition und Matrix-Multiplikation aus Definition (3.2.1) zu einem Ring, dem* Matrizenring. *Die neutralen Elemente sind $0 \in R^{n\times n}$ bzgl. der Addition und $E_n \in R^{n\times n}$ bzgl. der Multiplikation.*

Beweis. Die Eigenschaften (i)–(v) aus Satz 3.2.3. □

Bemerkung.

(i) $R^{1\times 1}$ kann mit R identifiziert werden.

(ii) $R^{n\times n}$ ist für $n \geq 2$ nicht kommutativ. Für $n = 2$ sieht man das an

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

und ein solches Beispiel lässt sich für jedes $n \geq 2$ finden.

(iii) $R^{n\times n}$ ist für $n \geq 2$ nicht nullteilerfrei (sogar wenn R ein Körper ist). Es gibt sogar $A \in R^{n\times n}, A \neq 0$, mit $A^2 = 0$, wie man an dem Beispiel $A = \begin{pmatrix} \cdots & 0 & 1 \\ & 0 & 0 \\ & & \vdots \end{pmatrix}$ sieht. Insbesondere ist $R^{n\times n}$ für $n \geq 2$ kein Körper.

(iv) $R^{n\times n}$ ist auch mit komponentenweiser Multiplikation ein Ring (sogar ein kommutativer Ring). Dieser Ring ist aber nicht besonders interessant. Mit komponentenweiser Multiplikation ist man nicht auf quadratische Matrizen beschränkt, auch $R^{m\times n}$ wird damit zu einem Ring.

3.2.4 Die lineare Gruppe

Definition. Die Einheitengruppe des Matrizenringes $R^{n\times n}$ (vgl. §2.2.2) wird die *allgemeine lineare Gruppe* über R vom Grad n genannt, geschrieben

$$\mathrm{GL}_n(R) := (R^{n\times n})^\times = \{A \in R^{n\times n} \mid A \text{ invertierbar}\}.$$

Die invertierbaren Matrizen heißen auch *regulär*. Das inverse Element zu $A \in \mathrm{GL}_n(R)$ wird die *inverse Matrix* zu A genannt, oder die *Inverse* von A.

Beispiel. $A = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} \in \mathbb{Q}^{2\times 2}$ ist regulär:

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

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

Also ist $A^{-1} = \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}$.

Bemerkung a. Mit $A \in \mathrm{GL}_n(R)$ ist auch $A^t \in \mathrm{GL}_n(R)$ und $(A^t)^{-1} = (A^{-1})^t$.

Beweis. Nach Satz 3.2.3ix gilt

$$A^t \cdot (A^{-1})^t = (A^{-1} \cdot A)^t = E_n^t = E_n,$$

und

$$(A^{-1})^t \cdot A^t = (A \cdot A^{-1})^t = E_n^t = E_n.$$

□

Übung. Es seien $A, B \in R^{n \times n}$.

(i) Kann man aus $A \cdot B = E_n$ schließen, dass A regulär und B die Inverse von A ist?

(ii) Wenn A als regulär vorausgesetzt wird, ist dann B notwendigerweise die Inverse von A? Was hat das mit Übung 2.1.3 zu tun?

3.3 Lineare Gleichungssysteme

3.3.1 Lineare Gleichungssysteme

In diesem Abschnitt sei K ein Körper.

Definition. Ein *lineares Gleichungssystem* über K, kurz LGS, hat die Form

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ & & & & \vdots & & & & \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m \end{array}$$

mit $a_{ij}, b_j \in K$ (die *Koeffizienten* des LGS). Das sind m Gleichungen in den n *Unbekannten* $x_1, \ldots, x_n$.

Eine *Lösung* des LGS ist ein Spalten-n-Tupel $\begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \in K^n$ $(= K^{n\times 1})$ derart, dass alle m Gleichungen erfüllt sind, wenn s_i für x_i eingesetzt wird $(i = 1, \ldots, n)$. Die Menge aller Lösungen wird mit $\mathbb{L}$ bezeichnet. Das LGS heißt *homogen*, wenn $b_1 = b_2 = \cdots = b_m = 0$, sonst *inhomogen*.

Aufgabe: Gegeben a_{ij} und b_i, bestimme alle Lösungen!

Beispiel a. Es sei $K = \mathbb{R}$ und $n = 2$; statt x_1, x_2 nimm x, y.

$$x^2 + y^2 = 1 \qquad \text{und} \qquad xy = 1 \qquad \text{sind nicht linear.}$$

Beispiel b. $n = 2, m = 2$.

$$\text{(i)} \begin{matrix} x + y = 2 \\ x - y = 0 \end{matrix} \qquad \text{(ii)} \begin{matrix} x + y = 2 \\ x + y = 0 \end{matrix} \qquad \text{(iii)} \begin{matrix} x + y = 2 \\ 3x + 3y = 6 \end{matrix}$$

Lösung:

(i) Aus $x - y = 0$ folgt $x = y$. Einsetzen in $x + y = 2$ liefert $2x = 2$, also $x = 1$. Ergebnis: $\mathbb{L} = \{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\}$ (genau eine Lösung).

(ii) Es folgt der Widerspruch $0 = 2$. Ergebnis: $\mathbb{L} = \emptyset$ (keine Lösung).

(iii) Aus $x + y = 2$ folgt $y = 2 - x$. Einsetzen in $3x + 3y = 6$ liefert $3x + 6 - 3x = 6$, also $6 = 6$. Das ist redundant und x bleibt „frei“. Ergebnis: $\mathbb{L} = \{\begin{pmatrix} x \\ 2 - x \end{pmatrix} \mid x \in K\}$ (mehr als eine Lösung).

Die gezeigten Lösungswege mittels Auflösen und Einsetzen nennt man *algebraische Lösungswege*. Es gibt auch *geometrische Lösungswege*, die aber in der Vorlesung nicht thematisiert werden.

3.3.2 Äquivalenzumformungen

In diesem Abschnitt sei wieder K ein Körper. Unsere Untersuchungen zielen darauf ab, die folgenden Frage zu beantworten.

(i) Wie löst man Gleichungen mit beliebig vielen Unbekannten? (Eine algebraische Lösung ist bevorzugt.)

(ii) Gibt es einen systematischen Weg?

(iii) Wie viele Lösungen kann es dabei geben?

Satz. *Die Lösungsmenge eines* LGS *ändert sich nicht, wenn*

(i) zwei Gleichungen vertauscht werden, oder

(ii) das c-fache ($c \in K$) einer Gleichung zu einer anderen addiert wird, oder

(iii) eine Gleichung mit einem $c \in K$ ($c \neq 0$) multipliziert wird.

Diese Umformungen heißen Äquivalenzumformungen.

Beweis. Die Aussagen (i) und (iii) sind klar. Um (ii) zu beweisen, können wir wegen (i) annehmen, dass die betreffenden Gleichungen die ersten beiden sind, also

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \end{array}$$

Nach der Umformung in (ii) werden daraus die beiden Gleichungen

$$\begin{array}{rcrcccrcr} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ (a_{21}+ca_{11})x_1 & + & (a_{22}+ca_{12})x_2 & + & \cdots & + & (a_{2n}+ca_{1n})x_n & = & b_2+cb_1 \end{array}$$

Ist nun $\begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \in K^n$ mit

$$\sum_{j=1}^{n} a_{1j}s_j = b_1$$

und

$$\sum_{j=1}^{n} a_{2j}s_j = b_2,$$

dann gilt auch

$$\sum_{j=1}^{n}(a_{1j}+ca_{2j})s_j = \sum_{j=1}^{n} a_{1j}s_j + c\sum_{j=1}^{n} a_{2j}s_j = b_1 + cb_2.$$

Damit ist jede Lösung des ursprünglichen LGS auch eine Lösung des umgeformten LGS. Das ursprüngliche LGS erhält man aus dem Umgeformten LGS durch Addition des $(-c)$-fachen der ersten Gleichung auf die zweite. Damit ist jede Lösung des umgeformten LGS auch eine Lösung des ursprünglichen LGS. Daraus folgt die Behauptung. □

Beispiel. Äquivalenzumformungen am Beispiel 3.3.1b:

$$\begin{array}{rcl} x+y &=& 2 \mid \cdot(-1) \\ x-y &=& 0 \end{array} \xleftarrow{+} \iff \begin{array}{rcl} x+y &=& 2 \\ -2y &=& -2 \mid \cdot(-\frac{1}{2}) \end{array}$$

$$\iff \begin{array}{rcl} x+y &=& 2 \\ y &=& 1 \mid \cdot(-1) \end{array} \xleftarrow{+} \iff \begin{array}{rcl} x &=& 1 \\ y &=& 1 \end{array}$$

Die Lösungsmenge lautet also $\mathbb{L} = \{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\}$.

Bemerkung.

(i) Äquivalenzumformungen sind eine (bessere) Alternative zum „Auflösen und Einsetzen“.

(ii) Wir haben in dem Beispiel nur mit den Koeffizienten des LGS gerechnet. Wir können uns sparen, die Unbekannten mit aufzuschreiben, wenn wir die Koeffizienten am „richtigen Platz“ belassen ($\to$ Matrix eines LGS).

3.3.3 Die Koeffizientenmatrix

Es sei K ein beliebiger Körper.

Definition. Gegeben sei das LGS über K:

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ & & & & \vdots & & & & \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m \end{array}$$

mit $a_{ij}, b_i \in K$ für alle $1 \le i \le m, 1 \le j \le n$. Die Matrix $A := (a_{ij}) \in K^{m\times n}$ heißt die *Koeffizientenmatrix*, und das Spalten-m-Tupel $b := (b_i) \in K^m$ heißt die *rechte Seite* des LGS. Als *erweiterte Koeffizientenmatrix* bezeichnen wir die Matrix

$$(A, b) = \begin{pmatrix} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{pmatrix} \in K^{m\times(n+1)}.$$

Für die Lösungsmenge des LGS schreiben wir $\mathbb{L}(A, b)$.

Bemerkung.

(i) Eine *Lösung* des LGS ist ein Spalten-n-Tupel $s := \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \in K^n$ mit

$$\sum_{j=1}^{n} a_{ij} s_j = b_i \text{ für jedes } i = 1, \ldots, m.$$

(ii) $\mathbb{L}(A, b) \subseteq K^n$.

(iii) Die „Namen“ der Unbekannten spielen jetzt keine Rolle mehr.

Beispiel. $K = \mathbb{Q}$ und $n = m = 4$. Das LGS

$$\begin{array}{rcrcrcrcl} x_1 & + & 2x_2 & & & + & x_4 & = & 1 \\ x_1 & + & 2x_2 & + & 2x_3 & + & 3x_4 & = & 5 \\ 2x_1 & + & 4x_2 & & & + & 3x_4 & = & 5 \\ & & & & 3x_3 & + & 2x_4 & = & 3 \end{array}$$

hat die erweiterte Koeffizientenmatrix

$$\begin{pmatrix} 1 & 2 & 0 & 1 & 1 \\ 1 & 2 & 2 & 3 & 5 \\ 2 & 4 & 0 & 3 & 5 \\ 0 & 0 & 3 & 2 & 3 \end{pmatrix} \in \mathbb{Q}^{4\times 5}.$$

Man zeigt mit Äquivalenzumformungen (Rechnung siehe Vorlesung):

$$\mathbb{L} = \left\{ \begin{pmatrix} -2-2t \\ t \\ -1 \\ 3 \end{pmatrix} \,\middle|\, t \in \mathbb{Q} \right\} = \left\{ \begin{pmatrix} -2 \\ 0 \\ -1 \\ 3 \end{pmatrix} + t \cdot \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix} \,\middle|\, t \in \mathbb{Q} \right\} \subseteq \mathbb{Q}^4.$$

3.3.4 Matrixmultiplikation und LGS

Wir setzen weiter voraus, dass K ein Körper ist. Wir wollen hier zeigen, wie man lineare Gleichungssysteme mithilfe von Matrizen formulieren kann.

Bemerkung a. Es sei $A = (a_{ij}) \in K^{m\times n}$ und $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$. Nach

Definition der Matrixmultiplikation (Spezialfall $l = 1$) ist

$$A \cdot x = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in K^m \quad \text{mit } b_i = \sum_{j=1}^{n} a_{ij} x_j \text{ für } i = 1, \ldots, m.$$

Aus diesem Grund schreiben wir das LGS über K mit erweiterter Koeffizientenmatrix $(A, b) \in K^{m \times (n+1)}$ formal als Matrixgleichung

$$A \cdot x = b,$$

wobei $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ ein Spalten-n-Tupel ist, das aus Unbekannten besteht. Eine Lösung von $A \cdot x = b$ ist ein Element $s \in K^n$ mit $As = b$ Die Lösungsmenge von $A \cdot x = b$ ist also gegeben durch

$$\mathbb{L}(A, b) = \{s \in K^n \mid As = b\}.$$

Beispiel. Das LGS

$$\begin{array}{rcrcrcl} 2x_1 & + & x_2 & - & x_3 & = & 5 \\ x_1 & - & x_2 & & & = & 1 \end{array}$$

wird als Matrixgleichung geschrieben:

$$\underbrace{\begin{pmatrix} 2 & 1 & -1 \\ 1 & -1 & 0 \end{pmatrix}}_{A} \cdot \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}}_{x} = \underbrace{\begin{pmatrix} 5 \\ -1 \end{pmatrix}}_{b}.$$

Schreibweise. Es sei $A \in K^{m \times n}$. Wir schreiben

(i) φ_A für die Abbildung $\varphi_A : K^n \to K^m, x \mapsto A \cdot x$.

(ii) $Ax = b$ für das lineare Gleichungssystem mit erweiterter Koeffizientenmatrix (A, b).

Bemerkung b.

(i) Für jedes $s \in \mathbb{L}(A,b)$ gilt

$$\mathbb{L}(A,b) = s + \mathbb{L}(A,0) := \{s+u \,|\, u \in \mathbb{L}(A,0)\}.$$

(ii) Das Bild von φ_A lautet $\varphi_A(K^n) = \{b \in K^m \,|\, Ax = b \text{ lösbar}\}$.

