Vorkurs zur linearen Algebra

Sommersemester 2015

Oliver Braun

RWTH Aachen

basierend auf einer Vorlage von
Prof. Dr. Gabriele Nebe
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64

Fassung vom 10. März 2015

Inhaltsverzeichnis

Kapitel 1

Einleitung

Das Ziel dieses Kurses ist es, den Studienanfängern im Sommersemester den Einstieg in die für sie in diesem Semester anspruchsvollste Vorlesung, die lineare Algebra, zu erleichtern. Diese Vorlesung, die ursprünglich geometrisch motiviert war, wurde im Laufe ihrer Geschichte jedoch mehr und mehr abstrahiert. Die Zeitplanung eines Hochschulsemesters gestattet es in der Regel nicht, den Inhalt der Vorlesung so darzustellen, wie er sich entwickelt hat; vielmehr ist die Vorlesung - und dies gilt in der Regel für alle mathematischen Vorlesungen - ein aus Jahrzehnten der Forschung entstandenes Destillat, das die aus heutiger Sicht "bestmöglichen" Ergebnisse in einer kompakten und neu organisierten Form enthält.
Der Kurs soll Ihnen den Einstieg in diese abstrakte Welt erleichtern und die Sprache vermitteln, in welcher die Probleme der linearen Algebra - und anderer mathematischer Gebiete - formuliert und gelöst werden. Dabei ist der Kurs zeitlich sehr kurz gehalten. Das vorliegende Skript umfasst die Inhalte dieses Kurses und geht stellenweise etwas darüber hinaus. Lassen Sie sich daher vom Umfang des Skripts nicht abschrecken.
Das Kapitel zur Aussagenlogik wird im Kurs übersprungen. Es zu lesen lohnt sich jedoch, denn es enthält wichtige Grundprinzipien für das mathematische Arbeiten. Kurz gehe ich im Kurs auf Beweise und Beweistechniken ein, das verschriftlichte Kapitel zu diesem Thema ist gegebenenfalls umfangreicher. Einige Beweistechniken finden sich bereits im Kapitel zur Aussagenlogik.
Die übrigen Kapitel werden möglichst vollständig im Kurs besprochen.

Kapitel 2

Aussagenlogik

Lernziele: Symbole und Kalkül der Aussagenlogik, Wahrheitstafeln,

und	oder	nicht	impliziert	folgt aus	äquivalent
$\wedge$	$\vee$	$\neg$	$\Rightarrow$	$\Leftarrow$	$\Leftrightarrow$

1 Aussagen und ihre Verknüpfungen.

Zwei Aspekte sind interessant an Aussagen: Erstens, welcher Sachverhalt durch sie beschrieben wird, welchen Sinn oder Bedeutung sie haben, zweitens, ob sie wahr oder falsch sind. Zu dem ersten Aspekt soll hier nichts gesagt werden, insbesondere verzichten wir auf eine Definition, was eine Aussage ist. Wichtig für uns ist alleine der zweite Aspekt, dass man einer Aussage genau einen der Wahrheitswerte **wahr** (w) oder **falsch** (f) zuordnen kann und dass man aus Aussagen neue Aussagen durch Verknüfungen wie „und“, „oder“ oder Verneinung konstruieren kann, sodass der Wahrheitswert der zusammengesetzten Aussage einzig und allein von den Wahrheitswerten der Ausgangsaussagen abhängt.
Beispiel. 1.) „5 ist eine Primzahl“ ist eine wahre Aussage.
2.) „1 ist eine Primzahl“ ist eine falsche Aussage.
3.) „$5^2 - 1 = (5-1)(5+1)$“ ist eine wahre Aussage.
4.) „$n^2 = 25$“ ist keine Aussage, weil n nicht hinreichend spezifiziert ist.

Definition 1.1. *1.) Eine Aussage A hat entweder den* **Wahrheitswert wahr** *($W(A) = w$) oder* **falsch** *($W(A) = f$).*
2.) Zwei Aussagen mit demselben Wahrheitswert heißen **äquivalent**.
3.) Ist A eine Aussage, so auch ihre **Verneinung** *$\neg A$ (nicht A). Es gilt: $W(\neg A) = w$ genau dann, wenn $W(A) = f$ oder tabellarisch ausgedrückt:*

A	$\neg A$
w	f
f	w

.

4.) Sind A, B Aussagen, so auch ihre **Konjunktion** *$A \wedge B$ (A und B). Es gilt: $W(A \wedge B) = w$ genau dann, wenn gleichzeitig $W(A) = w$ und $W(B) = w$.*
5.) Sind A, B Aussagen, so auch ihre **Disjunktion** *$A \vee B$ (A oder B). Es gilt: $W(A \vee B) =$*

f genau dann, wenn gleichzeitig $W(A) = f$ und $W(B) = f$.

Die letzte Definition ist etwas hinterhältig. Wir geben daher für die Konjunktion und die Disjunktion noch die **Wahrheitstafel**n an: In der ersten Zeile stehen die Aussagen und in den Spalten darunter die Wahrheitswerte der Aussagen, sodass alle Kombinationen der Wahrheitswerte von A und B vorkommen:

A	B	$A \wedge B$	$A \vee B$
w	w	w	w
w	f	f	w
f	w	f	w
f	f	f	f

Insbesondere sehen wir, dass unser „Oder“ ein nichtausschließendes Oder ist. Man kann nun aus diesen drei Grundverknüfungen von Aussagen neue Verknüfungen definieren, von denen einige weniger wichtig sind, wie das „Entweder Oder“, also das ausschließende Oder, andere grundlegend wie etwa die **Implikation** $\Rightarrow$. Bevor wir dies tun, wollen wir noch einige Rechenregeln für die Verknüpfungen von Aussagen auflisten, die das Leben oft einfacher machen:

Satz 1.2. *Seien A, B, C Aussagen. Dann gilt:*
1.) $W(\neg(\neg A)) = W(A)$*, d. h. A und $\neg(\neg A)$ sind äquivalente Aussagen.*
2.) **Kommutativität der Konjunktion***:*
$W(A \wedge B) = W(B \wedge A)$.
3.) **Kommutativität der Disjunktion***:*
$W(A \vee B) = W(B \vee A)$.
4.) **Assoziativität der Konjunktion***:*
$W(A \wedge (B \wedge C)) = W((A \wedge B) \wedge C)$.
5.) **Assoziativität der Disjunktion***:*
$W(A \vee (B \vee C)) = W((A \vee B) \vee C)$.
6.) **Distributivität der Disjunktion gegenüber der Konjunktion***:*
$W(A \vee (B \wedge C)) = W((A \vee B) \wedge (A \vee C))$.
7.) **Distributivität der Konjunktion gegenüber der Disjunktion***:*
$W(A \wedge (B \vee C)) = W((A \wedge B) \vee (A \wedge C))$.

Beweis. Wir begnügen uns mit dem Beweis von 1.) und von 7.). Die anderen ergänzen Sie nach demselben Prinzip. Wir erstellen sukzessive die Wahrheitstafeln der beiden Aussagen und sehen dass die entsprechenden Wahrheitswerte gleich sind. Es ist darauf zu achten, dass alle Kombinationen der Wahrheitswerte der Ausgangsaussagen vorkommen, also 2, 4 oder 8. Die Zahlen in der zweiten Reihe geben an, in welcher Reihenfolge die Spalten auszufüllen sind.
1.)

$\neg$	$(\neg$	$A)$	A
3	2	1	1
w	f	w	w
f	w	f	f

Die Gleichheit der ersten und der letzten Spalte beweisen die Behauptung.
7.)

A	$\wedge$	$(B$	$\vee$	$C)$	$(A$	$\wedge$	$B)$	$\vee$	$(A$	$\wedge$	$C)$
1	3	1	2	1	1	2	1	3	1	2	1
w	w	w	w	w	w	w	w	w	w	w	w
w	w	w	w	f	w	w	w	w	w	f	f
w	w	f	w	w	w	f	f	w	w	w	w
w	f	f	f	f	w	f	f	f	w	f	f
f	f	w	w	w	f	f	w	f	f	f	w
f	f	w	w	f	f	f	w	f	f	f	f
f	f	f	w	w	f	f	f	f	f	f	w
f	f	f	f	f	f	f	f	f	f	f	f

Weil die beiden mit 3 überschiebenen Spalten übereinstimmen, ist der Beweis erbracht. q.e.d.

Während der gerade angeschriebene Satz noch einigermaßen einleuchtend ist, haben Anfänger meist Schwierigkeiten mit den Verneinungen von Konjunktionen und Diskunktionen.

Satz 1.3. *Seien A, B Aussagen. Dann gilt:*
1.) **Verneinung der Konjunktion***:*
$W(\neg(A \wedge B)) = W(\neg A \vee \neg B)$.
(Das $\neg$-Zeichen bindet stärker als $\vee$, sodass die rechte Seite als $W((\neg B) \vee (\neg A))$ zu lesen ist.)
2.) **Verneinung der Disjunktion***:*
$W(\neg(A \vee B)) = W(\neg A \wedge \neg B)$.

Beweis. 1.) Mit Wahrheitstafel (4 Kombinationen). Übung.
2.) Aus 1.) und Satz 1.2 1.): Setze $C := \neg A$ und $D := \neg B$.[1] Nach 1.) sind dann $C \vee D$ und $\neg(\neg C \wedge \neg D)$ äquivalent. Also sind auch die Verneinungen $\neg(C \vee D)$ und $\neg C \wedge \neg D$ äquivalent. Indem wir C zu A und D zu B umtaufen, steht die Behauptung da. q.e.d.

2 Implikation und Äquivalenz

Wir kommen jetzt zu zwei wichtigen Verknüpfungen von Aussagen, die bei Beweisen und bei Algorithmen besonders wichtig sind.

Definition 2.1. *Seien A, B Aussagen.*
Die **Implikation** *$A \Rightarrow B$, auch gelesen als A impliziert B oder B folgt aus A, bezeichnet die Aussage $\neg A \vee B$.*
Die **Äquivalenz** *$A \Leftrightarrow B$, auch gelesen als A äquivalent zu B, bezeichnet die Aussage $(A \Rightarrow B) \wedge (B \Rightarrow A)$.*

[1] Das Zeichen := bedeutet: Was links steht wird durch das, was rechts steht, definiert.

Wir hatten bereits früher über die Wahrheitswerte Äquivalenz definiert. Wenn wir es hier nochmals definieren, müssen wir zeigen, dass es dasselbe ist.
1.) Die Wahrheitstafel für die Implikation ist (zeilenweise):

A	w	w	f	f
B	w	f	w	f
$A \Rightarrow B$	w	f	w	w

Insbesondere ist $\Rightarrow$ nicht kommutativ in dem Sinne, dass $A \Rightarrow B$ äquivalent (im Sinne von Definition 1.1 2) ist mit $B \Rightarrow A$. Manchmal schreibt man letzteres auch als $A \Leftarrow B$, gelesen als A folgt aus B. Man beachte, dass die Umgangssprache an dieser Stelle sehr unsauber ist.
2.) Die Wahrheitstafel für die Äquivalenz ist :

A	w	w	f	f
B	w	f	w	f
$A \Leftrightarrow B$	w	f	f	w

Insbesondere sind A und B genau dann äquivalent, wenn ihre Wahrheitswerte übereinstimmen, d. h. die neue Definition steht im Einklang mit Definition 1.1 2.).

