Mathematische Grundlagen

Vorlesung WS 2013/14

Gabriele Nebe

RWTH Aachen

Prof. Dr. Gabriele Nebe
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64

Inhaltsverzeichnis

1 Aussagen, Mengen, Abbildungen **5**

1 Aussagenlogik. (1. Vorlesung) . . . 5
1.1 Aussagen und ihre Verknüpfungen. . . . 5
1.2 Implikation und Äquivalenz . . . 7
2 Mengen. . . . 9
2.1 Notation . . . 9
2.2 Mengenoperationen (2. Vorlesung) . . . 10
2.3 Quantoren und Mengenfamilien. . . . 14
3 Abbildungen. (3. Vorlesung) . . . 15
3.1 Definition und erste Beispiele . . . 15
3.2 Abzählen. (4. Vorlesung) . . . 18
3.3 Komposition von Abbildungen. . . . 23
4 Partitionen und Äquivalenzrelationen. (6. Vorlesung) . . . 28
5 Vollständige Induktion und Rekursion (7. Vorlesung) . . . 33
5.1 Axiome und Prinzipien . . . 33
5.2 Anordnung der natürlichen Zahlen . . . 37
5.3 Das allgemeine Assoziativgesetz . . . 40
5.4 Produkt und Potenzen natürlicher Zahlen . . . 42
5.5 Wichtige Folgen natürlicher Zahlen (10.Vorlesung) . . . 43

2 Reelle und komplexe Zahlen **47**

6 Axiome für Gruppen, Ringe und Körper . . . 47
6.1 Gruppen 11. Vorlesung am 19.11.2013 . . . 47
6.2 Ringe 11. Vorlesung am 19.11.2013 . . . 50
6.3 Körper 12. Vorlesung am 20.11.2013 . . . 53
7 Axiome für den reellen Zahlkörper . . . 53
7.1 Angeordnete Körper 12. Vorlesung am 20.11.2013 . . . 54
7.2 Der reelle Zahlkörper 12. Vorlesung am 20.11.2013 . . . 55
7.3 Absolutbetrag und Abstand, 13. Vorlesung 26.11.2013 . . . 56
7.4 Quadratische Gleichungen, 13. Vorlesung 26.11.2013 . . . 58
8 Der komplexe Zahlkörper . . . 59
8.1 Konstruktion aus dem reellen Zahlkörper, 13. Vorlesung 26.11.2013 59
8.2 Die Gausssche Zahlenebene . . . 61
8.3 Euklidische Geometrie, 16. Vorlesung am 4.12. . . . 65

3 Körper und Ringe konstruktiv **71**
9 Ringe, 17. Vorlesung am 10.12. 71
9.1 Die ganzen Zahlen 71
9.2 Der EUKLIDische Algorithmus für ganze Zahlen 73
9.3 Restklassenkörper von $\mathbb{Z}$, 18.Vorlesung am 11.12. 76
9.4 Der Polynomring über einem Körper, 19.Vorlesung am 17.12. 78
9.5 Der EUKLIDische Algorithmus für Polynomringe über Körpern . . . 80
9.6 Der Polynomring als Halbgruppenring. 83
10 Quotientenkörper, 20. Vorlesung am 7.1.14 85
10.1 Konstruktion der rationalen aus den ganzen Zahlen 85
10.2 Konstruktion der rationalen Funktionen aus den Polynomen 87
11 Der Körper der reellen Zahlen. Am 21. und 28.1., 22. und 23. Vorlesung . . 89
11.1 Der Ring der rationalen CAUCHY-Folgen. 89
11.2 Definition der reellen Zahlen 91
11.3 Anordnung, Abstand, Betrag. 92
11.4 Rationale Zahlen als reelle Zahlen. 93
11.5 Ordnungsvollständigkeit des reellen Zahlkörpers. 94
12 Kettenbrüche, letzte Vorlesung am 3.2. 96
12.1 Kettenbrüche und gute Approximationen 96
12.2 Periodische Kettenbrüche und quadratische Gleichungen. 99
12.3 Die Kettenbruchentwicklung der Eulerschen Zahl. 100

4 Ergänzungen und Wiederholung **103**
13 Gleichungssysteme, Einschub am 14.1.2014, 21. Vorl. 103
13.1 Fasern einer Abbildung 103
13.2 Die Substitutionsmethode 104
13.3 Lineare-affine Geometrie 106

Kapitel 1

Aussagen, Mengen, Abbildungen

1 Aussagenlogik. (1. Vorlesung)

Lernziele: Symbole und Kalkül der Aussagenlogik, Wahrheitstafeln,

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

1.1 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.

1.2 Implikation und Äquivalenz

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

Definition 1.4. *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*

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

$(A \Rightarrow B) \wedge (B \Rightarrow A)$.

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 1.5. *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.

2 Mengen.

Lernziel: Einfache Notation, Konstruktionen und Identitäten der Mengenlehre: Teilmengen, Potenzmenge, Vereinigung und Durchschnitt, kartesische Produkte, Vergleich mit Aussagenlogik, Umgang mit Quantoren

2.1 Notation

In diesem Abschnitt möchte ich Ihnen nicht erklären, was eine Menge ist, sondern eher, wie man Mengen konstruieren, manipulieren und benutzen kann. Eine Menge ist eine Ansammlung von Objekten, den sogenannten **Element**en 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.) $A := \{3, 5, 7, 11, 13, 17\}$, die Menge der Primzahlen zwischen 3 und 17. Es gibt verschiedene Beschreibungen für dieselbe Menge:
Aufzählende Form: $A_1 = \{3, 5, 7, 11, 13, 17\}$
oder auch $A_2 = \{11, 13, 17, 5, 3, 5, 7\}$.
(In einer Menge kommt es nicht auf die Reihenfolge der Elemente an und es kommt kein Element mehrfach vor.)
Beschreibende Form:

$$A_3 = \{n \in \mathbb{N} \mid 3 \leq n \leq 17 \text{ und } n \text{ ist Primzahl } \}.$$

Definition 2.1. *(Notation 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 sagen wir $a \notin M$.*

2.) *Zwei Mengen M und N sind* **gleich**, *kurz $M = N$, genau dann wenn sie dieselben Elemente enthalten, also $a \in M$ genau dann wenn $a \in N$.*

3.) *Die Menge, die keine Elemente enthält, heißt die* **leere Menge** $\emptyset$ *oder auch* $\{\}$.

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:*
$(N \subseteq M) :\Leftrightarrow (a \in N \Rightarrow a \in M)$

5.) Für eine Menge M heißt

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

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

Beispiel 1.) $\emptyset \subseteq M$ für jede Menge M.
2.) Eine beschreibende Form für die leere Menge ist z.B. $E = \{n \in \mathbb{N} \mid n < 0\}$.
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:

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

Übung: Zeigen Sie unter Benutzung von Definition 2.1 2.) dass die drei Beschreibungen in Beispiel oben die gleiche Menge beschreiben, also $A_1 = A_2 = A_3$ gilt. (Beachte: Um die Gleichheit zweier Mengen, sagen wir A, B zu zeigen, müssen wir die Äquivalenz $x \in A \Leftrightarrow x \in B$ zeigen, also zwei Implikationen.)

Beispiel. **Russellsche Antinomie** (B. Russel[2], E. Zermelo[3])
Sei M eine Menge.

$$N_M := \{a \in M \mid a \notin a\}$$

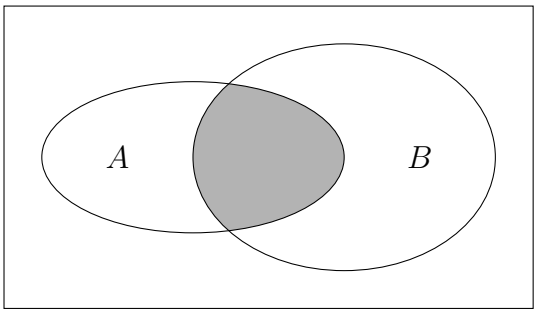
ist dann auch eine Menge.
Behauptung: $N_M \notin M$.
Beweis: Angenommen $N_M \in M$. Es gibt nun zwei Möglichkeiten:
1.) $N_M \in N_M$, so folgt aus der Definition von N_M (von links nach rechts gelesen), dass $N_M \notin N_M$, Widerspruch.
2.) $N_M \notin N_M$, so folgt aus der Beschreibung von N_M (von rechts nach links gelesen), dass $N_M \in N_M$ sein muss. Ein Widerspruch.
Also ist die Behauptung bewiesen.
Insbesondere bildet die Gesamtheit G aller Mengen keine Menge, ansonsten wäre auch N_G eine Menge und damit $N_G \in G$ (im Widerspruch zur oben bewiesenen Behauptung).

2.2 Mengenoperationen (2. Vorlesung)

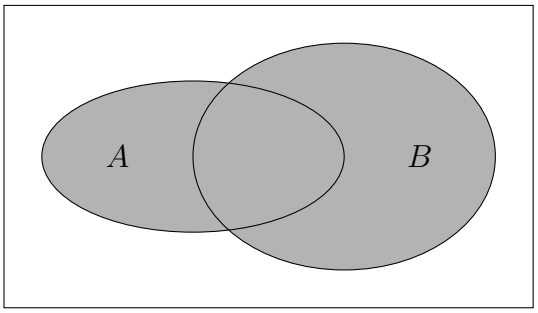
Wir wollen in Analogie zu den drei Verknüpfungen von Aussagen die Entsprechungen für Mengen einführen. Manchmal sind die Akzente hier etwas anders, aber eigentlich läßt sich alles übertragen. Wir präsentieren die Definitionen zusammen mit den zugehörigen Venn[4]-Diagrammen, die ein sich selbst erklärender Appell an die Anschauung sind.

Definition 2.2. *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.*

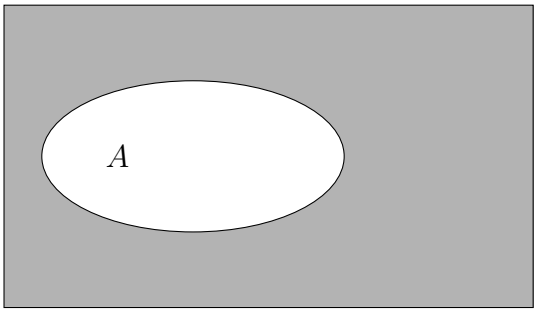
[2] Bertrand Arthur William Russell 1872 - 1970
[3] Ernst Friedrich Ferdinand Zermelo 1871 - 1953
[4] John Venn 1834 - 1923



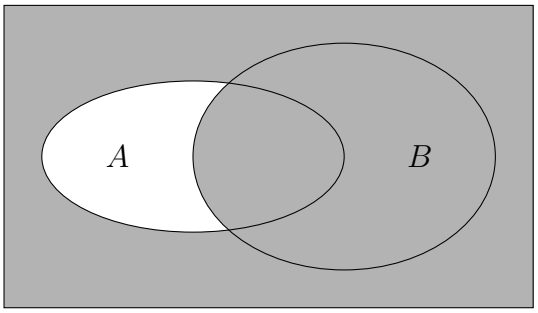
2) $A \cup B := \{m \in M \mid m \in A \text{ oder } m \in B\}$ *heißt die* **Vereinigung** *der Mengen* A *und* B*.*



3.) $\overline{A} := M \setminus A := \{m \in M \mid m \notin A\}$ *heißt das* **Komplement** *von* A *in* M*.*



4) $A \setminus B := \{m \in M \mid m \in A \text{ und } m \notin B\} = A \cap \overline{B}$ *heißt die* **Differenzmenge** A *ohne* B*.*



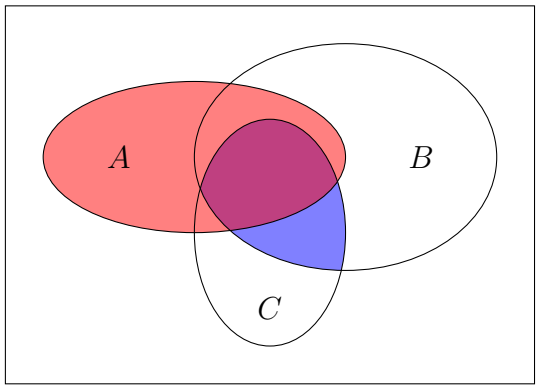
Wir haben also durch $\cap, \cup, {}^{-}$ Verknüfungen auf $\mathrm{Pot}(M)$. Diese gehorchen Gesetzen, die in genauer Analogie zu den Eigenschaften von $\wedge, \vee, \neg$ stehen, die wir in Satz 1.2 kennengelernt hatten.

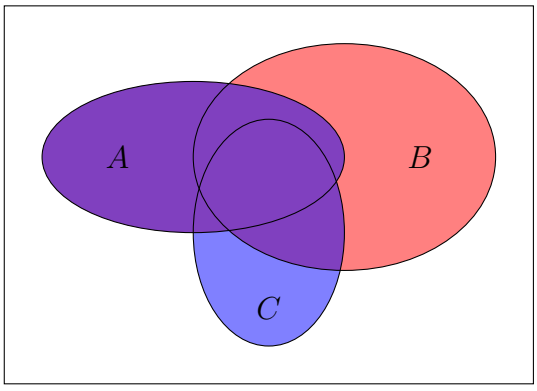
Satz 2.3. *Seien $A, B, C \subseteq M$. Dann gilt:*
1.) $\overline{\overline{A}} = A$.
2.) **Kommutativität des Durchschnittes***:*
$A \cap B = B \cap A$.
3.) **Kommutativität der Vereinigung***:*
$A \cup B = B \cup A$.
4.) **Assoziativität des Durchschittes***:*
$A \cap (B \cap C) = (A \cap B) \cap C$.
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 Satz 1.2. Wir wollen exemplarisch 6.) beweisen und gleichzeitig das zugehörige VENN-Diagramm als Erinnerungsstütze, Kurznotation für den Beweis angeben.

$$
\begin{gathered}
x \in A \cup (B \cap C) \Leftrightarrow \\
x \in A \vee x \in (B \cap C) \Leftrightarrow \\
x \in A \vee (x \in B \wedge x \in C) \Leftrightarrow \\
(x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \Leftrightarrow \\
(x \in A \cup B) \wedge (x \in A \cup C) \Leftrightarrow \\
x \in (A \cup B) \cap (A \cup C))
\end{gathered}
$$

VENN-Diagramme:





q.e.d.

Übung: Man beweise die übrigen Aussagen des letzten Satzes und male die zugehörigen VENN-Diagramme. Diese Übung sollten Sie als sehr einfach empfinden.

Analog zu Satz 1.3 gilt natürlich der folgende Satz, dessen Beweis wir auch als Übungsaufgabe lassen:

Satz 2.4. *Seien $A, B \subseteq M$. Dann gilt:*
1.) $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
2.) $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Man könnte jetzt in völliger Analogie zur Aussagenlogik weitermachen. Aber das Analogon der Implikation bei Mengen ist nicht so wichtig; hingegen spielt die **symmetrische Differenz**, also das Analogon zum ausschließenden Oder, eine wichtigere Rolle, wie Sie in der Übung sehen werden.

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 machten. Rein formal kommt hier eine Teilmenge der Potenzmenge heraus, aber die Idee her wird eine neue Menge konstruiert.

Definition 2.5. *(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**[5] *der Mengen M und N oder auch die Paarmenge.*

Bemerkung 2.6. *(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.) $M \times \emptyset = \emptyset$.

[5] René Descartes 1596 - 1650

2.3 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 2.7. *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 2.8. *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 2.9. *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 2.10. *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. 1.) an der Tafel vorgemacht q.e.d.

3 Abbildungen. (3. Vorlesung)

3.1 Definition und erste Beispiele

Lernziele: Definition von Abbildung, Defintionsbereich, Wertebereich, Bild, bijektive Abbildungen
Motivierendes Beispiel: Der Graph von $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$.

Definition 3.1. *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 $M \times N$ mit folgender Bedingung:*
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 $(m, n) \in f$.[6] *Statt „$f \subseteq M \times N$ Abbildung“ schreibt man:*

$$f : M \to N$$

oder ausführlicher:

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

2) Ist $f : M \to N$ eine Abbildung, so heißt M der **Definitionsbereich** *von f, N der* **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.
Beispiel. Sei $M := N := \mathbb{R}$. Dann ist der Kreis

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

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

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 diesen Übelstand auch 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 $k_2([-1, 1]) = [-1, 0]$.
Noch ein Beispiel für Funktionen und nicht-Funktionen von $\underline{3}$ nach $\underline{4}$. Wenn man ein neues

Konzept einführt, schaut man zunächst, ob alte Konzepte damit in Beziehung stehen. Wir gehen unsere bisherigen Betrachtungen durch.
Beispiel. 1.) Sei $\mathcal{A}$ eine Menge von Aussagen. Die Zuweisung der Wahrheitswerte ist eine Abbildung:

$$W : \mathcal{A} \to \{w, f\} : A \mapsto W(A).$$

2.) 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.

Das nächste Konzept, welches wir in der Sprache der Abbildungen umformulieren wollen, ist das der Teilmenge.

Bemerkung 3.2. *Sei M eine Menge.*
1) Jede Teilmenge $T \subseteq M$ von M legt eine Abbildung $\chi_T : M \to \{0, 1\}$ fest durch die Vorschrift: $\chi_T(m) = 1$ genau dann, wenn $m \in T$. χ_T heißt die **charakteristische Funktion** *von T. Sie ist gegeben durch*

$$\chi_T : M \to \{0, 1\} : m \mapsto \begin{cases} 1, & m \in T \\ 0, & m \notin T \end{cases}$$

2) Jede Abbildung $\alpha : M \to \{0, 1\}$ legt eine Teilmenge T von M fest, nämlich $T := \{m \in M \mid \alpha(m) = 1\}$, sodass $\alpha = \chi_T$.

Beweis. Es ist nur zu zeigen, dass $\alpha = \chi_T$ ist in 2). Zwei Abbildungen f und g sind gleich, genau dann wenn sie den gleichen Definitionsbereich M und Wertebereich haben und wenn für alle $m \in M$ die Funktionswerte $f(m) = g(m)$ gleich sind. Der Definitionsbereich von α und von χ_T ist jedesmal M, der Wertebereich ist $\{0, 1\}$. Es gilt für $m \in M$, dass $\alpha(m) = 1$ genau dann wenn $m \in T$ also genau dann wenn $\chi_T(m) = 1$ ist. Ansonsten ist $\alpha(m) = \chi_T(m) = 0$. Also stimmen die beiden Abbildungen überein. q.e.d.

Die Konstruktion im zweiten Teil der Bemerkung ist von allgemeiner Bedeutung. Wir unterstreichen dies durch eine Definition:

Definition 3.3. *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) Sei $T \subseteq M$ und $\chi_T : M \to \{0, 1\}$ die charakteristische Funktion von T. Dann ist $\chi_T^{-1}(\{1\}) = T$, $\chi_T^{-1}(\{0\}) = M \setminus T$.
2) Faser von $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, (x, y) \mapsto x$.
3) Fasern von $g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, (x, y) \mapsto y$ sind Funktionen.

Wir besprechen einen besonders wichtigen Fall von Abbildungen, wo alle Fasern einelementig sind.

Satz 3.4. *Sei $f : M \to N$ eine Abbildung. Dann sind folgende Aussagen äquivalent:*
1) $f^{-1} := \{(n, m) \in N \times M \mid (m, n) \in f\}$ ist eine Abbildung von N nach M, also

$$f^{-1} : N \to M.$$

2) Für jedes $n \in N$ besteht die Faser $f^{-1}(\{n\})$ von f über n aus genau einem Element von M.
Ist eine und damit auch die andere dieser Bedingungen erfüllt, so heißt f **bijektiv** *oder eine* **Bijektion** *und $f^{-1} : N \to M$ die zu f* **inverse Abbildung** *oder auch* **Umkehrfunktion** *(die dann auch bijektiv ist).*

Beweis. 1) $\Rightarrow$ 2) Wir nehmen an, dass das oben definierte $f^{-1} \subseteq N \times M$ eine Abbildung von N nach M ist. Sei $n \in N$. Man verifiziert für die Faser $f^{-1}(\{n\})$ von f über n:

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

(Man beachte die unterschiedlichen Bedeutungen von f^{-1}, einmal gemäß Definition 3.3 und einmal gemäß der Definition aus Satz 3.4 1.) Die Gleichheit dieser beiden Mengen zeigt man dadurch, dass man verifiziert, dass jede der beiden Mengen in der anderen enthalten ist:
Sei also $m \in f^{-1}(\{n\})$, d.h. $(m, n) \in f$. Dann ist $(n, m) \in f^{-1}$ nach Definition von f^{-1} und somit $m = f^{-1}(n) \in \{f^{-1}(n)\}$. Somit gilt $f^{-1}(\{n\}) \subseteq \{f^{-1}(n)\}$.
Für die umgekehrte Richtung genügt es, das einzige Element $m := f^{-1}(n)$ zu betrachten. Dann ist $(n, m) \in f^{-1}$, also $(m, n) \in f$ und somit $f(m) = n$, also $m \in f^{-1}(\{n\})$. Daher auch $\{f^{-1}(n)\} \subseteq f^{-1}(\{n\})$ und die beiden Mengen sind gleich.
2) $\Rightarrow$ 1) Wir müssen zeigen, dass $f^{-1} := \{(n, m) \in N \times M \mid (m, n) \in f\}$ eine Abbildung von N nach M ist, also, dass für jedes $n \in N$ genau ein $m \in M$ existiert mit $(n, m) \in f^{-1}$. Sei also $n \in N$. Dann besteht wegen 2) die Faser $f^{-1}(\{n\})$ aus genau einem Element, dieses werde mit m bezeichnet. Dann ist $m \in M$ und $(m, n) \in f$. Somit nach Definition $(n, m) \in f^{-1}$. Weiter ist m eindeutig, denn seien $m, m' \in M$ mit $(n, m) \in f^{-1}$ und $(n, m') \in f^{-1}$. Dann gilt $(m, n) \in f$ und $(m', n) \in f$, also $m \in f^{-1}(\{n\})$ und $m' \in f^{-1}(\{n\})$. Da diese Faser aber genau ein Element enthält folgt damit $m = m'$. q.e.d.

Wie wird man also vorgehen, wenn man zeigen will, dass eine Abbildung $f : M \to N$ bijektiv ist? Typischerweise wird man eine Abbildung $g : N \to M$ suchen, die ein Kanditat für die Umkehrabbildung ist. Alsdann wird man zeigen: Für alle $m \in M$ und alle $n \in N$ gilt:

$$f(m) = n \Leftrightarrow g(n) = m.$$

Damit ist dann gezeigt, dass f bijektiv ist und $g = f^{-1}$ die Umkehrfunktion ist.
Beispiel. Eine Teilmenge $f \subseteq \mathbb{R} \times \mathbb{R}$ ist genau dann eine Funktion, wenn jede Parallele ($= \{a\} \times \mathbb{R}$ für $a \in \mathbb{R}$) zur y-Achse ($= \{0\} \times \mathbb{R}$) den Graphen, also f, genau einmal schneidet. Sie ist bijektiv genau dann, wenn zusätzlich jede Parallele ($= \mathbb{R} \times \{a\}$ für $a \in \mathbb{R}$) zur x-Achse ($= \mathbb{R} \times \{0\}$) den Graphen auch genau einmal schneidet. Dann erhält man die Umkehrfunktion durch Vertauschen der Rollen von x- und y-Achse.
Beispiel. Sei S eine Menge. Die Diagonale

$$\Delta(S) := \{(s, s) \mid s \in S\} \subseteq S \times S$$

ist eine Abbildung von S in sich. Diese Abbildung wird die **Identität**sabbildung von S genannt und mit id_S bezeichnet, also

$$\mathrm{id}_S : S \to S : s \mapsto s.$$

Zum Beweis der Bijektivität überzeugt man sich davon, dass id_S gleich ihrer Umkehrfunktion ist.