(iii) Die Faser von φ_A zu $b \in K^m$ lautet

$$\varphi_A^{-1}(\{b\}) = \{s \in K^n \,|\, As = b\} = \mathbb{L}(A,b).$$

Beweis. (i) Es sei $s \in \mathbb{L}(A,b)$, d.h. $s \in K^n$ mit $As = b$. Für ein beliebiges $t \in K^n$ folgt unter Benutzung von Satz 3.2.3(v):

$$\begin{aligned} t \in \mathbb{L}(A,b) &\Leftrightarrow At = b \Leftrightarrow At = As \\ &\Leftrightarrow A(t-s) = 0 \Leftrightarrow t - s \in \mathbb{L}(A,0) \Leftrightarrow t \in s + \mathbb{L}(A,0). \end{aligned}$$

□

3.4 Der Gauß-Algorithmus

Es sei K ein beliebiger Körper.

3.4.1 Zeilentransformationen

Wir führen die Äquivalenzumformungen eines LGS jetzt nur noch für seine erweiterte Koeffizientenmatrix durch.

Definition. Es seien $m, n \in \mathbb{N}$. Eine *elementare Zeilentransformation* ist eine Abbildung

$$t : K^{m\times n} \to K^{m\times n}, \quad A \mapsto t(A),$$

von einem der drei Typen τ, α, μ, wobei $1 \le i, j \le m$ und $c \in K$:

(i) τ_{ij}: vertauscht die i-te und j-te Zeile von A.

(ii) $\alpha_{ij}(c), i \neq j$: addiert das c-fache der j-ten Zeile zur i-ten Zeile von A.

(iii) $\mu_i(c)$ mit $c \neq 0$: multipliziert die i-te Zeile von A mit c.

Wir schreiben $A \rightsquigarrow B$, wenn die Matrix B aus A durch eine endliche Folge von elementaren Zeilentransformationen hervorgeht.

Beispiel. $K = \mathbb{Q}, m = 3, n = 4$.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 1 \\ -1 & -1 & 5 & 6 \end{pmatrix} \overset{\tau_{23}}{\rightsquigarrow} \begin{pmatrix} 1 & 2 & 3 & 4 \\ -1 & -1 & 5 & 6 \\ 0 & 0 & 1 & 1 \end{pmatrix} \overset{\alpha_{12}(2)}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 13 & 16 \\ -1 & -1 & 5 & 6 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$\overset{\mu_2(-1)}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 13 & 16 \\ 1 & 1 & -5 & -6 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Bemerkung.

(i) Jede elementare Zeilentransformation t ist *umkehrbar*, d.h. es gibt eine elementare Zeilentransformation t so dass gilt: $t \circ t' = t' \circ t = \mathrm{id}_{K^{m\times n}}$.

(ii) Die Relation $\rightsquigarrow$ ist eine Äquivalenzrelation auf $K^{m\times n}$. Gilt $A \rightsquigarrow B$, so nennen wir A und B *Gauß-äquivalent*.

Beweis. Übung (vgl. Satz 3.3.2). **Umkehrung von $\alpha_{ij}(c)$ ist $\alpha_{ij}(-c)$.** □

Satz. *Es seien $(A, b), (A', b') \in K^{m\times(n+1)}$ die erweiterten Koeffizientenmatrizen zweier linearer Gleichungssysteme. Es gilt:*

$$(A, b) \rightsquigarrow (A', b') \quad \Longrightarrow \quad \mathbb{L}(A, b) = \mathbb{L}(A', b').$$

Beweis. Elementare Zeilentransformationen der erweiterten Koeffizientenmatrix stellen Äquivalenzumformungen des LGS im Sinne von Satz 3.3.2 dar. Damit gilt

$$\mathbb{L}(A, b) = \mathbb{L}(\tau_{ij}(A, b)) = \mathbb{L}(\alpha_{ij}(c)(A, b)) = \mathbb{L}(\mu_i(c)(A, b)).$$

Die Behauptung ergibt sich durch Induktion nach der Anzahl der angewendeten elementaren Zeilentransformationen. □

Übung. Gilt auch die Umkehrung des Satzes, d.h. folgt aus $\mathbb{L}(A, b) = \mathbb{L}(A', b')$, dass $(A, b) \rightsquigarrow (A', b')$?

Beweis. Nein, z.B. $(A, b) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ und $(A', b') = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

□

Frage. Es seien $A, A' \in K^{m\times n}$. Folgt aus $\mathbb{L}(A, 0) = \mathbb{L}(A', 0)$, dass $A \rightsquigarrow A'$?

3.4.2 Zeilenstufenform

Weiterhin sei K ein beliebiger Körper.

Ziel: Bringe eine gegebene Matrix durch eine Folge elementarer Zeilentransformationen auf eine „einfache“ bzw. „praktische“ Gestalt (hängt vom Problem ab). Für LGS ist folgende Gestalt „praktisch“.

Definition. Es sei $A \in K^{m\times n}$. Für $i = 1, \dots, m$ bezeichne z_i die i-te Zeile von A. Definiere $k_i \in \{1, \dots, n+1\}$ als die Anzahl der führenden Nullen von z_i plus 1. Dann sagen wir A hat *Zeilenstufenform*, wenn

$$k_1 < k_2 < \cdots < k_r < k_{r+1} = \cdots = k_m = n+1$$

für ein $0 \le r \le m$ ist. Wir nennen r die *Stufenzahl* von A und $k_1, \dots, k_r$ die *Stufenindizes*.

Bemerkung. Die Definition von k_i bedeutet, dass z_i die Form

$$z_i = \begin{pmatrix} 0 & \dots 0 & \blacksquare & \star & \dots & \star \end{pmatrix}$$

hat, wobei $\blacksquare$ und $\star$ beliebige Einträge aus K sind, aber $\blacksquare \neq 0$ ist, und $\blacksquare$ genau an der k_i-ten Stelle steht. Enthält z_i nur Nullen, so ist $k_i = n+1$.

Eine Matrix hat demnach Zeilenstufenform, wenn sie so aussieht:

$$\left(\begin{array}{ccc|cccccccccc}
0 & \cdots & 0 & \blacksquare & \star & \cdots & \star & \star & \star & \cdots & \star & \star & \cdots & \star \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \blacksquare & \star & \cdots & \star & \star & \cdots & \star \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & & & \vdots & & & \\
\vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \ddots & & \star & \vdots & & \vdots \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \blacksquare & \star & \cdots & \star \\
\hline
0 & \cdots & 0 & 0 & \cdots & & 0 & 0 & \cdots & & 0 & & \cdots & 0 \\
\vdots & & \vdots & \vdots & & & \vdots & \vdots & & & \vdots & & \vdots & \\
0 & \cdots & 0 & 0 & \cdots & & 0 & 0 & \cdots & & 0 & & \cdots & 0
\end{array}\right)$$

Die $\blacksquare$ bilden die „Stufen“ und k_i ist der Spaltenindex der i-ten Stufe. Es gilt

$$r = \text{ Anzahl Stufen} = \text{Anzahl nicht-Null-Zeilen}.$$

Null-Zeilen dürfen in der Zeilenstufenform nur am unteren Ende der Matrix vorkommen, und es gibt genau $m-r$ davon. Insbesondere hat die Nullmatrix aus $K^{m\times n}$ Zeilenstufenform mit Stufenzahl $r = 0$.

Frage. Es seien $A, A' \in K^{m\times n}$ in Zeilenstufenform. Folgt aus $A \rightsquigarrow A'$, dass A und A' gleiche Stufenzahl (Stufenindizes) haben?

3.4.3 Gauß-Algorithmus I

Es sei K ein Körper.

Satz. *Jede Matrix $A \in K^{m\times n}$ kann durch eine Folge elementarer Zeilentransformationen (vom Typ τ und α) auf Zeilenstufenform gebracht werden.*

Bemerkung a. Der Satz besagt, dass jede Matrix A Gauß-äquivalent zu einer Matrix in Zeilenstufenform ist. Die Zeilenstufenform ist allerdings nicht eindeutig. Jede Matrix, die Gauß-äquivalent zu A und in Zeilenstufenform ist, nennen wir *eine Zeilenstufenform von A.*

Algorithmus (Gauß)**.** *Es sei $A = (a_{ij}) \in K^{m\times n}$. Für $j = 1, \ldots, n$ bezeichne s_j die j-te Spalte von A. Die folgenden Schritte überführen A in Zeilenstufenform.*

1. *Ist A die Nullmatrix oder eine $(1 \times n)$-Matrix, dann Stopp.*
2. *Setze $k := \min\{j \mid 1 \leq j \leq n, s_j \neq 0\}$.*
3. *Wähle ein i mit $a_{ik} \neq 0$ und wende τ_{1i} an. (τ_{11} ist erlaubt.)*
4. *Für jedes $i = 2, \ldots, m$ wende $\alpha_{i1}(-\frac{a_{ik}}{a_{1k}})$ an.*
5. *Führe die Schritte* 1. – 5. *rekursiv mit der Matrix $(a_{ij})_{\substack{2\leq i\leq m\\ k<j\leq n}} \in K^{(m-1)\times(n-k)}$ aus.*

Bemerkung b.

(i) Der Gauß-Algorithmus ist ein Algorithmus, der Matrizen auf Zeilenstufenform bringt. Das Lösen von linearen Gleichungssystemen ist eine wichtige Anwendung, die wir in den Abschnitten (3.4.4) und (3.4.5) herausarbeiten werden, aber bei weitem nicht die einzige Anwendung.

(ii) Der Gauß-Algorithmus verändert nicht die Größe einer Matrix. Insbesondere dürfen Null-Zeilen (streng genommen) nicht einfach weggelassen werden. Beim Lösen von (homogenen und inhomogenen) linearen Gleichungssystemen ist das aber trotzdem sinnvoll, da Null-Zeilen redundante Gleichungen repräsentieren.

(iii) Es folgt eine Erläuterung der einzelnen Schritte:

1. Jede Nullmatrix und jede $1 \times n$-Matrix ist in Zeilenstufenform.
2. Die k-te Spalte ist die erste Spalte von links, die nicht komplett aus Nullen besteht.

3. Falls in der k-ten Spalte ganz oben eine Null steht, dann tausche die oberste Zeile gegen eine andere, so dass das nicht mehr der Fall ist.
4. Addiere geeignete Vielfache der obersten Zeile zu allen anderen Zeilen, so dass alle anderen Zeilen Null-Einträge in der k-ten Spalte bekommen.
5. Mache rekursiv weiter mit der Teilmatrix, die in der zweiten Zeile und der $k+1$-ten Spalte beginnt.

(iv) Die k's aus allen rekursiven Durchläufen sind genau die Stufenindizes $k_1, \ldots, k_r$ der Zeilenstufenform, die am Ende herauskommt. Insbesondere durchläuft der Algorithmus genau r Rekursionsschritte.

(v) Nach den Schritten 3. und 4. wird die transformierte Matrix wieder mit (a_{ij}) bezeichnet.

Beispiel.

$$\begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ 2 & -4 & 6 & 9 & 1 \\ -1 & 2 & -1 & -3 & -6 \\ 1 & -2 & 5 & 4 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ 0 & 0 & 2 & 1 & -4 \\ 0 & 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

(Rechnung siehe Vorlesung)

3.4.4 Homogene LGS

Als Anwendung des Gauß-Algorithmus stellen wir ein Lösungsverfahren für homogene Lineare Gleichungssysteme vor.

Anwendung (Lösungsverfahren für homogene LGS)**.**
Gegeben sei ein homogenes LGS mit Koeffizientenmatrix $A \in K^{m \times n}$.

1. Bringe A mittels elementarer Zeilentransformationen auf Zeilenstufenform (z.B. mit Algorithmus 3.4.3).
2. Die r Unbekannten, die zu den Spalten mit den Stufenindizes $k_1, \ldots, k_r$ gehören, werden *abhängig* genannt, die anderen $n-r$ Unbekannten werden *frei* genannt.
3. Ersetze die freien Unbekannten durch Parameter $t_1, \ldots, t_{n-r} \in K$.
4. Löse von unten nach oben nach den abhängigen Unbekannten auf (*Rückwärtssubstitution*).

Beispiel. Für die Matrix $A \in \mathbb{Q}^{4\times 5}$ aus Beispiel 3.4.3 ergibt sich:

$$A \rightsquigarrow \begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ 0 & 0 & 2 & 1 & -4 \\ 0 & 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad \mathbb{L}(A,0) = \left\{ \left. \begin{pmatrix} 2t_1 - \frac{31}{2}t_2 \\ t_1 \\ \frac{1}{2}t_2 \\ 3t_2 \\ t_2 \end{pmatrix} \right| t_1, t_2 \in \mathbb{Q} \right\}.$$

(Rechnung siehe Vorlesung)

Bemerkung.

(i) Ein homogenes LGS hat immer eine Lösung, nämlich die *triviale Lösung* $0 \in K^n$.

(ii) Hat ein homogenes LGS weniger Gleichungen als Unbekannte ($m < n$), so gibt es nicht-triviale Lösungen.
Die Umkehrung dieser Aussage gilt nicht!

Erklärung: In Zeilenstufenform ist immer $r \leq m$. Aus $m < n$ folgt also $r < n$ bzw. $n - r > 0$. Da $n - r$ die Anzahl der freien Unbekannten ist, gibt es mehr als eine Lösung.

(iii) Für ein homogenes LGS sind folgende Aussagen äquivalent:

- Das LGS ist nicht-trivial lösbar.
- $\mathbb{L} \neq \{0\}$.
- Das LGS ist nicht eindeutig lösbar.
- Es gibt freie Unbekannte ($n - r > 0$).

Vorsicht bei der Aussage „das LGS hat unendlich viele Lösungen“: der Körper kann endlich sein!

Übung. Es seien $A, A' \in K^{m\times n}$ in Zeilenstufenform mit $A \rightsquigarrow A'$. Man zeige als teilweise Antwort auf Frage 3.4.2: Hat A die Stufenzahl n, so hat auch A' die Stufenzahl n.