Die Wahrheitstafel der Implikation macht am Anfang manchmal Schwierigkeiten mit der Anschauung. Aber man mache sich klar, dass man aus einer falschen Annahme alles Mögliche folgern kann: Die Folgerung ist richtig, aber über die Richtigkeit des Gefolgerten weiß man nichts. In Beweisen und bei Algorithmen folgert man immer aus richtigen oder zumindest als richtig angenommene Aussagen. Zwei Eigenschaften der Implikation sind im Hinblick auf Beweise wichtig:

Bemerkung 2.2. *Sind A, B, C Aussagen so gilt :*
*1.) (***Kontraposition***)*

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A).$$

*2.) (***Transitivität***) Gilt $A \Rightarrow B$ und $B \Rightarrow C$, so gilt auch $A \Rightarrow C$.*
Mit anderen Worten: $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$ ist immer eine wahre Aussage.
*3.) (***Ringschluss***) Gilt $A \Rightarrow B$ und $B \Rightarrow C$ und $C \Rightarrow A$, so sind je zwei der drei Aussagen A, B, C äquivalent.*
*4.) (***Widerspruchsbeweis***) Sei A eine Aussage und F eine falsche Aussage. Dann gilt:*

$$A \Leftrightarrow (\neg A \Rightarrow F)$$

Beweis. 1.) Ein letztes Mal per Wahrheitstafel:

$(A$	$\Rightarrow$	$B)$	$\Leftrightarrow$	$(\neg$	B	$\Rightarrow$	$\neg$	$A)$
1	2	1	4	2	1	3	2	1
w	w	w	w	f	w	w	f	w
w	f	f	w	w	f	f	f	w
f	w	w	w	f	w	w	w	f
f	w	f	w	w	f	w	w	f

Weil in der Spalte unter 4 nur w vorkommt, ist die Behauptung gezeigt.
2.) Übung.
3.) Sofort aus 2.) q.e.d.

Seltener braucht man das „entweder oder“ und das „weder noch“. Wir lassen es als Übung diese beiden auf die drei Grundverknüfungen zurückzuführen. Man beachte, es gibt manchmal mehrere äquivalente Möglichkeiten.

3 Quantoren und Mengenfamilien.

Wir müssen unsere sprachlichen Ausdrucksmöglichkeiten erweitern. Beispielsweise können wir den Durchschnitt zweier Teilmengen einer Menge bilden und damit durch Iteration auch den Durchschnitt endlich vieler Teilmengen. Aber das reicht nicht aus, insbesondere dann nicht, wenn wir es mit unendlichen Mengen zu tun haben.

Definition 3.1. *Ist M eine Menge so schreiben wir:*
1.) statt “für alle Elemente m der Menge M (gilt ...)” kürzer “ für alle $m \in M$ (gilt ...)” oder noch kürzer “ $\forall m \in M$ (gilt ...)”,
2.) statt “es gibt ein Element $m \in M$ (mit ...)“ oder “es existiert ein Element $m \in M$ (mit ...)“ kürzer “$\exists m \in M$ (mit ...)”.

Als Anwendung dieses neuen Ausdrucksmöglichkeit können wir den Durchschnitt und die Vereinigung von einer Menge von Teilmengen definieren.

Definition 3.2. *Sei $\mathcal{U}$ eine Menge von Teilmengen einer Menge M, also $\mathcal{U} \subseteq \mathrm{Pot}(M)$.*
1.) Der **Durchschnitt** *von $\mathcal{U}$ (oder der Mengen aus $\mathcal{U}$) ist definiert als*

$$\begin{aligned} \bigcap_{T\in\mathcal{U}} T &:= \{m \in M \mid m \in T \text{ für alle } T \in \mathcal{U}\} \\ &= \{m \in M \mid \forall\, T \in \mathcal{U} \text{ gilt } m \in T\}. \end{aligned}$$

2.) Die **Vereinigung** *von $\mathcal{U}$ (oder der Mengen aus $\mathcal{U}$) definiert als*

$$\begin{aligned} \bigcup_{T\in\mathcal{U}} T &:= \{m \in M \mid m \in T \text{ für (mindestens) ein } T \in \mathcal{U}\} \\ &= \{m \in M \mid \exists\, T \in \mathcal{U} \text{ mit } m \in T\}. \end{aligned}$$

Beispiel Definiert man für $n \in \mathbb{N}$ die Menge $T_n := \{d \in \mathbb{N} \mid d \text{ teilt } n\}$ (also die Menge aller Teiler von n), so ist

$$\bigcap_{n\in\mathbb{N}} T_n = \{1\}, \quad \bigcup_{n\in\mathbb{N}} T_n = \mathbb{N}.$$

Beweis: $\bigcap_{n\in\mathbb{N}} T_n = \{1\}$, denn $1 \in T_n$ für alle n und $T_1 = \{1\}$.
$\bigcup_{n\in\mathbb{N}} T_n = \mathbb{N}$, da $n \in T_n$ für alle $n \in \mathbb{N}$.

Bemerkung 3.3. *Sei M eine nicht leere Menge. Ist $\mathcal{U} := \emptyset \subseteq \mathrm{Pot}(M)$, so gilt*

$$\bigcap_{T\in\mathcal{U}} T = M \text{ und } \bigcup_{T\in\mathcal{U}} T = \emptyset$$

Beweis. Wir beweisen die erste Behauptung und lassen die zweite als Übung:

$$\begin{aligned}\bigcap_{T\in\mathcal{U}} T &= \{m \in M \mid \forall\, T \in \mathcal{U} \text{ gilt } m \in T\} \\ &= \{m \in M \mid\ T \in \mathcal{U} \Rightarrow m \in T\} \\ &= M\end{aligned}$$

denn die Prämisse "$T \in \mathcal{U}$" der Implikation "$T \in \mathcal{U} \Rightarrow m \in T$" ist nie erfüllt, da $\mathcal{U} = \emptyset$, sodass die Implikation immer richtig ist. q.e.d.

Bemerkung 3.4. *Sei I eine Menge und $(T_i)_{i\in I}$ eine Mengenfamilie mit $T_i \subseteq M$ Dann gilt:*
1.)

$$\overline{\bigcap_{i\in I} T_i} = \bigcup_{i\in I} \overline{T_i}.$$

2.)

$$\overline{\bigcup_{i\in I} T_i} = \bigcap_{i\in I} \overline{T_i}.$$

Beweis. Wir zeigen nur 1.), 2.) lassen wir als Übung.

$$\begin{aligned}& x \in \overline{\bigcap_{i\in I} T_i} \\ \Longleftrightarrow\ & x \notin \bigcap_{i\in I} T_i \\ \Longleftrightarrow\ & \neg \left(x \in \bigcap_{i\in I} T_i \right) \\ \Longleftrightarrow\ & \neg (\ \forall\ i \in I\ :\ x \in T_i) \\ \Longleftrightarrow\ & \exists\ i \in I\ :\ x \notin T_i \\ \Longleftrightarrow\ & \exists\ i \in I\ :\ x \in \overline{T_i} \\ \Longleftrightarrow\ & x \in \bigcup_{i\in I} \overline{T_i}\end{aligned}$$

q.e.d.

Kapitel 3

Beweise und Beweistechniken

Der Beweis ist eine der Mathematik eigene Erscheinung, auf die ich in diesem Kapitel kurz eingehen möchte. Während andere Naturwissenschaften oft auf empirische Beweise (Beobachtungen, Experimente und Versuchsreihen) setzen, bedient sich die Mathematik logischer Schlussweisen, um unzweifelhafte Begründungen für Tatsachen zu finden. Auf diese Weise behalten bewiesene Resultate der Mathematik für immer ihre Gültigkeit und können gegebenfalls noch Jahrzehnte später für aktuelle Forschungen herangezogen werden.
Das Finden von Beweisen dient aber auch Ihrer eigenen Absicherung, denn "offensichtliche" Tatsachen können sich durchaus als falsch erweisen. Eine solche "offensichtliche Tatsache" findet sich im folgenden Beispiel (Achtung, es folgt eine falsche Aussage).

1 Beispiele

Beispiel. Wir betrachten die Behauptung "Für jede natürliche Zahl n (das sind die Zahlen $1, 2, 3, ...$, die Sie zum Zählen verwenden), ergibt der Ausdruck n^2+n+41 eine Primzahl."
Es ist nun durchaus naheliegend, dies an einigen Beispielen zu überprüfen. Setzt man für n die Zahl 1 ein, so erhält man 43, für $n = 2$ ergibt sich 47, $n = 3$ liefert 53. Man überzeugt sich leicht, dass dies allesamt Primzahlen sind.
In der Tat erhält man für jeden Wert bis einschließlich $n = 39$ eine Primzahl als Ergebnis. Dennoch ist die behauptete Aussage falsch, denn setzt man für n die Zahl 40 ein, so erhält man

$$40^2 + 40 + 41 = 40(40 + 1) + 41 = 40 \cdot 41 + 41 = (40 + 1) \cdot 41 = 41^2.$$

Dies ist sicherlich keine Primzahl.
In diesem Beispiel findet sich eine wichtige Erkenntnis, nämlich dass man eine falsche Aussage widerlegen kann, indem man ein einfaches Gegenbeispiel angibt - es ist keine ausgefeilte Begründung dafür nötig, warum die Aussage nicht richtig sein kann.
Ein anderer Grund, warum Beweise für die Mathematik nötig und nützlich sind, wird an den folgenden zwei Sätzen[1] ersichtlich.

Satz 1.1 (Euklid)**.** *Es gibt unendlich viele Primzahlen.*

[1] Ein Satz ist eine bewiesene - also korrekte - mathematische Aussage

Satz 1.2 (Wiles)**.** *Die Gleichung $a^n + b^n = c^n$ hat für positive ganze Zahlen a, b, c, n mit $n > 2$ keine Lösung. (Diese Aussage ist auch als großer Fermatscher Satz bekannt).*

Betrachten wir zunächst den ersten Satz. Sicherlich kennen wir die ersten paar Primzahlen noch aus der Schule: $2, 3, 5, 7, 11, 13, ...$ und in der Tat finden wir unter den natürlichen Zahlen immer wieder Primzahlen, egal wie weit wir gehen. Doch welchen Grund haben wir anzunehmen, dass es unter den unendlich vielen Zahlen immer wieder Primzahlen gibt? Wie wir an unserem ersten Beispiel gesehen haben, ist Vorsicht angebracht. Jedoch gibt es einen bestechend einfachen Beweis, der uns die Existenz unendlich vieler Primzahlen garantiert. Manche von Ihnen haben diesen Beweis vielleicht sogar in Ihrer Schullaufbahn gesehen.
Die Notwendigkeit eines Beweises ergibt sich aus der Unendlichkeit der Zahlen - es ist nicht menschenmöglich, jede Zahl darauf zu prüfen, ob sie eine Primzahl ist.
Selibiges gilt für den Fermatschen Satz. Für jedes einzelne n könnte man nach Lösungen der betrachteten Gleichung suchen - etwa mit einem Computer. Diese Vorgehensweise kann jedoch nicht zum Ziel führen. Genau zu diesem Thema gibt es ein Zitat des bekannten Mathematikers John Conway, welches hier passen ist.

Well, how many numbers are there to be dealt with? You've got to do it for infinitely many numbers. So, after you've done it for one, how much closer have you got? Well, there's still infinitely many left. After you've done it for a thousand numbers, how many, how much closer have you got? Well, there's still infinitely many left. After you've done it for a million, well, there's still infinitely many left. In fact, you haven't done very many, have you? [2]

Daher benötigt man einen Beweis, eine abstrakte und allgemeine Begründung, warum die Aussage richtig ist. Lassen Sie sich jedoch nicht täuschen: Während der Beweis für die Unendlichkeit der Primzahlen relativ gut verstïndlich und kurz ist, ist der Beweis von Wiles für den Fermatschen Satz hochkompliziert und etwa 100 Seiten lang. Von der Verständlichkeit einer Aussage lässt sich also in der Regel nur schwer auf die Verständlichkeit eines eventuellen Beweises schließen.
Ein Beweistyp, der gerne benutzt wird, ist der Beweis durch Widerspruch, den ich Ihnen an einem Beispiel vormachen werde. Das ihm zugrundeliegende Prinzip ist im Kapitel über Aussagenlogik beschrieben. Beachten Sie, dass ein direkter Beweis einem Widerspruchsbeweis in der Regel vorzuziehen ist.