Definition 3.5. *Für Mengen M, N wird die Menge aller Abbildungen von M nach N mit N^M bezeichnet. (Also $f : M \to N$ bedeutet dasselbe wie $f \in N^M$.)*

$$N^M := \{f \mid f : M \to N\}.$$

Bemerkung 3.6. *Sei M eine Menge. Dann ist*

$$\chi : \mathrm{Pot}(M) \to \{0, 1\}^M : T \mapsto \chi_T$$

eine Bijektion mit inverser Bijektion

$$\{0, 1\}^M \to \mathrm{Pot}(M) : \alpha \mapsto \alpha^{-1}(\{1\}).$$

Beweis. An der Tafel. Bezug zur Bemerkung (3.2). q.e.d.

3.2 Abzählen. (4. Vorlesung)

Beispiele für Mengen $\mathbb{N} := \{1, 2, 3, \ldots\}$, die **Menge der natürlichen Zahlen**
$\mathbb{N}_0 := \mathbb{Z}_{\geq 0} := \{0, 1, 2, 3, \ldots\}$, Menge der natürliche Zahlen mit Null.
$\mathbb{Z} = \{\ldots - 3, -2, -1, 0, 1, , 2, , 3, \ldots\}$, die **Menge der ganzen Zahlen**.
$\mathbb{R}$, die **Menge aller reellen Zahlen**, deren Charakterisierung Sie in der Analysis I kennenlernen.
$\mathbb{Q} = \{\frac{a}{b} \in \mathbb{R} \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$, die **Menge der rationalen Zahlen**.

Für $n \in \mathbb{N}_0$ bezeichne $\underline{n} := \{1, 2, 3, \ldots, n\} = \{a \in \mathbb{N} \mid a \leq n\}$.
Es ist $\underline{0} = \emptyset$.

Wiederholung: Bijektive Abbildungen. Eine Teilmenge $f \subseteq M \times N$ heißt Funktion, falls für alle $m \in M$ genau ein $n \in N$ existiert mit $(m, n) \in f$. Schreiben: $n = f(m)$.
Eine Abbildung $f : M \to N$ heißt bijektiv (oder eine Bijektion), falls für alle $n \in N$ genau ein $m \in M$ existiert, mit $f(m) = n$ (die Faser von jedem Element im Wertebereich also genau ein Element hat). Dann ist $f^{-1} : N \to M$, $f(m) \mapsto m$ eine Funktion, die sogenannte Umkehrfunktion.
Klar: Ist $f : M \to N$ eine Bijektion, so auch $f^{-1} : N \to M$.
Zwei Mengen, zwischen denen eine bijektive Abbildung existiert, wird man anschaulich gesprochen als gleich groß ansehen.

Definition 3.7. *Eine Menge M heißt* **endlich**, *falls eine Zahl $n \in \mathbb{Z}_{\geq 0}$ und eine Bijektion $\zeta : \underline{n} \to M$ existieren. Man schreibt $|M| = n$ und sagt M hat n Elemente. ζ heißt eine* **Abzählfunktion** *für M. Existiert keine Abzählfunktion, so heißt M* **unendlich**.
Eine Menge M heißt **abzählbar**, *falls M endlich ist oder eine Bijektion $\zeta : \mathbb{N} \to M$ existiert. Anderenfalls heißt M* **überabzählbar**.

Vormachen: Zeige, dass eine Menge M nicht gleichzeitig 2 und n Elemente haben kann mit $n > 2, n \in \mathbb{N}$.

Satz 3.8. *Sei M eine Menge von endlichen Mengen. Dann ist*

$$M \to \mathbb{Z}_{\geq 0} : X \mapsto |X|$$

eine wohldefinierte Abbildung. Insbesondere gilt $|\underline{n}| = n$ für alle $n \in \mathbb{Z}_{\geq 0}$.

Beweis. Später. q.e.d.

Folgerung 3.9. *Seien M, N endliche Mengen. Dann gilt:*
1.) Sind M, N **disjunkt**, *d. h. $M \cap N = \emptyset$, dann gilt*

$$|M \cup N| = |M| + |N|.$$

2.) Allgemein gilt

$$|M \cup N| = |M| + |N| - |M \cap N|,$$

was man auch oft schreibt als

$$|M \cup N| + |M \cap N| = |M| + |N|.$$

3.)

$$|M \times N| = |M| \cdot |N|.$$

Beweis. 1.) Bei Vereinigungen von paarweie disjunkten Mengen benutzen wir das Symbol $\uplus$ statt $\cup$. Wir wollen also zeigen $|M \uplus N| = |M| + |N|$. Zu diesem Zweck seien $\alpha : \underline{|M|} \to M$ und $\beta : \underline{|N|} \to N$ Bijektionen. Dann ist

$$\gamma : \underline{|M| + |N|} \to M \uplus N : i \mapsto \begin{cases} \alpha(i) & i \in \underline{|M|} \\ \beta(i - |M|) & i \notin \underline{|M|} \end{cases}$$

auch eine Bijektion (Nachweis Übung), was die Behauptung zeigt. (Frage: Wo und wie ist Satz 3.8 eingegangen?)
2.) Wir haben:

$$\begin{aligned} M &= (M - N) \uplus (M \cap N) \\ N &= (N - M) \uplus (M \cap N) \\ M \cup N &= (M - N) \uplus (M \cap N) \uplus (N - M) \end{aligned}$$

und bekommen nach 1.):

$$\begin{aligned} |M| &= |M - N| + |M \cap N| \\ |N| &= |N - M| + |M \cap N| \\ |M \cup N| &= |M - N| + |M \cap N| + |N - M|. \end{aligned}$$

Zieht man die Summe der ersten beiden Gleichungen von der dritten ab, so steht die Behauptung da.
3.) Wir lassen es als Übungsaufgabe, eine entsprechende Bijektion anzugeben. q.e.d.

Hier sind zwei Beispiele für zwei abzählbar unendliche Mengen.

Satz 3.10. *$\mathbb{Z}$ und $\mathbb{N} \times \mathbb{N}$ sind abzählbar unendlich.*

Beweis. Dass beide Mengen unendlich sind, ist klar. Wir zeigen nur, dass sie abzählbar sind.
Definiere $\zeta : \mathbb{N} \to \mathbb{Z}$ durch

$$\zeta(n) = \begin{cases} n/2 & \text{falls } n \text{ gerade} \\ -(n-1)/2 & \text{falls } n \text{ ungerade.} \end{cases}$$

Dann ist ζ eine Bijektion. Die Umkehrabbildung ist gegeben durch

$$\eta : \mathbb{Z} \to \mathbb{N} : z \mapsto \begin{cases} -2z + 1 & \text{falls } z \leq 0 \\ 2z & \text{falls } z > 0. \end{cases}$$

Da beides offenbar Abbildungen sind, muss also nur noch für alle $n \in \mathbb{N}$ und alle $z \in \mathbb{Z}$ die Äquivalenz

$$n = \eta(z) \Leftrightarrow z = \zeta(n)$$

gezeigt werden, was wir als Übung lassen.
Für $\mathbb{N} \times \mathbb{N}$ ist dies schon etwas trickreicher und beruht auf dem ersten **Cantorschen Diagonalverfahren.** Man stellt sich $\mathbb{N} \times \mathbb{N}$ als nach rechts und unten unendliches Rechteck vor. Für jedes $n \in \mathbb{N}$ haben wir dann eine "Diagonale"

$$D(n) := \{(a, b) \in \mathbb{N} \times \mathbb{N} | a + b - 1 = n\} = \{(1, n), (2, n-1), \ldots, (n, 1)\},$$

die aus genau n Elementen besteht. Dann liegt $(a,b) \in \mathbb{N} \times \mathbb{N}$ auf der Diagonalen $D(a+b-1)$ an der a-ten Stelle, sodass sich für (a,b) in der Abzählung die Nummer

$$(\sum_{n=1}^{a+b-2} n) + a = (a+b-1)(a+b-2)/2 + a$$

anbietet. Die Abbildung

$$\alpha : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (a,b) \mapsto (a+b-1)(a+b-2)/2 + a$$

ist die Umkehrabbildung der gewünschten Bijektion. q.e.d.

Übung: Zeige, dass α eine Bijektion ist, d. h. dass für jedes $n \in \mathbb{N}$ genau ein $(a,b) \in \mathbb{N} \times \mathbb{N}$ existiert mit $\alpha((a,b)) = n$. (Hinweis: Satz 3.8 kann natürlich benutzt werden.)

Definition 3.11. *Sei $f : M \to N$ eine Abbildung und $\emptyset \neq T \subseteq M$ eine Teilmenge von M. Dann heißt die Abbildung*

$$f_{|T} : T \to N : t \mapsto f(t)$$

die **Einschränkung** *von f auf T.*

Übung: Zeige, dass in dieser Situation die Einschränkung

$$\epsilon_T : N^M \to N^T : f \mapsto f_{|T}$$

eine Abbildung ist. Vergleiche die Fasern dieser Einschränkung mit N^{M-T}.

Hier nun die Evidenz für $|N^M| = |N|^{|M|}$ bei endlichen Mengen M, N.

Satz 3.12. *Seien M, N beliebige Mengen und $M = S \uplus T$ mit nicht leeren Teilmengen $S, T \subseteq M$ von M. Dann ist*

$$\alpha : N^{S \uplus T} \to N^S \times N^T : f \mapsto (f_{|S}, f_{|T})$$

eine bijektive Abbildung.

Beweis. Hier ist die Umkehrabbildung:

$$\zeta : N^S \times N^T \to N^{S \uplus T} : (g,h) \mapsto \zeta(g,h)$$

mit

$$\zeta((g,h)) : S \uplus T \to N : x \mapsto \begin{cases} g(x) & \text{falls } x \in S \\ h(x) & \text{falls } x \in T. \end{cases}$$

(Eigentlich müsste man $\zeta((g,h))$ schreiben, was aber unüblich ist.) Beachte, da x entweder in S oder in T liegt, haben wir eine widerspruchsfreie Definition. Wir zeigen, dass α (wie auseinanderschneiden) und ζ (wie zusammensetzen) invers zueinander sind, d. h. für alle $f \in N^{S \uplus T}$ und $(g,h) \in N^S \times N^T$ gilt:

$$\alpha(f) = (g,h) \Leftrightarrow \zeta((g,h)) = f,$$

was wir als sehr einfache Übung lassen. q.e.d.

Beispiel (Tupelmenge X^n) Sei X eine Menge.
Eine Abbildung

$$f : \underline{n} \to X : i \mapsto f_i := f(i)$$

heißt eine X-wertige **Folge** der Länge n oder n-**Tupel** mit Werten in X, denn die übliche Notation für ein solches f ist

$$f = (f(1), f(2), \ldots, f(n)) = (f_1, f_2, \ldots, f_n)$$

(Manchmal läßt man sogar die Klammern weg.) Die Menge aller n-Tupel wird mit X^n statt $X^{\underline{n}}$ bezeichnet.
Wir wollen uns den Unterschied zwischen Mengen und Folgen klarmachen, indem wir für den Fall $X := \{1, 2, 3\}$die Abbildung

$$X^3 \to \mathrm{Pot}(X) : (a_1, a_2, a_3) \to \{a_1, a_2, a_3\}$$

studieren. Beispielsweise sind 6 Folgen in der Faser von $\{1, 2, 3\}$, nämlich

$$(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1).$$

Man ist somit geneigt zu sagen, dass eine endliche Folge so etwas wie eine endliche Menge mit einer Reihenfolge ist. Das ist aber nur ein Teil der Wahrheit. Den zweiten Unterschied zwischen Folgen und Mengen sieht man, wenn man die Faser von $\{1, 2\}$ untersucht. Z. B. sind $(1, 1, 2), (2, 1, 1)$ in dieser Faser. (Wieviele Elemente hat die Faser?) Also bei der Folge können auch noch Wiederholungen eingebaut sein, die bei Mengen ja unberücksichtigt bleiben.
Nehmen wir z. B. $X := \{a, b, c, \ldots, z\}$, das Alphabet. Dann würde man ein Wort aus 4 Buchstaben (nicht notwendig verschieden) als ein Element von X^4, also als Folge, ansehen. Das Bild dieser Folge lässt die Bildung vieler Folgen mit diesem Bild zu. Manche von ihnen nennt die Umgangssprache Anagramm. (Welche genau? Z. B. ist “lauf” ein Anagramm von “faul”.)

Übung: Zeige, dass

$$M \times M \to M^2 : \{\{m\}, \{m, n\}\} \to \{(1, m), (2, n)\}$$

eine Bijektion ist. Wir werden in Zukunft nicht mehr zwischen diesen beiden Mengen unterscheiden. Unsere identische Notation (m, n) für die Elemente beider Mengen deutet dies bereits an und ist durch diese Aufgabe gerechtfertigt.

Beginn 5. Vorlesung

An dieser Stelle ist an einen berühmten klassischen Satz zu erinnern, welcher auf dem zweiten **Cantorschen Diagonalverfahren** beruht, mit dem Cantor bewiesen hat, dass die Menge $\mathbb{R}$ der reellen Zahlen überabzählbar ist. Wir setzen das Resultat in einen etwas anderen Kontext.

Satz 3.13. *1.)* $\mathrm{Pot}(\mathbb{N})$ *ist überabzählbar.*
2.) $\mathrm{Pot}_{endl}(\mathbb{N}) := \{A \subseteq \mathbb{N} |\ A$ *endlich* $\}$ *ist abzählbar.*

Beweis. 1.) Angenommen Pot(ℕ) ist abzählbar. Dann existiert eine bijektive Abbildung

$$\zeta : \mathbb{N} \to \mathrm{Pot}(\mathbb{N}) : n \mapsto A_n$$

Wenn ζ bijektiv ist, ist insbesondere $\mathrm{Bild}(\zeta) = \mathrm{Pot}(\mathbb{N})$. Wir bekommen also einen Widerspruch, wenn wir eine Teilmenge $T \subseteq \mathbb{N}$ angeben, die nicht im Bild von ζ liegt. Diese Folge liefert uns das zweite CANTORsche Diagonalverfahren:

$$T := \{k \in \mathbb{N} \mid k \notin A_k\}.$$

Dann ist $T \notin \mathrm{Bild}(\zeta)$, denn angenommen $T = \zeta(n)$ für ein $n \in \mathbb{N}$. Dann gilt also $T = A_n$ und somit

$$(\star) \quad \forall k \in \mathbb{N} : k \in T \Leftrightarrow k \in A_n.$$

Diese Aussage ist aber falsch, da ihre Verneinung richtig ist. Betrachte nämlich $k = n$. Dann gilt $n \in T \Leftrightarrow n \notin A_n$.
2.) Der Beweis wird von der Notation her einfacher, wenn wir $\mathbb{N}$ durch $\mathbb{N}_0$ ersetzen. Die Abbildung

$$\alpha : \mathrm{Pot}_{endl}(\mathbb{N}_0) \to \mathbb{Z}_{\geq 0} : T \mapsto \sum_{i \in \mathbb{N}_0} \chi_T(i) \cdot 2^i = \sum_{i \in T} 2^i$$

ist wohldefiniert, denn in der Summe kommen nur endlich viele Summanden $\neq 0$ vor. Z. B $\alpha(\emptyset) = 0$ und $\alpha(\{0,1,3,5\}) = 2^0 + 2^1 + 2^3 + 2^5 = 43$. Wir verzichten auf einen formalen Beweis, dass α bijektiv ist, sondern überlegen z. B. nur, was die Faser von α über 135 ist.

$$\begin{aligned} 135 &= 1 + 2 \cdot 67 \\ &= 1 + 2 \cdot (1 + 2 \cdot 33) \\ &= 1 + 2 \cdot (1 + 2 \cdot (1 + 2 \cdot 16)) \\ &= 2^0 + 2^1 + 2^2 + 2^7 \end{aligned}$$

Also kann die Faser nur $\{\{0,1,2,7\}\}$ sein (warum doppelte Klammern?) und ist es auch in der Tat. Entsprechend müsste man jetzt jede Faser behandeln: Jede von ihnen muss einelementig sein. q.e.d.

3.3 Komposition von Abbildungen.

Lernziel: Komposition von Abbildungen, injektive Abbildungen und Linksinverse, surjektive Abbildungen und Rechtsinverse, Charakterisierung endlicher Mengen.

Wir wollen jetzt etwas mit den Abbildungen machen: Abbildungen in andere Abbildungen einsetzen.

Lemma 3.14. *Sind $f : S \to T$ und $g : T \to U$ Abbildungen, so ist*

$$g \circ f := \{(s,u) \in S \times U \mid \begin{array}{c} \text{es existiert ein } t \in T \text{ mit} \\ (s,t) \in f \text{ und } (t,u) \in g \end{array} \}$$

eine Abbildung von S nach U: $g \circ f : S \to U$.

Beweis. $g \circ f \subseteq S \times U$ ist klar. Sei $s \in S$. Dann existiert ein $t \in T$ mit $(s,t) \in f$, nämlich $t = f(s)$. Da g auch Abbildung ist, existiert auch ein $u \in U$ mit $(t,u) \in g$, nämlich $u = g(t)$. Also ist $(s,u) \in g \circ f$. (Damit ist die Existenz des Bildes verifiziert, jetzt kommt die Eindeutigkeit:) Seien $(s,u), (s,u') \in g \circ f$. Dann gibt es $t \in T$ mit $(s,t) \in f, (t,u) \in g$ und $t' \in T$ mit $(s,t') \in f, (t',u') \in g$. Da f Abbildung ist, folgt $t = t'$. Also folgt jetzt, da g Abbildung ist, $u = u'$. q.e.d.

Definition 3.15. *Die in Lemma 3.14 definierte Abbildung*

$$g \circ f : S \to U : s \mapsto g(f(s))$$

heißt die **Komposition** *(oder Hintereinanderausführung) von f mit g.*

Beispiel. 0) Ist $\emptyset \neq T \subseteq M$ eine Teilmenge, so ist die **Einbettung** $\iota_T : T \to M, \iota_T(t) := t$ eine Funktion. $\iota_T = \{(t,t) \mid t \in T\} \subseteq T \times M$. (Achtung ι_T unterscheidet sich von der identischen Funktion id_T.)
1) Ist $f : M \to N$ eine Abbildung und $\emptyset \neq T \subseteq M$ eine Teilmenge mit zugehöriger Einbettung $\iota : T \to M : t \mapsto t$, so gilt für die Einschränkung von f auf T

$$f_{|T} = f \circ \iota.$$

2.) Ist $f : M \to N$ eine bijektive Abbildung, so gilt

$$f \circ f^{-1} = \mathrm{id}_N \text{ und } f^{-1} \circ f = \mathrm{id}_M .$$

3) Für $n \in \mathbb{N}$ und $z \in \mathbb{Z}$ bezeichnet $z \bmod n$ (sprich z modulo n) die eindeutige Zahl $r \in \mathbb{Z}, 0 \leq r < n$ mit

$$z = qn + r \text{ für ein } q \in \mathbb{Z},$$

also der kleinste nichtnegative Rest, der beim Dividieren von z durch n bleibt. Sei also

$$\mu_n : \mathbb{Z} \to \mathbb{Z} : z \mapsto z \bmod n,$$

dann gilt: $\mu_n \circ \mu_n = \mu_n$.

Eine absolut grundlegende Eigenschaft der Komposition ist die Assoziativität. Der folgende Satz ist zwar sehr einfach zu beweisen, jedoch grundlegend für die gesamte Gruppentheorie und vieles andere in der Mathematik.

Satz 3.16. *(***Assoziativität** *der Komposition von Abbildungen) Sind $\alpha : A \to B$, $\beta : B \to C$, $\gamma : C \to D$ Abbildungen, so gilt*

$$(\gamma \circ \beta) \circ \alpha = \gamma \circ (\beta \circ \alpha).$$

(Man beachte, $\gamma \circ \beta : B \to D$ und $\beta \circ \alpha : A \to C$, so dass alle Kompositionen auf beiden Seiten der Gleichung wohldefinierte Abbildungen von A nach D sind.)

Beweis. Sei $a \in A$. Dann gilt: einerseits

$$((\gamma \circ \beta) \circ \alpha)(a) = (\gamma \circ \beta)(\alpha(a)) = \gamma(\beta(\alpha(a)))$$

und andererseits

$$(\gamma \circ (\beta \circ \alpha))(a) = \gamma((\beta \circ \alpha)(a)) = \gamma(\beta(\alpha(a)))$$

q.e.d.

Übung: Sei $\nu : M \to N$ eine bijektive Abbildung. Man zeige:

$$\overline{\nu} : M^M \to N^N : \alpha \mapsto \nu \circ \alpha \circ \nu^{-1}$$

ist eine Bijektion.

Wir hatten gesagt, eine Abbildung ist genau dann bijektiv, wenn die Faser über jedem Element des Wertebereiches genau ein Element hat. Dies kann man auf zwei Arten abschwächen.

Definition 3.17. *Sei $f : M \to N$ eine Abbildung.*
1) f heißt **injektiv** *oder* **eineindeutig**, *falls jede Faser von f aus höchstens einem Element besteht, d. h., zu jedem $n \in N$ existiert höchstens ein $m \in M$ mit $f(m) = n$.*
2) f heißt **surjektiv** *oder eine Abbildung* **auf** N, *falls keine Faser von f leer ist, d. h. zu jedem $n \in N$ existiert mindestens ein $m \in M$ mit $f(m) = n$, mit anderen Worten:* $\mathrm{Bild}(f) = N$.

Beispiele:
1) Sei $T \subseteq M$ eine Teilmenge von M. Dann ist die Einbettung

$$\iota_T : T \to M : t \mapsto t$$

injektiv (oder eine Injektion).
Ist $\alpha : M - T \to T$ irgendeine Abbildung, so ist

$$\pi : M \to T : m \mapsto \begin{cases} m & \text{falls } m \in T \\ \alpha(m) & \text{falls } m \notin T \end{cases}$$

surjektiv (oder Surjektion), allerdings nicht so kanonisch wie ι_T. Beachte: $\alpha \circ \iota_T = \mathrm{id}_T$.
2) Sei M eine nicht leere endliche Menge. Dann ist

$$|\ | : \mathrm{Pot}(M) \to \{0, 1, \ldots, |M|\} : T \mapsto |T|$$

eine surjektive Abbildung, die für $|M| > 1$ nicht bijektiv ist. Die Faser von $|\ |$ über n , $0 \leq n \leq |M|$ besteht aus allen n-elementigen Teilmengen von M, $\mathrm{Pot}_n(M) := |\ |^{-1}(n) = \{T \subseteq M \mid |T| = n\}$.
Bijektive Abbildungen $\alpha : M \to N$ waren dadurch gekennzeichnet, dass $\alpha^{-1} : N \to M$ eine Abbildung war. Es gilt dann $\alpha^{-1} \circ \alpha = \mathrm{id}_M$ und $\alpha \circ \alpha^{-1} = \mathrm{id}_N$. Hier ist eine Charakterisierung von injektiven und von surjektiven Abbildungen.