3.4.5 Inhomogene LGS

Bemerkung. Nicht jedes inhomogene LGS hat eine Lösung. Über jedem Körper ist z.B. $0 \cdot x = 1$ unlösbar. Allgemein ist die lineare Gleichung $a \cdot x = b$ genau dann lösbar, wenn $a \neq 0$ oder $b = 0$ ist.

Anwendung (Lösungsverfahren für inhomogene LGS)**.**
Gegeben sei ein homogenes LGS mit erweiterter Koeffizientenmatrix $(A, b) \in K^{m\times(n+1)}$. Man bringe (A, b) mittels elementarer Zeilentransformationen auf Zeilenstufenform (z.B. mit Algorithmus 3.4.3).
Lösungsentscheidung. Es seien $k_1, \ldots, k_r$ die Stufenindizes der Zeilenstufenform. Die Lösbarkeit kann am Index k_r abgelesen werden: Ist $r > 0$ und $k_r = n + 1$, so ist das LGS unlösbar. In der Tat hat dann die r-te Zeile, welche die unterste Nicht-Null-Zeile ist, die Form $\begin{pmatrix} 0 & \cdots & 0 & \blacksquare \end{pmatrix}$. Sie entspricht einer nach der Bemerkung unlösbaren Gleichung $0 \cdot x_1 + \cdots + 0 \cdot x_n = b \neq 0$. Ist dagegen $r = 0$ oder $k_r \leq n$, so ist das LGS lösbar.
Lösungsmenge. Man betrachtet zunächst nur das homogene System (d.h. man ignoriert die Spalte b bzw. setzt sie gleich 0). Gemäß Anwendung 3.4.4 definiert man freie und abhängige Unbekannte und bestimmt die Lösungsmenge $\mathbb{L}(A, 0)$. Weiter bestimmt man eine beliebige Lösung $s \in \mathbb{L}(A, b)$, z.B. indem alle freien Unbekannten gleich 0 gesetzt werden. Die Lösungsmenge ergibt sich dann als

$$\mathbb{L}(A, b) = \{s + u \,|\, u \in \mathbb{L}(A, 0)\} = s + \mathbb{L}(A, 0). \tag{3.1}$$

Beweis. Die Lösungsentscheidung ist klar. Gleichung (3.1) wird in Bemerkung 3.3.4 b bewiesen. □

Beispiel. $n = m = 4$.

$$A = \begin{pmatrix} 1 & -2 & 3 & 4 \\ 2 & -4 & 6 & 9 \\ -1 & 2 & -1 & -3 \\ 1 & -2 & 5 & 4 \end{pmatrix} \in \mathbb{Q}^{4\times 4}, \qquad b = \begin{pmatrix} 2 \\ 1 \\ -6 \\ 1 \end{pmatrix} \in \mathbb{Q}^4.$$

Wie in Beispiel 3.4.3 haben wir

$$(A, b) \rightsquigarrow \begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ 0 & 0 & 2 & 1 & -4 \\ 0 & 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Damit ergibt sich

$$\mathbb{L}(A, b) = \left\{ \begin{pmatrix} 2t + \frac{31}{2} \\ t \\ -\frac{1}{2} \\ -3 \end{pmatrix} \,\middle|\, t \in \mathbb{Q} \right\} = \left\{ \begin{pmatrix} \frac{31}{2} \\ 0 \\ -\frac{1}{2} \\ -3 \end{pmatrix} + t \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix} \,\middle|\, t \in \mathbb{Q} \right\}.$$

(Rechnung siehe Vorlesung.) Wie in (3.1) schreiben wir auch:

$$\mathbb{L}(A,b) = \underbrace{\begin{pmatrix} \frac{31}{2} \\ 0 \\ -\frac{1}{2} \\ -3 \end{pmatrix}}_{\text{spezielle Lsg.}} + \underbrace{\mathbb{Q} \cdot \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix}}_{\mathbb{L}(A,0)}$$

Wir notieren noch ein Kriterium für die eindeutige Lösbarkeit von linearen Gleichungssystemen.

Bemerkung. Es sei A' eine Zeilenstufenform von A. Folgende Aussagen sind äquivalent:

(i) $Ax = b$ hat für jedes $b \in K^m$ höchstens eine Lösung.

(ii) $Ax = 0$ ist eindeutig lösbar (nur trivial).

(iii) A' hat Stufenzahl n.

(iv) φ_A ist injektiv. (Zur Definition von φ_A siehe Schreibweise 3.3.4.)

Insbesondere ist dann $m \geq n$.

Beweis. (i)⇒(ii): Setze $b := 0$.
(ii)⇒(iii): Da es keine freien Unbekannten geben kann, muss A' Stufenzahl n haben.
(iii)⇒(iv): Da A' Stufenzahl n hat, gibt es keine freien Unbekannten, also höchstens eine Lösung.
(iv)⇒(i): Klar aus der Definition von φ_A (vgl. auch Bemerkung 3.3.4 b). □

Übung. Wie sieht die reduzierte Zeilenstufenform von A aus, wenn die Aussagen der Bemerkung gelten?

3.4.6 Reduzierte Zeilenstufenform

Beim Lösen von (homogenen oder inhomogenen) LGS mit den vorgestellten Verfahren kann man auch die Rückwärtssubstitution durch elementare Zeilentransformationen darstellen.

Beispiel. Wir formen die Zeilenstufenform aus Beispiel 3.4.5 weiter um:

$$(A,b) \rightsquigarrow \begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ 0 & 0 & 2 & 1 & -4 \\ 0 & 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -2 & 0 & 0 & \frac{31}{2} \\ 0 & 0 & 1 & 0 & -\frac{1}{2} \\ 0 & 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

(Rechnung siehe Vorlesung.)
Hieraus kann man die Lösungsmenge ohne weitere Rechnung direkt ablesen:

$$\mathbb{L}(A,b) = \begin{pmatrix} \frac{31}{2} \\ 0 \\ \frac{1}{2} \\ -3 \end{pmatrix} + \mathbb{Q} \cdot \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Um das zu systematisieren machen wir die folgende

Definition. Es sei $A \in K^{m\times n}$.

(i) A hat *reduzierte Zeilenstufenform*, wenn A Zeilenstufenform hat (vgl. 3.4.2) und zusätzlich gilt:

$$\text{Für alle } 1 \leq j \leq r \text{ ist } a_{1k_j} = a_{2k_j} = \ldots = a_{j-1,k_j} = 0, a_{jk_j} = 1$$

(ii) A hat *Normalform*, wenn A reduzierte Zeilenstufenform hat und zusätzlich gilt:

$$\text{Für alle } 1 \leq i \leq r \text{ ist } k_i = i.$$

Bemerkung.

(i) Eine Matrix hat reduzierte Zeilenstufenform, wenn sie so aussieht:

$$\left(\begin{array}{ccc|cccccccccc} 0 & \cdots & 0 & 1 & \star & \cdots & \star & 0 & \star & \cdots & 0 & \star & \cdots & \star \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & \star & \cdots & 0 & \star & \cdots & \star \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & & & \vdots & & & \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \ddots & & 0 & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 & \star & \cdots & \star \\ \hline 0 & \cdots & 0 & 0 & \cdots & & 0 & 0 & \cdots & & 0 & & \cdots & 0 \\ \vdots & & \vdots & \vdots & & & \vdots & \vdots & & & \vdots & & \vdots & \\ 0 & \cdots & 0 & 0 & \cdots & & 0 & 0 & \cdots & & 0 & & \cdots & 0 \end{array}\right)$$

wobei $\star$ beliebige Einträge aus K sind.

(ii) Eine Matrix hat Normalform, wenn sie so aussieht:

$$\left(\begin{array}{ccccc|c} 1 & 0 & 0 & \cdots & 0 & \\ 0 & 1 & 0 & \cdots & 0 & \\ 0 & 0 & \ddots & & \vdots & \star \\ \vdots & \vdots & & 1 & 0 & \\ 0 & 0 & \cdots & 0 & 1 & \\ \hline & & 0 & & & 0 \end{array}\right)$$

wobei $\star$ ein beliebiger „Block“ ist.

3.4.7 Gauß-Algorithmus II

Satz. *Jede Matrix $A \in K^{m\times n}$ kann durch eine Folge elementarer Zeilentransformationen (vom Typ τ, α und μ) auf reduzierte Zeilenstufenform gebracht werden. Mit Spaltenvertauschungen kann A weiter auf Normalform gebracht werden.*

Übung. Man schreibe die einzelnen Schritte eines Algorithmus auf, der eine gegebene Matrix in Zeilenstufenform auf reduzierte Zeilenstufenform bringt (mittels elementarer Zeilentransformationen).

Bemerkung a. Beim Lösen von (homogenen und inhomogenen) linearen Gleichungssystemen darf man auch Spalten vertauschen, wenn man über die Zuordnung zwischen Spalten und Unbekannten in geeigneter Weise Buch führt und die „b-Spalte“ an ihrer Stelle belässt. Spaltenvertauschungen gehören üblicherweise nicht zum Gauß-Algorithmus.

Beispiel a. Spaltenvertauschungen können die Rechnung abkürzen. Z.B. kann man

$$(A,b) := \begin{pmatrix} x_1 & x_2 & x_3 & b \\ 2 & 1 & -1 & 2 \\ -2 & 0 & 1 & -6 \\ 1 & 0 & 0 & 3 \end{pmatrix}$$

allein durch Spaltenvertauschungen auf die Zeilenstufenform

$$\begin{pmatrix} x_2 & x_3 & x_1 & b \\ 1 & -1 & 2 & 2 \\ 0 & 1 & -2 & -6 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

bringen. Weiter kommt man in zwei Schritten zur reduzierten Zeilenstufenform:

$$\begin{pmatrix} x_2 & x_3 & x_1 & b \\ 1 & -1 & 2 & 2 \\ 0 & 1 & -2 & -6 \\ 0 & 0 & 1 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} x_2 & x_3 & x_1 & b \\ 1 & 0 & 0 & -4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

Diese ist gleichzeitig Normalform, und man liest als Lösungsmenge ab:

$$\mathbb{L}(A,b) = \left\{ \begin{pmatrix} 3 \\ -4 \\ 0 \end{pmatrix} \right\}.$$

(Man achte auf die Reihenfolge der Einträge!)

Beispiel b. Über $K = \mathbb{Q}$ sei die folgende erweiterte Koeffizientenmatrix in Normalform gegeben:

$$(A, b) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 2 & 1 & 4 \\ 0 & 0 & 1 & 0 & -1 & 6 \end{pmatrix}.$$

Die Lösungsmenge kann man direkt ohne jede Rechnung ablesen:

$$\mathbb{L}(A, b) = \begin{pmatrix} 2 \\ 4 \\ 6 \\ 0 \\ 0 \end{pmatrix} + \mathbb{Q} \cdot \begin{pmatrix} 1 \\ 2 \\ 0 \\ -1 \\ 0 \end{pmatrix} + \mathbb{Q} \cdot \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \\ -1 \end{pmatrix}.$$

(Erläuterung in der Vorlesung.)

Bemerkung b. Das Beispiel lässt sich wie folgt verallgemeinern. Es sei

$$A = \left(\begin{array}{c|c} E_r & C \\ \hline 0 & 0 \end{array}\right) \in K^{m \times n}$$

(also $C \in K^{r \times (n-r)}$) in Normalform. Weiter sei

$$b = \begin{pmatrix} b' \\ \hline b'' \end{pmatrix} \in K^m$$

mit $b' \in K^r$ und $b'' \in K^{m-r}$.

(Wir stellen uns vor, dass die Matrix (A, b) aus der erweiterten Koeffizientenmatrix eines LGS durch elementare Umformungen und Spaltenvertauschungen der ersten n Spalten entstanden ist. Dann kann aus der Lösungsmenge $\mathbb{L}(A, b)$ die Lösungsmenge des ursprünglichen LGS gemäß Bemerkung a und Beispiel a bestimmt werden.)

Mit obigen Notationen gilt:

(i) $\mathbb{L}(A, 0) = \left\{ \begin{pmatrix} C \\ \hline -E_{n-r} \end{pmatrix} t \mid t \in K^{n-r} \right\}$.

(ii) $\mathbb{L}(A, b) = \emptyset \Leftrightarrow b'' \neq 0$.

(iii) Ist $b'' = 0$, dann ist $\begin{pmatrix} b' \\ \hline 0 \end{pmatrix} \in \mathbb{L}(A, b)$.

Beweis. Aus den Formeln für die Matrixmultiplikation folgt

$$\left(\begin{array}{c|c} E_r & C \\ \hline 0 & 0 \end{array}\right) \cdot \left(\begin{array}{c} C \\ \hline -E_{n-r} \end{array}\right) = 0 \in K^{m\times(n-r)}.$$

Daraus ergibt sich (i). (Alternativ kann Anwendung 3.4.4 zum Beweis von (i) verwendet werden.) Aussage (ii) ist die Lösbarkeitsentscheidung für das LGS mit erweiterter Koeffizientenmatrix (A, b) in Zeilenstufenform (siehe Anwendung 3.4.5). Die letzte Aussage folgt aus der Gestalt von (A, b). □

Diskrete Mathematik

Einleitung

In der Mathematik ist der Begriff „**diskret**“ als gegensätzlich zu „kontinuierlich“ zu verstehen. *Diskret* werden solche Strukturen genannt, die endlich sind oder – falls unendlich – zumindest schrittweise abzählbar; als *kontinuierlich* dagegen solche, die nicht schrittweise abzählbar sind. In diesem Sinne ist z.B. die Zahlenmenge der natürlichen Zahlen $\{1, 2, 3, \ldots\}$ diskret, während die Zahlenmenge der reellen Zahlen (Dezimalbrüche) kontinuierlich ist. Letzteres wird veranschaulicht, indem man sich die reellen Zahlen als eine kontinuierliche Zahlengerade (von $-\infty$ bis $+\infty$ mit 0 in der „Mitte“) vorstellt. Auf dieser reellen Zahlengerade sind dann die natürlichen Zahlen als eine abzählbare Folge von Punkten zu finden.