Satz 1.3. *$\sqrt{2}$ lässt sich nicht als Bruch zweier ganzer Zahlen schreiben.*

Beweis. Nehmen wir an, dass das Gegenteil der Fall ist, dass also $\sqrt{2} = \frac{p}{q}$ mit zwei ganzen Zahlen p und q. Überdies sei der Bruch $\frac{p}{q}$ vollständig gekürzt.
Aus unserer Annahme ergibt sich durch Quadrieren die Gleichung $2 = \frac{p^2}{q^2}$, was man zu $2q^2 = p^2$ umformt. Wir sehen, dass die linke Seite der Gleichung eine gerade Zahl ist, sodass dies auch für die rechte Seite gilt. Die recht Seite der Gleichung ist ein Quadrat, sodass sie sogar zwangsweise durch 4 teilbar ist (Versuchen Sie, dies zu beweisen!). Damit muss die linke Seite der Gleichung, also $2q^2$ durch 4 teilbar sein, also ist q^2 durch zwei

[2] John H. Conway, in "Fermat's Last Theorem", BBC Horizon

teilbar.
Damit sind sowohl p als auch q durch zwei teilbar. Allerdings hatten wir angenommen, dass der Bruch $\frac{p}{q}$ vollständig gekürzt ist. Somit haben wir einen Widerspruch erhalten, womit unsere Annahme, dass die zu zeigende Aussage falsch sei, nicht mehr haltbar ist. Damit ist der Beweis der Aussage erbracht. q.e.d.

Ich möchte dieses kurze Kapitel mit einem Beispiel für einen Beweis beenden, der für die Mathematik sehr typisch ist, nämlich ein Existenzbeweis. Wir werden gleich die Existenz zweier Zahlen mit einer bestimmten Eigenschaft beweisen, ohne zu sagen, um welche Zahlen es sich handelt.

Satz 1.4. *Es existieren reelle Zahlen x, y, sodass x^y rational ist, während x und y irrational sind. Dass eine Zahl x irrational ist, bedeutet dass x nicht in $\mathbb{Q}$ liegt, also nicht als Bruch ganzer Zahlen darstellbar ist. Rationalität bedeutet, in $\mathbb{Q}$ zu liegen.*

Beweis. Wir betrachten $\sqrt{2}^{\sqrt{2}}$. Ist diese Zahl rational, so sind wir fertig, denn $\sqrt{2}$ ist, wie wir gesehen haben, eine irrationale Zahl. Ist $\sqrt{2}^{\sqrt{2}}$ irrational, so ist $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$ sicherlich rational. q.e.d.

Wie Sie sehen, haben wir bewiesen, dass es solche x und y gibt, jedoch wissen wir nicht, ob $x = y = \sqrt{2}$ oder $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$ diese Zahlen sind. Dennoch ist die Aussage bewiesen.

Kapitel 4

Mengen und Abbildungen

1 Mengen.

Lernziel: Einfache Notation, Konstruktionen und Identitäten der Mengenlehre: Teilmengen, Potenzmenge, Vereinigung und Durchschnitt, kartesische Produkte.

1.1 Notation

In diesem Abschnitt möchte ich Ihnen nicht genau erklären, was eine Menge ist, sondern eher, wie man Mengen konstruieren, manipulieren und benutzen kann. **Eine Menge ist eine Ansammlung von unterscheidbaren Objekten, den sogenannten Elementen der Menge.** Beispiele für Mengen kennt der eine oder andere schon aus der Schule.
Beispiel. 1.) $\mathbb{N} := \{1, 2, 3, \ldots\}$, die Menge der natürlichen Zahlen.
2.) $\{3, 5, 7, 11, 13, 17\}$, die Menge der Primzahlen zwischen 3 und 17. Es gibt verschiedene Beschreibungen für dieselbe Menge:
Aufzählende Form: $\{3, 5, 7, 11, 13, 17\}$
oder auch $\{11, 13, 17, 5, 3, 5, 7\}$.
(In einer Menge kommt es nicht auf die Reihenfolge der Elemente an und es kommt kein Element mehrfach vor, es ist also zum Beispiel $\{1, 1, 3, 3, 3, 2\} = \{1, 2, 3\}$.)
Beschreibende Form:

$$\{n \in \mathbb{N} \mid 3 \leq n \leq 17 \text{ und } n \text{ ist Primzahl } \}.$$

Dies ist zu lesen als eine Menge, die aus den Elementen besteht, die links des Trennstrichs stehen und die Eigenschaft auf der rechten Seite erfüllen.
Diese Beispiele sollen nicht suggerieren, dass Mengen nur aus Zahlen zusammengestellt werden können. Man kann zum Beispiel die Menge aller Personen betrachten, die im Jahr 1955 geboren wurden.

Definition 1.1. *(Notationen für Mengen)*

1.) *Ist M eine Menge und a ein Element von M, so schreiben wir $a \in M$. Ist a kein Element von M, so schreiben wir $a \notin M$.*

2.) Zwei Mengen M und N sind genau dann **gleich**, *kurz $M = N$, wenn sie dieselben Elemente enthalten. Das heißt es ist genau dann $M = N$, wenn für alle $a \in M$ auch $a \in N$ gilt und umgekehrt.*

3.) Die Menge, die keine Elemente enthält, heißt die **leere Menge** $\emptyset$ *oder auch* $\{\}$. ***Man beachte den Unterschied zwischen*** $\emptyset$ ***und*** $\{\emptyset\}$**.**

4.) Eine Menge N heißt **Teilmenge** *der Menge M, $N \subseteq M$, falls für alle Elemente $a \in N$ gilt, dass $a \in M$. In Formeln:*
$(N \subseteq M) :\Leftrightarrow (a \in N \Rightarrow a \in M)$ [1]

5.) Dies bedeutet, dass für zwei Mengen M und N genau dann Gleichheit vorliegt, wenn $M \subseteq N$ und $N \subseteq M$ gelten.

6.) Für eine Menge M heißt

$$\mathrm{Pot}(M) := \{T \mid T \subseteq M\},$$

also die Menge aller Teilmengen von M, die **Potenzmenge** *von M.*

7.) Ist M endlich, so bezeichnet $|M|$ die Anzahl der Elemente von M.

Beispiel 1.) $\emptyset \subseteq M$ für jede Menge M.
2.) Eine beschreibende Form für die leere Menge ist z.B. $\emptyset = \{n \in \mathbb{N} \mid n < 0\}$.
3.) $\mathrm{Pot}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.
Man beachte, dass die Elemente dieser Menge ihrerseits wieder Mengen sind, was anfangs etwas verwirrend sein kann:

$$\{3\} \in \mathrm{Pot}(\{1,2,3\}) \Leftrightarrow \{3\} \subseteq \{1,2,3\} \Leftrightarrow 3 \in \{1,2,3\}.$$

Definition 1.2. *Wir vereinbaren die folgende Kurzschreibweise. Ist $n \in \mathbb{N}$, so setzen wir*

$$\underline{n} := \{1, 2, ..., n\} = \{n \in \mathbb{N} \mid n \leq n\}$$

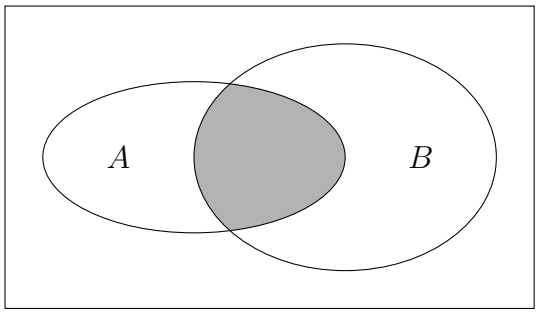
1.2 Mengenoperationen

Wir stellen hier Durchschnitt, Vereinigung und Differenz von Mengen vor. Dabei handelt es sich um Möglichkeiten aus gegebenen Mengen neue Mengen zu konstruieren. Wir präsentieren die Definitionen zusammen mit den zugehörigen VENN[2]-Diagrammen, die ein sich selbst erklärender Appell an die Anschauung sind.

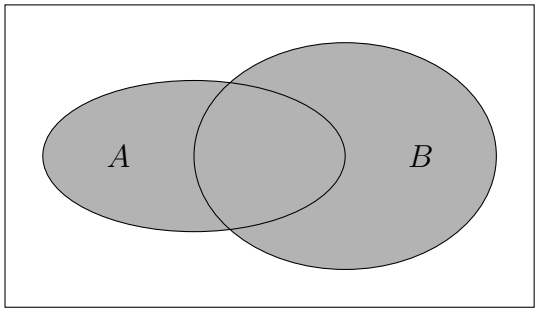
Definition 1.3. *Sei M eine Menge mit Teilmengen $A, B \subseteq M$.*
1) $A \cap B := \{m \in M \mid m \in A$ und $m \in B\}$ heißt der **Durchschnitt** *der Mengen A und B.*

[1] Dies sind Symbole der Aussagenlogik. Aus Zeitgründen behandeln wir die Aussagenlogik in diesem Kurs nicht genau. An die Symbole sollten Sie sich dennoch gewöhnen. $\Leftrightarrow$ bedeutet "genau dann, wenn", $x \Rightarrow y$ bedeutet "aus x folgt y". Der Doppelpunkt bedeutet, dass die linke Seite definiert wird durch den Ausdruck auf der rechten Seite.

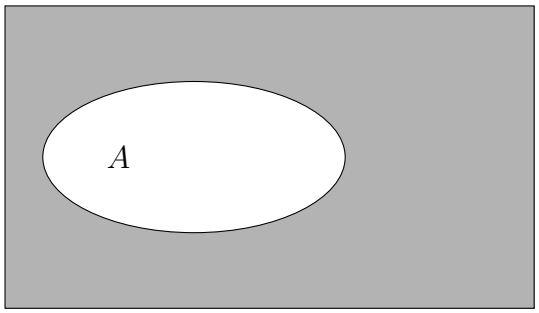
[2] JOHN VENN 1834 - 1923



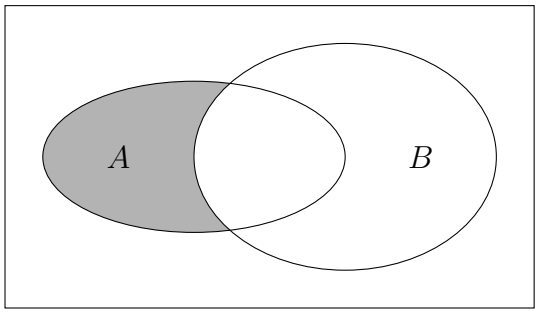
2) $A \cup B := \{m \in M \mid m \in A$ *oder* $m \in B\}$ *heißt die* **Vereinigung** *der Mengen* A *und* B. [3]



3.) $\overline{A} := M \setminus A := \{m \in M \mid m \notin A\}$ *heißt das* **Komplement** *von* A *in* M. *Eine andere häufige Schreibweise ist* A^c.



4) $A \setminus B := \{m \in M \mid m \in A$ *und* $m \notin B\} = A \cap \overline{B}$ *heißt die* **Differenzmenge** A *ohne* B. *Oftmals findet man auch die Schreibweise* $A - B$ *vor.*



[3]Dieses "oder" ist das Oder der Aussagenlogik; es handelt sich um ein einschließendes Oder. Das heißt die Aussage "A oder B" ist genau dann wahr, wenn mindestens eine der Aussagen A, B wahr ist.

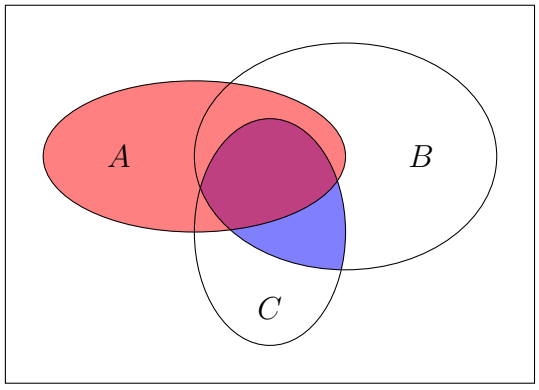
Wir haben also durch $\cap, \cup, \overline{\ }$ Verknüfungen auf $\mathrm{Pot}(M)$. Diese gehorchen den folgenden Gesetzen.