Satz 3.18. *Sei $\alpha : M \to N$ eine Abbildung. Es gilt:*
1) α ist genau dann injektiv, wenn eine Abbildung $\beta : N \to M$ mit $\beta \circ \alpha = \mathrm{id}_M$ existiert. Jedes derartige β ist surjektiv und heißt auch **Linksinverses** *von α.*
2) α ist genau dann surjektiv, wenn eine Abbildung $\gamma : N \to M$ mit $\alpha \circ \gamma = \mathrm{id}_N$ existiert. Jedes derartige γ ist injektiv und heißt auch **Rechtsinverses** *von α.*

Beweis. 1) Sei α injektiv. Für $n \in N$ mit $n \in \alpha(M)$ existiert ein eindeutiges $m \in M$ mit $\alpha(m) = n$, da α injektiv ist. Wir definieren $\beta(n) := m$. Für $n \in N$ mit $n \notin \alpha(M)$ wähle ein beliebiges $m \in M$ und setze $\beta(n) := m$. Klar: β ist Abbildung von N nach M und $\beta \circ \alpha = \mathrm{id}_M$.
Sei nun $\beta : N \to M$ ein Linksinverses von α, d. h. $\beta \circ \alpha = \mathrm{id}_M$. Sind $m, m' \in M$ mit $\alpha(m) = \alpha(m')$, so gilt

$$\begin{aligned} m &= \mathrm{id}_M(m) \\ &= \beta(\alpha(m)) \\ &= \beta(\alpha(m')) \\ &= m', \end{aligned}$$

d. h. α ist injektiv.
Sei nun $\beta : N \to M$ eine beliebige Abbildung mit $\beta \circ \alpha = \mathrm{id}_M$. Behauptung: β ist surjektiv. Bew.: Sei $m \in M$, dann gilt $m = \mathrm{id}_M(m) = \beta(\alpha(m))$, d. h. $m \in \beta(N)$. Da $m \in M$ beliebig vorgegeben war, ist somit β surjektiv.
2) Sei nun α surjektiv. Dann ist $\alpha^{-1}(\{n\}) \neq \emptyset$ für jedes $n \in N$. Definiere $\gamma : N \to M$ so dass $\gamma(n) \in \alpha^{-1}(\{n\})$ für alle $n \in N$. Dann gilt $\alpha \circ \gamma : N \to N, \alpha \circ \gamma(n) = \alpha(\gamma(n)) = n$ nach Wahl von $\gamma(n)$ und somit $\alpha \circ \gamma = \mathrm{id}_N$.
Sei nun $\gamma : N \to M$ ein beliebiges Rechtsinverses von α. Dann ist $\alpha \circ \gamma = \mathrm{id}_N$ und somit gilt für alle $n \in N$

$$n = \mathrm{id}_N(n) = (\alpha \circ \gamma)(n) = \alpha(\gamma(n)) \in \mathrm{Bild}(\alpha)$$

also ist α surjektiv. Weiter gilt γ ist injektiv, denn seien $n_1, n_2 \in N$ mit $\gamma(n_1) = \gamma(n_2)$. Dann

$$n_1 = \mathrm{id}_N(n_1) = (\alpha \circ \gamma)(n_1) = \alpha(\gamma(n_1)) = \alpha(\gamma(n_2)) = n_2.$$

q.e.d.

Bemerkung. Im Allgemeinen sind Links- und Rechtsinverse nicht eindeutig bestimmt.
1,) Die Funktion $f : \mathbb{Z} \to \mathbb{Z} : a \mapsto 2a$, ist injektiv, hat also ein Linksinverses, z.B.

$$g : \mathbb{Z} \to \mathbb{Z} : a \mapsto \begin{cases} a & \text{falls a ungerade ist} \\ a/2 & \text{falls a gerade ist.} \end{cases}$$

Jedoch kann man die ungeraden Zahlen (die ja nicht im Bild der Funktion f sind), auf beliebige ganze Zahlen abbilden. Eine andere Linksinverse wäre z.B.

$$g : \mathbb{Z} \to \mathbb{Z} : a \mapsto \begin{cases} (a-1)/2 & \text{falls a ungerade ist} \\ a/2 & \text{falls a gerade ist.} \end{cases}$$

2.) Ebenso hat die surjektive, nicht injektive Funktion

$$g : \mathbb{Z} \to \mathbb{Z} : a \mapsto \begin{cases} a & \text{falls a ungerade ist} \\ a/2 & \text{falls a gerade ist.} \end{cases}$$

mehrere Rechtsinverse, u. a. das f aus 1.) Finde andere Rechstinverse!

Folgerung 3.19. *Eine Abbildung ist genau dann bijektiv, wenn sie injektiv und surjektiv ist. In dem Fall ist die Umkehrabbildung das eindeutig bestimmte Links- und Rechtsinverse.*

Wir beschließen den Abschnitt mit einer Charakterisierung endlicher Mengen, die allerdings die Wohldefiniertheit der Anzahl der Elemente einer endlichen Menge benutzt, die wir noch nicht bewiesen hatten, ebenso dass eine unendliche Menge immer eine abzählbar unendliche Teilmenge besitzt. Dies werden wir bei der vollständigen Induktion dann nachtragen.

Satz 3.20. *Sei M eine Menge. Folgende Aussagen sind äquivalent:*
1) M ist endlich.
2) Jede injektive Abbildung $\eta : M \to M$ von M in sich ist auch surjektiv.
3) Jede surjektive Abbildung $\tau : M \to M$ von M auf sich ist auch injektiv.

Beweis. (Später) q.e.d.

Das Hilbertsche [7] Hotel: Das ist ein Hotel mit abzählbar unendlich vielen Zimmern $Z = \{z_i \mid i \in \mathbb{N}\}$ der Einfachheit halber seien dies alles Einzelzimmer. Das Hotel ist voll belegt, in Zimmer z_i wohnt der Gast g_i (für alle $i \in \mathbb{N}$). Jetzt kommt ein weiterer Gast g an und möchte in dem Hotel übernachten. Der Portier will ihn schon wegschicken, da das Hotel ja voll ist, aber da meint der Mathematiker Hilbert zum neuen Gast: *Sicher können Sie bei uns wohnen, es wird gleich ein Zimmer für Sie frei.* Hilbert bittet jeden Gast g_i in das Zimmer z_{i+1} umzuziehen und siehe da, Zimmer z_1 wird frei. Dieses gibt es dem Gast g.
Jetzt kommt auch noch ein ganzer Reisebus mit abzählbar unendlich vielen neuen Gästen $R = \{r_i \mid i \in \mathbb{N}\}$ an und alle möchten in dem nach wie vor vollen Hotel übernachten. Dem Portier wird dies zu viel, aber Hilbert bleibt ganz ruhig und kann jedem neuen Gast ein Zimmer geben.

Übung: Wie stellt er dies an? Welche injektive Funktion $\sigma : G = \{g_i \mid i \in \mathbb{N}\} \to Z = \{z_i \mid i \in \mathbb{N}\}$ kann er wählen, sodass er eine Bijektion $R \to Z - \text{Bild}(\sigma)$ bekommt?

[7] David Hilbert 1862 - 1943

4 Partitionen und Äquivalenzrelationen. (6. Vorlesung)

Lernziel: Relationen als Teilmengen kartesischer Produkte, Äquivalenzrelationen und Partitionen, Gleichwertigkeit der beiden Begriffe und inhaltliche Ausdeutung, enger Zusammenhang mit Abbildungen.

Relationen in ihrer allgemeinen Form verallgemeinern den Funktionsbegriff: Sie sind einfach Teilmengen eines kartesischen Produktes. In dieser Allgemeinheit sind sie für einen Anfänger nicht nützlich. Daher beschränken wir uns auf Relationen auf einer Menge, die dann bestimmte Beziehungen der Elemente der Menge untereinander modellieren sollen. Der wichtigste Begriff ist der der Äquivalenzrelation, der den Gleichheitsbegriff abschwächt und den Begriff der "Gleichheit unter einem bestimmten Gesichtspunkt" formalisiert.

Definition 4.1. *Sei M eine Menge.*
1) Eine **Relation** *R auf M ist eine Teilmenge von $M \times M$. Statt $(m,n) \in R$ schreibt man auch mRn und sagt, m steht in Relation R zu n.*
2) Eine Relation R auf M heißt **reflexiv**, *falls mRm gilt für alle $m \in M$.*
3) Eine Relation R auf M heißt **symmetrisch**, *falls mRn immer nRm für alle $m,n \in M$ impliziert.*
4) Eine Relation R auf M heißt **transitiv**, *falls aus mRn und nRo stets mRo für alle $m,n,o \in M$ folgt.*
5) Eine reflexive, symmetrische und transitive Relation R auf M heißt **Äquivalenzrelation**. *Statt mRn sagt man auch m und n sind (bezüglich R) äquivalent.*
6) Ist R eine Äquivalenzrelation auf M und $m \in M$, so bezeichnet

$$[m]_R := \{n \in M \mid nRm\}$$

die **Äquivalenzklasse** *von m.*

Beispiele 1) $\leq$ ist eine Relation auf $\mathbb{R}$ in bekannter Weise in der Ebene visualisiert. $\leq$ ist reflexiv (im Unterschied zu $<$), nicht symmetrisch, allerdings transitiv. Insbesondere ist $\leq$ keine Äquivalenzrelation, sehr wohl aber $=$, der Durchschnitt von $\leq$ und $\geq$.
2) $R := M \times M$ ist eine Äquivalenzrelation auf M.
3) $\emptyset \subseteq M \times M$ ist symmetrisch, transitiv, aber nicht reflexiv, falls $M \neq \emptyset$.
4) Sei M eine Menge von Aussagen. Dann ist $\Leftrightarrow$ eine Äquivalenzrelation auf M.
5) 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 4.2. *Sei $\Gamma : M \to N$ eine Abbildung (Γ wie Gesichtspunkt). Dann ist $\sim_\Gamma \subseteq M \times M$ definiert durch $m \sim_\Gamma m'$ genau dann, wenn $\Gamma(m) = \Gamma(m')$, eine Äquivalenzrelation. Die Äquivalenzrelation $\sim_\Gamma$ heißt* **Bildgleichheit** *bezüglich Γ. Die Äquivalenzklassen sind genau die nichtleeren Fasern der Abbildung Γ.*

Beweis. $\sim_\Gamma$ ist eine Teilmenge von $M \times M$, also eine Relation. Sie ist reflexiv, da für alle $m \in M$ der Funktionswert $\Gamma(m) = \Gamma(m)$ definiert ist. Sie ist transitiv, denn ist $\Gamma(a) = \Gamma(b)$ und $\Gamma(b) = \Gamma(c)$, so auch $\Gamma(a) = \Gamma(c)$ da Gleichheit transitiv ist. Ebenso folgt die Symmetrie von $\sim_\Gamma$ aus der Symmetrie von $=$. q.e.d.

Die vier Äquivalenzrelationen aus dem vorherigen Beipiel kann man von hierher sehr klar verstehen:
Bei 1) mit der Gleichheit als Äquivalenzrelation nimmt man $\Gamma := \mathrm{id}_{\mathbb{R}}$,
Bei 2) nimmt man eine konstante Funktion $\Gamma := \kappa_a : M \to \{a\}$.
Bei 4) nimmt man $\Gamma := W : M \to \{0, 1\}$ als die Wahrheitsfunktion.
Bei 5) nimmt man $\Gamma : M \to \mathbb{R} : G_{a,b} \mapsto a$ als die Steigung.

Äquivalenzrelationen sind inhaltlich, jedoch nicht formal dasselbe wie Partitionen, also Aufteilungen einer Mengen.

Definition 4.3. *Sei M eine Menge.*
0) Zwei Teilmengen X, Y von M heißen **disjunkt**, *falls $X \cap Y = \emptyset$.*
1) Eine **Partition** *P von M ist eine Teilmenge $P \subseteq \mathrm{Pot}(M)$ mit*

a) für alle $X \in P, X \neq \emptyset$, b) $M = \bigcup_{X \in P} X$ und c) $X \cap Y = \emptyset$ für alle $X, Y \in P, X \neq Y$.

Also ist M die disjunkte Vereinigung der Mengen aus P und man schreibt die letzten beiden Bedingungen kurz so:

$$M = \biguplus_{X \in P} X$$

2) Sei P eine Partition auf M. Die Elemente von P heißen auch **Klassen**. *Ist X eine Klasse, so nennt man ein Element von X auch* **Vertreter** *der Klasse. Eine Teilmenge von M, die aus jeder Klasse von P genau einen Vertreter enthält, nennt man auch* **Vertretermenge** *oder* **Transversale**. *Eine Abbildung $v : P \to M$ mit $v(X) \in X$ für alle $X \in P$ heißt* **Vertreterabbildung** *oder auch* **Transversale**.

Ist P eine Partition von M, so gehört jedes Element von M zu genau einem $X \in P$, d. h.

$$f_P : M \to P : m \mapsto X \in P \text{ mit } m \in X$$

ist eine Abbildung, genannt die **natürliche Abbildung** zu P. Hier ist der Zusammenhang zwischen Äquivalenzrelationen und Partitionen.

Satz 4.4. *Sei M eine Menge.*
1) Ist $\sim$ eine Äquivalenzrelation auf M, so bilden **Äquivalenzklassen** *definiert durch*

$$[m_0] := [m_0]_\sim := \{m \in M \mid m \sim m_0\}$$

für $m_0 \in M$ eine Partition von M. Diese wird üblicherweise mit $M/\sim$ bezeichnet.
2) Ist P eine Partition von M, so ist $\sim_P$ definiert durch $m \sim_P n$ genau dann, wenn ein $X \in P$ existiert mit $m \in X$ und $n \in X$ eine Äquivalenzrelation.
3) Es gilt $M/\sim_P = P$ für alle Partitionen P von M und $\sim_{(M/\sim)} = \sim$ für jede Äquivalenzrelation $\sim$ auf M.

Beweis. 1) Sei $P := M/\sim = \{[m]_\sim \mid m \in M\}$. Zu zeigen: P ist eine Partition von M.

$\emptyset \notin P$, da jede Äquivalenzklasse $[m]_\sim$ sicherlich das Element $m \in M$ enthält (da $\sim$ reflexiv ist).

$\bigcup_{X\in P} X = M$, da jedes $m \in M$ in seiner Äquivalenzklasse $m \in [m]_\sim \in P$ liegt.

Die wichtigste Eigenschaft ist

Zwei Äquivalenzklassen sind entweder disjunkt oder gleich.

Dazu seien $a, b \in M$ mit $[a]_\sim \cap [b]_\sim \neq \emptyset$. Wir müssen zeigen, dass dann $[a]_\sim = [b]_\sim$ gilt. Dazu sei $c \in [a]_\sim \cap [b]_\sim$. Dann gilt $c \sim a$ und $c \sim b$, also auch $a \sim c$ und $c \sim b$ (Symmetrie) und wegen der Transitivität damit auch $a \sim b$.
Zeigen nur $[a]_\sim \subseteq [b]_\sim$, die Umkehrung geht dann genauso und insgesamt ergibt sich die Gleichheit der beiden Äquivalenzklassen.
Dazu sei $d \in [a]_\sim$. Dann ist $d \sim a$ und wegen $a \sim b$ und der Transitivität gilt dann auch $d \sim b$ und somit $d \in [b]_\sim$.
2) Übung.
3) Sei P eine Partition auf M. Dann ist $M/\sim_P = \{[m]_{\sim_P} \mid m \in M\}$. Um zu zeigen, dass diese Partition wieder gleich P ist, bemerken wir, dass

$$[m]_{\sim_P} = \{n \in M \mid \text{ es gibt ein } X \in P \text{ mit } m \in X \text{ und } n \in X\}$$

genau das Element X von P ist, welches m enthält. Also ist $M/\sim_P = \{X \mid X \in P\} = P$.
Sei andererseits $\sim$ eine Äquivalenzrelation auf M. Für jedes Paar $m, n \in M$ müssen wir zeigen, dass $m \sim n$ genau dann, wenn $m \sim_{(M/\sim)} n$ gilt. Beides heißt aber, dass m und n zu derselben Menge von $M/\sim$ gehören. q.e.d.

Teil 3) von Satz 4.4 kann man auch so ausdrücken:

Bemerkung 4.5. *Die Abbildungen*

$$part : \{\text{Äquivalenzrelationen auf } M\} \to \{\text{Partitionen von } M\} : \sim \mapsto M/\sim$$

und

$$aequ : \{\text{Partitionen von } M\} \to \{\text{Äquivalenzrelationen auf } M\} : P \mapsto \sim_P$$

sind zueinander inverse Bijektionen. Insbesondere gibt es auf einer Menge genausoviele Partitionen wie Äquivalenzrelationen.

Ein wichtiges Wort zur Philosophie von $M/\sim$: Per Definition ist dies zwar eine Partition der Menge M, aber die Idee ist, die Elemente von $M/\sim$ nicht als Teilmengen von M anzusehen, sondern als Elemente einer neuen Menge.

Satz 4.6. *(1) Sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Dann gibt es eine Menge P und eine surjektive Abbildung $\Gamma : M \to P$, sodass $\sim = \sim_\Gamma$. Jede Äquivalenzrelation ist also Bildgleichheit unter einer surjektiven Abbildung.*
(2) Ist $\Gamma : M \to N$ eine surjektive Abbildung und $P := M/\sim_\Gamma$ die zur Bildgleichheit gehörige Partition, so ist $f : P \to N : [m]_{\sim_\Gamma} \mapsto \Gamma(m)$ eine wohldefinierte Bijektion.
(3) Sind $\Gamma_1 : M \to P_1$ und $\Gamma_2 : M \to P_2$ zwei surjektive Abbildungen, so gilt $\sim_{\Gamma_1} = \sim_{\Gamma_2}$ genau dann, wenn eine Bijektion $f : P_1 \to P_2$ existiert mit $\Gamma_2 = f \circ \Gamma_1$.

Beweis. (1) Sei $P := M/\sim$ die Menge aller Äquivalenzklassen und definiere $\Gamma : M \to P : m \mapsto [m]_\sim$. Dann ist Γ surjektiv und die Fasern von Γ sind genau die Äquivalenzklassen von $\sim$.
(2) Wohldefiniertheit: Sei $[m_1] = [m_2]$. Dann ist aber auch $\Gamma(m_1) = \Gamma(m_2)$ und damit das Bild von $[m]$ unter f unabhängig von der Wahl des Vertreters m. Die Abbildung f ist injektiv, denn

$$f([m_1]) = f([m_2]) \Leftrightarrow \Gamma(m_1) = \Gamma(m_2) \Leftrightarrow [m_1] = [m_2].$$

Außerdem ist f surjektiv, da Γ surjektiv ist.
(3) Ist $\Gamma_2 = f \circ \Gamma_1$ für eine Bijektion f, so gilt für $m, n \in M$

$$\Gamma_1(m) = \Gamma_1(n) \Leftrightarrow f(\Gamma_1(m)) = f(\Gamma_1(n)) \Leftrightarrow \Gamma_2(m) = \Gamma_2(n)$$

also sind die Äquivalenzrelationen $\sim_{\Gamma_1}$ und $\sim_{\Gamma_2}$ gleich. Sind umgekehrt die Äquivalenzrelationen gleich, so natürlich auch die durch sie definierten Partitionen $M/\sim_{\Gamma_1} = M/\sim_{\Gamma_2} =: P$. Nach (2) gibt es dann aber eine Bijektion zwischen P und N_1 und auch zwischen P und N_2. q.e.d.

Übung: Wieviele dreiklassige Äquivalenzrelationen gibt es auf $\underline{7}$? (Hinweis: Benutze den letzten Satz und zähle zuerst die surjektiven Abbildungen $\underline{7} \to \underline{3}$. Wieviele von diesen ergeben dieselbe Äquivalenzrelation auf $\underline{7}$? Suche auch alternative Möglichkeiten des Zählens.)

Das nachfolgende Beispiel soll uns zeigen, dass der Umgang mit Äquivalenzklassen allen sehr geläufig ist, wenn auch nur unbewusst und in sehr ausgewählten, allerdings wichtigen Beispielen.

Historisch war der Übergang von den natürlichen Zahlen $1, 2, 3, \ldots$ zu den ganzen Zahlen, wo noch $0, -1, -2, \ldots$ hinzukamen, ein recht langwieriger Prozess. Wie kann man diesen ausdrücken durch die gerade einführten Konzepte? Wir nehmen an, wir kennen $\mathbb{N}$, d. h. wir gehen von den natürlichen Zahlen aus.
Beispiel Definiere

$$\tilde{\mathbb{Z}} := \mathbb{N} \times \mathbb{N}/\sim \text{ mit } (m, n) \sim (m', n') \Leftrightarrow n + m' = n' + m$$

Wenn Sie die Menge der ganzen Zahlen $\mathbb{Z}$ schon als bekannt voraussetzen und $\mathbb{N}$ eingebettet in $\mathbb{Z}$ ist, dann ist

$$\varphi : \tilde{\mathbb{Z}} \to \mathbb{Z}, [(m, n)] \mapsto m - n$$

eine Bijektion:
Beweis. φ ist "wohldefiniert" (eine Abbildung). φ ist injektiv (nach Definition von $\sim$). φ ist surjektiv (leicht).
Setzt man $\mathbb{Z}$ nicht als bekannt voraus, sondern benutzt $\tilde{\mathbb{Z}}$ um die ganzen Zahlen zu konstruieren, so ist einiges zu überlegen:
1.) Wie finden wir $\mathbb{N}$ in $\tilde{\mathbb{Z}}$ wieder? Antwort:

$$\nu : \mathbb{N} \to \tilde{\mathbb{Z}} : n \mapsto [(n + 1, 1)]_\sim$$

ist injektiv (Beweis später) (ν wie natürliche Einbettung), also wir identifizieren $n \in \mathbb{N}$ mit $[(n+1,1)]_\sim \in \tilde{\mathbb{Z}}$.
2.) Wie addiert man in $\tilde{\mathbb{Z}}$, sodass sich die Addition von $\mathbb{N}$ fortsetzt und andererseits $[(m,n)]_\sim$ eine Lösung von $x_{(m,n)} + n = m$ ist? Genauer:
a) $\nu(a) + \nu(b) = \nu(a+b)$ für alle $a, b \in \mathbb{N}$ und
b) $[(m,n)]_\sim + \nu(n) = \nu(m)$ für alle $m, n \in \mathbb{N}$.
Antwort:

$$+ : \tilde{\mathbb{Z}} \times \tilde{\mathbb{Z}} \to \tilde{\mathbb{Z}} : ([(m,n)]_\sim, [(s,t)]_\sim) \mapsto [(m+s, n+t)]_\sim$$

ist wohldefiniert, also vertreterunabhängig, und erfüllt a) und b). (Beweis später).
Wir sehen sehr leicht, dass $\tilde{\mathbb{Z}}$ gegeben ist durch

$$\ldots, -2 := [(1,3)]_\sim, -1 := [(1,2)]_\sim, 0 := [(1,1)]_\sim, 1 := [(2,1)]_\sim, 2 := [(3,1)]_\sim, \ldots$$

Mit anderen Worten ganze Zahlen sind nichts anderes als Äquivalenzklassen von Gleichungen, wie wir sie oben sahen.

Beispiel 4.7. *(Rationale Zahlen) Sei*

$$M := \mathbb{Z} \times \mathbb{N} = \{(a,b) \mid a \in \mathbb{Z} \text{ und } b \in \mathbb{N}\}.$$

Wir definieren eine Äquivalenzrelation $\sim \subseteq M \times M$ *durch*

$$(a,b) \sim (c,d) \text{ genau dann wenn } ad = bc.$$

Die Äquivalenzklasse $[(a,b)]_\sim$ *wird mit* $\frac{a}{b}$ *bezeichnet. Äquivalenzklassen können wir addieren und multiplizieren:*

$$[(a,b)] + [(c,d)] = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = [(ad+bc, bd)]$$

und

$$[(a,b)] \cdot [(c,d)] = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = [(ac, bd)].$$

Wir müssen zeigen, dass dies wohldefinierte *Verknüpfungen sind, also nicht von der Wahl des Vertreters* $(a,b) \in \frac{a}{b}$ *abhängen. Sei z.B.* $(a,b) \sim (a',b')$ *und* $(c,d) \sim (c',d')$*. Dann ist also* $ab' = a'b$ *und* $cd' = c'd$*. Dann gilt auch* $(ac, bd) \sim (a'c', b'd')$*, denn*

$$acb'd' = (ab')(cd') = (a'b)(c'd) = a'c'bd$$

und ebenso (Übung) $(ad+bc, bd) \sim (a'd' + b'c', b'd')$*. Kein Mensch denkt bei dem Bruch* $\frac{a}{b}$ *an eine Menge von Paaren ganzer Zahlen, sondern interpretiert* $\frac{a}{b}$ *als ein Element der Menge aller rationalen Zahlen. Das Kürzen ist eine Prozedur, die in jeder Äquivalenzklasse* $\frac{a}{b}$ *einen eindeutigen Vertreter (gekürzter Bruch) findet, und so eine Art* Normalform *für die Elemente in der Äquivalenzklasse bestimmt. Diese Normalform macht es leichter, Brüche (also Äquivalenzklassen) zu vergleichen.*

5 Vollständige Induktion und Rekursion (7. Vorlesung)

Lernziele: Axiomatik der natürlichen Zahlen, Rekursion und verschieden Versionen der vollständigen Induktion, Addition natürlicher Zahlen. Potenzierung von Abbildungen, Anordnung der natürlichen Zahlen.