In dieses Schema passen insbesondere die in der Elektro- bzw. Informationstechnik verwendeten Begriffe „digital“ und „analog“. Ein „digitaler Wert“ ist auf einer diskreten Menge definiert (mit den Elementen 0 und 1, also sogar auf einer endlichen Menge), während ein analoger Wert auf einem Kontinuum (z.B. auf einem bestimmten Abschnitt der reellen Zahlengerade) definiert ist.

Unter den mathematischen Disziplinen beschäftigt sich die **Analysis** mit kontinuierlichen Strukturen (insbesondere mit den reellen Zahlen) und die **Diskrete Mathematik** mit diskreten Strukturen. Die diskrete Mathematik, obwohl in der Form des Studiums der natürlichen Zahlen schon im Altertum präsent, wird aber erst seit dem 20. Jahrhundert als eigenständiges Gebiet betrachtet. So wie eine besondere Motivation für die Entwicklung der Analysis auf Anwendungen in der Physik zurückgeht, gilt das gleiche für die diskrete Mathematik und die Informatik. Offensichtlich sind die in der Informatik beschriebenen und untersuchten Objekte wie Digitalcomputer, Programme (Algorithmen), formale Sprachen, etc. diskreter Natur, während die in der klassischen Physik untersuchten Prozesse kontinuierlicher Natur sind (bzw. sich als kontinuierlich vorgestellt werden).

Wichtige diskrete Strukturen bzw. Objekte, die in dieser Vorlesung behandelt werden, sind endliche Mengen und Summen (Kap. Kombinatorik), endliche Graphen (Kap. Graphentheorie), das Zahlsystem der ganzen Zahlen und Polynome (beides Kap. Algebraische Strukturen).

Kapitel 4

Kombinatorik

4.1 Permutationen und Kombinationen

Es sei A in diesem Abschnitt eine endliche Menge mit $|A| = n$.

4.1.1 Permutationen

Definition a. Es sei $k \in \mathbb{N}, k \leq n$. Eine *$k$-Permutation* aus A ist eine geordnete Auswahl von k verschiedenen Elementen aus A. Eine n-Permutation aus A wird auch kurz *Permutation von A* genannt.

Mit „geordneter Auswahl“ ist gemeint, dass es auf die Reihenfolge der Auswahl ankommt. Mathematisch ist eine k-Permutation aus A ein k-Tupel über A (vgl. Definition 1.4.1 b), dessen Einträge paarweise verschieden sind. Dementsprechend werden k-Permutationen in derselben Schreibweise wie Tupel notiert.

Eine Permutation von A kann auch als eine „Anordnung“ von A aufgefasst werden.

Beispiel a.

(i) $(4, 3, 2), (4, 2, 3)$ und $(3, 5, 1)$ sind verschiedene 3-Permutationen aus $\underline{5}$.

(ii) $(1, 2, 1)$ ist keine Permutation.

(iii) $(1, 3, 5, 2, 4)$ und $(5, 4, 3, 2, 1)$ sind Permutationen von $\underline{5}$.

(iv) Die Medaillenverteilung nach einem 100m-Lauf mit 8 Läufern ist eine 3-Permutation aus $\underline{8}$.

(v) Die aktuelle Bundesligatabelle ist eine Permutation von $\underline{18}$.

Definition b. Für $n \in \mathbb{N}$ heißt

$$n! := 1 \cdot 2 \cdot \ldots \cdot n$$

die *Fakultät von n*. Wir setzen $0! := 1$.

Satz. *Es sei $k \in \mathbb{N}, k \leq n$. Die Anzahl der k-Permutationen aus A beträgt $\frac{n!}{(n-k)!}$. Die Anzahl der Permutationen von A beträgt $n!$.*

Beweis. Wir bilden alle k-Tupel $(a_1, \ldots, a_k)$ über A mit paarweise verschiedenen Einträgen. Dabei gibt es

$$\begin{aligned} n &\text{ Möglichkeiten für } a_1, \\ n-1 &\text{ Möglichkeiten für } a_2, \\ &\vdots \\ n-(k-1) &\text{ Möglichkeiten für } a_k, \end{aligned}$$

also $n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}$ Möglichkeiten insgesamt. □

Beispiel b.

(i) Die Anzahl der 2-Permutationen aus $\underline{3}$ ist $\frac{3!}{(3-2)!} = 6$.

(ii) Es gibt genau $\frac{8!}{(8-3)!} = 6 \cdot 7 \cdot 8 = 336$ mögliche Medaillenverteilungen (Gold, Silber, Bronze) auf 8 Läufer.

(iii) Es gibt $18! \approx 6,4 \cdot 10^{15}$ mögliche Bundesligatabellen aus 18 Mannschaften.

4.1.2 Kombinationen

Definition. Es sei $k \in \mathbb{N}, k \leq n$. Eine *$k$-Kombination* aus A ist eine ungeordnete Auswahl von k verschiedenen Elementen aus A.

Mit „ungeordneter Auswahl“ ist gemeint, dass es auf die Reihenfolge der Auswahl nicht ankommt. Mathematisch ist eine k-Kombination aus A eine k-elementige Teilmenge von A. Dementsprechend werden k-Kombinationen in derselben Schreibweise wie Mengen notiert.

Beispiel a.

(i) Es sei $A = \underline{5} = \{1, 2, 3, 4, 5\}$. Dann sind $\{4, 3, 2\} = \{4, 2, 3\}$ und $\{3, 5, 1\}$ verschiedene 3-Kombinationen aus A.

(ii) Ein ausgefüllter Lottoschein ist eine 6-Kombination aus $\underline{49}$.

(iii) Die Bundesliga-Absteiger bilden einen 3-Kombination aus $\underline{18}$.

(iv) Eine Skathand ist eine 10-Kombination aus $\underline{32}$.

Satz. *Es sei $k \in \mathbb{N}$ mit $k \leq n$. Die Anzahl der k-Kombinationen aus A beträgt $\frac{n!}{k!(n-k)!}$.*

Beweis. Aus einer k-Kombination wird durch Anordnung eine k-Permutation. Jede k-Kombination kann gemäß Satz 4.1.1 auf $k!$ Arten angeordnet werden. Z.B.

$$\{2,3,4\} \subseteq \underline{5} \overset{Anordnung}{\longrightarrow} (2,3,4),(2,4,3),(3,2,4),(3,4,2),(4,2,3),(4,3,2)$$

$$\{1,3\} \subseteq \underline{5} \overset{Anordnung}{\longrightarrow} (1,3),(3,1)$$

Also gilt

$$k! \cdot \#k\text{-Kombinationen} = \#k\text{-Permutationen}.$$

Da die rechte Seite nach Satz 4.1.1 gleich $\frac{n!}{(n-k)!}$ ist, folgt die Behauptung durch Division durch $k!$. □

Beispiel b.

(i) Die Anzahl der 2-Kombinationen aus $\underline{4}$ ist $\frac{4!}{2!(4-2)!} = 6$.

(ii) Es gibt $\frac{49!}{6!43!} = 13983816$ Möglichkeiten, einen Lottoschein auszufüllen.

(iii) Es gibt $\frac{18!}{3!15!} = 816$ Möglichkeiten, drei von 18 Mannschaften absteigen zu lassen.

(iv) Es gibt $\frac{32!}{10!22!} \approx 64512240$ mögliche Skathände.

4.1.3 Tupel

Bemerkung. Es sei A eine Menge und $k \in \mathbb{N}$. Ein k-Tupel über A ist eine geordnete Auswahl von k beliebigen (nicht notwendigerweise verschiedenen) Elementen aus A.

Beispiel.

(i) Eine natürliche Zahl mit maximal k Dezimalstellen ist ein k-Tupel über $\{0,1,\ldots,9\}$.

(ii) Das Resultat einer Klausur mit k Teilnehmern und 11 möglichen Noten (von 1.0 bis 5.0) ist ein k-Tupel über $\underline{11}$. Nummeriert man die Teilnehmer von 1 bis k und ist a_i die Note von Teilnehmer i, dann ist das Resultat das Tupel $(a_1,\ldots,a_k)$.

(iii) Teilmengen von $\underline{n}$ können durch n-Tupel über $\{0,1\}$ „kodiert“ werden.

Erklärung: Der Teilmenge $M \subseteq \underline{n}$ wird das n-Tupel $\iota_M := (x_1, \ldots, x_n) \in \{0,1\}^n$ zugeordnet, das folgendermaßen definiert ist:

$$x_i := \begin{cases} 1, & \text{falls } i \in M, \\ 0, & \text{falls } i \notin M. \end{cases}$$

„Kodiert“ bedeutet hier, dass die Abbildung

$$\mathrm{Pot}(\underline{n}) \to \{0,1\}^n, \quad M \mapsto \iota_M$$

eine Bijektion ist.

Z.B. werden $\{2,4\} \subseteq \underline{5}$ das 5-Tupel $(0,1,0,1,0)$, und $\{2,3\} \subseteq \underline{3}$ das 3-Tupel $(0,1,1)$ zugeordnet.

Satz. *Es sei A eine endliche Menge mit $|A| = n$ und $k \in \mathbb{N}$. Die Anzahl der k-Tupel über A beträgt n^k.*

Beweis. Klar. □

Folgerung. $|\mathrm{Pot}(A)| = 2^n$.

Beweis. Der Satz und Beispiel (iii). □

4.1.4 Multimengen

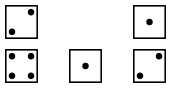
Definition. Es sei $k \in \mathbb{N}$. Eine *k-Multimenge über A* ist eine ungeordnete Auswahl von k beliebigen (nicht notwendigerweise verschiedenen) Elementen aus A.

Schreibweise. Eine Multimenge ist eine „Menge mit Wiederholungen“ und wird mit den modifizierten Mengenklammern $\{^*$ und $^*\}$ notiert.

Bemerkung. Eine k-Multimenge über A kann kodiert werden durch ein n-Tupel über $\mathbb{N}_0$, dessen Einträge sich zu k aufsummieren. Dazu nummeriert man die Elemente von A, etwa $A = \{a_1, \ldots, a_n\}$, und gibt im i-ten Eintrag des Tupels an, wie oft a_i in der Multimenge vorkommt. Wir nennen dieses Tupel das *Häufigkeitstupel* der Multimenge.

Beispiel.

(i) Ein Lostopf ist eine Multimenge, aber in der Regel keine Menge, da gewisse Lose mehrfach vorkommen können (z.B. Nieten).

(ii) Das Resultat eines Kniffel-Wurfs (Wurf mit 5 Würfeln gleichzeitig) ist eine 5-Multimenge über $\underline{6}$. Der Wurf  bedeutet z.B. die Multimenge $\{^*2, 1, 4, 1, 2^*\} = \{^*1, 1, 2, 2, 4^*\}$. Als 6-Tupel über $\mathbb{N}_0$ geschrieben bedeutet dieser Wurf $(2, 2, 0, 1, 0, 0)$.

(iii) Der Notenspiegel einer Klausur mit k Teilnehmern und 11 möglichen Noten (von 1.0 bis 5.0) ist eine k-Multimenge über $\underline{11}$. Der Notenspiegel ist das anonymisierte Resultat der Klausur. Nummeriert man die Teilnehmer von 1 bis k und ist a_i die Note von Teilnehmer i, dann ist der Notenspiegel die k-Multimenge $\{^*a_1, \ldots, a_k{}^*\}$. Üblicherweise wird ein Notenspiegel als Tabelle der Häufigkeiten der einzelnen Noten angegeben. Diese Tabelle ist gerade das oben erwähnte Häufigkeitstupel von A, ein 11-Tupel über $\mathbb{N}_0$.

Satz. *Es sei A eine endliche Menge mit $|A| = n$ und $k \in \mathbb{N}$. Die Anzahl der k-Multimengen über A beträgt $\frac{(n+k-1)!}{k!(n-1)!}$.*

Beweis. Es sei $k \in \mathbb{N}$. Wir zählen die n-Tupel $(l_1, \ldots, l_n)$ über $\mathbb{N}_0$ mit $\sum_{i=1}^{n} l_i = k$. Dazu kodieren wir Tupel dieser Art als $(n + k - 1)$-Tupel über $\{0, 1\}$, indem wir für jedes Komma eine Null und für jedes $l_i > 0$ genau l_i viele Einsen schreiben. Aus dem Tupel $(2, 2, 0, 1, 0, 0)$ wird z.B. das Wort 1101100100. Offensichtlich gehört zu jedem n-Tupel über $\mathbb{N}_0$, dessen Einträge sich zu k aufsummieren, ein $(n+k-1)$-Tupel mit k Einsen und $n-1$ Nullen. Umgekehrt entsteht jedes $(n + k - 1)$-Tupel mit k Einsen und $n - 1$ Nullen aus einem n-Tupel über $\mathbb{N}_0$, dessen Einträge sich zu k aufsummieren.

Ein $(n+k-1)$-Tupel aus k Einsen und $n-1$ Nullen ist eindeutig durch die Positionen der k vielen Einsen gegeben, entspricht also einer k-Kombination aus $\underline{n + k - 1}$. Gemäß Satz 4.1.2 lautet die gesuchte Anzahl somit $\frac{(n+k-1)!}{k!(n-1)!}$. □

4.2 Binomialkoeffizienten

Es seien in diesem Abschnitt $n, k \in \mathbb{N}_0$.

4.2.1 Definition und Binomischer Lehrsatz

Definition. Für $k \leq n$ heißt

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

der *Binomialkoeffizient „n über k“*.

Nach Satz 4.1.2 ist $\binom{n}{k}$ gleich der Anzahl der k-Kombinationen aus einer n-elementigen Menge. Insbesondere ist $\binom{n}{k}$ stets eine ganze Zahl. Es gilt $\binom{n}{0} = \binom{n}{n} = 1$ für alle $n \in \mathbb{N}_0$ und $\binom{n}{1} = \binom{n}{n-1} = n$ für alle $n \in \mathbb{N}$.