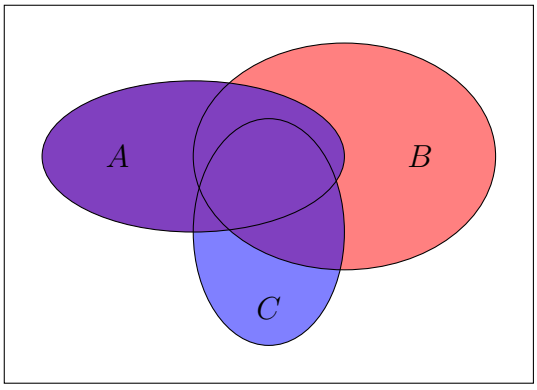
Satz 1.4. *Seien $A, B, C \subseteq M$. Dann gilt:*
1.) $\overline{\overline{A}} = A$.
2.) **Kommutativität des Durchschnittes***:*
$A \cap B = B \cap A$.
3.) **Kommutativität der Vereinigung***:*
$A \cup B = B \cup A$.
4.) **Assoziativität des Durchschittes***:*
$A \cap (B \cap C) = (A \cap B) \cap C$.
5.) **Assoziativität der Vereinigung***:*
$A \cup (B \cup C) = (A \cup B) \cup C$.
6.) **Distributivität der Vereinigung gegenüber dem Schnitt***:*
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
7.) **Distributivität des Schnittes gegenüber der Vereinigung***:*
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Beweis. Der Beweis folgt direkt aus den Regeln der Aussagenlogik. Wir wollen exemplarisch 6.) beweisen und gleichzeitig das zugehörige Venn-Diagramm als Erinnerungsstütze und Kurznotation für den Beweis angeben.

$$
\begin{gathered}
x \in A \cup (B \cap C) \Leftrightarrow \\
x \in A \text{ oder } x \in (B \cap C) \Leftrightarrow \\
x \in A \text{ oder } (x \in B \text{ und } x \in C) \Leftrightarrow \\
(x \in A \text{ oder } x \in B) \text{ und } (x \in A \text{ oder } x \in C) \Leftrightarrow \\
(x \in A \cup B) \text{ oder } (x \in A \cup C) \Leftrightarrow \\
x \in (A \cup B) \cap (A \cup C)
\end{gathered}
$$

Venn-Diagramme:





q.e.d.

Eine weitere wichtige mengentheoretische Konstruktion ist das kartesische Produkt. Es unterscheidet sich grundsätzlich von den bisherigen Operationen $\cup, \cap, \overline{\ }$, die aus Teilmengen einer Menge eine neue Teilmenge machen. Rein formal kommt hier eine Teilmenge der Potenzmenge der Potenzmenge heraus, aber von der Idee her wird eine neue Menge konstruiert.

Definition 1.5. *(formale Definition) Seien M, N Mengen.*
1) Für $m \in M$ und $n \in N$ bezeichnet

$$(m, n) := \{\{m\}, \{m, n\}\}$$

das **geordnete Paar** *der beiden Elemente.*
2)

$$M \times N := \{(m, n) \mid m \in M, n \in N\}$$

heißt das **kartesische Produkt**[4] *der Mengen M und N oder auch die Paarmenge.*

Bemerkung 1.6. *(anschauliche Definition des kartesischen Produkts)*
Für $(m_1, n_1), (m_2, n_2) \in M \times N$ gilt:
$(m_1, n_1) = (m_2, n_2)$ genau dann, wenn $m_1 = m_2$ und $n_1 = n_2$.

Beweis. $(m_1, n_1) = \{\{m_1\}, \{m_1, n_1\}\}$ ist eine Menge. Diese enthält ein Element, falls $m_1 = n_1$ ist, ansonsten zwei Elemente. Ist $m_1 = n_1$, so ist $(m_1, n_1) = (m_2, n_2)$ genau dann, wenn (m_2, n_2) auch nur ein Element enthält und dieses Element gleich $\{m_1\}$ ist, also genau dann, wenn $m_2 = n_2 = m_1$ ist. Gilt aber $m_1 \neq n_1$, so hat (m_1, n_1) zwei Elemente (die ihrerseits wieder Mengen sind) und sich durch die Anzahl ihrer Elemente unterscheiden: $\{m_1\}$ enthält genau ein Element und $\{m_1, n_1\}$ enhält genau zwei Elemente. Also gilt $(m_1, n_1) = (m_2, n_2)$ genau dann, wenn $\{m_1\} = \{m_2\}$ und $\{m_1, n_1\} = \{m_2, n_2\}$ also genau dann wenn $m_1 = m_2$ und $n_1 = n_2$ gelten. q.e.d.

Einfache Beispiele.
1.) $\mathbb{R} \times \mathbb{R}$ kann man als reelle Ebene visualisieren. Dies setzt natürlich die Visualisierung von $\mathbb{R}$ als Zahlengerade voraus.
2.) $\{a, b\} \times \{1, 2, 3\} = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$.
3.) $\{1, 2\} \times \{2, 3, 4\} = \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)\}$.
4.) $M \times \emptyset = \emptyset$ für jede Menge M.
Wir schließen diesen Abschnitt mit einem Beispiel aus der Kombinatorik.

Definition 1.7. *1) Sei $n \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Dann definieren wir $n!$ durch $0! := 1$ und $n! := n \cdot (n-1)!$ für alle $n \in \mathbb{N}$.*
2) Sei $n \in \mathbb{N}$ und $0 \leq k \leq n$. Dann nennen wir $\binom{n}{k} := \frac{n!}{k!(n-k)!}$ den Binomialkoeffizienten n über k.

Satz 1.8. *Sei $n \in \mathbb{N}$ und M eine n-elementige Menge. Sei $0 \leq k \leq n$. Dann ist die Anzahl der k-elementigen Teilmengen von M gerade $\binom{n}{k}$.*

[4] René Descartes 1596 - 1650

Beweis. Um eine k-elementige Teilmenge von M herzustellen, müssen wir k Elemente aus M auswählen. Für das erste Element haben wir n Möglichkeiten, ein Element auszuwählen. Für das zweite Element haben wir dann noch $n-1$ Wahlmöglichkeiten. Dies setzt sich bis zum k-ten Element fort, was uns insgesamt

$$n \cdot (n-1) \cdot (n-2) \cdot ... \cdot (n-k-1) = \frac{n!}{(n-k)!}$$

Wahlmöglichkeiten liefert. Man beachte jedoch, dass diese Anzahl größer ist als die Anzahl der k-elementigen Teilmengen, da wir der Tatsache, dass es in einer Menge nicht auf die Reihenfolge der Elemente ankommt, noch nicht Rechnung getragen haben. Denken wir uns die k-elementige Teilmenge, die wir ausgewählt haben als eine Liste mit k Einträgen, so können wir die k Elemente, die wir aus M ausgewählt haben, nach Belieben auf diese Liste verteilen. Das heißt, dass wir für das erste Element k Möglichkeiten haben, eine Position zu wählen, für das zweite Element haben wir noch $k-1$ Möglichkeiten, und so weiter, was schießlich auf $k!$ identische Teilmengen führt.
Insgesamt haben wir also $\frac{1}{k!}\frac{n!}{(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$ Wahlmöglichkeiten für eine k-elementige Teilmenge von M.
Man beachte, dass dies den Fall einer 0-elementigen Teilmenge, also der leeren Menge, einschließt.
Wir haben außerdem mit diesem Argument gezeigt, dass der Bruch $\frac{n!}{k!(n-k)!}$ stets eine ganze (sogar natürliche) Zahl ist, da die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge sicherlich stets eine ganze Zahl ist. q.e.d.

2 Abbildungen.

2.1 Definition und erste Beispiele

Lernziele: Definition von Abbildung, Definitionsbereich, Wertebereich, Bild, bijektive Abbildungen

Definition 2.1. *Seien M, N Mengen.*
1) Eine **Abbildung** *oder* **Funktion** *f von M nach N ist eine Teilmenge $f \subseteq M \times N$ des kartesischen Produktes $M \times N$, die die folgende Bedingung erfüllt:*
Für jedes $m \in M$ gibt es genau ein $n \in N$ mit $(m,n) \in f$. Man nennt n auch das (bezüglich f) m zugeordnete Element und schreibt $n = f(m)$ statt $(m,n) \in f$.[5] *Statt „$f \subseteq M \times N$ Abbildung“ schreibt man:*

$$f : M \to N$$

oder ausführlicher:

$$f : M \to N : m \mapsto f(m).$$

Achtung: *Man beachte den Unterschied zwischen $\to$ und $\mapsto$.*
2) Ist $f : M \to N$ eine Abbildung, so heißt M der **Definitionsbereich** *von f, N der*

[5] Manchmal nennt man auch das, was wir als Funktion bezeichnet haben, den Graphen einer Funktion und stellt sich die Funktion als Zuordnung vor.

Wertebereich *und für $T \subseteq M$ heißt*

$$f(T) := \{f(m) \mid m \in T\} (\subseteq N)$$

das **Bild** *von T unter f, im Falle $T = M$ heißt* $\mathrm{Bild}(f) := f(M)$ *das* **Bild** *von f.*

Man beachte: Eigentlich sind Abbildungen über zwei Bedingungen definiert, eine Existenz- und eine Eindeutigkeitsbedingung.

Definition 2.2. *Sind M und N zwei Mengen, so bezeichnen wir mit*
$N^M := \{f \ : \ M \to N \mid f$ *ist eine Abbildung.*$\}$
die Menge aller Abbildungen von M nach N.

Beispiel. Sei $M := N := \mathbb{R}$. Dann ist der Kreis

$$k := \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\}$$

keine Abbildung von $M = \mathbb{R}$ nach $N = \mathbb{R}$. Erstens gibt es nicht zu jedem $x \in M$ ein $y \in N$ mit $(x, y) \in k$, z. B. nicht für $x = 2$. Diesen Übelstand kann man dadurch beheben, dass man $\mathbb{R}$ durch das abgeschlossene Intervall

$$M := [-1, 1] := \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$$

ersetzt. Zweitens existieren für jedes x mit $-1 < x < 1$ zwei $y \in N$ mit $(x, y) \in k$. Wir können auch diesen Übelstand beheben, indem wir zwei Abbildungen definieren:

$$\begin{aligned} k_1 : [-1, 1] &\to \mathbb{R}; x \mapsto \sqrt{1 - x^2}, \\ k_2 : [-1, 1] &\to \mathbb{R}; x \mapsto -\sqrt{1 - x^2} \end{aligned}$$

und wir erhalten $k = k_1 \cup k_2$, wobei k_1 und k_2 Abbildungen sind, k jedoch nicht mehr. Der Definitionsbereich für beide k_i ist $M = [-1, 1]$, der Wertebereich $N = \mathbb{R}$ und die Bilder sind $k_1([-1, 1]) = [0, 1]$ und $k_2([-1, 1]) = [-1, 0]$.
Beispiel. 1.) Seien $\underline{3} := \{1, 2, 3\}$ und $\underline{4} := \{1, 2, 3, 4\}$. Dann ist
$f := \{(1, 1), (1, 2), (2, 3), (3, 4)\} \subseteq \underline{3} \times \underline{4}$
keine Abbildung von $\underline{3}$ nach $\underline{4}$. Jedoch ist
$g := \{(1, 2), (2, 4), (3, 3)\} \subseteq \underline{3} \times \underline{4}$
eine Abbildung von $\underline{3}$ nach $\underline{4}$.
2.) $h \ : \ \underline{3} \to \underline{4}$, $\begin{cases} 1 \mapsto 2 \\ 2 \mapsto 4 \\ 3 \mapsto 3 \end{cases}$ ist eine Abbildung und stimmt mit g aus 1.) überein.
3.) Sei M eine Menge, $\mathcal{P} := \mathrm{Pot}(M)$. Dann ist $^- : \mathcal{P} \to \mathcal{P}$ eine Abbildung. Ebenso sind $\cup$ und $\cap \ : \mathcal{P} \times \mathcal{P} \to \mathcal{P}$ Abbildungen.