5.1 Axiome und Prinzipien

Definition 5.1. *(*Peano**-Axiome**) Sei N eine Menge und $\nu : N \to N$ eine Abbildung. (N, ν) erfüllt die* Peano[8]*-Axiome, falls gilt:*
(1) ν ist injektiv und $N - \text{Bild}(\nu)$ besteht aus genau einem Element. Dieses Element sei mit 1_N bezeichnet.
(2) Ist $M \subseteq N$ eine Teilmenge von N mit den beiden Eigenschaften

$$(a)\ 1_N \in M \text{ und } (b)\ \nu(M) \subseteq M$$

so ist $M = N$.
Ist N irgendeine Menge, für die eine Abbildung ν mit den obigen Eigenschaften existiert, so sagen wir auch, dass N die Peano*-Axiome erfüllt.*

Man sollte etwa folgende Visualisierung vor Augen haben, wobei der erste Punkt 1_N ist:

$$\bullet \to \bullet \to \bullet \to \bullet \to \bullet \to \dots$$

Man beachte, dass $N \to \nu(N) : n \mapsto \nu(n)$ eine Bijektion ist. Also N steht in Bijektion zu einer echten Teilmenge. ν heißt üblicherweise Nachfolgerabbildung und das Inverse $\pi := \nu^{-1} : N - \{1_N\} \to N$ die Vorgängerabbildung.

Wir stellen uns auf denselben Standpunkt wie Leopold Kronecker[9], der gesagt hat: „Die natürlichen Zahlen sind vom lieben Gott geschaffen, alles andere in der Mathematik ist nur Menschenwerk.“ Dieser Standpunkt ist nicht der einzige, den man einnehmen kann. Richard Dedekind[10] hat gesagt: „Die natürlichen Zahlen sind freie Schöpfungen des menschlichen Geistes.“ Wir werden später eine mögliche Konstruktion der natürlichen Zahlen sehen, die auf John von Neumann[11], dem Pionier der Computer, zurückgeht. Da wir jetzt nicht die Zeit haben, uns in weitere Einzelheiten zu verlieren, machen wir uns Kroneckers Standpunkt zu eigen und gehen von folgender Bemerkung aus.

Bemerkung 5.2. *(Axiom) Die Menge der natürlichen Zahlen $\mathbb{N} := \{1, 2, 3, 4, \dots\}$ erfüllt die* Peano*-Axiome mit $1_{\mathbb{N}} = 1$ und $\nu(n) := n + 1$ für alle $n \in \mathbb{N}$ und $\pi(n) = n - 1$ für alle $n \in \mathbb{N} - \{1\}$.*

[8] Giuseppe Peano 1858 - 1932
[9] Leopold Kronecker 1823 - 1891
[10] Julius Wilhelm Richard Dedekind 1831 - 1916
[11] John von Neumann 1903 - 1957

Aus den PEANO-Axiomen leiten wir jetzt zwei wichtige Prinzipien her: das Beweisprinzip der vollständige Induktion und die Definition durch Rekursion. Beide sind volkstümlich gesprochen wissenschaftliche Umschreibungen dessen, was man sonst mit "u.s.w." abkürzt, also eine mathematisch fundierte Methode, "und so weiter" zu sagen.

Satz 5.3. *(***Vollständige Induktion***)*
Für jedes $n \in \mathbb{N}$ sei $A(n)$ eine Aussage. Gilt der
Induktionsanfang: $A(1)$
und der
Induktionsschluss: $A(n) \Rightarrow A(n+1)$ *für alle* $n \in \mathbb{N}$,
so gilt $A(n)$ für alle $n \in \mathbb{N}$.

Beweis. Sei

$$M := \{n \in \mathbb{N} \mid A(n) \text{ ist wahr } \}.$$

Dann ist $M \subseteq \mathbb{N}$ und wir müssen zeigen, dass $M = \mathbb{N}$ ist. Dazu benutzen wir das 2. PEANO-Axiom. Denn nach Voraussetzung gilt $1 \in M$. Außerdem gilt für jedes $m \in M$ auch dass $m + 1 \in M$ liegt. Also erfüllt M die Voraussetzung des 2. PEANO-Axioms und somit ist $M = \mathbb{N}$. q.e.d.

Bei der Definition durch Rekursion haben wir gleich Gelegenheit, das neue Beweisprinzip anzuwenden.

Satz 5.4. *(Definition durch* **Rekursion***)*
Sei M eine Menge und für jedes $n \in \mathbb{N}$ sei $\alpha_n : M^n \to M$ eine Abbildung. Ist $m \in M$, so gibt es eine eindeutige Funktion $f : \mathbb{N} \to M$ mit

$$f(1) = f_1 = m \text{ und } f(n+1) = f_{n+1} = \alpha_n(f_1, \ldots, f_n).$$

Beweis. Sei $T := \{n \in \mathbb{N} \mid f(1), \ldots, f(n) \text{ wohldefiniert } \}$.
Offenbar gilt $1 \in T$, d. h. die Induktionsverankerung ist gegeben.
Wir nehmen nun an, dass $n \in T$ gilt.
Dann ist $f_{n+1} = \alpha_n(f_1, \ldots, f_n) \in M$ wohldefiniert, d. h. $n + 1 \in T$.
Nach Satz 5.3 ist also $T = \mathbb{N}$ und die Behauptung bewiesen. q.e.d.

Satz 5.5. *(***Eindeutigkeit der natürlichen Zahlen***) Sei (N, ν) eine Menge mit Nachfolgerfunktion, die die* PEANO*-Axiome erfüllt. Dann gibt es eine eindeutige Bijektion $\varphi : \mathbb{N} \to N$ mit $\varphi(n+1) = \nu(\varphi(n))$ für alle $n \in \mathbb{N}$.*

Beweis. Eindeutigkeit: Seien $\varphi : \mathbb{N} \to N$ und $\varphi' : \mathbb{N} \to N$ zwei solche Bijektionen und sei

$$M := \{n \in \mathbb{N} \mid \varphi(n) = \varphi'(n)\}.$$

Wir wollen zeigen, dass $M = \mathbb{N}$ gilt und benutzen dazu das 2. PEANO-Axiom. Angenommen $\varphi(1) \neq 1_N$. Dann hätte $\varphi(1)$ einen Vorgänger in N, der aber auch ein Urbild in $\mathbb{N}$ hat, welches dann aber Vorgänger von 1 in $\mathbb{N}$ sein muss. Da dies ein Widerspruch ist, folgt $\varphi(1) = 1_N$.
Ebenso erhält man $\varphi'(1) = 1_N$ und damit $1 \in M$.

Sei nun $n \in M$. Wir wollen zeigen, dass dann auch $n+1 \in M$ ist woraus nach dem 2. PEANO-Axiom dann $M = \mathbb{N}$ folgt. Es ist

$$\varphi(n+1) = \nu(\varphi(n)) \overset{n\in M}{=} \nu(\varphi'(n)) = \varphi'(n+1).$$

Existenz: Definieren $\varphi : \mathbb{N} \to N$ rekursiv durch $\varphi(1) := 1_N$. Ist $\varphi(n)$ schon definiert, so setzen wir $\varphi(n+1) := \nu(\varphi(n))$. Dies definiert eine Funktion $\varphi : \mathbb{N} \to N$ nach Satz 5.4. Um zu zeigen, dass φ bijektiv ist, zeigen wir, dass das analog definierte $\psi : N \to \mathbb{N}$ mit $\psi(1_N) = 1$ und $\psi(\nu(n)) := \psi(n) + 1$ für alle $n \in \mathbb{N}$ sowohl rechts- als auch linksinvers zu φ ist:
$\psi \circ \varphi : \mathbb{N} \to \mathbb{N}$ erfüllt dass

$$(\psi\circ\varphi)(1) = \psi(\varphi(1)) = \psi(1_N) = 1 \text{ und } (\psi\circ\varphi)(n+1) = \psi(\nu(\varphi(n))) = \psi(\varphi(n))+1 = n+1$$

für alle $n \in \mathbb{N}$. Also nach dem Prinzip der Rekursion (oder auch dem Eindeutigkeitsteil dieses Beweises, da auch $\mathrm{id}_{\mathbb{N}}$ diese Bedingungen erfüllt) gilt $\psi \circ \varphi = \mathrm{id}_{\mathbb{N}}$.
Ebenso zeigt man, dass $\varphi \circ \psi = \mathrm{id}_N$ gilt. q.e.d.

Dieser Satz zeigt, dass die Menge $\mathbb{N}$ der natürlichen Zahlen mit der Nachfolgerfunktion $\nu : \mathbb{N} \to \mathbb{N} : n \mapsto n+1$ im wesentlichen (d.h. bis auf eine eindeutig bestimmte, die Nachfolgerfunktion und die 1 respektierende Bijektion) die einzige Menge ist, die die Peano-Axiome erfüllt. Dieses "im wesentlichen" schließt aber z.B. auch die Menge der ganzen Zahlen $\mathbb{Z}$, die ja nach Satz 3.10 in Bijektion zu $\mathbb{N}$ steht, mit ein. Denn allgemein gilt:

Übung: Ist M eine Menge mit einer Bijektion $f : M \to \mathbb{N}$, so erfüllt (M, ν) die Peano-Axiome, wenn man $1_M := f^{-1}(1)$ und $\nu(m) := f^{-1}(f(m)+1)$ definiert. Benutze dies, um das Prinzip der vollständigen Induktion für Mengen wie $\{k, k+1, k+2, \ldots\}$ zu formulieren und zu begründen. (Hinweis: Diese Menge ist gleich Bild(ν^k). Potenzen von Abbildungen werden gleich definiert.)

Definition 5.6. *(Potenzen einer Abbildung)*
Sei $\alpha : M \to M$ eine Abbildung. Die **Potenz***en α^n mit $n \in \mathbb{N}$ von α sind (rekursiv) definiert durch*

$$\alpha^1 := \alpha \text{ und } \alpha^{n+1} := \alpha^n \circ \alpha \text{ für alle } n \in \mathbb{N}.$$

Nach Satz 5.4 ist damit offenbar eine Folge in M^M definiert.

Bemerkung 5.7. *Man könnte jetzt auf die Idee kommen, eine zweite Folge in M^M zu definieren durch*

$$\alpha^{(1)} := \alpha \text{ und } \alpha^{(n+1)} := \alpha \circ \alpha^{(n)} \text{ für alle } n \in \mathbb{N}.$$

Dann gilt $\alpha^n = \alpha^{(n)}$ für alle $n \in \mathbb{N}$.
Beweis: Induktionsverankerung: $\alpha^1 = \alpha^{(1)}$ ist klar, da beide Seiten nach Definition gleich α sind.
Induktionsannahme: $\alpha^n = \alpha^{(n)}$.

Induktionsschluss: Zeige aus der Induktionsannahme folgt $\alpha^{n+1} = \alpha^{(n+1)}$.

$$\begin{aligned}
\alpha^{n+1} &= \alpha^n \circ \alpha \text{ (Definition)} \\
&= \alpha^{(n)} \circ \alpha \text{ (Induktionsvoraussetzung)} \\
&= (\alpha \circ \alpha^{(n-1)}) \circ \alpha \text{ (Definition)} \\
&= \alpha \circ (\alpha^{(n-1)} \circ \alpha) \text{ (Assoziativität von } \circ) \\
&= \alpha \circ (\alpha^{n-1} \circ \alpha) \text{ (Induktionsvoraussetzung)} \\
&= \alpha \circ \alpha^n \text{ (Definition)} \\
&= \alpha \circ \alpha^{(n)} \text{ (Induktionsvoraussetzung)} \\
&= \alpha^{(n+1)} \text{ (Definition)}
\end{aligned}$$

Wenn wir diesen Beweis analysieren, finden wir zwei Variationen des Induktionsprinzips: Erstens der Induktionsschritt geht nicht durch für $n = 1$, denn $1 - 1$ ist nicht definiert. Zweitens haben wir die Induktionsvoraussetzung nicht nur für n benutzt sondern auch für $n - 1$. Um dies zu beheben beweisen wir die Aussage

$$A(n) : \alpha^n = \alpha^{(n)} \wedge \alpha^{n+1} = \alpha^{(n+1)}$$

Dann ist $A(1)$ klar.
Der Induktionsschluss geht i.w. wie oben: $A(n) \Rightarrow A(n+1)$:
Es ist klar, dass $A(n) \Rightarrow \alpha^{n+1} = \alpha^{(n+1)}$. Es genügt also zu zeigen, dass $A(n) \Rightarrow \alpha^{n+2} = \alpha^{(n+2)}$ und dies geht wie oben, wobei n durch $n+1$ ersetzt wird.

Bemerkung 5.8. *Ist α injektiv, so auch α^n injektiv für jedes $n \in \mathbb{N}$, wie man sehr leicht durch Induktion einsieht, da die Komposition injektiver Abbidlungen wieder injektiv ist.*

Bemerkung 5.9. *Wir definieren die Addition natürlicher Zahlen*

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, (n, m) \mapsto \nu^m(n) =: n + m$$

Es gilt für alle $n, m \in \mathbb{N}$ $(n + m) + 1 = n + (m + 1)$, denn für $n, m \in \mathbb{N}$ ist $(n + m) + 1 = \nu(\nu^m(n)) = \nu^{m+1}(n) = n + (m + 1)$.

Lemma 5.10. *Sie $\alpha : M \to M$ eine Abbildung und $m, n \in \mathbb{N}$. Dann gilt:*
1.) $\alpha^{n+m} = \alpha^m \circ \alpha^n$.
2.) $\alpha^{n+m} = \alpha^n \circ \alpha^m$.

Beweis. 1.) Induktion nach m (für alle $n \in \mathbb{N}$).
Als $A(m) :=$ für alle $n \in \mathbb{N}$ gilt $\alpha^{n+m} = \alpha^m \circ \alpha^n$.
$A(1)$: Ist in Bemerkung 5.7 gezeigt worden.
$A(m) \Rightarrow A(m+1)$:

$$\begin{aligned}
\alpha^{n+(m+1)} &= \alpha^{(n+m)+1} \text{ (Bemerkung 5.9)} \\
&= \alpha \circ \alpha^{(n+m)} \text{ (Beispiel 5.7)} \\
&= \alpha \circ (\alpha^m \circ \alpha^n) \text{ (Induktionsvoraussetzung)} \\
&= (\alpha \circ \alpha^m) \circ \alpha^n \text{ (Assoziativität)} \\
&= \alpha^{m+1} \circ \alpha^n \text{ (Beispiel 5.7)}
\end{aligned}$$

2.) Sehr einfache Übung. q.e.d.

Die gerade eingeführte Addition hat eine Reihe wichtiger Eigenschaften.

Satz 5.11. *1.) (Assoziativgesetz) Für alle $a, b \in \mathbb{N}$ gilt*

$$a + (b + n) = (a + b) + n \text{ für alle } n \in \mathbb{N}.$$

2.) (Kommutativgesetz der Addition) Für alle $a, n \in \mathbb{N}$ gilt:

$$a + n = n + a.$$

3.) (Additives Kürzen) Für $a, b, n \in \mathbb{N}$ gilt: Aus $a + n = b + n$ folgt $a = b$.

Beweis. 1.) Wir zeigen $a + (b + n) = (a + b) + n$ für alle $n \in \mathbb{N}$. Aber dies ist folgt aus Lemma 5.10 1:

$$(a + b) + n = \nu^n(a + b) = (\nu^n \circ \nu^b)(a) = \nu^{b+n}(a) = a + (b + n).$$

2.) $a + 1 = 1 + a$ für alle $a \in \mathbb{N}$ beweist sich durch Induktion mit Hilfe von 1. Nun folgt der allgemeine Fall aus Lemma 5.10:

$$(a + n) + 1 = 1 + (a + n) = \nu^{a+n}(1) = \nu^{n+a}(1) = 1 + (n + a) = (n + a) + 1$$

Der Vergleich des ersten und letzten Ausdruck liefert wegen der Injektivität der Nachfolgerfunktion $a + n = n + a$.
3.) ν ist injektiv, also auch ν^n (Beweis durch Induktion über n). Nun ist $\nu^n(a) = a + n$ also $a + n = b + n$ genau dann wenn $\nu^n(a) = \nu^n(b)$ genau dann wenn $a = b$ wegen der Injektivität von ν^n. q.e.d.

5.2 Anordnung der natürlichen Zahlen

Eng mit der Addition ist die Anordnung der natürlichen Zahlen verbunden.

Definition 5.12. *Auf $\mathbb{N}$ ist eine Relation, genannt* **Kleiner-Relation**, *in Zeichen $<$, festgelegt durch*

$$\{(a, b) \in \mathbb{N} \times \mathbb{N} | b \in \text{Bild}(\nu^a)\}.$$

$a < b$ wird gelesen als a kleiner b.

Lemma 5.13. *1) Für $a, b \in \mathbb{N}$ gilt: $a < b$ genau dann, wenn ein $c \in \mathbb{N}$ existiert mit $a + c = b$. Wir schreiben $c = b - a$, denn dieses c ist eindeutig bestimmt.*
2) Für alle $a \in \mathbb{N}$ ist $\mathbb{N} \setminus \text{Bild}(\nu^a) = \underline{a}$.
3) $<$ ist transitiv, d.h. ist $a < b$ und $b < c$ so ist $a < c$.

Beweis. 1.) $a < b$ genau dann, wenn $b \in \text{Bild}(\nu^a)$, also genau dann wenn ein $c \in \mathbb{N}$ existiert mit $b = \nu^a(c) = c + a = a + c$. Dieses c ist eindeutig, da ν^a injektiv ist.
2.) Induktion nach a. $a = 1$ nach Peano 1). Ist jetzt $\mathbb{N} \setminus \text{Bild}(\nu^a) = \underline{a}$, so ist

$$\nu(\mathbb{N}) \setminus \text{Bild}(\nu^{a+1}) = \nu(\mathbb{N} \setminus \text{Bild}(\nu^a)) = \{1 + 1, 2 + 1, \ldots, a + 1\}$$

Also $\mathbb{N} \setminus \text{Bild}(\nu^{a+1}) = \underline{a+1}$.
3.) Ist $a < b$ und $b < c$ so gibt es $x, y \in \mathbb{N}$ mit $b = \nu^a(x)$ und $c = \nu^b(y) = \nu^y(b)$. Dann ist

$$c = \nu^y(b) = \nu^y(\nu^a(x)) = \nu^{y+a}(x) = \nu^a(\nu^y(x))$$

und daher $c \in \text{Bild}(\nu^a)$ also $a < c$. q.e.d.

Hier sind die wichtigsten Eingenschaften der Kleinerrelation.

Satz 5.14. *1.)* $\mathbb{N}$ *ist durch* $<$ **total geordnet**, *d. h., für je zwei* $a, b \in \mathbb{N}$ *gilt genau eines von* $a < b, a = b$ *oder* $b < a$.
Kommentar: Im letzten Fall schreibt man auch $a > b$, *lies a größer b. Die ersten beiden Fälle faßt man zusammen durch* $a \leq b$, *lies a kleiner oder gleich b, die letzten beiden durch* $a \geq b$, *lies a größer oder gleich b.*
2.) $\mathbb{N}$ *ist durch* $<$ **wohlgeordnet**, *d. h., für jede nicht leere Teilmenge* $M \subseteq \mathbb{N}$ *existiert ein eindeutiges* $a \in M$ *mit*

$$a \leq m \text{ für alle } m \in M.$$

Man nennt a das **Minimum** *von M, kurz* $a = \min(M)$.
3.) $<$ *ist mit der Addition verträglich, d. h. für alle* $a, b, c \in \mathbb{N}$ *gilt:* $a < b$ *genau dann, wenn* $a + c < b + c$ *ist.*

Beweis. 1.) Angenommen $a \not< b$, also $b \in \mathbb{N} - \nu^a(\mathbb{N}) = \{1, 2, \ldots, a\} = \underline{a}$. Dann gilt $a = b$ oder $a \in \text{Bild}(\nu^b)$ also $b \leq a$.
2.) Sei $m \in M$. Falls $m = 1$, sind wir fertig. Sonst ist $\{x \in M | x \leq m\} \subseteq \underline{m}$ endlich. Wegen 1.) gibt es ein eindeutig bestimmtes kleinstes Element in dieser Menge (Induktion). Wegen 1.) erfüllt dieses kleinste Element a dann aber auch $a \leq m$ für alle $m \in M$.
3.) Es ist $a < b$ genau dann wenn ein $x \in \mathbb{N}$ existiert mit $\nu^a(x) = b$. Wir wenden die injektive Abbildung ν^c auf diese Gleichung an und erhalten

$$\nu^a(x) = b \Leftrightarrow \nu^c(\nu^a(x)) = \nu^c(b) \Leftrightarrow \nu^{a+c}(x) = b + c$$

q.e.d.

Übung: Zeige $\leq$ ist eine **partielle Ordung** auf $\mathbb{N}$, d. h. $\leq$ ist transitiv, reflexiv und **antisymmetrisch**, wobei letzteres bedeutet: $a \leq b$ und $b \leq a$ impliziert $a = b$. Man beachte, dass die Mengeninklusion ebenfalls eine partielle Ordnung ist, und zwar auf $\text{Pot}(M)$ für jede Menge $M \neq \emptyset$. Sobald aber M mehr als ein Element enthält, ist es keine totale Ordnung mehr.

Die Wohlordnung auf $\mathbb{N}$ erlaubt eine weitere Umformulierung des Induktionsprinzips:

Folgerung 5.15. *(***Prinzip des kleinsten Verbrechers***) Für jedes* $n \in \mathbb{N}$ *sei* $A(n)$ *eine Aussage. Sei*

$$M := \{n \in \mathbb{N} | A(n) \textit{ falsch}\} \subseteq \mathbb{N}$$

Wir wollen zeigen, dass $M = \emptyset$ *und führen* $M \neq \emptyset$ *zu einem Widerspruch, indem wir zeigen, dass M kein kleinstes Element besitzt.*

Beispiel. Wir zeigen, dass $\varphi : \mathrm{Pot}_{endl}(\mathbb{N}_0) \to \mathbb{N}_0, T \mapsto \sum_{i=0}^{\infty} \chi_T(i)2^i$ surjektiv ist. D.h. $A(n)$ is die Aussage: Es gibt eine endliche Teilmenge T von $\mathbb{N}_0$, so dass $\sum_{i\in T} 2^i = n$ ist. Sei $M := \{n \in \mathbb{N}_0 \mid A(n) \text{ ist falsch }\}$. Ist $M \neq \emptyset$, so hat M ein kleinstes Element, dieses nennen wir m_0. Es ist $m_0 \neq 0$, denn $\sum_{i\in\emptyset} 2^i = 0$, also $0 = \varphi(\emptyset)$. Unterscheide die beiden Fälle: $m_0 = 2m$ gerade und $m_0 = 2m + 1$ ungerade.
Ist $m_0 = 2m$, so ist wegen $m_0 \neq 0$ das $m < m_0$ und da m_0 minimal ist gibt es eine endliche Teilmenge T von $\mathbb{N}_0$ mit

$$\sum_{i\in T} 2^i = m.$$

Sei $S := \{i + 1 \mid i \in T\}$. Dann ist

$$\sum_{i\in S} 2^i = \sum_{i\in T} 2^{i+1} = 2m = m_0$$

ein Widerspruch.
Ist $m_0 = 2m+1$ so ist ebenfalls $m \in \mathbb{N}_0$ und $m < m_0$. Also gibt es ein T mit $\sum_{i\in T} 2^i = m$. Setze nun $S := \{i + 1 \mid i \in T\} \cup \{0\}$ um den entsprechenden Widerspruch zu erhalten.