Schreibweise. Es sei R ein kommutativer Ring. Für $a \in R$ und $z \in \mathbb{Z}$ schreiben wir

$$z.a := \begin{cases} \underbrace{a + a + \cdots + a}_{z \text{ Summanden}}, & \text{falls } z \in \mathbb{N} \\ 0, & \text{falls } z = 0 \\ -(-z.a), & \text{falls } z < 0 \end{cases}$$

Meist lassen wir den Punkt weg, d.h. wir schreiben za statt $z.a$.

Ist $z = xy$ für $x, y \in \mathbb{Z}$, dann gilt $z.a = x.(y.a)$ für alle $a \in R$.

Satz (Binomischer Lehrsatz)**.** *Es sei R ein kommutativer Ring. Für $a, b \in R$ und $n \in \mathbb{N}_0$ gilt*

$$\begin{aligned}(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\ &= \binom{n}{0} b^n + \binom{n}{1} a^1 b^{n-1} + \ldots + \binom{n}{n-1} a^{n-1} b^1 + \binom{n}{n} a^n.\end{aligned}$$

Beweis. Wir betrachten den Ausdruck $(a+b)^n = (a+b)\cdots(a+b)$ und nummerieren die Klammern mit $1, \ldots, n$. Für jeden der Summanden, die beim Ausmultiplizieren entstehen, wird aus jeder der n Klammern entweder das a oder das b ausgewählt. Bezeichnen wir mit I die Menge der Nummern der Klammern, aus denen a ausgewählt wird, so gilt

$$(a+b)^n = \sum_{I \subseteq \underline{n}} a^{|I|} b^{n-|I|}.$$

Hier durchläuft I alle Teilmengen von $\underline{n}$, d.h. I durchläuft $\mathrm{Pot}(\underline{n})$. Also hat die Summe $|\mathrm{Pot}(\underline{n})| = 2^n$ Summanden. Wir fassen nun jeweils alle Summanden $a^k b^{n-k}$ für gleiches k zusammen. Da es genau $\binom{n}{k}$ Teilmengen $I \subseteq \underline{n}$ mit $|I| = k$ gibt, erhalten wir

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

□

Korollar. *Es sei R ein Ring und p eine Primzahl mit $p.a = 0$ für alle $a \in R$ (z.B. $R = \mathbb{F}_p$ der Körper mit p Elementen). Dann ist*

$$(a+b)^p = a^p + b^p$$

für alle $a, b \in R$.

Beweis. Nach dem binomische Lehrsatz gilt

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{n-k}.$$

Für $0 < k < p$ ist

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdots (p-k+1)}{k!}$$

von der Form xp für ein $x \in \mathbb{N}$, also $\binom{p}{k}.a^k b^{p-k} = 0$. □

Übung. Man zeige mit Hilfe des Binomischen Lehrsatzes die Identität

$$\sum_{k=1}^{n} (-1)^k \binom{n}{k} = -1 \quad (n \geq 1).$$

4.2.2 Das Pascal'sche Dreieck

Satz. *Für alle $n, m \in \mathbb{N}_0$ gelten:*

(i) $\binom{n}{k} = \binom{n}{n-k}$ *für alle* $0 \leq k \leq n$,

(ii) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ *für alle* $1 \leq k \leq n-1$,

(iii) $\sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i} = \binom{m+n}{k}$ *für alle* $0 \leq k \leq n, m$. *(Vandermonde-Identität)*

Beweis. (i) Ist klar nach Definition.
(ii) Es sei $1 \leq k \leq n$. Wir teilen alle k-elementigen Teilmengen $I \subseteq \underline{n}$ auf in solche I, die n enthalten, und solche I, die n nicht enthalten. Die I's der zweiten Art sind Teilmengen von $\underline{n-1}$, also gibt es davon $\binom{n-1}{k}$ viele. Die I's der ersten Art sind die Vereinigung von $\{n\}$ mit einer $(k-1)$-elementigen Teilmengen von $\underline{n-1}$, also gibt es davon $\binom{n-1}{k-1}$ viele. Da die Anzahl aller k-elementigen Teilmengen von $\underline{n}$ genau $\binom{n}{k}$ beträgt, folgt die Behauptung.
(iii) Als Übung. □

Die Binomialkoeffizienten lassen sich im sog. *Pascal'schen Dreieck* anordnen:

$n=0$:						1						
$n=1$:					1		1					
$n=2$:				1		2		1				
$n=3$:			1		3		3		1			
$n=4$:		1		4		6		4		1		
$n=5$:	1		5		10		10		5		1	
$n=6$:	1		6		15		20		15		6	1

Definiert man $\binom{n}{k} := 0$ für $k < 0$ und $k > n$, also „außerhalb des Dreiecks“, so gelten die Aussagen des Satzes uneingeschränkt für alle $k, n, m \in \mathbb{N}_0$.

Übung.

(i) Man zeige Teil (ii) des Satzes durch direktes Einsetzen der Definition und Umformung.

(ii) Man zeige mittels vollständiger Induktion, dass $\binom{n}{k}$ eine ganze Zahl ist. *Hinweis:* Verwende den Satz.

(iii) Man zeige den Binomischen Lehrsatz mittels vollständiger Induktion. *Hinweis:* Verwende den Satz.

(iv) Man zeige mittels vollständiger Induktion, dass $\sum_{i=1}^{n} i = \binom{n+1}{2}$. *Hinweis:* Verwende den Satz.

(v) Es seien $n_1, \ldots, n_r \in \mathbb{N}$ und $n = \sum_{i=1}^{r} n_i$. Man zeige: $\sum_{i=1}^{r} \binom{n_i}{2} \leq \binom{n-r+1}{2}$. Ist die Ungleichung scharf?

(vi) Man zeige mittels vollständiger Induktion:

$$\sum_{k=1}^{n} (-1)^k \binom{n}{k} = -1 \quad (n \geq 1).$$

Hinweis: Verwende den Satz.

(vii) Man zeige die Vandermonde-Identität mit einem kombinatorischen Beweis. *Hinweis:* Verallgemeinere den Beweis von Teil (ii) des Satzes.

(viii) Man zeige die Vandermonde-Identität mittels vollständiger Induktion.

4.3 Kombinatorische Beweisprinzipien

Wir formulieren nun systematisch einige kombinatorische Beweisprinzipien. Zum Teil wurden diese Prinzipien in den Beweisen der §§1–2 und in den Übungen schon angewendet.

4.3.1 Summenregel

Prinzip. Für disjunkte, endliche Mengen A und B gilt stets

$$|A \cup B| = |A| + |B|.$$

Das Prinzip lässt sich sofort auf endlich viele Mengen verallgemeinern: Für paarweise disjunkte, endliche Mengen $A_1, \ldots, A_r$ gilt stets

$$|\bigcup_{i=1}^{r} A_i| = \sum_{i=1}^{r} |A_i|.$$

Beispiel.

(i) Der Beweis von Satz 4.2.2(ii).

(ii) Ist $A \subseteq M$, so hat die *Komplementärmenge* $M \setminus A$ die Mächtigkeit $|M| - |A|$.

Übung.

(i) Wie viele Teilmengen von $\underline{6}$ gibt es, die höchstens 4 Elemente enthalten?

(ii) Man zeige mit Hilfe der Summenregel, dass $\sum_{i=0}^{n} \binom{n}{i} = 2^n$.

4.3.2 Produktregel

Prinzip. Für zwei beliebige endliche Mengen A und B gilt stets

$$|A \times B| = |A| \cdot |B|.$$

Das Prinzip lässt sich sofort auf endlich viele Mengen verallgemeinern: Für endliche Mengen $A_1, \ldots, A_r$ gilt stets

$$|A_1 \times \cdots \times A_r| = \prod_{i=1}^{r} |A_i|.$$

Insbesondere gilt für jede endliche Menge und jedes $n \in \mathbb{N}$:

$$|A^n| = |A|^n.$$

Beispiel.

(i) Der Beweis von Satz 4.1.2.

(ii) Der Beweis von Satz 4.1.4.

Übung a. Wie viele Tippreihen mit genau 4 Richtigen gibt es für eine feste Lotto-Ziehung?

Satz. *Es sei $\mathcal{A}$ eine Multimenge mit r verschiedenen Elementen $a_1, \dots, a_r$. wobei a_i mit Häufigkeit k_i auftritt. Sei $k = k_1 + \cdots + k_r$, die „Mächtigkeit" von $\mathcal{A}$. Die Anzahl der Anordnungen von $\mathcal{A}$ beträgt dann*

$$\frac{k!}{k_1! \cdots k_r!}.$$

1. Beweis. Wir betrachten statt $\mathcal{A}$ zunächst die Menge

$$A = \{a_{11}, \dots, a_{1k_1}, a_{21}, \dots, a_{2k_2}, \dots, a_{r1}, \dots, a_{rk_r}\},$$

in der die a_{ij} als verschieden angenommen werden. Offensichtlich ist $|A| = k$. Nach Satz 4.1.1 gibt es $k!$ verschiedene Anordnungen von A. Jede Anordnung von $\mathcal{A}$ entsteht aus einer Anordnung von A, indem man, für jedes i, alle a_{ij} durch a_i ersetzt. Diese Ersetzung, durchgeführt für ein festes i, macht genau $k_i!$ verschiedene Anordnungen von A gleich. Nach der Produktregel macht diese Ersetzung, durchgeführt für alle i, also genau $k_1! \cdots k_r!$ verschiedene Anordnungen von A gleich. Daraus ergibt sich die Formel $\frac{k!}{k_1! \cdots k_r!}$ für die Zahl der Anordnungen von $\mathcal{A}$. □

2. Beweis. Jede Anordnung von $\mathcal{A}$ entsteht auf eindeutige Weise aus folgendem Prozess: Wir wählen eine k_1-Kombination von $\underline{k}$; diese gibt die Positionen in der Anordnung an, an denen wir a_1 eintragen. (Es muss genau k_1 Positionen in der Anordnung geben, an denen a_1 steht.) Wir wählen dann eine k_2-Kombination aus den verbleibenden $k - k_1$ Positionen, um dort a_2 einzutragen, usw. Nach Produktregel gibt es für diesen Prozess genau $\binom{k}{k_1}\binom{k-k_1}{k_2}\binom{k-k_1-k_2}{k_3} \dots \binom{k-k_1-\dots-k_{r-1}}{k_r}$. (Der letzte Faktor ist identisch $\binom{k_r}{k_r} = 1$.) Durch Einsetzen und Kürzen ergibt sich die Formel. □

Übung b. (i) Wie viele verschiedene Wörter kann man durch Anordnung der Buchstaben `P,I,Z,Z,A` gewinnen?

(ii) Wie viele Möglichkeiten gibt es, aus 25 Fußballspielern zwei Mannschaftsaufstellungen (erste und zweite Mannschaft) mit je 11 Spielern zu machen?

(iii) Auf einem Kongress gibt es einen Hauptredner, der dreimal vortragen soll, und drei Nebenredner, die je zweimal vortragen sollen. Wie viele Vortragsprogramme sind möglich?

4.3.3 Inklusions-Exklusions-Prinzip

Prinzip. Für zwei beliebige endliche Mengen A und B gilt stets

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Das Prinzip lässt sich auf endlich viele Mengen verallgemeinern:

Satz. *Für endliche Mengen $A_1, \ldots, A_r$ gilt die Formel*

$$\begin{aligned} |\bigcup_{i=1}^{r} A_i| &= \sum_{k=1}^{r} (-1)^{k-1} \sum_{1 \le i_1 < \ldots < i_k \le r} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| \\ &= \sum_{k=1}^{r} (-1)^{k-1} \sum_{I \subseteq \underline{r}, |I|=k} |\bigcap_{i \in I} A_i|. \end{aligned}$$

Beweis. Setze $A := \bigcup_{i=1}^{r} A_i$. Wir rechnen nach, dass jedes Element $a \in A$ auf der rechten Seite der Formel tatsächlich genau einmal gezählt wird. Sei also a ein beliebiges fest gewähltes Element aus A. Definiere I_a als die Menge der Indizes i aller Mengen A_i, die a enthalten, d.h.

$$I_a := \{i \in \underline{r} \mid a \in A_i\}.$$

In der Formel werden Ausdrücke der Form $|\bigcap_{i \in I} A_i|$ für bestimmte Indexmengen $I \subseteq \underline{r}$ aufsummiert. Sei $I \subseteq \underline{r}$ eine beliebige solche Indexmenge. Dann wird das Element a in $|\bigcap_{i \in I} A_i|$ genau 1-mal gezählt, wenn $a \in \bigcap_{i \in I} A_i$, sonst 0-mal. Weiter gilt $a \in \bigcap_{i \in I} A_i$ genau dann wenn $i \in I_a$ für alle $i \in I$, also genau dann wenn $I \subseteq I_a$. Der Anteil von a an dem Ausdruck

$$\sum_{I \subseteq \underline{r}, |I|=k} |\bigcap_{i \in I} A_i|$$

für festes k beträgt somit

$$\sum_{I \subseteq I_a, |I|=k} 1 + \sum_{I \not\subseteq I_a, |I|=k} 0 = \sum_{I \subseteq I_a, |I|=k} 1,$$

also genau die Anzahl der k-elementigen Teilmengen von I_a. Diese Zahl hängt nur von $|I_a|$ ab, und beträgt $\binom{|I_a|}{k}$ falls $k \le |I_a|$ und 0 falls $k > |I_a|$. Der Anteil von a an der gesamten rechten Seite beträgt somit

$$\sum_{k=1}^{|I_a|} (-1)^{k-1} \binom{|I_a|}{k}.$$

Nach Übung 4.2 gilt für alle $m \in \mathbb{N}$:

$$\sum_{k=1}^{m} (-1)^k \binom{m}{k} = -1.$$

Damit ist gezeigt, dass a auf der gesamten rechten Seite genau einmal gezählt wurde. □

Für $r = 3$ ergibt sich z.B.