Definition 2.3. *Sei $f : M \to N$ eine Abbildung. Für $n \in N$ heißt*

$$f^{-1}(\{n\}) := \{m \in M \mid f(m) = n\} \qquad (\subseteq M)$$

die **Faser** *von f über n, die Faser von n, oder volles Urbild von n.*

Beispiel. 1) Die Abbildung $f := \{(1, 1), (2, 2)\} \subseteq \underline{2} \times \underline{3}$ hat die Fasern $f^{-1}(\{1\}) = \{1\}$, $f^{-1}(\{2\}) = \{2\}$ und $f^{-1}(\{3\}) = \emptyset$.
2) Die Abbildung $f := \{(1, 1), (2, 2), (3, 2)\} \subseteq \underline{3} \times \underline{2}$ hat die Fasern $f^{-1}(\{1\}) = \{1\}$ und $f^{-1}(\{2\}) = \{2, 3\}$.

2.2 Komposition, Bijektivität, Injektivität und Surjektivität

Definition 2.4. *(Komposition von Abbildungen)*
Seien M_1, M_2, M_3 Mengen und $f : M_1 \to M_2$ und $g : M_2 \to M_3$ Abbildungen. Dann ist $g \circ f : M_1 \to M_3,\ m \mapsto (g \circ f)(m) := g(f(m))$ eine Abbildung $M_1 \to M_3$, die so genannte Hintereinanderausführung von g nach f. In der Schreibweise, bei welcher f als Teilmenge von $M_1 \times M_2$ und g als Teilmenge von $M_2 \times M_3$ verstanden werden, ist die Komposition von g nach f gegeben durch $g \circ f = \{(m,n) \in M_1 \times M_3 \mid$ es existiert ein $x \in M_2$ mit $(m,x) \in f$ und $(x,n) \in g\}$.

Bemerkung 2.5. *Seien M_1, M_2, M_3, M_4 Mengen und $f : M_1 \to M_2$, $g : M_2 \to M_3$ und $h : M_3 \to M_4$ Abbildungen. Dann gilt $h \circ (g \circ f) = (h \circ g) \circ f$, d.h. es gilt das Assoziativgesetz für die Komposition von Abbildungen. Aus diesem Grund schreiben wir die Komposition auch ohne Klammerung.*

Beweis. Zum Beweis mache man sich nochmals klar, dass Gleichheit von Abbildungen bedeutet, dass die Definitions- und Wertebereiche übereinstimmen und dass die Abbildungen an jeder Stelle des Definitionsbereichs den gleichen Wert ergeben.
Sei $x \in M_1$. Dann gilt
$\big(h \circ (g \circ f)\big)(x) = h\big((g \circ f)(x)\big) = h(g(f(x))) = \big(h \circ g\big)(f(x)) = \big((h \circ g) \circ f\big)(x)$. q.e.d.

Definition 2.6. *(Identische Abbildung)*
Ist X eine Menge, so bezeichnen wir die Abbildung $\mathrm{id}_X : X \to X,\ x \mapsto x$ als Identität auf X.

Definition 2.7. *(Bijektivität)*
Seien M und N Mengen und $f : M \to N$ eine Abbildung. Wir nennen f bijektiv oder eine Bijektion, falls eine Abbildung $g : N \to M$ existiert, sodass $f \circ g = \mathrm{id}_N$ und $g \circ f = \mathrm{id}_M$.
In diesem Fall nennen wir g die Umkehrabbildung oder inverse Abbildung zu f und schreiben $f^{-1} := g$.
Man beachte den Unterschied zwischen der Faser und der Umkehrabbildung.

Satz 2.8. *Eine Abbildung $f : M \to N$ ist genau dann bijektiv, wenn für jedes $n \in N$ die Faser $f^{-1}(\{n\})$ genau ein Element besitzt.*

Beweis. Ist jede Faser einelementig, so konstruiert man leicht eine Umkehrabbildung, indem man jedes $n \in N$ auf das eindeutige Element in $f^{-1}(\{n\})$ abbildet.
Sei nun umgekehrt f bijektiv und $n \in N$. Dann ist $f(f^{-1}(n)) = n$, also ist $f^{-1}(\{n\})$ nicht die leere Menge. Hat man Elemente $x, y \in f^{-1}(\{n\})$, so ist $f(x) = f(y) = n$, also folgt durch Anwenden von f^{-1}, $x = y$, sodass $f^{-1}(\{n\})$ in der Tat einelementig ist. q.e.d.

Beispiel. 1) $f : \mathbb{R} \to \mathbb{R},\ x \mapsto 3x + 7$ ist eine bijektive Abbildung.
2) $f : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$ ist nicht bijektiv.
3) $f : \underline{4} \to \underline{4},\ x \mapsto \begin{cases} x+1 & \text{falls } x \in \{1,2,3\} \\ 1 & \text{falls } x = 4 \end{cases}$ ist eine bijektive Abbildung.

4) $f : \mathbb{N}_0 \to \mathbb{Z},\ n \mapsto \begin{cases} \frac{n}{2} & \text{falls } n \text{ gerade} \\ -\frac{n-1}{2} & \text{falls } n \text{ ungerade} \end{cases}$ ist eine Bijektion.
Dies werden wir später beweisen.

Definition 2.9. *(Injektivität und Surjektivität)*
Sei $f : M \to N$ eine Abbildung.
1) Wir nennen f injektiv (oder eine Injektion), falls f verschiedene Elemente von M auf verschiedene Elemente von N abbildet. In Formeln: $f(x) = f(y) \Rightarrow x = y$ für alle $x, y \in M$.
2) Wir nennen f surjektiv (oder eine Surjektion), falls für jedes $n \in N$ ein $m \in M$ existiert mit $f(m) = n$, oder anders gesagt, falls $\mathrm{Bild}(f) = N$.

Es folgen wichtige Charakterisierungen von Injektivität, Surjektivität und Bijektivität.

Satz 2.10. *Sei $f : M \to N$ eine Abbildung und $M \neq \emptyset$.*[6]
1) Die folgenden Aussagen sind äquivalent, was bedeutet, dass Aussage a) genau dann zutrifft, wenn Aussage b) zutrifft, und b) genau dann zutrifft, wenn c) zutrifft.

a) f ist injektiv.

b) Es existiert eine Abbildung $g : N \to M$ mit $g \circ f = \mathrm{id}_M$.

c) Jede Faser von f ist höchstens einelementig.

2) Die folgenden Aussagen sind äquivalent.

a) f ist surjektiv.

b) Es existiert eine Abbildung $g : N \to M$ mit $f \circ g = \mathrm{id}_N$.

c) Jede Faser von f ist mindestens einelementig.

3) Die folgenden Aussagen sind äquivalent.

a) f ist bijektiv.

b) f ist injektiv und surjektiv.

c) Jede Faser von f ist einelementig.

Beweis. Wir beweisen nur einen Teil der Aussagen, wobei ein wichtiges Beweisprinzip zum Tragen kommt, nämlich der so genannte Ringschluss. Der Ringschluss besagt in unserem Fall, dass man beweisen kann, dass drei Aussagen a), b) und c) äquivalent sind, indem man zeigt, dass aus a) die Aussage b) folgt, dass aus b) die Aussage c) folgt und dass sich aus c) wiederum a) folgern lässt.
2) Wir zeigen zunächst "a)⇒b)". Sei also f surjektiv. Dann gibt es zu jedem $n \in N$ ein $m_n \in M$ mit $f(m_n) = n$ (wobei der Index an m_n die Abhängigkeit von $n \in N$ verdeutlichen soll und sonst keine weitere Bedeutung hat). Wir wählen zu jedem $n \in N$

[6] Ist $M \neq \emptyset$, so ist auch $N \neq \emptyset$, da es sonst keine Abbildung $f : M \to N$ gibt. Um die Umkehrabbildungen jeweils konstruieren zu können, müssen die Mengen nichtleer sein.

ein solches m_n aus und definieren $g : N \to M$ durch die Vorschrift $n \mapsto m_n$. Es gilt dann für jedes $n \in N$

$$(f \circ g)(n) = f(g(n)) = f(m_n) = n,$$

also $f \circ g = \mathrm{id}_N$, was zu zeigen war.
Nun zeigen wir "b)⇒c)", das heißt wir nehmen als Voraussetzung die Existenz einer Funktion $g : N \to M$ wie in b) an und betrachten nun zu einem $n \in N$ die Faser $f^{-1}(\{n\})$. Da für jedes $n \in N$ gilt, dass $n = \mathrm{id}_N(n) = (f \circ g)(n) = f(g(n))$ gilt, haben wir $g(n) \in f^{-1}(\{n\})$.
Schließlich zeigen wir "c)⇒a)". Sei $n \in N$. Dann enthält nach Voraussetzung $f^{-1}(\{n\})$ mindestens ein Element, was eine Umformulierung der folgenden Aussage ist: zu jedem $n \in N$ existiert ein $m \in M$ mit $f(m) = n$. Also ist f surjektiv.
3) folgt aus 1) und 2). q.e.d.

Wir beweisen nun mit Hilfe dieses Satzes, dass $f : \mathbb{N}_0 \to \mathbb{Z}$, $n \mapsto \begin{cases} \frac{n}{2} & \text{falls } n \text{ gerade} \\ -\frac{n-1}{2} & \text{falls } n \text{ ungerade} \end{cases}$ eine bijektive Abbildung ist.

Beweis. f ist surjektiv, denn zu $z \in \mathbb{Z}$ sind Urbilder gegeben durch $2z$, falls $z \geq 0$, und $-2z + 1$, falls $z < 0$.
Wir zeigen nun, dass f injektiv ist. Seien dazu $m, n \in \mathbb{N}_0$ und $f(m) = f(n)$. Aufgrund dieser Gleichheit müssen m und n sicherlich beide gerade oder beide ungerade sein (sonst hätten ihre Bilder unter f verschiedene Vorzeichen), sodass zwei Fälle zu betrachten sind:
1) m und n sind gerade. Dann ist $\frac{n}{2} = \frac{m}{2}$, woraus $m = n$ folgt.
2) m und n sind ungerade, was die Gleichung $-\frac{n-1}{2} = -\frac{m-1}{2}$ liefert, woraus wiederum $m = n$ folgt.
f ist also injektiv und damit insgesamt eine Bijektion. q.e.d.

Mit den Begriffen, die wir bisher gelernt haben, können wir nun eine bekannte Aussage der Mengenlehre formulieren und beweisen.

Satz 2.11. *Sei M eine Menge und* $\mathrm{Pot}(M)$ *ihre Potenzmenge. Es existiert keine surjektive Abbildung $M \to \mathrm{Pot}(M)$.*

Beweis. Sei $f : M \to \mathrm{Pot}(M)$ eine Abbildung. Wir setzen $X := \{m \in M \mid m \notin f(m)\}$. Dies ist eine Teilmenge von M und somit ein Element von $\mathrm{Pot}(M)$.
Wir behaupten, dass X kein Urbild unter f besitzt, was damit gleichbedeutend ist, dass f nicht surjektiv ist.
Wenn nämlich $m \in M$ ein Urbild ist, dann haben wir zwei Fälle zu betrachten:
1) $m \in X$: In diesem Fall ist definitionsgemäß $m \notin f(m)$, jedoch ist nach Annahme $f(m) = X$, also $m \notin X$. Dies ist ein Widerspruch zur Annahme, dass $m \in X$.
2) $m \notin X$: Dann ist, da wiederum $X = f(m)$ gilt, $m \notin f(m)$. Nach Definition von X ist dann aber $m \in X$ und wir haben erneut einen Widerspruch erhalten.
Damit haben wir bewiesen, dass das Element $X \in \mathrm{Pot}(M)$ nicht im Bild von f liegt. Also ist f nicht surjektiv. q.e.d.