Es gibt noch eine Variante der vollständigen Induktion, die hierhin gehört, welche schon in Beispiel 5.7 angekündigt wurde und die wir als Übungsaufgabe lassen:

Bemerkung 5.16. *Für jedes $n \in \mathbb{N}$ sei $A(n)$ eine Aussage. Gilt der*
Induktionsanfang: $A(1)$
und der
Induktionsschluss: $A(i)$ *für alle* $i \leq n$ *impliziert* $A(n + 1)$ *für alle* $n \in \mathbb{N}$,
so gilt $A(n)$ *für alle* $n \in N$.

Beweis. Übung. q.e.d.

Nachtrag der fehlenden Beweise aus Abschnitt 3:
Satz 3.6: Ist $\mathcal{M}$ eine Menge von endlichen Mengen, so ist $|\cdot| : \mathcal{M} \to \mathbb{N} \cup \{0\}, X \mapsto |X|$ eine wohldefinierte Abbildung.
Erinnerung: Eine Menge X heißt **endlich**, falls eine Zahl $n \in \mathbb{N} \cup \{0\}$ und eine Bijektion $\zeta : \underline{n} \to X$ existieren. Dann nennt man $|X| := n$ die Anzahl der Elemente von X.
Beweis von Satz 3.6: (a) Seien $n, m \in \mathbb{N}$. Falls eine Bijektion $\varphi : \underline{n} \to \underline{m}$ existiert, gilt $n = m$.
Angenommen die Behauptung ist falsch für ein $n \in \mathbb{N}$. Dann ist sicherlich $n > 1$. Sei $n = n_0$ minimal in der Menge aller $n \in \mathbb{N}$ für die eine Bijektion $\varphi : \underline{n} \to \underline{m}$ mit $n \neq m$. Die Einschränkung von φ auf $\underline{n-1}$ ist bijektiv von $\underline{n-1}$ auf $\underline{m} - \{\varphi(n)\}$. Setze

$$\rho : \underline{m} - \{\varphi(n)\} \to \underline{m-1} : a \mapsto \begin{cases} a & \text{falls } a < \varphi(n) \\ a - 1 & \text{falls } a > \varphi(n) \end{cases},$$

sodass $\rho \circ \varphi_{|\underline{n-1}} : \underline{n-1} \to \underline{m-1}$ bijektiv ist, also $n - 1 = m - 1$, d. h. $n = m$, ein Widerspruch.
(b) Sei nun X eine endliche Menge, $n, m \in \mathbb{N}$ und $\zeta : \underline{n} \to X$ sowie $\zeta' : \underline{m} \to X$ Bijektionen. Dann ist auch $\zeta^{-1} \circ \zeta' : \underline{m} \to \underline{n}$ bijektiv, also $n = m$.
Ende der 8. Vorlesung, am 6.11.2013
Lemma. Ist M eine unendliche Menge, so gibt es eine injektive Abbildung $\mathbb{N} \to M$.

Beweis. Übung q.e.d.

Satz 3.20 Sei M eine Menge. Folgende Aussagen sind äquivalent:
1) M ist endlich.
2) Jede injektive Abbildung $\eta : M \to M$ von M in sich ist auch surjektiv.
3) Jede surjektive Abbildung $\tau : M \to M$ von M auf sich ist auch injektiv.

Beweis. 1) $\Rightarrow$ 2) Sei $|M| = n$ und $\zeta : \underline{n} \to M$ eine Abzählung, also eine Bijektion. Ist $\eta : M \to M$ injektiv, so auch $\eta \circ \zeta : \underline{n} \to M$. Also ist $\eta \circ \zeta : \underline{n} \to \eta(M)$ bijektiv und somit $|\eta(M)| = n = |M|$, d. h. $\eta(M) = M$ und η ist surjektiv.
2) $\Rightarrow$ 3) Ist $\tau : M \to M$ surjektiv, so hat τ nach 3.18 ein Rechtsinverses η, welches injektiv ist. Gemäß der Voraussetzung 2) ist η dann aber auch surjektiv, d. h. bijektiv. Also ist klar, dass τ die inverse Abbildung von η ist und somit injektiv. (Man hätte auch wieder mit 3.18 schließen können.)
3) $\Rightarrow$ 1) Wir zeigen, dass die Negierung von 1) die Negierung von 3) impliziert. M nicht endlich. Dann gibt es eine injektive Abbildung $f : \mathbb{N} \to M$, also eine Folge $f_1, f_2, \ldots$ mit $f_i \neq f_j$ für $i \neq j, f_i \in M$. Wir benutzen diese Folge, um eine surjektive, nicht injektive Abbildung von $\mathbb{N}$ auf M zu übertragen. Klar:

$$a : \mathbb{N} \to \mathbb{N} : i \mapsto \begin{cases} i-1 & i > 1 \\ 1 & i = 1 \end{cases}$$

ist eine solche Abbildung. Als surjektive, nicht injektive Abbildung von M auf sich bietet sich also an:

$$\tau : M \to M : m \mapsto \begin{cases} f_{i-1} & m = f_i \text{ für ein } i > 1 \\ f_1 & m = f_1 \\ m & m \notin f(\mathbb{N}) \end{cases} .$$

Es ist klar, dass diese Abbildung wohldefiniert, surjektiv und nicht injektiv ist. q.e.d.

5.3 Das allgemeine Assoziativgesetz

Hat man Summen von mehr als zwei Summanden, so gibt es mehrere Möglichkeiten zu klammern. Dass dies in Anwesenheit des Assoiativgesetzes keine Rolle spielt, wollen wir im Rahmen der Einführung des Summenzeichens bzw. Produktzeichens sehen.

Definition 5.17. *Sei M eine nicht leere Menge mit einer Verknüpfung $+ : M \times M \to M$. Für jede Folge $a = (a_n)_{n\in\mathbb{N}} : \mathbb{N} \to M$ definiert man die zugehörige* **Summe***nfolge oder* **Reihe** *$(\sum_{i=1}^{n} a_i)_{n\in\mathbb{N}}$ rekursiv durch*

$$\sum_{i=1}^{1} a_i := a_1 \text{ und } \sum_{i=1}^{n+1} a_i := (\sum_{i=1}^{n} a_i) + a_{n+1}.$$

Das n-te Glied der Summenfolge heißt die **Summe** *der a_i von $i = 1$ bis n. Entsprechend heißt das n-te Glied der Summenfolge zu $a \circ \nu^k$ die Summe $\sum_{i=k+1}^{n+k} a_i$ der a_i von $i = k+1$ bis $n + k$.*
Wird die Verknüpfung multiplikativ, also als $\cdot : M \times M \to M$, geschreiben, so schreibt man $\prod$ statt $\sum$ und spricht von der **Produktfolge**, *und das n-te Glied der Produktfolge heißt das* **Produkt** *der a_i von $i = 1$ bis n.*

Man beachte, dass der Wahl des Namens Summe oder Produkt nur mit der Wahl des Namens der Verknüpfung zu tun hat, nicht jedoch mit den Eigenschaften der Verknüpfung. Entsprechend git der nächste Satz auch in der multikplikativen Notation, obwohl wir ihn nur additiv aussprechen.

Satz 5.18. *(**Allgemeines Assoziativgesetz**). Sei M eine nicht leere Menge mit einer assoziativen Verknüpfung $+ : M \times M \to M$. Für jede Folge $a = (a_n)_{n\in\mathbb{N}} : \mathbb{N} \to M$ und jedes $k, n \in \mathbb{N}$ mit $1 \leq k < n$ gilt:*

$$\sum_{i=1}^{k} a_i + \sum_{i=k+1}^{n} a_i = \sum_{i=1}^{n} a_i,$$

Beweis. Induktion nach $n > k$ bei festem k. Der Induktionsanfang $n = k + 1$ ist die Defintion des Summenzeichens. Induktionsannahme:

$$(\sum_{i=1}^{k} a_i) + (\sum_{i=k+1}^{n} a_i) = \sum_{i=1}^{n} a_i,$$

Dann gilt:

$$\begin{aligned}
\sum_{i=1}^{k} a_i + \sum_{i=k+1}^{n+1} a_i &= \sum_{i=1}^{k} a_i + ((\sum_{i=k+1}^{n} a_i) + a_{n+1}) \\
&= (\sum_{i=1}^{k} a_i + \sum_{i=k+1}^{n} a_i) + a_{n+1} \\
&= (\sum_{i=1}^{n} a_i) + a_{n+1} \\
&= \sum_{i=1}^{n+1} a_i
\end{aligned}$$

q.e.d.

Also bei assoziativen Verknüpfungen kann man die Klammern auch weglassen. Das allgemeine Kommutativgesetz ist erheblich anspruchvoller zu beweisen. Wir formulieren es ohne Beweis.

Satz 5.19. *(**Allgemeines Kommutativgesetz**). Sei M eine nicht leere Menge mit einer assoziativen und kommutativen Verknüpfung $+ : M \times M \to M$. Für alle $n \in \mathbb{N}$ und jedes n-Tupel $(a_1, \ldots, a_n) \in M^n$ und jede Bijektion $\sigma : \underline{n} \to \underline{n}$ gilt:*

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} a_{\sigma(i)}$$

5.4 Produkt und Potenzen natürlicher Zahlen

Nach diesem allgemeinen Exkurs kommen wir wieder zu den Verknüpfungen natürlicher Zahlen.

Definition 5.20. *Das* **Produkt** *natürlicher Zahlen ist definiert als Verknüpfung*

$$\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (n, m) \mapsto n \cdot m := nm := \sum_{i=1}^{n} m$$

(wobei wir also von der konstanten Folge mit $a_i = m$ ausgehen).

Satz 5.21. *Für alle $m, m', n, o \in \mathbb{N}$ gilt:*
0.) (Einselement) $1 \cdot n = n \cdot 1 = n$.
1.) (Distributivgesetz) $(m + m')n = mn + m'n$.
2.) (Kommutativgesetz) $mn = nm$.
3.) (Assoziativgesetz) $(mn)o = m(no)$.
4.) (Kürzen) Aus $mn = m'n$ folgt $m = m'$.
5.) $m < m'$ impliziert $mn < m'n$.

Beweis. 0.) Sofort klar.
1,) Sofort aus dem allgemeinen Assoziativgesetz 5.18 für Addition.
Denn $(m + m')n = \sum_{i=1}^{m+m'} n = \sum_{i=1}^{m} n + \sum_{j=m+1}^{m+m'} n = \sum_{i=1}^{m} n + \sum_{j=1}^{m'} n = mn + m'n$.
2.) Induktion nach m.
Sei $A(m)$ die Aussage, für alle $n \in \mathbb{N}$ gilt $mn = nm$. Dann ist $A(1)$ richtig wegen 0. Für den Induktionsschluss rechnen wir

$$(m+1)n \overset{1}{=} mn + 1n \overset{0,IV}{=} nm + n1 = \sum_{i=1}^{n} m + \sum_{i=1}^{n} 1 \overset{5.19}{=} \sum_{i=1}^{n} (m+1) = n(m+1).$$

3.) Induktion nach m unter Benutzung von 1.) (Übung).
4.) folgt aus 5.), denn sei $mn = m'n$. Dann gilt entweder $m < m'$ und dann mit 5.) auch $mn < m'n$, oder $m > m'$ und dann auch $mn > m'n$ wegen 5.) oder $m = m'$. Da die ersten beiden Möglichkeiten auf einen Widerspruch führen gilt also $m = m'$.
5.) Interessanterweise scheint 4.) nicht so leicht, wenn überhaupt durch Induktion nach n beweisbar. Dieses ist das erste Mal, dass Sie das Phänomen sehen, dass eine stärkere Behauptung durch Induktion beweisbar ist, eine schwächere daraus folgende jedoch nicht, eben weil die Induktionsvoraussetzung zu schwach für den Induktionsschritt wird.
Sei $A(n)$ die Aussage $m < m' \Rightarrow nm < nm'$.
Dann gilt $A(1)$ trivialerweise (wegen 0).
Für den Induktionsschluss bemerken wir

$$\begin{aligned}(n+1)m &= \textstyle\sum_{k=1}^{n+1} m = \sum_{k=1}^{n} m + m = nm + m \quad (IV)\\ &< nm' + m < nm' + m' = \textstyle\sum_{k=1}^{n} m' + m' = sum_{k=1}^{n+1} m' = (n+1)m'\end{aligned}$$

wobei wir benutzt haben, dass für $a, b, c \in \mathbb{N}$ gilt $a < b$ genau dann wenn $a + c < b + c$, das war Satz 5.14 3). q.e.d.

Übung: Sei M eine nicht leere Menge und $\alpha : M \to M$. Zeige für $n, m \in \mathbb{N}$ gilt:

$$\alpha^{mn} = (\alpha^m)^n$$

Definition 5.22. *Das* **Potenzieren** *natürlicher Zahlen ist definiert als*

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N} : (n, m) \mapsto n^m := \prod_{i=1}^{m} n$$

Der Übergang von der Multiplikation zum Potenzieren ist sehr anlog zu dem Übergang von der Addition zur Multiplikation. Der folgende Satz sollte also in Analogie zu Satz 5.21 gesehen werden, ebenso wie sein Beweis. Man beachte aber. dass diese Analogie nicht zu weit geht, denn man hat kein Kommutativgesetz mehr, wie der erste Teil zeigt.

Satz 5.23. *Für alle $m, m', n, o \in \mathbb{N}$ gilt:*
1.) $m^1 = m$ *und* $1^m = 1$.
2.) $n^{m+m'} = n^m \cdot n^{m'}$
3.) $(mm')^n = m^n \cdot (m')^n$.
4.) $(n^m)^{m'} = n^{m \cdot m'}$.

Beweis. 1.) Klar.
2.) Sofort aus dem allgemeinen Assoziativgesetz 5.18 für Multiplikation.
3.) Übung aus dem Kommutativgesetz für Multiplikation.
4.) Übung. q.e.d.

Übung: Was ist zur Verträglichkeit der Kleiner-Relation mit dem Potenzieren zu sagen und zu beweisen?

Um in Zukunft lästige Fallunterscheidungen zu vermeiden, setzen wir unsere Verknüpfungen von $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ auf $\mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ in bekannter Weise fort, so dass die diversen Regeln gültig bleiben. Das einzige, was verboten ist, ist den Ausdruck 0^0 zu bilden, also Potenzieren ist nur definiert als Abbildung $\mathbb{N}_0 \times \mathbb{N}_0 - \{(0,0)\} \to \mathbb{N}_0$. Um dies zu beheben definieren wir $0^0 := 1$.
Ende der 9.Vorlesung am 12.11.2013

5.5 Wichtige Folgen natürlicher Zahlen (10.Vorlesung)

Lernziel: Formeln für wichtige Anzahlen, Binomialkoeffizienten, Abbildungen mit konstanter Fasergröße.
Übung: Seien M, N endliche Mengen mit m bzw. n Elementen, $m, n \in \mathbb{N}$. Dann gibt es eine Bijektion $N^M \to \underline{n}^{\underline{m}}$, die Injektivität, Surjektivität und Bijektivität respektiert. Hinweis: Geh von Bijektionen $M \to \underline{m}$ und $N \to \underline{n}$ aus und betrachte das Diagramm

$$\begin{array}{ccc} M & \to & N \\ \downarrow & & \downarrow \\ \underline{m} & \to & \underline{n} \end{array} .$$

Wir werden dies als Rechtfertigung nehmen, wenn wir mit den konkreten endlichen Mengen $\underline{m}$ statt mit abstrakten endlichen Mengen arbeiten. Die wichtigsten Folgen natürlicher Zahlen haben meistens einen kombinatorischen Hintergrund. Sie tauchen in unterschiedlichen Zusammenhängen immer wieder auf.

Definition 5.24. *1.) Sei* $0! := 1$ *und* $n! := (n-1)! \cdot n$ *für alle* $n \in \mathbb{N}$. *Das Folgenglied* $n!$ *heißt die* n-**Fakutät** *oder* **Fakultät** *von* n.
2.) Die Menge der bijektiven Abbildungen von M *in sich wird mit* S_M, *auch* **symmetrische Gruppe** *auf* M *genannt, bezeichnet. Statt* $S_{\underline{n}}$ *schreibt man* S_n *für* $n \in \mathbb{N}$.
3.) Für Mengen M, N *bezeichne* $(N^M)_{inj}$ *bzw.* $(N^M)_{surj}$ *die Menge der injektiven bzw. surjektiven Abbildungen von* M *nach* N

Der Name symmetrische Gruppe spielt darauf an, dass mit Komposition und Invertieren zwei Verknüpfungen auf S_M definiert sind, die den sogenannten Gruppenaxiomen genügen. Davon werden wir aber erst später hören.

Satz 5.25. *1.) Für* $n \in \mathbb{N}$ *gilt:* $|S_n| = n!$.
2.) Für $n, m \in \mathbb{N}$ *gilt* $|\underline{n}^{\underline{m}}| = n^m$.
3.) Für $n, m \in \mathbb{N}$ *mit* $n \leq m$ *gilt*

$$(\underline{m}^{\underline{n}})_{inj} = m(m-1)\cdots(m-n+1) = \prod_{i=0}^{n-1}(m-i)$$

Beweis. 1.) Zunächst ein etwas volkstümlicher Beweis oder eine Plausibilitätsbetrachtung, die wir dann zu einem richtigen Beweis umformulieren wollen: Sei $f \in S_n$. Für $f(1)$ hat man n Möglichkeiten. Nachdem $f(1)$ festgelegt ist, hat man für $f(2)$ noch $n-1$ Möglichkeiten, also insgesamt $n(n-1)$ Möglichkeiten. Danach bleiben für $f(3)$ noch $n-2$ Möglichkeiten etc.. Am Ende haben wir $|S_n| = n!$.
Der allgemeine Beweis ergibt sich als Spezialfall aus 3.).
2.) Vollständige Induktion mit Hilfe von Satz 3.12,der besagt, dass $N^{S \uplus T}$ und $N^S \times N^T$ gleichviele Elemente enthalten.
3.) Die Formel ist klar für $n = 1$. Betrachte

$$\epsilon : (\underline{m}^{\underline{n}})_{inj} \to (\underline{m}^{\underline{n-1}})_{inj} : f \mapsto f_{|\underline{n-1}}.$$

Dies ist eine surjektive Abbildung. Es ist nämlich sogar so, dass jede Abbildung $\varphi \in (\underline{m}^{\underline{n-1}})_{inj}$ sich auf genau $m-(n-1) = |\underline{m} - \mathrm{Bild}(\varphi)|$ Arten sich zu einer injektiven Abbildung $\underline{n} \to \underline{m}$ fortsetzen lässt. Da jede Abbildung sich in genau einer Faser von ϵ befindet, jede Faser $m-(n-1)$ Elemente enhält und die Induktionsvoraussetzung die Anzahl der Fasern liefert, folgt die Behauptung, indem wir das Produkt nehmen. q.e.d.

Man darf es mit den Formeln allein nicht bewenden lassen, sondern soll sich zumindest durch Betrachtung der Anfangsglieder einen Eindruck über Größenordnung und Wachstum der Folgen bzw. Doppelfolgen verschaffen. Ich lasse es in diesem Stadium als Übung.

Man vermisst im letzten Satz sicherlich eine Aussage über die Anzahl der surjektiven Abbildungen. Diese ist nicht ganz so einfach. Wir werden in einem Wiederholungskapitel, wo wir uns mehr auf die Kombinatorik konzentrieren werden, zurückkommen.

Definition 5.26. *Die* **Binomialkoeffizient***en sind als Glieder der Doppelfolge*

$$\mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0 : (n,k) \mapsto \binom{n}{k} := \begin{cases} 0 & \text{falls } k > n \\ \frac{n!}{k!(n-k)!} & \text{sonst} \end{cases}$$

definiert.

Achtung: Wir werden gleich sehen, dass $\frac{n!}{k!(n-k)!} \in \mathbb{N}_0$ ist für alle $n, k \in \mathbb{N}_0$. Genau genommen haben wir $\frac{a}{b}$ für beliebige $a, b \in \mathbb{N}_0$ noch nicht definiert. Ist jedoch $b \neq 0$ und gibt es ein $c \in \mathbb{N}_0$ mit $bc = a$, so ist dieses c eindeutig bestimmt und wird mit $c = \frac{a}{b} \in \mathbb{N}_0$ bezeichnet.
Erinnerung: Für eine Menge M und $k \in \mathbb{N}_0$ bezeichnet $\mathrm{Pot}_k(M) := \{T \subseteq M \mid |T| = k\}$ die Menge der k-elementigen Teilmengen von M.

Satz 5.27. *Für $n, k \in \mathbb{N}_0$ gilt:*

$$|\operatorname{Pot}_k(\underline{n})| = \binom{n}{k}.$$

Insbesondere ist $\binom{n}{k} \in \mathbb{N}_0$ für alle $n, k \in \mathbb{N}_0$ und somit sind die Binomialkoeffizienten wohldefiniert.

Beweis. Definiere

$$\varphi : (\underline{n}^k)_{inj} \to \operatorname{Pot}_k(\underline{n}) : \varphi((a_1, \ldots, a_k)) := \{a_1, \ldots, a_k\}.$$

Dann ist φ surjektiv. Die Faser von $\{a_1, \ldots, a_k\}$ ist

$$\begin{aligned} \varphi^{-1}(\{\{a_1, \ldots, a_k\}\}) &= \{(b_1, \ldots, b_k) \in \underline{n}^{\underline{k}} \mid \{b_1, \ldots, b_k\} = \{a_1, \ldots, a_k\}\} \\ &= \{(a_{\pi(1)}, \ldots, a_{\pi(k)}) \mid \pi \in S_k\} \end{aligned}$$

Also ist $|\varphi^{-1}(\{\{a_1, \ldots, a_k\}\})| = |S_k| = k!$ für beliebiges $\{a_1, \ldots, a_k\} \in \mathrm{Pot}_k(\underline{n})$. Da $(\underline{n}^k)_{inj}$ die disjunkte Vereinigung der Fasern von φ ist gilt

$$|(\underline{n}^k)_{inj}| = |\operatorname{Pot}_k(\underline{n})| \cdot k!$$

also

$$|\operatorname{Pot}_k(\underline{n})| = \frac{|(\underline{n}^k)_{inj}|}{k!} = \binom{n}{k}.$$

q.e.d.