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| = &+ |A_1| + |A_2| + |A_3| \\ &- |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ &+ |A_1 \cap A_2 \cap A_3|. \end{aligned}$$

Beispiel. Wie viele Zahlen zwischen 1 und 100 sind durch $2, 3$ oder 5 teilbar? Wir haben die Menge

$$A = \{i \in \mathbb{N} \mid i \leq 100, 2|i \vee 3|i \vee 5|i\}$$

zu zählen. Leicht zählbar sind die Mengen

$$A_n := \{i \in \mathbb{N} \mid i \leq 100, n|i\},$$

für alle $n \in \mathbb{N}$ ist nämlich $|A_n| = \lfloor \frac{100}{n} \rfloor$. Da A die Vereinigung $A = A_2 \cup A_3 \cup A_5$ ist, ergibt sich nach dem Inklusions-Exklusions-Prinzip

$$|A| = |A_2| + |A_3| + |A_5| - |A_2 \cap A_3| - |A_2 \cap A_5| - |A_3 \cap A_5| + |A_2 \cap A_3 \cap A_5|.$$

Es bleibt, die verschiedenen Durchschnitte zu zählen. Nun ist jede natürliche Zahl i genau dann durch 2 und 3 teilbar, wenn sie durch 6 teilbar ist. D.h. $A_2 \cap A_3 = A_6$. Analog ergibt sich $A_2 \cap A_5 = A_{10}, A_3 \cap A_5 = A_{15}, A_2 \cap A_3 \cap A_5 = A_{30}$. (Man beachte, dass $2, 3$ und 5 Primzahlen sind; allgemein gilt $A_n \cap A_m = A_{\mathrm{kgV}(n,m)}$ für beliebige $n, m \in \mathbb{N}$.) Also

$$\begin{aligned} |A| &= |A_2| + |A_3| + |A_5| - |A_6| - |A_{10}| - |A_{15}| + |A_{30}| \\ &= 50 + 33 + 20 - 16 - 10 - 6 + 3 = 74. \end{aligned}$$

Übung a. Die Bevölkerung von Aachen, die arbeitet oder studiert, betrage 150000. Wenn davon 20% studieren und 90% arbeiten, Wie viele Aachener Studenten arbeiten dann neben ihrem Studium?

Übung b. Es seien $n_1, \ldots, n_r \in \mathbb{N}$ und $n = \sum_{i=1}^{r} n_i$. Man gebe einen kombinatorischen Beweis für die Ungleichung $\sum_{i=1}^{r} \binom{n_i}{2} \leq \binom{n-r+1}{2}$ aus Übung 4.2.2v. *Hinweis*: Betrachte Mengen $A_1, \ldots, A_r$ Mengen mit $|A_i| = n_i$, für die es ein Element a gibt, so dass für alle $i, j \in \underline{r}$ mit $i \neq j$ gilt: $A_i \cap A_j = \{a\}$.

Beweis. Nach dem Inklusions-Exklusions-Prinzip ist $|\bigcup_{i=1}^{r} A_i| = n - r + 1$. Bezeichne $\mathrm{Pot}_2(A)$ die Menge der 2-elementigen Teilmengen von A. Zu zeigen ist: $\sum_{i=1}^{r} |\mathrm{Pot}_2(A_i)| \leq |\mathrm{Pot}_2(\bigcup_{i=1}^{r} A_i)|$. Trivialerweise ist $\bigcup_{i=1}^{r} \mathrm{Pot}_2(A_i) \subseteq \mathrm{Pot}_2(\bigcup_{i=1}^{r} A_i)$. Wegen $|A_i \cap A_j| = 1$ für $i \neq j$ sind die Mengen $\mathrm{Pot}_2(A_i)$ für $i = 1, \ldots, r$ paarweise disjunkt. Die Behauptung folgt also mit der Summenregel. □

4.3.4 Schubfachprinzip

Prinzip. Verteilt man n Elemente auf m Schubladen und ist $n > m$, so enthält eine Schublade mindestens zwei Elemente.

Beispiel. In jeder Menge von 13 Personen gibt es zwei, die im gleichen Monat Geburtstag haben.

4.4 Stirling'sche Zahlen

Die Binomialkoeffizienten wurden eingeführt, da sie beim Zählen von Teilmengen bzw. Multimengen fester Mächtigkeit auftreten. Die Stirling'schen Zahlen stellen zwei weitere Arten von Zählkoeffizienten dar. Sie treten auf beim Zählen von Partitionen mit fester Anzahl von Teilen bzw. beim Zählen von Permutationen mit fester Zykelzahl.

4.4.1 Stirling-Zahlen zweiter Art

Definition. Es seien $n, k \in \mathbb{N}_0$. Wir definieren

$$S_{n,k} := \text{Anzahl der Partitionen von } \underline{n} \text{ mit genau } k \text{ Teilen.}$$

Die Zahlen $S_{n,k}$ heißen *Stirling-Zahlen zweiter Art*. Partitionen mit k Teilen nennen wir auch kurz *k-Partitionen*.

Beispiel. Wie viele Möglichkeiten gibt es, n Studenten auf k Tutoriengruppen aufzuteilen, wobei keine Gruppe leer bleiben soll? Eine solche Aufteilung ist eine k-Partition von $\underline{n}$, somit gibt es $S_{n,k}$ Möglichkeiten.

Bemerkung. Für alle $n, k \in \mathbb{N}_0$ gelten:

(i) $S_{n,n} = 1$,

(ii) $S_{n,0} = 0$ falls $n > 0$,

(iii) $S_{n,k} = 0$ falls $k > n$.

Beweis.

(i) Es gibt genau eine n-Partition von $\underline{n}$. Das gilt auch für $n = 0$, da es genau eine Partition der leeren Menge gibt, und die hat 0 Teile.

(ii) Eine Partition einer nicht-leeren Menge muss mindestens 1 Teil haben.

(iii) Eine Partition von $\underline{n}$ kann höchstens n Teile haben.

□

Satz. *Für alle $n, k \in \mathbb{N}$ gilt $S_{n,k} = S_{n-1,k-1} + kS_{n-1,k}$.*

Beweis. Es sei $T_1 \cup \cdots \cup T_k = \underline{n}$ eine k-Partition von $\underline{n}$. Wir nehmen o.B.d.A. an, dass n in T_k liegt (die Nummerierung der Teile spielt keine Rolle). Entfernt man n aus T_k und $\underline{n}$, so bekommt man $T_1 \cup \cdots \cup T_{k-1} \cup (T_k \setminus \{n\}) = \underline{n-1}$. Je nachdem, ob $T_k \setminus \{n\}$ leer ist oder nicht, ist dies eine $(k-1)$-Partition oder eine k-Partition von $\underline{n-1}$. Umgekehrt entsteht jede k-Partition von $\underline{n}$ auf eine der folgenden Arten:

a) Hinzufügen des Teiles $\{n\}$ zu einer $(k-1)$-Partition von $\underline{n-1}$,

b) Hinzufügen des Elementes n zu einem der Teile einer k-Partition von $\underline{n-1}$.

Keine Partition kann auf beide Arten entstehen, denn bei a) liegt n stets in einem Teil der Mächtigkeit 1, bei b) stets in einem Teil der Mächtigkeit > 1. Folglich ist die Anwendung der Summenregel erlaubt. Bei a) gibt es $S_{n-1,k-1}$ viele $(k-1)$-Partitionen von $\underline{n-1}$, die jeweils auf eindeutige Art um den Teil $\{n\}$ ergänzt werden. Bei b) gibt es $S_{n-1,k}$ viele k-Partitionen von $\underline{n-1}$, bei denen auf jeweils k verschiedene Arten das Element n zu einem der Teile hinzugefügt wird. Nach Produktregel entstehen durch b) also $kS_{n-1,k}$ viele k-Partitionen von $\underline{n}$. Mit der Summenregel ergibt sich schließlich die Formel $S_{n,k} = S_{n-1,k-1} + kS_{n-1,k}$. □

Die Zahlen $S_{n,k}$ lassen sich im sog. *Stirling-Dreieck zweiter Art* anordnen:

$n = 0$:						1						
$n = 1$:					0		1					
$n = 2$:				0		1		1				
$n = 3$:			0		1		3		1			
$n = 4$:		0		1		7		6		1		
$n = 5$:	0		1		15		25		10		1	
$n = 6$:	0		1		31		90		65		15	1

Übung. Man zeige:

(i) Die Anzahl der surjektiven Abbildungen $\underline{n} \to \underline{k}$ beträgt $k! \cdot S_{n,k}$.

(ii) Es gilt $\sum_{k=0}^{m} S_{n,k} \cdot \frac{m!}{(m-k)!} = n^m$.
Tipp: n^m ist die Anzahl aller Abbildungen $\underline{m} \to \underline{n}$.

4.4.2 Stirling-Zahlen erster Art

Definition. Es seien $n, k \in \mathbb{N}_0$. Wir definieren

$$s_{n,k} := \text{Anzahl der Permutationen aus } S_n \text{ mit Zykelzahl } k.$$

Die Zahlen $s_{n,k}$ heißen *Stirling-Zahlen erster Art*.

Beispiel. Bei einem Treffen von n Philosophen teilen sich diese in k Diskussionsgruppen auf (Gruppen mit nur einer Person sind erlaubt). Die Teilnehmer jeder Gruppe setzen sich im Kreis hin und philosophieren über ein Thema. Wie viele mögliche Sitzordnungen gibt es? Antwort: $s_{n,k}$.

Bemerkung. Für alle $n, k \in \mathbb{N}_0$ gelten:

(i) $s_{n,n} = 1$,

(ii) $s_{n,0} = 0$ falls $n > 0$,

(iii) $s_{n,k} = 0$ falls $k > n$.

Beweis.

(i) Hat $\pi \in S_n$ die Zykelzahl n, so müssen alle Zykeln die Länge 1 haben, also ist $\pi = \mathrm{id}$. Das gilt auch für $n = 0$, denn das einzige Element aus S_0 hat Zykelzahl 0.

(ii) Die Zykelzahl eines Elementes von S_n mit $n > 0$ ist stets > 0.

(iii) Die Zykelzahl eines Elementes von S_n kann höchstens n betragen.

□

Satz. *Für alle $n, k \in \mathbb{N}$ gilt $s_{n,k} = s_{n-1,k-1} + (n-1)s_{n-1,k}$.*

Beweis. Eine Modifikation des Beweises von Satz 4.4.1 (Übung). □

Die Zahlen $s_{n,k}$ lassen sich im sog. *Stirling-Dreieck erster Art* anordnen:

$n=0$:						1						
$n=1$:					0		1					
$n=2$:				0		1		1				
$n=3$:			0		2		3		1			
$n=4$:		0		6		11		6		1		
$n=5$:	0		24		50		35		10		1	
$n=6$:	0	120		274		225		85		15		1

Übung.

(i) Man führe den Beweis des Satzes aus.

(ii) Man zeige $\sum_{k=0}^{n} s_{n,k} = n!$.

Kapitel 5

Graphentheorie

5.1 Grundbegriffe

5.1.1 Ungerichtete Graphen

Definition a. Ein (ungerichteter) *Graph* ist ein Paar $G = (V, E)$, bestehend aus einer endlichen Menge V und einer Menge E von zweielementigen Teilmengen von V. Die Elemente von V werden *Knoten* (engl. *vertex*) genannt, die Elemente von E *Kanten* (engl. *edge*). Es heißt $n_G := |V|$ die *Knotenzahl* und $m_G := |E|$ die Kantenzahl von G.

Bemerkung a. Das mathematische Modell für eine Kante zwischen den Knoten $u, v \in V$ ist hier die *zwei*elementige Teilmenge $\{u, v\} = \{v, u\} \subseteq V$. Das bedeutet, dass unsere Definition keine sog. „Schlingen“ zulässt, d.h. Kanten von einem Knoten zu sich selbst. Für die Kante $\{u, v\}$ verwenden wir alternativ auch die Schreibweise uv bzw. vu.

Ein weiteres mögliches mathematisches Modell für die Kanten ist, die Kantenmenge als eine symmetrische, antireflexive Relation auf der Knotenmenge aufzufassen.

Erlaubt ist der Graph $G = (\emptyset, \emptyset)$.

Bemerkung b. Andere verbreitete Definitionen von Graphen erlauben gerichtete Kanten, Schlingen, Mehrfachkanten, gewichtete Kanten, gefärbte Kanten, usw. Entsprechend muss das mathematische Modell für die Kantenmenge variiert werden.

Übung a. Jede Relation auf einer Menge V kann als ein gerichteter Graph (mit erlaubten Schlingen) veranschaulicht werden. Man mache sich klar, was jede einzelne der folgenden Eigenschaften der Relation für das Aussehen dieses Graphen bedeuten: symmetrisch, antisymmetrisch, reflexiv, antireflexiv, transitiv, Äquivalenzrelation, Totalordnung.

Übung b. Was wäre ein mathematisches Modell für einen ungerichteten Graphen mit Mehrfachkanten bzw. mit gewichteten Kanten?

In diesem und den folgenden Abschnitten sei $G = (V, E)$ stets ein Graph.

Definition b.

(i) Ist $uv \in E$ eine Kante, so werden u und v die *Endknoten* von uv genannt. In diesem Fall heißen u und v *adjazent* oder *benachbart*, sowie u *Nachbar* von v und umgekehrt.

(ii) Die Menge aller Nachbarn von $v \in V$ wird mit $\Gamma(v) := \Gamma_G(v)$ bezeichnet.

(iii) G heißt *vollständig*er Graph, wenn je zwei beliebige Knoten adjazent sind, also genau dann, wenn $m_G = \binom{n_G}{2}$.

(iv) Eine Kante $e \in E$ heißt *inzident* zu einem Knoten $v \in V$, wenn v ein Endknoten von e ist.

(v) Zwei verschiedene Kanten heißen *inzident*, wenn sie einen gemeinsamen Endknoten haben.

Übung c. In jedem Graph G gilt $m_G \leq \binom{n_G}{2}$.

5.1.2 Datenstruktur für Graphen

Es sei $G = (V, E)$ ein Graph mit $V = \{1, \ldots, n\}$ und $E = \{e_1, \ldots, e_m\}$.