Kapitel 5

Relationen

1 Definitionen und Beispiele

Definition 1.1. *Es sei M eine Menge. Eine (binäre oder zweistellige) Relation auf M ist eine Teilmenge R des kartesischen Produkts $M \times M$.*
Ist für zwei Elemente $a, b \in M$ das Element (a, b) in R enthalten, so sagen wir, dass a und b in Relation stehen und schreiben dafür auch aRb.

Einfache Beispiele für Relationen auf einer Menge M sind $R = \emptyset$, $R = M \times M$ und $R = \{(m, m) \mid m \in M\}$.
Beispiel. Wir betrachten nun als Beispiel die Teilbarkeitsrelation auf der Menge der ganzen Zahlen $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$.
Seien $a, b \in \mathbb{Z}$. Wir sagen a teilt b (in Zeichen $a \mid b$), falls eine ganze Zahl x existiert, sodass $a \cdot x = b$.
Diese Relation sollte aus der Schule bekannt sein, es gilt beispielsweise $3 \mid 6$, $2 \mid 14$ und so weiter.
Wir möchten nun einige Eigenschaften dieser Relation betrachten. Es gilt beispielsweise $5 \mid 10$ und $10 \mid 20$, woran man ablesen kann, dass auch $5 \mid 20$ gilt. Wir behaupten, dass dies eine allgemeingültige Eigenschaft für ganze Zahlen ist, die wir wie folgt formulieren. Seien $a, b, c \in \mathbb{Z}$ mit $a \mid b$ und $b \mid c$. Dann gilt auch $a \mid c$. Dies kann man wie folgt beweisen: Wegen $a \mid b$ existiert ein $x \in \mathbb{Z}$ mit $b = ax$. Aus $b \mid c$ leitet sich die Existenz eines $y \in \mathbb{Z}$ mit $c = by$ ab. Damit können wir schreiben: $c = by = (ax)y = a(xy)$. Damit haben wir $a \mid c$, was zu beweisen war.
Eine weitere Eigenschaft der Teilbarkeitsrelation ist, dass jede Zahl sich selbst teilt, denn es ist ja $x = x \cdot 1$ für alle $x \in \mathbb{Z}$.
Diese Eigenschaften führen uns zu der folgenden Definition.

Definition 1.2. *Sei M eine Menge und R eine Relation auf M. Wir nennen R*

1. ***symmetrisch**, falls für alle $a, b \in M$ aus aRb bereits bRa folgt.*
2. ***transitiv**, falls für $a, b, c \in M$ gilt, dass aus aRb und bRc folgt, dass aRc.*
3. ***reflexiv**, falls für alle $m \in M$ gilt, dass mRm.*

Bemerkung 1.3. *Die Teilbarkeitsrelation auf $\mathbb{Z}$ ist also transitiv und reflexiv. Sie ist jedoch nicht symmetrisch, denn es wird beispielsweise 4 von 2 geteilt, nicht jedoch 2 von 4.*

Beispiel. 1) Die Relation $\{(m,m) \mid m \in M\}$ (für eine beliebige Menge M) ist symmetrisch, transitiv und reflexiv.
2) Sei M eine Menge. Dann haben wir die Teilmengenrelation auf $\mathrm{Pot}(M)$. Diese ist gegeben durch
$\subseteq := \{(A,B) \in \mathrm{Pot}(M) \mid A \subseteq B\}$.
Diese Relation ist transitiv und reflexiv, jedoch nicht symmetrisch.
3) Wir betrachten die Relation $K := \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\}$. K ist sicherlich nicht reflexiv, denn es gilt zum Beispiel nicht $0K0$. Jedoch ist K symmetrisch, was aus dem Kommutativgesetz der Addition folgt. Der Leser untersuche als Übung, ob K transitiv ist.
4) $\Big\{\big((a,b),(c,d)\big) \in (\mathbb{Z} \times \mathbb{Z}) \times (\mathbb{Z} \times \mathbb{Z}) \;\Big|\; b - d = 0\Big\}$ ist eine Relation auf $\mathbb{Z} \times \mathbb{Z}$, die symmetrisch, transitiv und reflexiv ist.

2 Äquivalenzrelationen

In diesem Abschnitt betrachten wir spezielle Relationen, die uns im letzten Abschnitt bereits begegnet sind.

Definition 2.1. *Eine reflexive, symmetrische und transitive Relation heißt Äquivalenzrelation. Oft bezeichnet man Äquivalenzrelationen mit $\sim$.*
Ist M eine Menge und $\sim$ eine Äquivalenzrelation darauf, so bezeichnen wir für $m \in M$ die Menge

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

als die Äquivalenzklasse von m. Die Menge aller Äquivalenzklassen bezeichnen wir mit $M/\sim$.
Jedes Element einer Äquivalenzklasse bezeichnet man auch als Vertreter dieser Klasse und eine Teilmenge von M, die aus jeder Äquivalenzklasse genau einen Vertreter enthält, nennen wir Vertretersystem oder Transversale von $\sim$.

Bemerkung 2.2. *Sei M eine Menge, $\sim$ eine Äquivalenzrelation auf M und $m_1, m_2 \in M$. Dann gilt*

$$[m_1]_\sim = [m_2]_\sim \text{ oder } [m_1]_\sim \cap [m_2]_\sim = \emptyset,$$

d.h. zwei Äquivalenzklassen sind entweder disjunkt oder gleich.

Beweis. Um dies zu beweisen, genügt es, unter der Annahme, dass $[m_1]_\sim \cap [m_2]_\sim \neq \emptyset$, die Aussage $[m_1]_\sim = [m_2]_\sim$ zu zeigen. Sei also $x \in [m_1]_\sim \cap [m_2]_\sim$. Das bedeutet definitionsgemäß $x \sim m_1$ und $x \sim m_2$. Wegen der Symmetrie der Äquivalenzrelation bedeutet dies auch $m_1 \sim x$.
Wählt man nun ein $y \in [m_1]_\sim$, so gilt $y \sim m_1$ nach Definition. Da wir auch $m_1 \sim x$ haben, gilt aufgrund der Transitivität von $\sim$, dass $y \sim x$. Wegen $x \sim m_2$ gilt abermals aufgrund der Transitivität $y \sim m_2$. Das bedeutet $y \in [m_2]_\sim$, sodass wir $[m_1]_\sim \subseteq [m_2]_\sim$

gezeigt haben. Der Beweis der umgekehrten Inklusion funktioniert analog durch Tausch der Rollen von m_1 und m_2. q.e.d.

Beispiel. 1) Die Gleichheitsrelation $R = \{(m, m) \mid m \in M\} \subseteq M \times M$ ist eine Äquivalenzrelation.
2) Auf der Menge $\mathbb{R}$ ist $a \sim b :\Leftrightarrow |a| = |b|$ eine Äquivalenzrelation mit genau einer einelementigen und unendlich vielen zweielementigen Äquivalenzklassen.
3) Sei $M := \{G_{a,b} \mid a, b \in \mathbb{R}\}$ wobei $G_{a,b} := \{(x, ax + b) \mid x \in \mathbb{R}\}$ die Gerade durch $(0, b)$ mit Steigung a sei. Dann ist Parallelität von Geraden eine Äquivalenzrelation auf M, $G_{a,b} \sim G_{c,d}$ genau dann wenn $a = c$.

Bemerkung 2.3. *Seien M, N zwei Mengen und $f : M \to N$ eine Abbildung. Dann ist durch Bildgleichheit unter f eine Äquivalenzrelation $\sim_f$ auf M gegeben. Also:*
$a \sim_f b :\Leftrightarrow f(a) = f(b)$.
In der Tat lässt sich jede Äquivalenzrelation in der Form $\sim_f$ mit einem surjektiven f schreiben.

Beweis. Die Tatsache, dass $\sim_f$ eine Äquivalenzrelation ist, ist eine leichte Übungsaufgabe. Sei nun $\sim$ eine beliebige Äquivalenzrelation auf M. Definiere $M/\sim$ als die Menge aller Äquivalenzklassen von M und setze $f : M \to M/\sim,\ m \mapsto [m]_\sim$. Dann ist f sicherlich eine surjektive Abbildung und wir behaupten, dass $\sim = \sim_f$. Es seien dazu $m_1, m_2 \in M$. Ist nun einerseits $m_1 \sim m_2$, so ist $[m_1]_\sim = [m_2]_\sim$, was nach Definition von f gerade $f(m_1) = f(m_2)$ bedeutet. Ist andererseits $m_1 \sim_f m_2$, so gilt $[m_1]_\sim = f(m_1) = f(m_2) = [m_2]_\sim$, was bedeutet, dass $m_1 \sim m_2$. q.e.d.

Kapitel 6

Verknüpfungen und Ringe

1 Definitionen

Definition 1.1. *Eine Verknüpfung auf einer Menge M ist eine Abbildung $* : M \times M \to M$, wobei wir für $x, y \in M$ anstelle von $*(x, y)$ oftmals $x * y$ schreiben.*
Wir nennen $*$ assoziativ, falls $x * (y * z) = (x * y) * z$ für alle $x, y, z \in M$ gilt.
Wir nennen $*$ kommutativ, falls $x * y = y * x$ für alle $x, y \in M$ gilt.

Definition 1.2. *Sei M eine Menge und $*$ eine Verknüpfung darauf. Ein Element $e \in M$ mit der Eigenschaft $e * m = m * e = m$ für alle $m \in M$ nennen wir neutrales Element bezüglich $*$.*
Falls zu einem $m \in M$ ein $x \in M$ existiert mit $m * x = x * m = e$, so nennen wir m invertierbar bezüglich $*$ und x ein inverses Element zu m. Häufig bezeichnet man das zu m inverse Element mit m^{-1} oder $-m$.

Lemma 1.3. *Sei $*$ assoziativ. Neutrale und inverse Objekte bzgl. $*$ sind stets eindeutig bestimmt.*

Beweis. Seien e und e' zwei neutrale Elemente bezüglich $*$. Dann gilt $e = e * e' = e'$.
Sind n und n' zwei inverse Elemente zu einem Element m, so gilt
$n = n * e = n * (m * n') = (n * m) * n' = e * n' = n'$. q.e.d.

Lemma 1.4. *Es sei M eine Menge mit einer Verknüpfung, bezüglich welcher wir inverse Elemente mit $^{-1}$ bezeichnen, falls sie existieren. Dann ist $(m^{-1})^{-1} = m$ für alle invertierbaren $m \in M$.*

Dies lassen wir als Übungsaufgabe.

Bemerkung 1.5. *Betrachte $\mathbb{N} = \{1, 2, 3, ...\}$ mit der gewöhnlichen Addition natürlicher Zahlen als Verknüpfung. Dann gibt es kein neutrales Element bzgl. dieser Verknüpfung. Betrachtet man diese Verknüpfung jedoch auf der Menge $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$, so ist 0 das neutrale Element.*

Als Beispiel betrachten wir die Menge $\mathbb{Z}$ der ganzen Zahlen, die bereits aus der Schule bekannt ist. Auf $\mathbb{Z}$ haben wir die zwei Verknüpfungen

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z},\ (a, b) \mapsto a + b \text{ und } \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z},\ (a, b) \mapsto a \cdot b,$$

die beide assoziativ und kommutativ sind.
Das neutrale Element der Addition ist 0, denn bekanntlich gilt $0+z=z+0=z$ für jede ganze Zahl z. Zu jedem $z \in \mathbb{Z}$ existiert zudem ein inverses Element bezüglich $+$, nämlich $-z$.
Bezüglich der Multiplikation ist 1 das neutrale Element, denn $1 \cdot z = z \cdot 1 = z$ für alle $z \in \mathbb{Z}$. Bezüglich $\cdot$ sind 1 und -1 die einzigen invertierbaren Elemente.
Die zwei Verknüpfungen auf $\mathbb{Z}$ stehen bekanntlich durch das Distributivgesetz in Beziehung zu einander. Es gilt $x \cdot (y+z) = x \cdot y + x \cdot z$ für alle ganzen Zahlen x, y, z.
Diese Eigenschaften möchten wir nun zur Definition einer Klasse von abstrakten mathematischen Objekten heranziehen.