Satz 5.28. *(einige Identitäten für Binomialkoeffizienten) Seien $k, n \in \mathbb{N}_0$ mit $k \leq n$.*
(a) $\binom{n}{k} = \binom{n}{n-k}$.
(b) $k\binom{n}{k} = n\binom{n-1}{k-1}$.
(c) $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$. *(Additionstheorem der Binomialkoeffizienten)*
(d) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Beweis. (a) direkt aus der Definition oder aber auch: Die Komplementabbildung

$$C_{n,k} : \mathrm{Pot}_k(\underline{n}) \to \mathrm{Pot}_{n-k}(\underline{n}) : M \mapsto \underline{n} \setminus M$$

ist eine Bijektion (die Umkehrabbildung ist wieder $C_{n,n-k}$).
(b) Das kann man auch direkt nachrechnen aber auch hier steckt wieder eine Bijektion dahinter: Sei

$$X := \{(a, M) \mid a \in M, M \in \mathrm{Pot}_k(\underline{n})\}$$

und

$$Y := \{(a, N) \mid a \in \underline{n}, N \subseteq \underline{n} \setminus \{a\}, |N| = k - 1\}.$$

Dann ist $|X| = k\binom{n}{k}$ und $|Y| = n\binom{n-1}{k-1}$. Die Abbildung

$$\varphi : X \to Y : (a, M) \mapsto (a, M \setminus \{a\})$$

ist eine Bijektion mit Umkehrabbildung

$$\varphi^{-1} : Y \to X : (a, N) \mapsto (a, N \cup \{a\}).$$

Also $|X| = |Y|$.
(c) Ebenfalls durch Nachrechnen oder besser: Die Abbildung

$$\varphi : \mathrm{Pot}_k(\underline{n+1}) \to \mathrm{Pot}_k(\underline{n}) \uplus \mathrm{Pot}_{k-1}(\underline{n}) : M \mapsto \begin{cases} M & n+1 \notin M \\ M \setminus \{n+1\} & n+1 \in M \end{cases}$$

ist eine Bijektion. Also

$$\binom{n+1}{k} = |\mathrm{Pot}_k(\underline{n+1})| = |\mathrm{Pot}_k(\underline{n}) \uplus \mathrm{Pot}_{k-1}(\underline{n})| = \binom{n}{k} + \binom{n}{k-1}.$$

(d) Es ist

$$\mathrm{Pot}(\underline{n}) = \biguplus_{k=0}^{n} \mathrm{Pot}_k(\underline{n})$$

also wegen $|\mathrm{Pot}(\underline{n})| = |\{0,1\}^n|$ folgt

$$2^n = |\mathrm{Pot}(\underline{n})| = \sum_{k=0}^{n} |\mathrm{Pot}_k(\underline{n})| = \sum_{k=0}^{n} \binom{n}{k}.$$

q.e.d.

Beispiel. Definiere die aufsteigende Mengenfolge durch

$$\mathrm{Pot}^1(\emptyset) := \mathrm{Pot}(\emptyset), \mathrm{Pot}^{n+1}(\emptyset) := \mathrm{Pot}(\mathrm{Pot}^n(\emptyset))$$

Offenbar gilt für $a_n := |\mathrm{Pot}^n(\emptyset)|$

$$a_1 = 1, a_{n+1} = 2^{a_n} \text{ also } a_2 = 2, a_3 = 2^2 = 4, a_4 = 2^4 = 16, a_5 = 2^{16} = 65536$$

Zum Vergleich: Die Physiker haben irgendwann einmal die Anzahl der Protonen im Universum auf $136 \cdot 2^{256}$ geschätzt, also eine Zahl, die deutlich kleiner als a_6 ist.

Kapitel 2

Reelle und komplexe Zahlen

In diesem Kapitel wollen wir einerseits axiomatisch die reellen und komplexen Zahlen einführen, ohne einen Existenzbewies zu führen und andererseits geometrisches Verständnis dieser beiden grundlegenden Körper mehr heuristisch erarbeiten.

6 Axiome für Gruppen, Ringe und Körper

Lernziel: Gruppenaxiome und ihre Bedeutung, Rechnen in Körpern im Sinne von Addieren, Subtrahieren, Multiplizieren und Dividieren. Beispiele von Körpern: $\mathbb{Q}, \mathbb{R}, \mathbb{F}_2$.

Eine natürliche Vorgehensweise wäre nach dem vorangegangenen Kapitel, aus den natürlichen Zahlen die ganzen Zahlen, aus diesen die rationalen Zahlen, daraus wieder die reellen Zahlen und schließlich aus diesen wiedrum die komplexen Zahlen zu konstruieren. Wir verschieben diese Konstruktionen auf ein späteres Kapitel und werden die reellen Zahlen axiomatisch einführen, d. h. ein Axiomensystem für sie anzugeben und einfach ihre Existenz zu glauben. Danach geben wir eine Konstruktion der komplexen Zahlen aus den reellen Zahlen an und versuchen eine geometrische Vorstellung dieser beiden Körper zu erzeugen und den Umgang mit ihnen einzuüben.

6.1 Gruppen 11. Vorlesung am 19.11.2013

Jetzt ist der Zeitpunkt gekommen, wo wir erstmalig axiomatisch an unsere Probleme herangehen wollen. Es geht also darum, dass man sich fragt: Was ist der allgemeinste Rahmen für meine Schlüsse und Rechnungen? Kann ich aus einer Rechnung in einer konkreten Situation auf eine allgemeine Vermutung kommen und diese dann durch Übertragung der Schlüsse auch beweisen? Kann ich Analogien zwischen Situationen sehen, wo der Außenstehende keine Gemeinsamkeiten ahnt? Der erste Begriff, den wir kennenlernen wollen, ist der der Gruppe, welcher sich im Laufe des 19. Jahrhunderts herausgebildet hat. Zunächst werden wir ihn nur zur Definition von Zahlbereichen heranziehen, später werden wir sehen, daß er auch außerhalb der Zahlbereiche eine grundlegende Rolle spielt.

Definition 6.1. *Sei G eine nicht leere Menge und $\cdot : G \times G \to G$ eine Verknüpfung auf G.*

(a) Man nennt $(G, \cdot)$ **Gruppe**, *falls* $\cdot$ *folgende drei Axiome erfüllt:*
1) (Assoziativgesetz)

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

für alle $x, y, z \in G$.
2) (Einselement oder neutrales Element) Es existiert ein Element $1 \in G$ *mit*

$$1 \cdot g = g \cdot 1 = g$$

für alle $g \in G$.
Dieses Einselement ist dann eindeutig bestimmt, denn seien 1 und $1'$ zwei Einselemente in G. Dann gilt $1 = 1 \cdot 1' = 1'$.
3) (Inverses Element) Zu jedem $g \in G$ *existiert ein* $g^{-1} \in G$ *mit*

$$g \cdot g^{-1} = g^{-1} \cdot g = 1.$$

Dieses inverse Element ist dann eindeutig bestimmt, denn seien h und h' zwei inverse Elemente zu $g \in G$. Dann gilt

$$h = h \cdot 1 = h(gh') = (hg)h' = 1h' = h'.$$

Oft schreibt man gh *statt* $g \cdot h$.
(b) G *heißt* **abelsche Gruppe** *oder* **kommutative Gruppe** *falls zusätzlich noch das Kommutativgesetz 4) gilt:*
4) (Kommutativgesetz) Für alle $g, h \in G$ *gilt*

$$gh = hg.$$

Bei kommutativen Gruppen wird manchmal $+$ *statt* $\cdot$ *als Verknüpfungssymbol genommen. (Im Unterschied zu* $\cdot$ *läßt man* $+$ *nicht weg.)*
(c) $(G, \cdot)$ *heißt* **Halbgruppe**, *falls 1) erfüllt ist,* **Monoid** *oder* **Halbgruppe mit Eins**, *falls 1) und 2) erfüllt sind.*

Bemerkung: Es gilt $(gh)^{-1} = h^{-1}g^{-1}$.

Beweis: Wir müssen wegen der Eindeutigkeit des Inversen nur zeigen, dass $h^{-1}g^{-1}$ ein Inverses von gh ist.

$$\begin{aligned} (gh)(h^{-1}g^{-1}) &= g(hh^{-1})g^{-1} = gg^{-1} = 1 \\ (h^{-1}g^{-1})(gh) &= h^{-1}(g^{-1}g)h = h^{-1}h = 1 \end{aligned}$$

Möglicherweise haben Sie Schwierigkeiten, sich die Gruppenaxiome zu merken. Vielleicht ist es hilfreich, die drei Axiome in Beziehung zu den drei Axiomen der Äquivalenzrelation zu sehen: Assoziativität entspricht Transitivität, Existenz der Einselementes der Reflexivität und Existenz des Inversen der Symmetrie. Diese Zusammenhänge sind nicht zufällig, aber wir werden sie erst sehr viel später verstehen.

Viele Unterpunkte des folgenden Beispiels benutzen bereits Eigenschaften der reellen Zahlen, die wir nach wie vor als im Prinzip bekannt vorausssetzen.

Beispiele. 1.) Für $(\mathbb{N}, +)$ gilt nur das Assoziativgesetz und das Kommutativgesetz. (Kommutative Halbgruppe).
2.) $(\mathbb{Z}, +)$ ist eine Gruppe.
3.) Da die Komposition von Abbildungen assoziativ ist, ist $(M^M, \circ)$ eine Halbgruppe mit $1 = \mathrm{id}_M$ für jede Menge M. Diese ist nicht kommutativ, sobald M mehr als ein Element enthält. (Nicht kommutatives Monoid)
4.) $(S_M := Sym(M) := \{f \in M^M | f \text{ bijektiv}\}, \circ)$ ist eine Gruppe für jede Menge M. Diese ist nicht kommutativ, sobald M mehr als zwei Elemente enthält. In Falle $M := \underline{n}$ für $n \in \mathbb{N}$ schreibt man S_n statt $S_{\underline{n}}$. Man nennt S_M die **symmetrische Gruppe** auf M.
5.) $\mathbb{R}^2$ eine kommutative Gruppe mit der komponentenweiser Addition: Für $a, b \in \mathbb{R}^2$ definiert man:

$$a + b := (a_1 + b_1, a_2 + b_2)$$

Die Nullabbildung ist immer das neutrale Element oder 0-Element, wie man bei der additiven Sprechweise statt 1-Element sagt.

Bemerkung 6.2. *1.) Für Gruppen gilt das allgemeine Assoziativgesetz nach Satz 5.18.*
2.) Für abelsche Gruppen gilt das allgemeine Kommutativgesetz nach Satz 5.19.
3.) Eine nicht leere Teilmenge H einer Gruppe $(G, \cdot)$ heißt **Untergruppe** *von G, falls*

$$H \cdot H := \{h_1 h_2 | h_1, h_2 \in H\} \subseteq H$$

und

$$H^{-1} := \{h^{-1} | h \in H\} \subseteq H.$$

(Wie sehen diese Bedingungen bei abelschen Gruppen in additiver Schreibweise aus?)
4.) Ist $H \leq G$ Untergruppe von $(G, \cdot)$. Dann definiert $g_1 \sim_H g_2 :\Leftrightarrow g_1^{-1} g_2 \in H$ eine Äquivalenzrelation auf G, auch **Kongruenzrelation** *genannt. Die Kongruenzklassen heißen* **Nebenklassen** *oder* **Restklassen** *nach H und sind von der Form $gH := \{gh | h \in H\}$. (Man verifiziere, dass eine Äquivalenzrelation vorliegt unter dem Gesichtpunkt, wie Gruppen- und Äquivalenzaxiome einander entsprechen.)*

Bemerkung: Ist H Untergruppe von G, kurz $H \leq G$. Dann gilt $1_H = 1_G$, d. h. H hat dasselbe 1-Element wie G, denn 1_G hat sicherlich die Eigenschaften eines Einselements für $H \subseteq G$ und wegen $1_G = hh^{-1}$ für jedes $h \in H$ ist $1_G \in H$.
Beispiele. 1.) $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$. (Die Menge der Restklassen lässt sich anschaulich als Kreis deuten.)
2.) Für $0 \neq a \in \mathbb{R}^2$ ist

$$\{(ra_1, ra_2) | r \in \mathbb{R}\} \leq \mathbb{R}^2$$

eine Gerade durch den Nullpunkt. Die Restklassen sind die hierzu parallelen Geraden.
3.) Für $s, t \in \mathbb{R}$ sei

$$\alpha_{s,t} : \mathbb{R} \to \mathbb{R} : a \mapsto sa + t.$$

Beachte, geometrisch bedeutet $\mathbb{R}$ die Zahlengerade, $\alpha_{s,0}$ ist die **Streckung** der Zahlengerade mit Streckzentrum 0 und Streckfaktor s. Weiter bedeutet $\alpha_{1,t}$ die **Translation** oder Verschiebung der Zahlengeraden um t.
Es gilt $\alpha_{s,t} \in S_{\mathbb{R}}$, falls $s \neq 0$. Genauer

$$\mathrm{Aff}_1(\mathbb{R}) := \{\alpha_{s,t} | s \in \mathbb{R} - \{0\}, t \in \mathbb{R}\} \leq S_{\mathbb{R}}.$$

Zum Beweis der letzten Behauptung, beachte

$$\alpha_{s',t'} \circ \alpha_{s,t} = \alpha_{ss',t'+s't}$$

und

$$\alpha_{s,t}^{-1} = \alpha_{s^{-1},-s^{-1}t}.$$

(Einzelheiten Übung).
Übung: Seien $r_1, r_2 \in \mathbb{R}$ und $q_1, q_2 \in \mathbb{R}$ je zwei verschiedene Punkte. (Wenn man geometrisch denkt, sagt man häufig Punkt statt Element.) Zeige: Es gibt genau ein $\alpha \in \mathrm{Aff}_1(\mathbb{R})$ mit $\alpha(r_i) = q_i$ für $i = 1, 2$. (Man überlege sich, was unsere Gruppe mit der 2-Punkt-Skalierung von Temperaturskalen zu tun hat. Wie sieht z. B. die Umrechnung von Grad Celsius in Grad Fahrenheit.)

Für uns haben Gruppen zweierlei Bedeutung: Sie treten in den nachfolgenden Definitionen von Ringen und Körpern, also Zahlbereichen im weitesten Sinne, wieder auf als Teile der Definitionen. Zweitens haben Gruppen ein Eigenleben, welches fast alle Teile der Mathematik beeinflußt. Auf dieses kommen wir später zurück.

6.2 Ringe 11. Vorlesung am 19.11.2013

Bei den natürlichen Zahlen hatten wir bereits zwei Verknüpfungen, Addition und Multiplikation. Aber erst $(\mathbb{Z}, +, \cdot)$ erfüllt die Ringaxiome, die man braucht, um eine befriedigende Theorie aufzubauen. Ringe spielen sowohl in Algebra, Geometrie als auch Analysis eine grundlegende Rolle.

Definition 6.3. *Sei R eine nicht leere Menge mit zwei (inneren) Verknüpfungen $+$ (genannt Addition) und $\cdot$ (genannt Multiplikation).*
(a) $(R, +, \cdot)$ heißt ein **Ring** *mit Eins, falls*
1) $(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0;
2) $(R, \cdot)$ ist ein Monoid mit 1-Element $1 \neq 0$ [1].
3) Es gelten die beiden **Distributiv***gesetze:*

$$a(b + c) = ab + ac \qquad \text{für alle } a, b, c \in R.$$

und

$$(b + c)a = ba + ca \qquad \text{für alle } a, b, c \in R.$$

(b) Falls zusätzlich die Multiplikation kommutativ ist, spricht man von einem **kommutativen Ring mit Eins**.

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

Bemerkung 6.4. *Sei R ein Ring und $a \in R$. Dann gilt:*
1.) $0a = 0 = a0$.
2.) $(-1)a = -a$.

[1] Prinzipiell kann man bei Ringen und kommutativen Ringen mit Eins noch auf den Zusatz $1 \neq 0$ verzichten. Im Falle $1 = 0$ gibt es jedoch keine weiteren Elemente in dem Ring.

Beweis. 1.) $0a = (0+0)a = 0a + 0a$, also durch Subtraktion von $0a$ erhält man $0a = 0$. Die Identität $a0 = 0$ folgt analog.
2.) Es ist $a + (-1)a = (1 + (-1))a = 0a = 0$. q.e.d.

Die natürlichen Zahlen und die ganzen Zahlen spielen bei jedem Ring eine besondere Rolle, die ersteren beim Potenzieren, die letzteren beim Multiplizieren.

Bemerkung 6.5. *Sei $(R, +, \cdot)$ ein Ring.*
1.) Man hat eine Abbildung

$$\mathbb{Z} \times R \to R : (z, r) \mapsto zr := \begin{cases} 0 & \text{falls } z = 0 \\ \sum_{i=1}^{z} r & \text{falls } z > 0 \\ -\sum_{i=1}^{-z} r & \text{falls } z < 0 \end{cases}$$

die den beiden Distributivgesetzen genügt.
2.) Man hat eine Abbildung

$$\mathbb{N}_0 \times R \to R : (n, r) \mapsto r^n := \prod_{i=1}^{n} r$$

welche den üblichen Potenzgesetzen genügt, falls R kommutativ mit Eins ist. (Das leere Produkt ist als 1 definiert.)
3) In einem kommutativen Ring R mit Eins gilt das allgemeine Assoziativgesetz für die Addition, d. h. bei Summen von mehr als zwei Summanden kann man die Klammern weglassen. Entsprechendes gilt für die Multiplikation. Es gilt das allgemeine Kommutativgesetz für Addition und Multiplikation, d. h. auf die Reihenfolge von Summanden bzw. Faktoren braucht man auch nicht zu achten.

Satz 6.6. *(***Allgemeines Distributivgesetz***)*
Sei R ein Ring, $n, m \in \mathbb{N}$ und $A \in R^{m \times n}$. Dann gilt:

$$\prod_{i=1}^{m} \sum_{j=1}^{n} A_{ij} = \sum_{\varphi \in \underline{n}^{\underline{m}}} \prod_{i=1}^{m} A_{i\varphi(i)}$$

Beweis. Als Vorbereitung zeigt man durch eine einfache Induktion über m

$$(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$$

für $a_i, b_j \in R$ (Übung).
Den eigentlichen Beweis führen wir durch Induktion über die Anzahl m der Faktoren. Der Induktionsanfang $m = 1$ ist klar, da kein Produkt gebildet wird. Angenommen die

Behauptung gilt für m. Sei also $A \in R^{(m+1)\times n}$. Dann gilt:

$$\begin{aligned}\prod_{i=1}^{m+1}\sum_{j=1}^{n} A_{ij} &= (\prod_{i=1}^{m}\sum_{j=1}^{n} A_{ij}) \cdot \sum_{j=1}^{n} A_{m+1,j} \\ &= (\sum_{\varphi\in\underline{n}^{\underline{m}}}\prod_{i=1}^{m} A_{i\varphi(i)}) \cdot \sum_{j=1}^{n} A_{m+1,j} \\ &= \sum_{\psi\in\underline{n}^{\underline{m+1}}}\prod_{i=1}^{m+1} A_{i\psi(i)}\end{aligned}$$

wobei der letzte Schritt auf Grund der Vorbereitung möglich ist: Jedes $\varphi \in \underline{n}^{\underline{m}}$ lässt sich auf genau n Weisen zu einem $\psi \in \underline{n}^{\underline{m+1}}$, weil man alle Zahlen von 1 bis n als Wert $\psi(m+1)$ zu wählen hat. q.e.d.

Wer sich daran reibt, dass alle Summen auf der linken Seite gleich viele Summanden haben, kann sich vorstellen, dass einige Summanden Null sein können.

Folgerung 6.7. *(***Binomischer Lehrsatz***).*
Sei $(R,+,\cdot)$ ein kommutativer Ring mit Eins. Für $a,b \in R$ und $n \in \mathbb{N}$ gilt:

$$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$$

Beweis. Im allgemeinen Distributivgesetz wählen wir $m := n$ und $n := 2$ und $A_{i1} := a$ und $A_{i2} := b$ für $i = 1,\ldots,n$. Wegen der Kommutativität der Multiplikation gilt für $\varphi \in \underline{2}^{\underline{n}}$ mit $|\varphi^{-1}(\{1\})| = k$

$$\prod_{i=1}^{m} A_{i\varphi(i)} = a^k b^{n-k}.$$

Da die Anzahl dieser Abbildungen φ gleich $\binom{n}{k}$ ist, folgt die Behauptung. q.e.d.

Übung: Definiere den Begriff des Teilrings eines Ringes und zeige, dass $(\mathbb{Z},+,\cdot)$ keinen echten Teilring mit Eins enthält.
Ende der 11. Vorlesung am 19.11.2013
Bemerkung: Ist G eine Gruppe und $g \in G$, so ist

$$\rho_g : G \to G, x \mapsto xg$$

eine bijektive Abbildung mit Umkehrabbildung $\rho_g^{-1} = \rho_{g^{-1}}$.
Bemerkung: Es gibt genau einen Ring mit 2 Elementen: $\mathbb{F}_2 := (\{0,1\},+,\cdot)$ wobei $+$ und $\cdot$ definiert sind als

$+$	0	1
0	0	1
1	1	0

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

Übung: Für jede Primzahl p gibt es genau einen Ring mit p Elementen $\mathbb{F}_p$. Für $p = 3$ ergibt sich $\mathbb{F}_3 = (\{0, 1, a\}, +, \cdot)$ mit $a = -1$ wie folgt

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

$\cdot$	1	a
1	1	a
a	a	1

6.3 Körper 12. Vorlesung am 20.11.2013

Wie das Beispiel der ganzen Zahlen zeigt, kann man in einem kommutativen Ring mit Eins im Allgemeinen nicht durch Zahlen $\neq 0$ dividieren. Wenn dies doch der Fall ist, spricht man von einem Körper.

Definition 6.8. *Ein kommutativer Ring $(K, +, \cdot)$ mit Eins heißt* **Körper**, *falls $K^* := K - \{0\}$ mit der Multiplikation, also $(K^*, \cdot)$ eine abelsche Gruppe ist.*

Bemerkung 6.9. *Sei K ein Körper. Statt $a \cdot b^{-1}$ schreibt man auch $\frac{a}{b}$ für alle $a \in K, b \in K^*$. Man hat für $a, c \in K, b, d \in K^*$:*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} \text{ und } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Beweis.

$$\begin{aligned} bd \cdot (\frac{a}{b} + \frac{c}{d}) &= \frac{bda}{b} + \frac{bdc}{d} \\ &= da + bc. \end{aligned}$$

Teilt man die Gleichheit zwischen dem ersten und letzten Ausdruck durch bd, so folgt die erste Behauptung nach Kürzen. Die zweite lassen wir als Übung. q.e.d.

Beispiele:
1) $(\mathbb{R}, +, \cdot)$, kurz $\mathbb{R}$, ist ein Körper: der reelle Zahlkörper.
2) $(\mathbb{Q}, +, \cdot)$ mit

$$\mathbb{Q} := \{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\} \subseteq \mathbb{R}$$

ist ein Körper (Teilkörper von $\mathbb{R}$): der rationale Zahlkörper $\mathbb{Q}$. Man überzeugt sich leicht, dass $\mathbb{Q}$ keinen echten Teilkörper mehr enthält, wohl aber viele Teilringe.
3) $\mathbb{Z}$ ist kein Körper, sondern nur ein kommutativer Ring mit 1.
4) $\mathbb{F}_2$ und $\mathbb{F}_3$ von oben sind Körper.

7 Axiome für den reellen Zahlkörper

Lernziele: Axiome und Beispiele für angeordnete Körper, Axiom der oberen Grenze, reeller Zahlkörper, $\mathbb{R}$ als Zahlengerade, ARCHIMEDisches Axiom, Abstand und Absolutbetrag, univariate quadratische Gleichungen.

7.1 Angeordnete Körper 12. Vorlesung am 20.11.2013

Sie haben bereits in der Analysis Anordnungen von Körpern studiert. Damit Sie nicht einschlafen, mach ich es etwas anders und sehr kurz.

Definition 7.1. *Sei K ein Körper. Eine Teilmenge $P \subseteq K$ heißt* **Anordnung**[2] *auf K, falls*
1.) $P + P := \{p_1 + p_2 | p_1, p_2 \in P\} \subseteq P$ und $PP := \{p_1 p_2 | p_1, p_2 \in P\} \subseteq P$.
2.) $K = P \uplus \{0\} \uplus (-P)$.
(K, P) heißt dann ein **angeordneter Körper**.