Definition. Die *Adjazenzmatrix* von G ist die Matrix

$$A := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \in \{0,1\}^{n \times n} \text{ mit } a_{ij} := \begin{cases} 1 & \text{falls } ij \in E, \\ 0 & \text{falls } ij \notin E. \end{cases}$$

Die *Adjazenzliste* von G ist die Liste $\Gamma := (\Gamma(1), \Gamma(2), \ldots, \Gamma(n))$.

Die *Inzidenzmatrix* von G ist die Matrix

$$B := \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ \vdots & & & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nm} \end{pmatrix} \in \{0,1\}^{n \times m} \text{ mit } b_{ij} := \begin{cases} 1 & \text{falls } i \in e_j, \\ 0 & \text{falls } i \notin e_j. \end{cases}$$

Bemerkung. Die Adjazenzmatrix enthält 0 entlang der Diagonalen von a_{11} bis a_{nn} und ist spiegelsymmetrisch zu dieser Diagonalen. Die j-te Spalte der Inzidenzmatrix enthält genau zwei Einsen, nämlich zu den beiden Endknoten der Kante e_j.

Beispiel. Siehe Vorlesung.

5.1.3 Teilgraphen

Es sei $G = (V, E)$ ein Graph.

Definition. Ein Graph $G' = (V', E')$ wird *Teilgraph* von G genannt, geschrieben $G' \leq G$, wenn $V' \subseteq V$ und $E' \subseteq E$.

Beispiel. Ist $V' \subseteq V$, so wird durch $E' := E \cap \{uv \mid u, v \in V'\}$ ein Teilgraph (V', E') von G definiert. Dieser wird der *auf V' induzierte Teilgraph von G* genannt, geschrieben $G|_{V'}$.

5.1.4 Der Grad

Es sei $G = (V, E)$ ein Graph.

Definition. Wir definieren den *Grad* von $v \in V$ als $\deg(v) := |\Gamma(v)|$, also die Anzahl der Nachbarn von v bzw. die Anzahl der zu v inzidenten Kanten. Knoten mit Grad 0 heißen *isoliert*.

Bemerkung. $\sum_{v \in V} \deg(v) = 2m_G$.

Folgerung. *In jedem Graphen ist die Anzahl der Knoten mit ungeradem Grad gerade.*

Beispiel. Die Anzahl der Personen auf einer Party, die einer ungeraden Zahl von Gästen die Hand geben, ist gerade. (Aufgrund dieses Beispiel wird die Folgerung auch „Handschlagslemma“ genannt.)

5.1.5 Kantenzüge, Pfade, Kreise, Touren

Es sei $G = (V, E)$ ein Graph.

Definition. Es sei $l \in \mathbb{N}_0$.

(i) Ein *Kantenzug der Länge l in G* ist ein Tupel $(v_0, v_1, \ldots, v_l)$ von Knoten mit $v_i v_{i+1} \in E$ für alle $i = 0, \ldots, l-1$. Zu einem Kantenzug $(v_0, \ldots, v_l)$ sagen wir auch genauer *Kantenzug von v_0 nach v_l* oder *v_0-v_l-Kantenzug*, und die Knoten v_0, v_l werden sein *Anfangs-* bzw. *Endknoten* genannt. Der Kantenzug heißt *geschlossen* falls $v_0 = v_l$.

(ii) Ein Kantenzug $(v_0, \ldots, v_l)$ heißt *Pfad der Länge l in G*, falls die Knoten $v_0, \ldots, v_l$ paarweise verschieden sind. Zu einem Pfad $(v_0, \ldots, v_l)$ sagen wir auch genauer *Pfad von v_0 nach v_l* oder *v_0-v_l-Pfad*, und die Knoten v_0, v_l werden sein *Anfangs-* bzw. *Endknoten* genannt,

(iii) Ein *Kreis der Länge l in G* ist ein geschlossener Kantenzug $(v_0, \ldots, v_l)$, für den $l \geq 3$ und $(v_0, \ldots, v_{l-1})$ ein Pfad ist.

(iv) Eine *Tour der Länge l in G* ist ein geschlossener Kantenzug $(v_0, \ldots, v_l)$, für den die Kanten $v_0v_1, v_1v_2, \ldots, v_{l-1}v_l$ paarweise verschieden sind.

Bemerkung.

(i) Für jeden Knoten $v \in V$ ist (v) ein v-v-Pfad der Länge 0.

(ii) Jeder Kreis ist eine Tour, aber nicht umgekehrt.

(iii) Ist $(v_0, \ldots, v_l)$ ein Kreis, so ist auch $(v_1, \ldots, v_{l-1}, v_0, v_1)$ ein Kreis. Diese beiden Kreise sind formal verschieden! Liest man das Tupel $(v_0, \ldots, v_l)$ aber als Zykel $(v_0\ v_1\ \ldots\ v_{l-1})$, also als eine Permutation von V, so liefern beide Kreise denselben Zykel.

(iv) Ist $(v_0, \ldots, v_l)$ ein Kreis, so ist auch $(v_l, \ldots, v_0)$ ein Kreis. Diese beiden Kreise sind formal verschieden!

Beispiel. Siehe Vorlesung.

Übung. Ist eine Kante $e \in E$ *Teil* von zwei *verschiedenen* Kreisen von $G = (V, E)$, so besitzt auch $(V, E \setminus \{e\})$ einen Kreis. Hier ist zunächst geeignet zu definieren, was es heißt, dass e Teil eines Kreises ist, und wann zwei Kreise als gleich anzusehen sind.

Alternativ: Definiere eine *Kreiszahl k* von e und von G und zeige $k_{G'} = k_G - k_e$ für $G' = (V, E \setminus e)$.

5.1.6 Zusammenhang und Komponenten

Es sei $G = (V, E)$ ein Graph.

Definition. Die *Zusammenhangsrelation* $\sim$ auf V wird definiert durch

$$u \sim v :\Leftrightarrow \text{ es gibt einen } u\text{-}v\text{-Kantenzug in } G.$$

G heißt *zusammenhängend*, falls $u \sim v$ für alle $u, v \in V$, anderenfalls *unzusammenhängend*.

Bemerkung a. Offensichtlich ist $\sim$ eine Äquivalenzrelation (Übung). Wir lesen $u \sim v$ auch als „u ist verbunden mit v“ oder „u und v hängen zusammen“. Für alle $u, v \in V$ gilt:

$$u \sim v \Leftrightarrow \text{ es gibt einen } u\text{-}v\text{-Pfad in } G.$$

Beweis. $\Rightarrow$: Sei $u \sim v$ und sei $(v_0, v_1, \ldots, v_l)$ mit $v_0 = u$ und $v_l = v$ ein u-v-Kantenzug in G von minimaler Länge l. Angenommen $(v_0, v_1, \ldots, v_l)$ ist kein Pfad, d.h. $v_i = v_j$ für geeignete $0 \leq i < j \leq l$. Dann ist $(v_0, \ldots, v_i, v_{j+1}, \ldots, v_l)$ ein u-v-Kantenzug der Länge $l - (j - i) < l$ im Widerspruch zur Minimalität von l. Also ist die Annahme falsch und $(v_0, v_1, \ldots, v_l)$ ein Pfad.
$\Leftarrow$: trivial. □

Übung. Besitzt G einen Knoten vom Grad $n_G - 1$, so ist G zusammenhängend.

Definition. Die *Zusammenhangskomponenten* oder kurz *Komponenten* von G sind die induzierten Teilgraphen $G|_U$, wobei U die Äquivalenzklassen von V bzgl. $\sim$ durchläuft. Die Anzahl der Äquivalenzklassen von $\sim$ bezeichnen wir als *Komponentenzahl* r_G von G. Es heißt $G_v := G|_{[v]_\sim}$ die *Zusammenhangskomponente* von $v \in V$. Komponenten, die aus einem einzelnen Knoten bestehen, nennen wir *trivial*.

Beispiel. Siehe Vorlesung.

Bemerkung b. G ist genau dann zusammenhängend, wenn $r_G \leq 1$. Eine Komponente ist genau dann trivial, wenn sie keine Kanten enthält. Ein Knoten ist genau dann isoliert, wenn seine Zusammenhangskomponente trivial ist.

5.1.7 Die Zahlen n_G, m_G, r_G

Es sei $G = (V, E)$ ein Graph.

Lemma. *Für alle $u, v \in V$ gilt:*

(i) $r_{(V,E)} - 1 \leq r_{(V,E \cup \{uv\})} \leq r_{(V,E)}$.

(ii) $r_{(V,E \setminus \{uv\})} - 1 \leq r_{(V,E)} \leq r_{(V,E \setminus \{uv\})}$.

Beweis. i) Die neue Kante uv kann höchstens zwei Komponenten verbinden. ii) folgt aus i). □

Satz a (Untere Schranke für m_G)**.** $m_G \geq n_G - r_G$.

Beweis. Wir führen eine Induktion nach m_G. In einem Graph ohne Kanten ($m_G = 0$) sind alle Komponenten trivial, also $r_G = n_G$. Sei nun $m_G > 0$ und die Behauptung für kleineres m_G bereits bewiesen. Wähle ein $e \in E$ und setze $G' := (V, E \setminus \{e\})$. Nach Teil (ii) des Lemmas gilt $r_{G'} - 1 \leq r_G$. Mit der Induktionsvoraussetzung, angewendet auf G', folgt $n_G = n_{G'} \leq m_{G'} + r_{G'} = m_G - 1 + r_{G'} \leq m_G + r_G$. □

Folgerung a. *Ist G zusammenhängend, dann ist $m_G \geq n_G - 1$.*

Satz b (Obere Schranke für m_G)**.** $m_G \leq \binom{n_G+1-r_G}{2}$.

Beweis. Für $r_G = 1$ ist die Aussage $m_G \leq \binom{n_G}{2}$ klar. Für allgemeines r_G folgt sie daraus durch Summation über die Komponenten mittels Übung 4.2.2v. □

Folgerung b. *Ist G unzusammenhängend, so gilt $m_G \leq \binom{n_G-1}{2}$.*

Übung. Man zeige Folgerung b mittels vollständiger Induktion nach n_G.

Beweis. Sei $n = n_G$. Für $n = 1$ ist die Aussage trivial, für $n = 2$ lautet sie $0 \leq 0$ (Induktionsanfang). Sei nun $n \geq 3$. Sei oBdA $V = \underline{n}$.

Falls n isoliert ist, so folgt $m_G \leq \binom{n-1}{2}$ aus der Betrachtung von $G|_{\underline{n-1}}$. Sei also n nicht isoliert und G unzusammenhängend. Dann ist a) $\deg n \leq n - 2$ (Lemma), und b) $G|_{\underline{n-1}}$ unzusammenhängend (sonst G zusammenhängend). Mit Induktionsvoraussetzung, angewendet auf $G' := G|_{\underline{n-1}}$, folgt $m_G = m_{G'} \leq \binom{n-2}{2} + (n-2) = \frac{(n-2)(n-3)}{2} + (n-2) = \binom{n-1}{2}$. □

5.1.8 Brücken

Bemerkung a. Es seien $e = uv \in E, G' = (V, E \setminus \{e\})$. Folgende Aussagen sind äquivalent:

(i) $u \not\sim v$ in G',

(ii) $r_{G'} > r_G$.

Definition. Eine Kante $e = uv \in E$ heißt *Brücke* von G, wenn die Bedingungen aus Bemerkung a erfüllt sind, sonst *Nicht-Brücke* von G.

Beispiel. Ist $\deg u = 1$, so ist die einzige zu u inzidente Kante eine Brücke. Weitere Beispiele inkl. Bilder siehe Vorlesung.

Bemerkung b. Es seien $e = uv \in E, G' = (V, E \setminus \{e\})$. Folgende Aussagen sind äquivalent:

(i) e ist keine Brücke von G,

(ii) $u \sim v$ in G',

(iii) $r_{G'} = r_G$,

(iv) es gibt einen u-v-Kantenzug in G, der nicht über e führt,

(v) es gibt einen u-v-Pfad in G, der nicht über e führt,

(vi) e ist Teil eines Kreises in G.

Beweis. Die Äquivalenz (iv)⇔(v) benutzt Bemerkung (5.1.6). Der Rest ist trivial. □

Satz. *Ist $u \in V$ zu l Brücken inzident ($l \in \mathbb{N}$), so besitzt G mindestens l von u verschiedene Knoten von ungeradem Grad.*

Folgerung. *Haben in einem Graphen alle Knoten geraden Grad, so besitzt er keine Brücken.*

Beweis des Satzes. Seien $e_1, \dots e_l \in E$ zu u inzidente Brücken in G, $e_i = uv_i$. Setze $G' = (V, E \setminus \{e_1, \dots, e_r\})$. In G' liegen die Knoten $v_1, \dots, v_l$ in verschiedenen Zusammenhangskomponenten G'_{v_i}. Behauptung: jede der Komponenten G'_{v_i} enthält einen Knoten von ungeradem Grad in G. In der Tat, falls $\deg_G(v_i)$ gerade ist, so ist $\deg_{G'}(v_i)$ ungerade. Nach dem Handschlagslemma, angewendet auf G'_{v_i}, enthält dann G'_{v_i} einen weiteren Knoten $v'_i \neq v_i$ mit $\deg_{G'}(v'_i)$ ungerade. Wegen $v'_i \neq v_i$ ist aber $\deg_G(v'_i) = \deg_{G'}(v'_i)$, also ungerade. □

5.2 Distanz und gewichtete Graphen

5.2.1 Distanz

Es sei $G = (V, E)$ ein Graph.

Definition. Für alle $v, w \in V$ mit $v \sim w$ definieren wir die *Distanz* zwischen v und w als

$$d(v, w) := \min\{l \in \mathbb{N}_0 \mid \text{in } G \text{ existiert ein } v\text{-}w\text{-Pfad der Länge } l\} \in \mathbb{N}_0.$$

Für alle $v, w \in V$ mit $v \not\sim w$ wird $d(v, w) := \infty$ gesetzt.