Definition 1.6. *Sei R eine nichtleere Menge, die zwei Verknüpfungen besitzt, die wir mit $+$ und $\cdot$ bezeichnen. Wir nennen dann $(R, +, \cdot)$ einen kommutativen Ring mit 1 (kurz Ring), falls gilt*

1. *(a) Die Verknüpfung $+$ ist assoziativ und kommutativ.*
   (b) Es existiert ein neutrales Element bezüglich $+$ in R, welches wir mit 0 (oder zur Verdeutlichung mit 0_R) bezeichnen.
   (c) Zu jedem $r \in R$ existiert ein inverses Element bezüglich $+$, welches wir mit $-r$ bezeichnen.
2. *(a) Die Verknüpfung $\cdot$ ist assoziativ und kommutativ.*
   (b) Es existiert ein neutrales Element bezüglich $\cdot$ in R, welches wir mit 1 (oder zur Verdeutlichung mit 1_R) bezeichnen.
3. *Die zwei Verknüpfungen sind distributiv im folgenden Sinne: für alle $x, y, z \in R$ gilt*

$$x \cdot (y+z) = x \cdot y + x \cdot z.$$

Die Verknüpfung $+$ nennen wir die Addition des Rings, $\cdot$ die Multiplikation des Rings.

Konvention Wir verwenden in Ringen die übliche Konvention "Punkt- vor Strichrechnung", d.h. wir lesen $x \cdot y + z$ stets als $(x \cdot y) + z$.
Wir lassen zudem oftmals das Symbol $\cdot$ aus; man lese also xy als $x \cdot y$.
Das Inverse eines multiplikativ invertierbaren $r \in R$ bezeichnen wir mit r^{-1} und wir setzen

$$R^* := \{r \in R \mid r \text{ invertierbar}\}$$

Bemerkung 1.7. *Die Definition des Rings besitzt verschiedene Abschwächungen. So werden beispielsweise auch Ringe betrachtet, in denen $\cdot$ nicht kommutativ ist, oder Ringe, welche kein neutrales Element 1 bezüglich der Multiplikation besitzen. Letztere werden als Ringe ohne Eins oder auch als "Rnge" bezeichnet.*
In diesem Kurs wird ein Ring jedoch stets kommutativ sein und eine Eins besitzen.

Beispiel Die Ringdefinition ist mit suggestiven Schreibweisen versehen, etwa 0 und 1, die an Ringe aus Zahlen erinneren, die uns vertraut sind. Um klarzustellen, dass diese Schreibweisen wirklich bloße Analogien sein sollen, betrachten wir zunächst ein Beispiel, das den meisten Teilnehmern des Kurses wahrscheinlich noch nicht bekannt ist.
Sei M eine Menge mit zwei Teilmengen T_1 und T_2. Dann definieren wir

$$T_1 \Delta T_2 := (T_1 \cup T_2) - (T_1 \cap T_2),$$

die so genannte symmetrische Differenz von T_1 und T_2.
Es ist nun $R := (\mathrm{Pot}(M), \Delta, \cap)$ ein kommutativer Ring mit 1 (es ist $1_R = M$ und $0_R = \emptyset$). Man verifiziere dies als Übungsaufgabe. Was sind die (bezüglich $\cdot$) invertierbaren Elemente des Rings?
Beispiel Bekanntere Beispiele für Ringe sind die aus der Schule bekannten $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$.

Lemma 1.8. *Aus den Ringaxiomen lassen sich für einen Ring R folgende Eigenschaften ableiten.*
a) $0 \cdot r = r \cdot 0 = 0$ *für alle* $r \in R$
b) $(-1) \cdot r = r \cdot (-1) = -r$ *für alle* $r \in R$
c) $(-a)(-b) = ab$ *für alle* $a, b \in R$.

Beweis. a) Es ist $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, woraus durch Addition des additiv inversen Elements von $0 \cdot a$ die Behauptung folgt.
b) $r + (-1)r = (1 + (-1))r = 0 \cdot r = 0$.
c) Es ist nach b) $(-a)(-b) = (-1)(-ab)$, woraus folgt

$$(-a)(-b) + (-ab) = (-1)(-ab) + (-ab) = ((-1) + 1) \cdot (-ab) = 0 \cdot (-ab) = 0.$$

Das heißt, dass $(-a)(-b)$ das inverse Element zu $-ab$ ist, und somit mit ab übereinstimmt. q.e.d.

2 Die Kongruenzrelation und Restklassenringe von $\mathbb{Z}$

Definition 2.1. *Sei $n \in \mathbb{Z}$. Wir nennen zwei ganze Zahlen $a, b \in \mathbb{Z}$ "kongruent modulo n", in Zeichen $a \equiv b \pmod{n}$, falls $n \mid (a - b)$, also falls die Differenz von a und b durch n teilbar ist.*
Eine alternative Schreibweise ist $a \equiv_n b$.

Satz 2.2. *Die Relation "kongruent modulo n" ist eine Äquivalenzrelation auf $\mathbb{Z}$.*

Beweis. Reflexivität: Sei $x \in \mathbb{Z}$. Dann ist $x - x = 0$ und 0 ist sicherlich durch n teilbar, sodass $x \equiv x \pmod{n}$.
Symmetrie: Seien $x, y \in Z$ mit $x \equiv y \pmod{n}$. Das heißt $n \mid x - y = -(y - x)$, und somit $n \mid y - x$. Es folgt $y \equiv x \pmod{n}$, die Relation ist also symmetrisch.
Transitivität: Es seien $x, y, z \in \mathbb{Z}$, $x \equiv y \pmod{n}$ und $y \equiv z \pmod{n}$. Es sind also $x - y$

und $y - z$ durch n teilbar, sodass wir schreiben können $x - y = n \cdot a$ und $y - z = n \cdot b$ mit $a, b \in \mathbb{Z}$. Dann ist jedoch

$$x - z = x - y + y - z = (x - y) + (y - z) = na + nb = n(a + b),$$

also $x \equiv z \pmod{n}$, womit die Transitivität der Relation gezeigt ist. q.e.d.

Bemerkung 2.3. *Wir erinnern kurz an die Division mit Rest. Sind a und $b \neq 0$ ganze Zahlen, so existeren eindeutig bestimmte ganze Zahlen $q, r \in Z$ mit der Eigenschaft $a = qb + r$ und $0 \leq r < b$.*
Es gilt $a \equiv b \pmod{n}$ genau dann, wenn a und b bei Division mit Rest durch n den gleichen Rest lassen.

Beweis. Es sei zunächst $a \equiv b \pmod{n}$. Nach Division mit Rest können wir a und b schreiben als $a = q_1 n + r_1$, $b = q_2 n + r_2$ mit $0 \leq r_i < n$.
Es gilt $a - b = n(q_1 - q_2) + r_1 - r_2$, und da n die Differenz $a - b$ teilt, teilt n auch $r_1 - r_2$. Ohne Einschränkung können wir annhemen, dass $r_1 - r_2 \geq 0$. Es ist $r_1 - r_2 < n - r_2 \leq n$ und somit $r_1 - r_2 = 0$.
Lassen umgekehrt a und b den gleichen Rest bei Division durch n, so können wir schreiben $a = q_1 n + r$, $b = q_2 n + r$, sodass $a - b = q_1 n + r - q_2 n - r = (q_1 - q_2)n$. In der Tat sind also a und b kongruent modulo n. q.e.d.

Beispiel 1) $1 \equiv -1 \pmod{2}$
2) $3 \equiv 15 \pmod{3}$
3) $6 \equiv -2 \pmod{8}$
4) $12 \equiv 19 \pmod{7}$
5) Für alle ganzen Zahlen x, y gilt $x \equiv y \pmod{1}$.

Als nächstes möchten wir feststellen, dass die Kongruenzrelation auf $\mathbb{Z}$ verträglich ist mit den Verknüpfungen $+$ und $\cdot$.

Lemma 2.4. *Seien $a, a', b, b', n \in \mathbb{Z}$ mit $a \equiv a' \pmod{n}$ und $b \equiv b' \pmod{n}$. Dann gelten*
1) $a + b \equiv a' + b' \pmod{n}$
2) $ab \equiv a'b' \pmod{n}$

Beweis. 1) $(a + b) - (a' - b') = (a - a') + (b - b')$. Da a zu a' und b zu b' modulo n kongruent sind, gibt es ganze Zahlen x, y mit $a - a' = nx$ und $b - b' = ny$. Damit haben wir also $(a + b) - (a' + b') = nx + ny = n(x + y)$ und dies ist durch n teilbar. Also sind $a + b$ und $a' + b'$ zu einander kongruent.
2) Dies beweist man analog mit Hilfe der Gleichung $ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b'$. q.e.d.

Satz 2.5. *Wir bezeichen mit $\mathbb{Z}/n\mathbb{Z}$ die Menge aller Äquivalenzklassen bezüglich $\equiv_n$, also $\mathbb{Z}/n\mathbb{Z} := \mathbb{Z}/\equiv_n$. Weitere Schreibweisen sind $\mathbb{Z}/(n)$ und $\mathbb{Z}/n$.* [1]

[1] Von der ebenfalls verbreiteten Schreibweise $\mathbb{Z}_n$ ist aus verschiedenen Gründen Abstand zu nehmen.

Die Menge $\mathbb{Z}/n\mathbb{Z}$ wird vermöge der folgenden Verknüpfungen zu einem Ring:

$$+ \ : \ \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \ ([a]_{\equiv_n}, [b]_{\equiv_n}) \mapsto [a+b]_{\equiv_n}$$

und

$$\cdot \ : \ \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \ ([a]_{\equiv_n}, [b]_{\equiv_n}) \mapsto [a \cdot b]_{\equiv_n}$$

Diesen Ring bezeichnen wir als Restklassenring von $\mathbb{Z}$ modulo n.

Beweis. Es ist lediglich zu zeigen, dass diese vertreterweise definierten Verknüpfungen (d.h. man bildet die Summe zweier Äquivalenzklassen, indem man die Klasse der Summe zweier Vertreter bildet) wohldefiniert sind, also nicht von der Wahl der Vertreter abhängen. Um zu illustrieren, warum dies wichtig ist, betrachten wir die Äquivalenzrelation auf $\mathbb{N}$ mit den folgenden Klassen: $[1] = \{1, 3\}$, $[2] = \{2, 4\}$, $[5] = \{5\}$ und der Klasse $\{6, 7, 8, ...\}$. Würden wir auf der Menge dieser Äquivalenzklassen eine Addition durch vertreterweise Addition in $\mathbb{N}$ definieren, erhielten wir $[3] = [1] + [2] = [3] + [2] = [5]$, aber $[5] \neq [3]$.
Die zu zeigende Aussage ist aber gerade die Aussage des vorangegangenen Lemmas. Die restlichen Ringeigenschaften folgen nun aus denen von $\mathbb{Z}$. q.e.d.