Beispiel: Ist K ein angeordneter Körper so gilt immer $1 = 1^2 \in P$ und $-1 \in -P$. Insbesondere ist $1 \neq -1$, also kann $\mathbb{F}_2$ nicht angeordnet werden. Es ist auch $-1 \neq 1 + 1$, also kann $\mathbb{F}_3$ nicht angeordnet werden.

Bemerkung 7.2. *Ist (K, P) ein angeordneter Körper, so definiert man*

$$<:= \{(a, b) \in K \times K | b - a \in P\} \subseteq K \times K$$

oder $\leq := < \cup =$ als zugehörige Totalordnung und $P = \{a \in K | 0 < a\} = K_{>0}$.

Übung: Verifiziere die bekannten Eigenschaften für $\leq$, definiere Intervalle in K, obere und untere Schranken von Mengen.

Lemma 7.3. *Sei K ein angeordneter Körper. Dann ist*

$$\alpha : \mathbb{N} \to K : n \mapsto n1 = \sum_{i=1}^{n} 1$$

die einzige injektive Abbildung, die verträglich (siehe Beweis) ist mit der Anordnung, der Addition und der Multiplikation.

Beweis. Offenbar hat K genau ein Element a mit $a^2 = a$ und $a \neq 0$, sodass es neben α keine weitere Abbildung mit den genannten Eigenschaften gibt. Offenbar gilt $0 < 1$. Indem wir auf beide Seiten 1 addieren, folgt $1 < 2 \cdot 1$ und allgemeiner $n \cdot 1 < (n + 1) \cdot 1$ für alle $n \in \mathbb{N}$. Also $\alpha(i) < \alpha(j) \Leftrightarrow i < j$ für alle $i, j \in \mathbb{N}$. Somit ist α ordnungstreu und injektiv. Die Additivität von α:

$$\alpha(i + j) = \alpha(i) + \alpha(j)$$

für alle $i, j \in \mathbb{N}$ folgt bereits aus Bemerkung 6.5 1. Die Multiplikativität gilt auch im allgemeineren Rahmen von Ringen (Übung). q.e.d.

Beispiel: Das entsprechende $\alpha : \mathbb{N} \to \mathbb{F}_3$ ist nicht injektiv.

Wir können und werden also $\mathbb{N}$ als eine Teilmenge des angeordneten Körpers K ansehen, indem wir $n \in \mathbb{N}$ mit $\alpha(n)$ identifizieren. Ebenso ist $\mathbb{Z} = \{[(n, m)] \mid n, m \in \mathbb{N}\}$ in K

[2] Genauer sollte man sagen, die Menge der positiven Elemente einer Anordnung von K.

eingebettet durch $[(n,m)] \mapsto \alpha(n) - \alpha(m)$. Analog können und werden wir auch die rationalen Zahlen $\mathbb{Q} := \{[(a,b)] \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$ in K eingebettet betrachten, da durch α eindeutige mit der Multiplikation und Addition verträgliche Abbildungen von $\mathbb{Z}$ (bzw. $\mathbb{Q}$) nach K definiert werden. Diese sind ebenfalls injektiv (Achtung hier benutzen wir die Tatsache, dass K angeordnet ist).
Also

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq K$$

für jeden angeordneten Körper K.

Definition 7.4. *Ein angeordneter Körper heißt* **ordnungsvollständig**[3]*, falls jede nach oben beschränkte Menge $\emptyset \neq M \subseteq K$ eine kleinste obere Schranke, also ein* **Supremum** $\sup(M)$ *hat, d. h. für alle $\emptyset \neq M \subseteq K$ gilt*

$$S_o(M) := \{a \in K | m \leq a \ \forall m \in M\} \neq \emptyset \Rightarrow \exists \ \sup(M) \in S_o(M) \text{ mit } \sup(M) \leq s \ \forall s \in S_o(M).$$

(Die Menge $S_o(M)$ der oberen Schranken von M hat eine untere Schranke, die in $S_o(M)$ liegt, also auch obere Schranke von M ist.)

Übung: Man zeige, dass die Ordnungsvollständigkeit dazu äquivalent ist, dass jede nach unten beschränkte Menge eine kleinste untere Schranke, kurz ein Infimum hat. (Hinweis: Die Multiplikation mit -1 dreht die Ordnungsrelation um.)

Beispiel. $\mathbb{Q}$ (mit der bekannten Anordnung) ist nicht ordnungsvollständig.

Beweis. $M := \{a \in \mathbb{Q} | a^2 \leq 2\}$ ist nach oben beschränkt, z. B. $2 \in S_o(M)$. Denn offenbar ist $a \in M \Rightarrow a^2 \leq 2 < 4 = 2^2$ also $a < 2$.
Weiter gilt $S_o(M) = \{b \in \mathbb{Q} | \ b > 0 \wedge 2 \leq b^2\}$ (Übung).
Würde also $s := \sup(M)$ existieren, so gilt $s^2 = 2$. Da s eine positive rationale Zahl ist, bekommen wir $a, b \in \mathbb{N}$ mit $s = a/b$, d. h.

$$a^2 = 2b^2,$$

was der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ widerspricht, denn 2 käme links mit gerader und rechts mit ungerader Vielfachheit vor. q.e.d.

7.2 Der reelle Zahlkörper 12. Vorlesung am 20.11.2013

Definition 7.5. *Ein angeordneter ordnungsvollständiger Körper, kurz vollständiger angeordneter Körper, heißt* **reeller Zahlkörper** *und wird mit $\mathbb{R}$ bezeichnet.*

[3] In der Analysisvorlesung haben Sie an dieser Stelle einfach „vollständig“gesagt.

Diese etwas komische Definition bedarf eines Kommentares. Es zeigt sich, dass erstens ein derartiger Körper existiert und zweitens, dass je zwei solche Körper auf genau eine Art identifiziert werden können, sodass Anordnung, Addition und Multiplikation mit der Identifikation verträglich sind. Wir werden diese Behauptungen später beweisen. Ab jetzt bezeichnet $\mathbb{R}$ einen festen vollständigen angeordneten Körper.
An Tafel die Eindeutigkeit erläutert.
Ende der 12. Vorlesung am 20.11.2013

Ab jetzt arbeiten wir nur noch mit unserer Kopie von $\mathbb{R}$.

Wir wollen eine wichtige Folgerung aus dem Supremumaxiom ziehen.

Satz 7.6. *(*Archimed**isches Axiom**)*
Seien $a, b \in \mathbb{R}_{>0}$. Dann existiert ein $n \in \mathbb{N}$ mit $na > b$.

Beweis. Nach Division durch a können wir oBdA $a = 1$ annehmen. Angenommen es existiert ein $b > 0$ mit $n \leq b$ für alle $n \in \mathbb{N}$. Dann gibt es eine kleinste obere Schranke $b_0 \leq b$ für $\mathbb{N}$. Da es sich um die kleinste obere Schranke handelt, existiert ein $n \in \mathbb{N}$ mit $n > b_0 - 1$. Also ist $n + 1 > b_0$, was ein Widerspruch ist, denn $n + 1 \in \mathbb{N}$ und b_0 war obere Schranke für $\mathbb{N}$. q.e.d.

7.3 Absolutbetrag und Abstand, 13. Vorlesung 26.11.2013

Für das geometrische Verständnis der Zahlengerade sind die verwandten Begriffe des Absolutbetrages und des Abstandes wichtig.

Definition 7.7.

$$|\ |: \mathbb{R} \to \mathbb{R}_{\geq 0} : a \mapsto \begin{cases} a & \text{falls } a \geq 0 \\ -a & \text{falls } a < 0 \end{cases}$$

heißt der **Absolutbetrag** *auf $\mathbb{R}$ und*

$$d : \mathbb{R} \times \mathbb{R} \to \mathbb{R} : (a, b) \mapsto |a - b|$$

heißt die **Abstand***sfunktion auf $\mathbb{R}$.*

Bemerkung: Der Abstand erfüllt folgende Eigenschaften einer **Metrik**:
1.) $d(a, b) \geq 0$ für alle $a, b \in \mathbb{R}$ und $d(a, b) = 0 \Leftrightarrow a = b$.
2.) $d(a, b) = d(b, a)$ für alle $a, b \in \mathbb{R}$.
3.) $d(a, b) \leq d(a, c) + d(c, b)$ für alle $a, b, c \in \mathbb{R}$.

Wir wollen den Absolutbetrag benutzen, um die Struktur der multiplikativen Gruppe $\mathbb{R}^* = (\mathbb{R}^*, \cdot)$ der reellen Zahlen zu untersuchen. Dazu brauchen wir zwei neue Begriffe.

Definition 7.8. *Seien $(G,\cdot)$ und $(H,\cdot)$ Gruppen. Eine Abbildung*

$$\varphi : G \to H$$

heißt **Homomorphismus**, *genauer Gruppenhomomorphimus, falls*

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) \qquad \forall g_1, g_2 \in G$$

gilt. Ist φ zusätzlich noch bijektiv, so heißt φ **Isomorphismus**.

Bemerkung 7.9. *Seien $(G,\cdot)$ und $(H,\cdot)$ Gruppen. Dann wird das* Cartesi*sche Produkt $G \times H$ mit der komponentenweisen Multiplikation*

$$(G \times H) \times (G \times H) \to G \times H : ((g_1, h_1), (g_2, h_2)) \mapsto (g_1 g_2, h_1 h_2)$$

zu einer Gruppe, genannt das **direkte Produkt** *$G \times H$ von G und H. Es sind*

$$\pi_G : G \times H \to G : (g,h) \mapsto g \text{ und } \pi_H : G \times H \to H : (g,h) \mapsto h$$

Gruppenhomomorphismen.

Übung: Ist $\varphi : G \to H$ ein Gruppenisomorphismus, dann auch $\varphi^{-1} : H \to G$.
Übung: Zwei Gruppen G, H heißen **isomorph**, genau dann wenn ein Isomorphismus $\varphi : G \to H$ existiert. In Zeichen $G \cong H$. Zeigen Sie, dass Isomorphie von Gruppen eine Äquivalenzrelation ist.

Satz 7.10. *1.)*

$$|\ |\ : (\mathbb{R}^*,\cdot) \to (\mathbb{R}_{>0},\cdot) : a \mapsto |a|$$

und

$$\operatorname{sign} : (\mathbb{R}^*,\cdot) \to (\{\pm 1\},\cdot) : a \mapsto \frac{a}{|a|}$$

sind Gruppenhomomorphismen.
2.)

$$(|\ |, \operatorname{sign}) : \mathbb{R}^* \to \mathbb{R}_{>0} \times \{\pm 1\} : a \mapsto (|a|, \operatorname{sign}(a))$$

ist ein Gruppenisomorphismus.
3.) Sei $a \in P = \mathbb{R}_{>0}$, $a \neq 1$. Dann ist

$$\operatorname{pot}_a : (\mathbb{R},+) \to (\mathbb{R}_{>0},\cdot) : x \mapsto a^x.$$

ist ein Gruppenisomorphismus mit inversem Isomorphismus

$$\log_a : (\mathbb{R}_{>0},\cdot) \to (\mathbb{R},+) : r \mapsto \log_a(r)$$

Beweis. 1.) Einfache Übung.
2.) Offenbar ist nach 1.) die Abbildung ein Homomorphismus, also multiplikativ. Wir müssen die Bijektivität zeigen. Dies tun wir durch Angabe des inversen Isomorphismus:

$$\mathbb{R}_{>0} \times \{\pm 1\} \to \mathbb{R}^* : (p,s) \mapsto ps.$$

3.) Dies werden Sie später in der Analysis beweisen. q.e.d.

7.4 Quadratische Gleichungen, 13. Vorlesung 26.11.2013

Satz 7.11. *Die Abbildung*

$$q : \mathbb{R}_{\geq 0} := \{a \in \mathbb{R} | a \geq 0\} \to \mathbb{R}_{\geq 0} : x \mapsto x^2$$

ist bijektiv. Die Umkehrabbildung wird als **Quadratwurzel***funktion, kurz* $\sqrt{\ }$*, bezeichnet.*

Beweis. Zeigen zunächst dass q streng **monoton** steigend ist, d. h. $a, b \in \mathbb{R}_{\geq 0}$ mit $a < b$ impliziert $q(a) < q(b)$, also $a^2 < b^2$. Dies folgt, da

$$b^2 - a^2 = \underbrace{(b-a)}_{\in P} \underbrace{(b+a)}_{\in P+P \subseteq P} > 0 \text{ denn } b > a \text{ und } a, b \in \mathbb{R}_{\geq 0}$$

Die strenge Monotonie impliziert, dass q injektiv ist. Wir müssen noch zeigen, dass q surjektiv ist. Sei $c \in \mathbb{R}_{\geq 0}$. Da $0^2 = 0$ ist können wir annehmen, dass $c > 0$ gilt. Betrachte zuerst den Fall $c \geq 1$. Wieder ist $c = 1$ klar. Für $c > 1$ ist dann

$$M_c := \{a \in \mathbb{R} | a^2 \leq c\}$$

durch c^2 nach oben beschränkt und wir sehen (Übung), dass

$$\sup(M_c)^2 = c, \text{ also } \sqrt{c} = \sup(M_c).$$

Ist $0 < c < 1$, so gilt $1 < 1/c$ und man bekommt $\sqrt{c} = 1/\sqrt{1/c}$.
Jedenfalls ist klar, dass q und $\sqrt{\ }$ invers zueinander sind. q.e.d.

Folgerung 7.12. *Die Faser von*

$$Q : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$$

über r ist leer für $r < 0$, die einelementige Menge $\{0\}$ für $r = 0$ und die zweielementige Menge $\{\sqrt{r}, -\sqrt{r}\}$ für $r > 0$.

Beweis. Wegen $(-1)^2 = 1$ sofort aus 7.11. q.e.d.

Folgerung 7.13. *Der Absolutbetrag $|\ |$ und Q haben dieselben Fasern, d. h. die Äquivalenzrelationen der Bildgleichheit stimmen überein: $\sim_{|\ |} = \sim_Q$, ebenso ihre Bilder, welche $\mathbb{R}_{\geq 0}$ sind. Also existiert nach Satz 4.4 eine Bijektion, welche die beiden Abbildungen verbindet. In der Tat gilt*

$$q \circ |\ \ | = Q, \text{ also } q(|a|) = Q(a)\ \forall a \in \mathbb{R},$$

d. h. $q : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ ist diese Bijektion.

Alle sind bestens mit der quadratischen Ergänzung vertraut. Also bekommen wir eine weitere Folgerung.

Folgerung 7.14. *Seien $a, b \in \mathbb{R}$. Genau dann hat die quadratische Gleichung $x^2 + ax + b = 0$ eine Lösung in $\mathbb{R}$, wenn die* **Diskriminante** *$d := a^2 - 4b$ gilt $d \geq 0$.*

Übung: Zeige die Diskriminante einer quadratischen Gleichung ist das Quadrat der Differenz der beiden Lösungen. Wann hat man also genau eine Lösung?

8 Der komplexe Zahlkörper

Lernziele: Naive Konstruktion aus $\mathbb{R}$, Rolle der komplexen Konjugation, Polarzerlegung und Analyse der multiplikativen Gruppe $\mathbb{C}^*$, die affine Gruppe $\mathrm{Aff}_1(\mathbb{C})$ und GAUSSsche Zahlenebene, ebene EUKLIDische Geometrie.

8.1 Konstruktion aus dem reellen Zahlkörper, 13. Vorlesung 26.11.2013

Dass in $\mathbb{R}$ nicht jede quadratische Gleichung eine Lösung hat, ist ein Defizit, welches aber eng mit der Anordnung des Körpers verbunden ist. Auf Grund der quadratischen Ergänzung ist sofort klar: Enthält ein Körper K den Körper $\mathbb{R}$ als Teilkörper und eine Lösung von x^2+1, so hat jede reelle quadratische Gleichung eine Lösung in K. Zwei Fragen stellen sich: Gibt es überhaupt einen solchen Körper K? Wenn ja, hat K selbst Lösungen für jede seiner quadratischen Gleichungen?

Lemma 8.1. *Falls ein Körper K existiert, der $\mathbb{R}$ als Teilkörper und eine Lösung i von x^2+1 enthält, so bildet*

$$\mathbb{C}_h := \{a+bi | a,b \in \mathbb{R}\}$$

einen Teilkörper von K.

Beweis. Wegen des Kommutativgesetzes für die Addition und des Distributivgestzes ist

$$\mathbb{C}_h \times \mathbb{C}_h \to \mathbb{C}_h : (a+bi, c+di) \mapsto (a+c)+(b+d)i$$

die einzige Möglichkeit für die Addition in $\mathbb{C}_h$. Man rechnet leicht nach, dass $(\mathbb{C}_h, +)$ eine abelsche Gruppe ist. Wie sieht es mit der Multiplikation aus: Es muss wegen Kommutativgesetze und Distributivgesetze

$$(a+bi)(c+di) = ac + adi + bci + bdi^2 = (ac-bd)+(ad+bc)i$$

sein für alle $a,b,c,d \in \mathbb{R}$. Da K ein Körper ist, zeigt unsere Rechnung, dass $\mathbb{C}_h$ ein Teilring von K ist. Es ist in der Tat ein Teilkörper, denn

$$(a+bi)^{-1} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$$

für $(a,b) \in \mathbb{R}^2 - \{(0,0)\}$. q.e.d.

Ende der 13. Vorlesung am 26.11.2013

Das letzte Lemma ist mit Vorsicht zu genießen: Es sagt nicht, dass ein solcher Körper $\mathbb{C}_h$ existiert, sondern nur, dass er eindeutig (bis auf Isomorphie) ist, falls er existiert. Aber, was wichtiger ist, es gibt uns einen Konstruktionshinweis. Den nehmen wir sehr ernst, denn das Lemma sagt ja, wenn diese Formeln nicht funktionieren, dann geht es gar nicht.

Definition 8.2. *Der* **komplexe Zahlkörper** $\mathbb{C} = (\mathbb{C}, +, \cdot)$ *ist definiert wie folgt:*
1.) Als Menge und additive Gruppe $(\mathbb{C}, +) := (\mathbb{R}^2, +)$ *(vgl. Beispiel zu Beginn des Kapitels)*
2.) Die Multiplikation ist definiert durch

$$\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C} : ((a, b), (c, d)) \mapsto (ac - bd, ad + bc)$$

Satz 8.3. *1.)* $(\mathbb{C}, +, \cdot)$ *ist ein Körper.*
2.) $\iota : \mathbb{R} \to \mathbb{C} : a \mapsto (a, 0)$ *ist injektiv und verträglich mit Addition und Multiplikation, sodass wir* $\mathbb{R}$ *mit* $\iota(\mathbb{R})$ *identifizieren, d.h.* $a = (a, 0)$ *setzen für alle* $a \in \mathbb{R}$ *und somit* $\mathbb{R}$ *als Teilkörper von* $\mathbb{C}$ *ansehen. (*ι *ist ein injektiver Körperhomomorphismus).*
Insbesondere hat man mit $i := (0, 1)$ *eine eindeutige Darstellung* $z = a + bi$ *für jedes* $z \in \mathbb{C}$ *mit* $a, b \in \mathbb{R}$.
3.) $\mathbb{C}$ *kann nicht angeordnet werden.*

Beweis. 1.) Man rechnet die Körperaxiome nach unter Benutzung der Tatsache, dass $\mathbb{R}$ ein Körper ist. (Später werden wir dies konzeptueller machen. Jetzt ist es eine lange, aber leichte Aufgabe.)
2.) Die Injektivität ist klar, ebenso die Additivität und Multiplikativität von ι, z. B.

$$\iota(a + b) = (a + b, 0) = (a, 0) + (b, 0) = \iota(a) + \iota(b) \qquad \forall a, b \in \mathbb{R}.$$

3.) Angenommen $P \subseteq \mathbb{C}$ ist eine Anordnung. Dann ist offenbar (Übung) $1 \in P$, d. h. $1 \in P$ und $-1 \in -P$. Wegen $\mathbb{C} = P \uplus \{0\} \uplus (-P)$ haben wir für i zwei Möglichkeiten: $i \in P$ oder $i \in -P$. Da $i^2 = -1$ und $P^2 \subset P$ entfällt die erste Möglichkeit. Die zweite impliziert $-i \in P$, welches denselben Widerspruch liefert. Also hat $\mathbb{C}$ keine Anordnung. q.e.d.

Es stellt sich die Frage, ob $\mathbb{R}$ als Teilkörper von $\mathbb{C}$ besonders ausgezeichnet ist. Dies ist in der Tat der Fall und hängt mit der Einbettung der natürlichen Zahlen und damit auch der rationalen Zahlen in $\mathbb{C}$ zusammen. Wir können dies aber erst später, wenn wir über Grenzwerte gesprochen haben, beweisen. An dieser Stelle begnügen wir uns mit einer Abbildung, die die Rolle der reellen Zahlen heraustellt.

Definition 8.4. *Die Abbildung*

$$^- : \mathbb{C} \to \mathbb{C} : z = a + bi \mapsto \overline{z} := a - bi \qquad (a, b \in \mathbb{R})$$

heißt **komplexe Konjugation**.

Hier sind die geometrischen und algebraischen Eigenschaften der komplexen Konjugation.

Satz 8.5. *1.) Die komplexe Konjugation ist ein Körperautomorphismus, d. h. sie ist bijektiv, additiv und multiplikativ. Sie ist darüberhinaus zu sich selbst invers.*
2.) Die reellen Zahlen bilden die Fixpunkte der komplexen Konjugation, d. h.

$$\mathbb{R} = \mathrm{Fix}(^-) := \{z \in \mathbb{C} | \overline{z} = z\}.$$

Beweis. 1.) Offenbar ist $^-$ selbstinvers und insbesondere bijektiv. Die Additivität von $^-$ ist offensichtlich, d. h. ein Gruppenisomorphismus $^- : (\mathbb{C}, +) \to (\mathbb{C}, +)$ liegt vor, da Definitions- und Werteberech übereinstimmen, spricht man von einem (Gruppen-) Automorphismus. Die Homomorphieeigenschaft für die Multiplikation müssen wir nachrechnen:

$$\begin{aligned}\overline{(a+bi)(c+di)} &= \overline{(ac-bd)+(ad+bc)i} \\ &= (ac-bd)-(ad+bc)i \\ &= (a-bi)(c-di) \\ &= \overline{(a+bi)} \cdot \overline{(c+di)}\end{aligned}$$

2.) Klar. q.e.d.

8.2 Die Gausssche Zahlenebene

Spricht man geometrisch, so sagt man nicht, dass $\mathbb{R}$ ein Teilkörper von $\mathbb{C}$ ist (das wäre algebraisch gesprochen), sondern man stellt sich $\mathbb{C}$ als Ebene $\mathbb{R}^2$ vor und bezeichnet den Teilkörper $\mathbb{R}$ von $\mathbb{C}$, also $\mathrm{Fix}(^-)$ als die **reelle Achse** und die Menge der Antifixpunkte von $^-$

$$\{z \in \mathbb{C} \mid \overline{z} = -z\} = \mathbb{R}i := \{ri \mid r \in \mathbb{R}\}$$

als die **imaginäre Achse**. Die komplexe Konjugation ist dann eine Spieglung an der reellen Achse, die die imaginäre Achse in sich überführt.

Bemerkung Für $z = a + bi \in \mathbb{C}$ mit $a, b \in \mathbb{R}$ heißt a der **Realteil** $\mathrm{Re}(z)$ und b der **Imaginärteil** $\mathrm{Im}(z)$ von z. Dann gilt

$$\mathrm{Re}(z) = \frac{z+\overline{z}}{2} \text{ und } \mathrm{Im}(z) = \frac{z-\overline{z}}{2i}.$$

und Re, Im sind Gruppenhomomorphismen $(\mathbb{C}, +) \to (\mathbb{R}, +)$.