Bemerkung. Für alle $v, w \in V$ gelten:

(i) $d(v, w) = 0 \Leftrightarrow v = w$,

(ii) $d(v, w) < \infty \Leftrightarrow v \sim w$.

G ist genau dann zusammenhängend, wenn $d(v, w) < \infty$ für alle $v, w \in V$.

```
BREITENSUCHE(Γ, w)
 1  initialisiere array d[1, ..., n] mit allen Einträgen gleich ∞
 2  initialisiere array p[1, ..., n] mit allen Einträgen gleich NIL
 3  initialisiere leere queue Q (FIFO)
 4  d[w] ← 0
 5  INSERT(Q, w)
 6  while Q ist nicht leer
 7  do v ← EXTRACT(Q)
 8      for u ∈ Γ(v)
 9      do if d[u] = ∞
10            then INSERT(Q, u)
11                 d[u] ← d[v] + 1
12                 p[u] ← v
13  return d, p
```

Abbildung 5.1: Prozedur Breitensuche

5.2.2 Breitensuche

Die *Breitensuche* ist ein Algorithmus, der, beginnend bei einer Wurzel $w \in V$, alle Knoten der Zusammenhangskomponente von w mit aufsteigender Distanz durchläuft. Er eignet sich also zur Berechnung der Zusammenhangskomponenten von G, insbesondere zur Bestimmung der Brücken und zur Prüfung des Graphen auf Zusammenhang. Außerdem können mit der Breitensuche die Distanzen $d(v, w)$ sowie kürzeste Pfade von v nach w für jeden Knoten v bestimmt werden. Die kürzesten Pfade von jedem v zu w können dadurch angegeben werden, dass man jedem $v \in V$ einen *Vorgänger* mit kleinerer Distanz zu w zuordnet. Aus den Vorgängern erhält man dann umgekehrt einen kürzesten Kantenzug von v nach w, indem man, ausgehend von v, sukzessive zum jeweiligen Vorgänger übergeht.

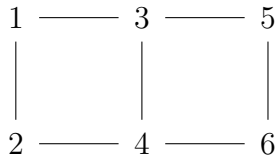
Algorithmus. *Es sei G ein Graph mit Knotenmenge $V = \{1, \ldots, n\}$, gegeben als Adjazenzliste Γ, und es sei $w \in V$. Die in Abbildung 5.2.2 dargestellte Prozedur* BREITENSUCHE *berechnet zu jedem $v \in V$ die Distanz $d(v) := d(v, w)$ sowie einen Vorgänger $p(v)$ in einem kürzesten v-w-Pfad.*

Die verwendete Datenstruktur `queue` ist eine Warteschlange im „First-in-first-out“-Modus. Der Aufruf INSERT(Q, x) hängt das Element x am Ende der Warteschlange ein, der Aufruf EXTRACT(Q) entnimmt das Element, das am Anfang der Warteschlange steht.

Bemerkung a. Da der Verlauf der Breitensuche davon abhängt, in wel-

cher Reihenfolge Knoten in die Warteschlange aufgenommen werden, spielt die Anordnung der Adjazenzlisten eine Rolle, die bestimmt in welcher Reihenfolge die Knoten in der `for`-Schleife bearbeitet werden. An folgendem Beispiel wird deutlich, wie die Anordnung der Adjazenzlisten den Verlauf und das Ergebnis für p, nicht aber das Ergebnis für d beeinflusst.

Beispiel. Betrachte folgenden Graph mit $V = \underline{6}$ und Wurzel $w = 1$:



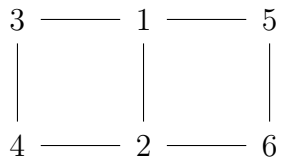
Die erste Tabelle zeigt den Ablauf der Breitensuche, wenn die Adjazenzlisten mit aufsteigender Nummerierung angeordnet sind. Jede Zeile entspricht dabei einem Durchlauf der `while`-Schleife und gibt folgendes an: die Zustände der Datenstrukturen d, p, Q zu Beginn der `while`-Schleife, das von EXTRACT gelieferte v, dessen Adjazenzliste $\Gamma(v)$, und die Teilliste der $u \in \Gamma(v)$ mit $d[u] = \infty$.

d	p	Q	v	$\Gamma(v)$	$d[u] = \infty$
$(0, \infty, \infty, \infty, \infty, \infty)$	$(-, -, -, -, -, -)$	(1)	1	$(2, 3)$	$(2, 3)$
$(0, 1, 1, \infty, \infty, \infty)$	$(-, 1, 1, -, -, -)$	$(2, 3)$	2	$(1, 4)$	(4)
$(0, 1, 1, 2, \infty, \infty)$	$(-, 1, 1, 2, -, -)$	$(3, 4)$	3	$(1, 4, 5)$	(5)
$(0, 1, 1, 2, 2, \infty)$	$(-, 1, 1, 2, 3, -)$	$(4, 5)$	4	$(2, 3, 6)$	(6)
$(0, 1, 1, 2, 2, 3)$	$(-, 1, 1, 2, 3, 4)$	$(5, 6)$	5	$(3, 6)$	$()$
$(0, 1, 1, 2, 2, 3)$	$(-, 1, 1, 2, 3, 4)$	(6)	6	$(4, 5)$	$()$
$(0, 1, 1, 2, 2, 3)$	$(-, 1, 1, 2, 3, 4)$	$()$			

Die nächste Tabelle zeigt den Ablauf, wenn die Adjazenzlisten mit absteigender Nummerierung angeordnet sind.

d	p	Q	v	$\Gamma(v)$	$d[u] = \infty$
$(0, \infty, \infty, \infty, \infty, \infty)$	$(-, -, -, -, -, -)$	(1)	1	$(3, 2)$	$(3, 2)$
$(0, 1, 1, \infty, \infty, \infty)$	$(-, 1, 1, -, -, -)$	$(3, 2)$	3	$(5, 4, 1)$	$(5, 4)$
$(0, 1, 1, 2, 2, \infty)$	$(-, 1, 1, 3, 3, -)$	$(2, 5, 4)$	2	$(4, 1)$	$()$
$(0, 1, 1, 2, 2, \infty)$	$(-, 1, 1, 3, 3, -)$	$(5, 4)$	5	$(6, 3)$	(6)
$(0, 1, 1, 2, 2, 3)$	$(-, 1, 1, 3, 3, 5)$	$(4, 6)$	4	$(6, 3, 2)$	$()$
$(0, 1, 1, 2, 2, 3)$	$(-, 1, 1, 3, 3, 5)$	(6)	6	$(5, 4)$	$()$
$(0, 1, 1, 2, 2, 3)$	$(-, 1, 1, 3, 3, 5)$	$()$			

Übung a. Wir betrachten den folgenden Graph mit $V = \underline{6}$ und Wurzel $w = 1$:



Man beschreibe den Verlauf der Breitensuche mit einer Tabelle wie im Beispiel, wobei die Adjazenzlisten mit aufsteigender Nummerierung angeordnet sind.

Übung b. Geben Sie eine Schleifeninvariante für die while-Schleife in der Breitensuche an.

Bemerkung b. Die *Tiefensuche* wird realisiert, wenn man die queue (FIFO) durch einen stack (LIFO=„Last-in-first-out“) ersetzt. Geht es nur um die Bestimmung der Zusammenhangskomponente von w bzw. um die Prüfung des gesamten Graphen auf Zusammenhang, dann spielt es keine Rolle, ob Breiten- oder Tiefensuche verwendet wird.

5.2.3 Dijkstra's Algorithmus

Definition. Ein (ungerichteter) *gewichteter Graph* ist ein Tripel $G = (V, E, f)$, wobei (V, E) ein Graph ist und w eine *Gewichtsfunktion* $f : E \to \mathbb{R}_{\geq 0}$. Für jede Teilmenge $T \subseteq E$ und jeden Kantenzug $z = (v_0, \ldots, v_l)$ in G definieren wir deren *Gewichte* als $f(T) := \sum_{e \in T} f(e)$ bzw. $f(z) := \sum_{i=1}^{l} f(v_{i-1}v_i)$.

Für alle $v, w \in V$ mit $v \sim w$ definieren wir die *Distanz* zwischen v und w als

$$d(v, w) := \min\{f(z) \mid z \text{ ist } v\text{-}w\text{-Pfad in } G\} \in \mathbb{R}_{\geq 0}.$$

Für alle $v, w \in V$ mit $v \not\sim w$ wird $d(v, w) := \infty$ gesetzt.

Der Algorithmus von *Dijkstra* (1959) ist eine modifizierte Form der Breitensuche, die, beginnend bei einer Wurzel $w \in V$, für jeden Knoten der Zusammenhangskomponente von w die Distanz $d(v, w)$ sowie einen v-w-Pfad z mit minimalem Gewicht, d.h. mit $f(z) = d(v, w)$, berechnet.

Algorithmus. *Es sei $G = (V, E, f)$ ein gewichteter Graph mit Knotenmenge $V = \{1, \ldots, n\}$, gegeben als Adjazenzliste Γ, und es sei $w \in V$. Die in der Abbildung unten dargestellte Prozedur* DIJKSTRA *berechnet zu jedem $v \in V$ die Distanz $d(v) := d(v, w)$ sowie einen Vorgänger $p(v)$ in einem v-w-Pfad von minimalem Gewicht.*

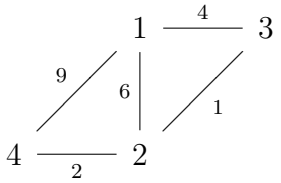
```
DIJKSTRA(Γ, w, f)
 1  initialisiere array d[1, ..., n] mit allen Einträgen gleich ∞
 2  initialisiere array p[1, ..., n] mit allen Einträgen gleich NIL
 3  initialisiere priority queue Q mit Elementen 1, ..., n und allen Prioritäten = ∞
 4  d[w] ← 0
 5  INSERT(Q, w, d[w])
 6  while Q nicht leer
 7  do v ← EXTRACTMIN(Q)
 8      for u ∈ Γ[v]
 9      do if d[v] + f(uv) < d[u]
10            then d[u] ← d[v] + f(uv)
11                 p[u] ← v
12                 INSERT(Q, w, d[w])
13  return d, p
```

Abbildung 5.2: Prozedur Dijkstra

Die verwendete Datenstruktur `priority queue` ist eine sog. *Vorrangwarteschlange*, bei der jedem ihrer Element ein *Prioritätswert* zugeordnet ist. Der Aufruf INSERT(Q, x, n) fügt das Element x in die Warteschlange ein und ordnet x die Priorität $n \geq 0$ zu. Falls x bereits in der Warteschlange enthalten ist, wird nur die Priorität neu auf n gesetzt. Der Aufruf EXTRACTMIN(Q) entnimmt das Element mit der niedrigsten Priorität.

Beweis. Wird v aus Q extrahiert, so wird $d[v]$ anschließend nicht mehr verändert. Wir beweisen, dass $d[v]$ zu diesem Zeitpunkt bereits die Distanz zu w ist. □

Beispiel. Betrachte folgenden gewichteten Graph mit $V = \underline{4}$ und Wurzel $w = 1$:

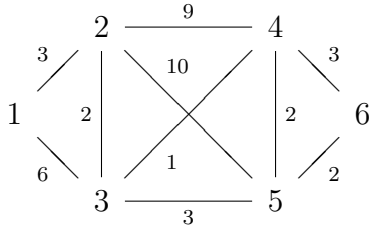


Die erste Tabelle zeigt den Ablauf des Dijkstra-Algorithmus, wenn die Adjazenzlisten mit aufsteigender Nummerierung angeordnet sind. Jede Zeile entspricht dabei einem Durchlauf der `while`-Schleife und gibt folgendes an: die Zustände der Datenstrukturen d, p, Q zu Beginn der `while`-Schleife, das von EXTRACTMIN gelieferte v, dessen Adjazenzliste $\Gamma(v)$, und die Teilliste der $u \in \Gamma(v)$ mit $d[v] + f(uv) < d[u]$. Die Vorrangwarteschlange Q wird jetzt

als Menge geschrieben. Die Prioritäten in Q brauchen nicht extra aufgelistet werden, da sie mit den Werten $d[v]$ übereinstimmen.

d	p	Q	v	$\Gamma(v)$	$d[v] + f(uv) < d[u]$
$(0, \infty, \infty, \infty)$	$(-, -, -, -)$	$\{1, 2, 3, 4\}$	1	$(2, 3, 4)$	$(2, 3, 4)$
$(0, 6, 4, 9)$	$(-, 1, 1, -)$	$\{2, 3, 4\}$	3	$(1, 2)$	(2)
$(0, 5, 4, 9)$	$(-, 3, 1, -)$	$\{2, 4\}$	2	$(1, 2, 4)$	(4)
$(0, 5, 4, 8)$	$(-, 3, 1, 2)$	$\{4\}$	4	$(1, 2)$	$()$
$(0, 5, 4, 8)$	$(-, 3, 1, 2)$	$\{\}$			

Übung a. Betrachte folgenden gewichteten Graph mit $V = \underline{6}$ und Wurzel $w = 1$:



Man beschreibe den Verlauf des Dijkstra-Algorithmus mit einer Tabelle wie im Beispiel, wobei die Adjazenzlisten mit aufsteigender Nummerierung angeordnet sind.

Übung b. Geben Sie eine Schleifeninvariante für die while-Schleife im Dijkstra-Algorithmus an und versuchen Sie damit, die Korrektheit zu beweisen.

Literaturverzeichnis

[1] M. Aigner. *Diskrete Mathematik.* Vieweg, 2004.

[2] H. Anton. *Lineare Algebra.* Spektrum, 1995.

[3] A. Beutelspacher. *Lineare Algebra.* Vieweg, 2003.

[4] G. Fischer. *Lineare Algebra.* Vieweg, 2005.

[5] S. Teschl G. Teschl. *Mathematik für Informatiker, Band 1.* Springer, 2007.

[6] K. Jänich. *Lineare Algebra.* Springer, 2003.

[7] A. Steger. *Diskrete Strukturen.* Springer, 2001.

[8] K. Meyberg und P. Vachenauer. *Höhere Mathematik.* Springer, 2001.