Konvention Es ist üblich, eine Restklasse $[x]$ im Ring $\mathbb{Z}/n\mathbb{Z}$ einfach mit x zu bezeichnen. Wir folgen dieser Konvention in diesem Text.
Es ist zudem üblich, in einem beliebigen Ring $2 := 1+1$, $3 := 1+1+1$ etc. zu definieren.
Beispiel Das Rechnen im Restklassenring $\mathbb{Z}/12\mathbb{Z}$ sollte Ihnen von der Uhrzeit her vertraut sein (je nach Belieben kann man dies auch als Rechnung in $\mathbb{Z}/24\mathbb{Z}$ auffassen). So ist etwa 12 Stunden nach 3 Uhr wieder 3 Uhr und 3 Stunden nach 11 Uhr 2 Uhr, was sich in den Gleichungen $3 + 12 \equiv 3 \pmod{12}$ und $11 + 3 \equiv 2 \pmod{12}$ widerspiegelt.
Beispiel Wir möchten untersuchen, ob wir für die Gleichung $43 = x^2 + 4y^2$ Lösungen mit $x, y \in \mathbb{Z}$ finden können. Nehmen wir an, dass dies zutrifft, d.h. wir haben ganze Zahlen x, y mit $43 = x^2 + 4y^2$. Da wir nun eine Gleichung in ganzen Zahlen haben, müssen die beiden Seiten dieser Gleichung jeweils in derselben Äquivalenzklasse modulo 4 liegen. Aus $43 = x^2 + 4y^2$ folgt also $[43]_4 = [x^2 + 4y^2]_4$. Es ist $43 \equiv 3 \pmod{4}$ und $4y^2 \equiv 0 \pmod{4}$ (als Vielfaches von 4), sodass sich diese Gleichung zu $[3] = [x^2] = [x]^2$ reduziert.
Man rechnet jedoch leicht nach, dass Quadrate ganzer Zahlen modulo 4 kongruent zu 0 oder 1 sind:
$0^2 = 0 \equiv 0 \pmod{4}$
$1^2 = 1 \equiv 1 \pmod{4}$
$2^2 = 4 \equiv 0 \pmod{4}$
$3^2 = 9 \equiv 1 \pmod{4}$.
Weitere Zahlen müssen wir nicht betrachten, da $\{0, 1, 2, 3\}$ ein vollständiges Vertretersystem der Äquivalenzklassen von $\mathbb{Z}/4\mathbb{Z}$ ist. Die obige Gleichung in $\mathbb{Z}/4\mathbb{Z}$ kann also keine Lösung besitzen. Dies bedeutet aber, dass unsere ursprüngliche Annahme falsch war, und keine Lösung der ersten Gleichung in ganzen Zahlen existieren kann.

3 Der (erweiterte) euklidische Algorithmus

Definition 3.1. *Es sei R ein Ring und $a, b \in R$ mit $(a, b) \neq (0, 0)$. Ein Element $d \in R$ heißt größter gemeinsamer Teiler von a und b, in Zeichen $\mathrm{ggT}(a, b)$, falls gilt $d \mid a$, $d \mid b$*

und für jedes $r \in R$ mit $r \mid a$ und $r \mid b$ gilt $r \mid d$. Für den Fall $(a,b) = (0,0)$ setzen wir $\mathrm{ggT}(0,0) = 0$.

Bemerkung 3.2. *Der* ggT *ist nur bis auf multiplikativ invertierbare Elemente eindeutig bestimmt. D.h. -1 ist genauso ein* ggT *von 4 und 5, wie 1 es ist. Schreibt man also* $1 = \mathrm{ggT}(4,5)$*, so ist diese Gleichung so zu lesen, dass 1* ***ein*** *größter gemeinsamer Teiler von 4 und 5 ist.*
Die Tatsache, dass gewisse Ringe die Auszeichnung eines eindeutigen größten gemeinsamen Teilers (z.B. in $\mathbb{Z}$ durch die Forderung, dass der ggT *positiv sein soll) zulassen, bleibt davon unberührt.*

Man zeige als Übungsaufgabe, dass in einem Ring R mit $0 \neq a \in R$ gilt: $a = \mathrm{ggT}(a,0)$.

Nun werden wir einen Algorithmus kennenlernen, der es uns ermöglicht, im Ring $\mathbb{Z}$ für $(a,b) \in (\mathbb{Z}\times\mathbb{Z}) - \{(0,0)\}$ den ggT von a und b sowie ganze Zahlen $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = xa + yb$ zu berechnen. Eine solche Darstellung des ggT nennt man eine Bézout-Identität[2]

Algorithmus 3.3. *(*Euklid**ischer Algorithmus**[3]*)*
Eingabe: $a, b \in \mathbb{Z}$.
Ausgabe: $\mathrm{ggT}(a,b)$ *sowie $x, y \in \mathbb{Z}$ mit $xa + yb = \mathrm{ggT}(a,b)$.*
Algorithmus: Falls $a = 0$ ist, so gib —b— aus, ist $b = 0$ so gib —a— aus. Sonst:
Setze $r_0 := |a|$, $x_0 := 1$, $y_1 := 0$,
$r_1 := |b|$, $x_1 := 0$, $y_1 := 1$.
Für $i \geq 1$ sei q_i definiert durch $r_{i-1} = q_i r_i + r$ mit $0 \leq r < |r_i|$ (Division mit Rest). Setze nun
$r_{i+1} := r = r_{i-1} - q_i r_i$,
$x_{i+1} := x_{i-1} - q_i x_i$,
$y_{i+1} := y_{i-1} - q_i y_i$.
Nach endlich vielen Schritten hat man das erste $n \in \mathbb{N}$ mit $r_{n+1} = 0$.
Dann ist $r_n = \mathrm{ggT}(|a|,|b|) = \mathrm{ggT}(a,b)$ *und* $r_n = \underbrace{x_n \cdot \mathrm{sgn}(a)}_{=:x} \cdot a + \underbrace{y_n \cdot \mathrm{sgn}(b)}_{=:y} \cdot b$.

Anstelle eines Beweises werden wir eine Reihe von Beispielen betrachten. Da der Algorithmus so wie er hier definiert wurde sehr technisch erscheint, führen wir ihn auf eine etwas klarere Weise durch.

Beispiel Wir möchten den ggT von 73 und 53 berechnen und ihn als $x \cdot 73 + y \cdot 53$ darstellen. Dazu führen wir zunächst sukzessive Divisionen mit Rest durch:

$$\begin{aligned}
\underline{73} &= 1 \cdot \underline{53} + 20 \\
\underline{53} &= 2 \cdot \underline{20} + 13 \\
\underline{20} &= 1 \cdot \underline{13} + 7 \\
\underline{13} &= 1 \cdot \underline{7} + 6 \\
\underline{7} &= 1 \cdot \underline{6} + \underline{1} \\
\underline{6} &= 6 \cdot \underline{1} + 0
\end{aligned}$$

[2] Étienne Bézout 1730 - 1783
[3] Euklid von Alexandria 3. Jahrhundert v. Chr.

Dabei ist die doppelt unterstrichene Zahl der ggT (da in der Zeile danach der Rest bei der Division 0 ist), die einfach unterstrichenen Zahlen benötigen wir, um die gesuchte Darstellung des ggT herzustellen. Dazu betrachten wir die Zeile, in welcher der ggT auftaucht, und stellen die Gleichung geeignet um:

$$\underline{7} = 1 \cdot \underline{6} + \underline{\underline{1}} \text{ wird zu } 1 = \underline{7} - \underline{6} \quad (\dagger)$$

Im nächsten Schritt ist die dritte Zeile von unten zu betrachten. Wir ersetzen nun nämlich den Divisionsrest aus dieser Zeile in (†):

$$\underline{13} = 1 \cdot \underline{7} + 6 \text{ wird zu } 6 = \underline{13} - \underline{7}.$$

In (†) eingesetzt:

$$1 = \underline{7} - \underline{6} = \underline{7} - (\underline{13} - \underline{7}) = 2 \cdot \underline{7} - \underline{13}.$$

Hier erkennen wir nun den Sinn des Unterstreichens: $2 \cdot \underline{7}$ sollte hier nämlich nicht zu 14 ausgerechnet werden, da die 7 wiederum im nächsten Schritt ersetzt werden muss.
Dieses Verfahren führen wir nun solange durch, bis wir eine Gleichung der Form $1 = x \cdot 73 + y \cdot 53$ erhalten haben. Hier ist die gesamte Rechnung:

$$\begin{aligned}
1 &= \underline{7} - \underline{6} \\
&= \underline{7} - (\underline{13} - \underline{7}) \\
&= 2 \cdot \underline{7} - \underline{13} \\
&= 2 \cdot (\underline{20} - \underline{13}) - \underline{13} \\
&= 2 \cdot \underline{20} - 3 \cdot \underline{13} \\
&= 2 \cdot \underline{20} - 3 \cdot (\underline{53} - 2 \cdot \underline{20}) \\
&= 8 \cdot \underline{20} - 3 \cdot \underline{53} \\
&= 8 \cdot (\underline{73} - \underline{53}) - 3 \cdot \underline{53} \\
&= 8 \cdot \underline{73} - 11 \cdot \underline{53}
\end{aligned}$$

Abschließend ist also $1 = \text{ggT}(73, 53) = 8 \cdot 73 - 11 \cdot 53$. Um die Verbindung zu der technischen Beschreibung des Algorithmus herzustellen, deuten wir kurz an, wo man die r_i und q_i in der hier vorgestellten Methode wiederfindet.

$$\begin{aligned}
\underbrace{\underline{73}}_{r_0} &= \underbrace{\underline{1}}_{q_1} \cdot \underline{53} + 20 \\
\underbrace{\underline{53}}_{r_1} &= \underbrace{\underline{2}}_{q_2} \cdot \underline{20} + 13 \\
\underbrace{\underline{20}}_{r_2} &= \underbrace{\underline{1}}_{q_3} \cdot \underline{13} + 7 \\
&\dots
\end{aligned}$$

Bemerkung 3.4. *Im obigen Beispiel ist es nicht von Belang, ob man mit $r_0 = 73$ oder $r_0 = 53$ beginnt (auch allgemein spielt diese Reihenfolge keine Rolle). Beginnt man mit der kleineren Zahl, so liefert dies lediglich den zusätzlichen Schritt $\underline{53} = 0 \cdot \underline{73} + 53$.*

Neben der offensichtlichen Anwendung des EUKLIDischen Algorithmus gibt es noch eine weitere sehr nützliche Anwendung, die wir nun kennenlernen werden.

Satz 3.5. *Die Menge der multiplikativ invertierbaren Elemente des Rings $\mathbb{Z}/n\mathbb{Z}$ ist*

$$\{[x] \in \mathbb{Z}/n\mathbb{Z} \mid \text{ggT}(x,n) = 1\}.$$

Beweis. Es ist hier die Gleichheit der zwei Mengen $\{[x] \in \mathbb{Z}/n\mathbb{Z} \mid [x] \text{ invertierbar}\}$ und $\{[x] \in \mathbb{Z}/n\mathbb{Z} \mid \text{ggT}(x,n) = 1\}$ zu zeigen. Dazu zeigen wir die beidseitige Teilmengenbeziehung. Wir verwenden die vereinbarte Kurzschreibweise $[x] = x$.
"$\subseteq$": Sei x invertierbar. Dann gibt es ein $y \in \mathbb{Z}/n\mathbb{Z}$ mit $1 = xy$. Schreibt man dies mit der Definition der Kongruenzrelation aus, erhält man die folgende Gleichung ganzer Zahlen: $1 = xy + nt$ für ein geeignetes $t \in \mathbb{Z}$. Nun behaupten wir, dass $1 = \text{ggT}(x,n)$. Sicherlich ist 1 ein gemeinsamer Teiler von x und n. Sei nun d ein weiterer gemeinsamer Teiler von x und n. Dann teilt dieser auch $xy + tn = 1$, womit die Behauptung gezeigt ist.
"$\supseteq$": Sei $\text{ggT}(x,n) = 1$. Dann finden wir $a, b \in \mathbb{Z}$ mit $1 = xa + nb$, woraus sofort folgt, dass xy modulo n kongruent zu 1 ist, was gerade Invertierbarkeit von x im Ring $\mathbb{Z}/n\mathbb{Z}$ bedeutet. q.e.d.