(Beweis als Übung.)

Wir hatten bei den reellen Zahlen den Absolutbetrag besprochen, der einerseits einen Gruppenhomomorphismus von $\mathbb{R}^*$ auf $\mathbb{R}_{>0}$ definierte und andererseits eine Metrik, also etwas Geometrisches auf $\mathbb{R}$ induzierte. Mit Hilfe der komplexen Konjugation können wir den Absolutbetrag von $\mathbb{R}$ auf $\mathbb{C}$ fortsetzen.

Definition 8.6.

$$|\ \ | : \mathbb{C} \to \mathbb{R}_{\geq 0} : z \mapsto |z| := \sqrt{z\overline{z}}$$

heißt der **Absolutbetrag** *oder einfach* **Betrag** *der komplexen Zahlen.*

Satz 8.7. *1.) Der Absolutbetrag der komplexen Zahlen ist wohldefiniert und setzt den der reellen Zahlen fort.*
2.) Für $z \in \mathbb{C}$ gilt $|z| = 0 \Leftrightarrow z = 0$.
3.) Für $z_1, z_2 \in \mathbb{C}$ gilt $|z_1 z_2| = |z_1||z_2|$. Insbesondere ist die Einschränkung

$$\mathbb{C}^* \to \mathbb{R}_{>0} : z \mapsto |z|$$

ein Gruppenhomomorphismus.
4.) Es gilt die **Dreiecksungleichung***:*

$$|z_1 + z_2| \leq |z_1| + |z_2| \qquad \forall z_1, z_2 \in \mathbb{C}.$$

Beweis. 1.) Sei $z = a + bi$ mit $a, b \in \mathbb{R}$. Dann haben wir

$$z\overline{z} = a^2 + b^2 \geq 0,$$

sodass die Quadratwurzel definiert und somit $|z|$ wohldefiniert ist. Falls $z \in \mathbb{R}$, also $b = 0$, ist $|z| = |a|$ also gleich dem für $\mathbb{R}$ definierten Absolutbetrag von z.
2.) Klar mit Beweis von 1.).
3.) Dies folgt aus der Multiplikativität von $\overline{\ }$:

$$|z_1 z_2|^2 = z_1 z_2 \overline{z_1 z_2} = z_1 z_2 \overline{z_1} \overline{z_2} = (|z_1||z_2|)^2$$

Die Injektivität des Quadrierens auf $\mathbb{R}_{\geq 0}$, vgl. Satz 7.11 liefert die Behauptung.
4.) Die Behauptung ist klar, falls $z_1 = 0$. Im Fall $z_1 \neq 0$ können wir wegen 3.) nach Division durch z_1 annehmen, dass $z_1 = 1$ ist. Sei dann $z_2 = a + bi$ mit $a, b \in \mathbb{R}$. Die Behauptung ist dann äquivalent zu

$$\sqrt{(1+a)^2 + b^2} \leq 1 + \sqrt{a^2 + b^2}$$

Da Quadrieren auf $\mathbb{R}_{\geq 0}$ streng monoton steigend ist, ist dies äquivalent zu

$$(1+a)^2 + b^2 \leq 1 + 2\sqrt{a^2 + b^2} + a^2 + b^2$$

also zu

$$a \leq \sqrt{a^2 + b^2}$$

was nach Quadrieren zu der offensichtlichen Ungleichung

$$a^2 \leq a^2 + b^2$$

äquivalent ist. q.e.d.

Dieser grundlegende Satz hat zwei Arten von wichtigen Konsequenzen: für die Geometrie von $\mathbb{C}$ und für die gruppentheoretische Struktur von $\mathbb{C}^*$.

Folgerung 8.8. *Die Abbildung*

$$d : \mathbb{C} \times \mathbb{C} \to \mathbb{R}_{\geq 0} : (p, q) \mapsto |p - q|$$

ist eine Metrik auf $\mathbb{C}$*. Wir sagen* $d(p, q)$ *ist der* **Abstand** *von* q *und* q *in* $\mathbb{C}$*.*

Beweis. 1.) $d(p, q) = 0 \iff p = q$ ist klar.
2.) $d(p, q) = d(q, p) \qquad \forall p, q \in \mathbb{C}$ ist auch klar.
3.) $d(p, q) \leq d(q, r) + d(r, p) \forall p, q, r \in \mathbb{C}$ folgt aus der Dreiecksungleichung.
q.e.d.

Ende der 14. Vorlesung am 26.11.

Folgerung 8.9. *1.) Der Einheitskreis* $S^1 := \{z \in \mathbb{C} |\ |z| = 1\ \} \leq \mathbb{C}^*$ *ist eine Untergruppe von* $\mathbb{C}^*$.
2.)

$$\zeta : \mathbb{C}^* \to \mathbb{R}_{>0} \times S^1 : z \mapsto (|z|, \frac{z}{|z|})$$

ist ein Isomorphismus, genannt **Polarzerlegung**.

Beweis. 1.) (Sei $z = c + si \in S^1$ mit $c, s \in \mathbb{R}$. Dann gilt $z \in S^1 \Leftrightarrow c^2 + s^2 = 1$, so dass der Name Einheitskreis nach PYTAGORAS[4] gerechtfertigt erscheint.) Die Behauptung folgt sofort aus der Multiplikativität von $|\ \ |$ und $1 \cdot 1 = 1$.
2.) Die Homomorphieeigenschaft ist klar. Man rechnet nach, dass

$$\mathbb{R}_{>0} \times S^1 \to \mathbb{C}^* : (r, n) \mapsto rn$$

die Umkehrabbildung ist, sodass ein Isomorphismus vorliegt. q.e.d.

Zwar hätte man das CARTESIsche Produkt einer Geraden mit einem Kreis eher als Kreiszylinder vorgestellt, aber bis auf Verzerrungen stimmt dies mit $\mathbb{C}^* = \mathbb{R}^2 - \{(0,0)\}$ überein. Wir wollen jetzt S^1 als Gruppe genauer analysieren und brauchen dazu einige Eigenschaten des Sinus und des Cosinus, die wir ohne Beweis auflisten:

Satz 8.10. *1.) Die Sinus- und die Cosinusfunktion sind* 2π*-periodische Abbildungen*

$$\sin, \cos : \mathbb{R} \to \mathbb{R}$$

d. h. $\sin(x + 2\pi) = \sin(x)$ *und* $\cos(x + 2\pi) = \cos(x)$ *für alle* $x \in \mathbb{R}$. *Dabei ist* 2π *der Umfang des Einheitskreises. (Nach Satz 4.6 sind diese Funktionen also eigentlich auf* $\mathbb{R}/2\pi\mathbb{Z}$ *definiert.)*
2.) Die Bilder von sin *und* cos *sind das abgeschlossene Intervall* $[-1, 1]$.
3.) Es gilt $\cos(x)^2 + \sin(x)^2 = 1$ *für alle* $x \in \mathbb{R}$.
4.) Auf dem Intervall $[0, \pi]$ *ist* cos *streng monoton fallend von* $\cos(0) = 1$ *bis* $\cos(\pi) = -1$. *Weiter gilt* $\cos(-x) = cos(x)$ *für alle* $x \in \mathbb{R}$.
5.) $\sin(x) = \cos(x - \pi/2)$ *für alle* $x \in \mathbb{R}$.
6.) Es gelten die Additionstheoreme

$$\begin{aligned} \cos(a+b) &= \cos(a)\cos(b) - \sin(a)\sin(b) \\ \sin(a+b) &= \cos(a)\sin(b) + \sin(a)\cos(b) \end{aligned}$$

für alle $a, b \in \mathbb{R}$.
7.) Die Bogenlänge der Kurve

$$[0, a] \to \mathbb{R}^2 : t \mapsto (\cos(t), \sin(t))$$

ist für $0 \leq a \leq 2\pi$ *gleich* a. *Daher heißt* a *auch der (positiv)* **orientierte Winkel** *zwischen* $(1, 0)$ *und* $(\cos(a), \sin(a))$ *mit Scheitelpunkt* $(0, 0)$.

[4] PYTHAGORAS von Samos etwa 569 - 475 v. C.

Beweis. in der Analysis. q.e.d.

Satz 8.11. *1.)* $\mathbb{R}/2\pi\mathbb{Z} := \{a + 2\pi\mathbb{Z} |\ a \in \mathbb{R}\}$ *ist eine Gruppe bezüglich der vertreterweise definierten Addition:*

$$(a + 2\pi\mathbb{Z}) + (b + 2\pi\mathbb{Z}) := (a + b) + 2\pi\mathbb{Z} \qquad \forall a, b \in \mathbb{R}.$$

und

$$\nu : (\mathbb{R}, +) \to (\mathbb{R}/2\pi\mathbb{Z}, +) : a \mapsto a + 2\pi\mathbb{Z}$$

ist ein Gruppenhomomorphismus.
2.) Die Abbildung

$$\varphi : (\mathbb{R}, +) \to S^1 : t \mapsto \cos(t) + \sin(t)i$$

ist ein surjektiver Gruppenhomomorphismus, der über ν *faktorisiert mit Hilfe von*

$$\psi : (\mathbb{R}/2\pi\mathbb{Z}, +) \to (S^1, \cdot) : t + 2\pi\mathbb{Z} \mapsto \cos(t) + \sin(t)i,$$

d. h. $\psi \circ \nu = \varphi$.
3.) ψ *ist ein Isomorphismus von Gruppen.*

Beweis. 1.) Es ist nur die Vertreterunabhängigkeit der neu definierten Addition zu zeigen. (an Tafel vormachen). Der Rest folgt sofort aus den Gruppeneigenschaften von $(\mathbb{R}, +)$.
2.) Wir zeigen zuerst die Surjektivität von φ. Sei $c + si \in S^1$. Wegen $c^2 + s^2 = 1$ gibt es nach Satz 8.10 genau ein $t \in [0, \pi]$ mit $\cos(t) = c$. (Dieses t heißt auch der (nicht orientierte) Winkel zwischen 1 und $c + si$.) Im Falle $s \geq 0$ gilt $c + si = \cos(t) + \sin(t)i$, sonst $c + si = \cos(2\pi - t) + \sin(2\pi - t)i$. Jedenfalls ist bereits die Einschränkung von φ auf das halboffene Intervall $[0, 2\pi)$ bijektiv und φ selbst surjektiv.
Dass φ ein Homomorphismus ist, ist äquivalent zu den Additionstheoremen für sin und cos, die wir jetzt nie wieder vergessen können.
Da sin und cos periodisch sind mit der Periode 2π, zeigt uns der Anfang dieses Beweises, dass die Fasern von φ gerade die Restklassen von $\mathbb{R}$ nach $2\pi\mathbb{Z}$ sind. Somit ist ψ nicht nur wohldefiniert, sondern sogar bijektiv. $\psi \circ \nu = \varphi$ gilt nach Definition.
3.) Sofort aus 2.) q.e.d.

Halten wir die folgende Form der **Polarzerlegung** fest: Jedes $z \in \mathbb{C}^*$ kann geschrieben werden als

$$\boxed{z = r(\cos(\varphi) + \sin(\varphi)i)}$$

mit eindeutigem $r = |z|$ und eindeutigem $\varphi \in [0, 2\pi)$, genannt das **Argument** $\arg(z)$ von z, und die Multiplikation erfolgt durch Multiplikation der Beträge und Addition (mod 2π) der Winkel.
Die **Polarkoordinaten** einer komplexen Zahl $z \neq 0$ sind definiert als $(|z|, \arg(z)) \in \mathbb{R}_{>0} \times [0, 2\pi)$.

Folgerung 8.12. *Jede quadratische Gleichung* $x^2 + ax + b$ *mit* $a, b \in \mathbb{C}$ *hat eine Lösung in* $\mathbb{C}$*, genauer zwei Lösungen, wenn die Diskriminante* $d := a^2 - 4b$ *ungleich Null ist, sonst genau eine Lösung, der man üblicherweise die Vielfachheit* 2 *gibt, weil in diesem Fall* $x^2 + ax + b = (x + a/2)^2$.

Beweis. Wegen der quadratischen Ergänzung brauchen wir nur die Gleichung $x^2 = z = r(\cos(\varphi) + \sin(\varphi)i)$ zu untersuchen. Diese hat die Lösungen $\pm\sqrt{r}(\cos(\varphi/2) + \sin(\varphi/2)i)$, also in Polarkoordianten $\sqrt{r}(\cos(\varphi/2) + \sin(\varphi/2)i)$ und $\sqrt{r}(\cos(\varphi/2 + \pi) + \sin(\varphi/2 + \pi)i)$. q.e.d.

Übung: Finde alle komplexen Lösungen der Gleichungen $x^3 = 1$ und $x^7 = -1$. Zeige, dass die Lösungen der ersten Gleichung eine Untergruppe von S^1 bilden. Tun dies die Lösungen der zweiten Gleichung auch?

8.3 EUKLIDische Geometrie, 16. Vorlesung am 4.12.

Wir betrachten jetzt das CARTESIsche Produkt $\mathbb{R}^2$ als Modell einer Ebene, so wie wir $\mathbb{R}$ das Modell einer Geraden betrachtet haben. Unsere Betrachtung hätte sehr gut vor die Einführung der komplexen Zahlen gepasst. An dieser Stelle haben wir jedoch den Vorteil, dass uns diverse geometrische Strukturen, die üblicherweise mit dem $\mathbb{R}^2$ in Verbindung gebracht werden, bereits durch die komplexen Zahlen, genauer durch die GAUSSsche Zahlenebene geschenkt werden. Man muss sich jedoch vor Augen halten, dass Begriffe wie Abstand, Skalarprodukt, Winkel, Strecke, affine Abbildung etc. aus einem sehr viel allgemeineren Kontext kommen. Dass sie uns über die GAUSSsche Zahlenebene für den $\mathbb{R}^2$ geradezu geschenkt werden, nehmen wir dankbar an.

Definition 8.13. *Sei $n \in \mathbb{N}$. Dann wird $\mathbb{R}^n$ mit der komponentenweisen Addition*

$$+ : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n, (a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

zu einer abelschen Gruppe. Auf $\mathbb{R}^n$ heißt die (äußere) Verknüpfung

$$\mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n : (s, a) \mapsto sa := s \cdot a := (sa_1, \ldots, sa_n)$$

die **Multiplikation mit Skalaren** *und für festes $s \in \mathbb{R}$ die Abbildung*

$$\sigma_s : \mathbb{R}^n \to \mathbb{R}^n : a \mapsto sa$$

die **Streckung** *um den Faktor s mit Zentrum $0 := (0, \ldots, 0)$.*

Bemerkung: Die Multiplikation mit Skalaren erfüllt die folgenden Rechenregeln:
$s(a + b) = sa + sb \; \forall s \in \mathbb{R}, a, b \in \mathbb{R}^n$ (Distributivgesetz), d. h. σ_s ist ein Gruppenhomomorphismus von $(\mathbb{R}^n, +)$.
$(s + t)a = sa + ta \; \forall s, t \in \mathbb{R}, a \in \mathbb{R}^n$ (Distributivgesetz).
$(st)a = s(ta) \; \forall s, t \in \mathbb{R}, a \in \mathbb{R}^n$ („Assoziativgesetz“), d. h. $\sigma_{st} = \sigma_s \circ \sigma_t$.
$1a = a \; \forall a \in \mathbb{R}^n$, d. h. $\sigma_1 = \mathrm{id}_{\mathbb{R}^n}$.

(Beweis als Übung)

Definition 8.14. *Sei $n \in \mathbb{N}$. Dann heißt*

$$\Phi : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R} : (a, b) \mapsto \sum_{i=1}^{n} a_i b_i$$

das **Standardskalarprodukt** *auf* $\mathbb{R}^n$*, die von* Φ *induzierte quadratische Form*

$$q : \mathbb{R}^n \to \mathbb{R} : a \mapsto \Phi(a,a) = \sum_{i=1}^{n} a_i^2$$

heißt **Quadratsumme** *und*

$$|\ \ | : \mathbb{R}^n \to \mathbb{R}_{\geq 0} : a \mapsto \sqrt{\Phi(a,a)}$$

heißt die zugehörige **Längenfunktion**.

Bemerkung 8.15. *0.) Die Längenfunktion ist durch den Satz von Pythagoras motiviert. (an Tafel erläutern)*
1.) Für $n = 2$ *ist die Qudadratsumme bzw. Längenfunktion bereits in* $\mathbb{C}$ *betrachtet worden als* $z\overline{z}$ *bzw.* $\sqrt{z\overline{z}}$*.*
2.) Für beliebiges n *lässt sich die Quadratsumme aus der Längenfunktion reproduzieren:*

$$q(a) = |a|^2 \ \forall a \in \mathbb{R}^n$$

und das Standardskalarprodukt aus der Quadratsumme:

$$\Phi(a,b) = \frac{1}{2}(q(a+b) - q(a) - q(b)) \ \forall a, b \in \mathbb{R}^n$$

3.) Das Standardskalarprodukt hat folgende Eigenschaften:
a) (Linearität in der ersten Komponente) $\Phi(a + a', b) = \Phi(a,b) + \Phi(a',b)$ *und* $\Phi(sa, b) = s\Phi(a,b) \qquad \forall a, a', b \in \mathbb{R}^n, s \in \mathbb{R}$.
b) (Symmetrie) $\Phi(a,b) = \Phi(b,a) \qquad \forall a, b \in \mathbb{R}^n$.
c.) (Positive Definitheit) $\Phi(a,a) > 0 \qquad \forall a \in \mathbb{R}^n - \{0\}$.

Ende der 15. Vorlesung am 3.12.

Damit einerseits für die Länge die Dreiecksungleichung gilt und wir andererseits einen Winkel zwischen zwei Vektoren definieren können, brauchen wir die folgende Ungleichung.

Lemma 8.16. *(*Cauchy-Schwarz**-Ungleichung**[5]*) Seien* $a, b \in \mathbb{R}^n$*. Dann gilt:*

$$\Phi(a,a)\Phi(b,b) - \Phi(a,b)^2 \geq 0.$$

Beweis. Es ist

$$(\sum_{i=1}^{n} a_i^2)(\sum_{j=1}^{n} b_j^2) - (\sum_{i=1}^{n} a_i b_i)^2 = \sum_{i,j}(a_i^2 b_j^2 - a_i b_i a_j b_j) = \sum_{i<j} a_i^2 b_j^2 - 2a_i b_i a_j b_j + a_j^2 b_i^2 = \sum_{i<j}(a_i b_j - a_j b_i)^2 \geq 0.$$

q.e.d.

[5] Augustin Louis Cauchy 1789 - 1857, Hermann Amandus Schwarz 1843 - 1921

Folgerung 8.17. *1.) Die Längenfunktion $|\ |$ auf $\mathbb{R}^n$ erfüllt die Dreiecksungleichung:*

$$|a+b| \leq |a| + |b| \qquad \forall a, b \in \mathbb{R}^n.$$

2.) $(\mathbb{R}^n, d)$ ist ein **metrischer Raum**, *wobei*

$$d : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_{\geq 0} : (a, b) \mapsto |a - b|,$$

d. h. der Abstand d ist eine Metrik vgl. Folgerung 8.8.
3.) Für $a, b \in \mathbb{R}^n - \{0\}$ gibt es ein eindeutiges $\alpha \in [0, \pi]$, genannt der (nicht orientierte) **Winkel** *$\measuredangle(a, b)$ von a, b, mit*

$$\boxed{\cos(\alpha) = \frac{\Phi(a, b)}{|a||b|}}$$

Beweis. 1.) u. 2.) Übung analog zum 2-dimensionalen Fall.
3.) Aus der CAUCHY-SCHWARZ-Ungleichung und den Eigenschaften des Cosinus. q.e.d.

Besonders ausgezeichnet ist der Fall, wenn der Winkel $\pi/2$ ist, also ein rechter Winkel. Man sagt dann, dass die Vektoren **orthogonal** zueinander sind oder **senkrecht** aufeinander stehen: $\Phi(a, b) = 0$.

Es gibt jetzt zwei Arten von geometrischen Eigenschaften zu diskutieren, und zwar diejenigen, wo 0 ausgezeichnet ist und diejenigen, wo kein Punkt ausgezeichnet ist. Wir beginnen mit den ersteren.

Definition 8.18. *Sei $\theta : \mathbb{R}^n \to \mathbb{R}^n$ eine Abbildung.*
1.) θ heißt **linear**, *falls $\theta(sa + tb) = s\theta(a) + t\theta(b)$ für alle $s, t \in \mathbb{R}, a, b \in \mathbb{R}^n$.*
2.) Ist θ linear, so heißt θ **orthogonal**, *falls $|\theta(a)| = |a|$ für alle $a \in \mathbb{R}^n$.*

Klar: Lineare Abbildungen bilden 0 auf 0 ab.

Lemma 8.19. *1.) Lineare Abbildungen θ bilden* **Strecken**, *also Teilmengen von $\mathbb{R}^n$ der Form*

$$V(a, b) := \{(1 - s)a + sb \mid s \in [0, 1]\} \text{ mit } a, b \in \mathbb{R}^n$$

auf Strecken ab, genauer die Verbindungsstrecke $V(a, b)$ wird auf die Verbindungsstrecke $V(\theta(a), \theta(b))$ abgebildet: $\theta(V(a, b)) = V(\theta(a), \theta(b))$.
2.) Lineare Abbildungen θ bilden **Geraden** *$G(a, b)$ mit $a, b \in \mathbb{R}^n, a \neq b$, auf Geraden oder einpunktige Mengen (degenerierte Geraden) ab, wobei*

$$G(a, b) := \{(1 - s)a + sb \mid s \in \mathbb{R}\} \text{ mit } a, b \in \mathbb{R}^n.$$

Genauer die Gerade $G(a, b)$ durch $a, b, a \neq b$ wird auf $G(\theta(a), \theta(b))$, welches im Falle $\theta(a) = \theta(b)$ zu einer einpunktigen Menge degeneriert, abgebildet: $\theta(G(a, b)) = G(\theta(a), \theta(b))$.
3.) Orthogonale Abbildungen θ respektieren Skalarprodukte und Winkel, d. h.

$$\Phi(\theta(a), \theta(b)) = \Phi(a, b) \qquad \forall a, b \in \mathbb{R}^n$$

und

$$\measuredangle(a,b) = \measuredangle(\theta(a),\theta(b)) \qquad \forall a,b \in \mathbb{R}^n - \{0\}.$$

Insbesondere ist θ bijektiv.

Beweis. 1.) 2.) sofort aus der Definition. Leichte Übung.
3.) Wir zeigen zuerst, dass θ injektiv ist. Sei also $a, b \in \mathbb{R}^n$ und $\theta(a) = \theta(b)$. Dann ist $\theta(a-b) = 0$, also $|a-b| = 0$, also $a = b$.

$$\begin{aligned}
\Phi(\theta(a),\theta(b)) &= \frac{1}{2}(|\theta(a)+\theta(b)|^2 - |\theta(a)|^2 - |\theta(b)|^2) \\
&= \frac{1}{2}(|\theta(a+b)|^2 - |\theta(a)|^2 - |\theta(b)|^2) \\
&= \frac{1}{2}(|a+b|^2 - |a|^2 - |b|^2) \\
&= \Phi(a,b)
\end{aligned}$$

Somit ist wegen der Injektivität die Winkelinvarianz auch klar.
Die Surjektivität schwieriger, es wird in der Vorlesung Lineare Algebra 1 bewiesen werden.
q.e.d.

Bemerkung 8.20. *Die Menge alle linearen Abbildungen von $\mathbb{R}^n$ nach $\mathbb{R}^n$ bildet einen Ring, wobei die Addition werteweise definiert ist und die Multiplikation die Komposition von Abbildungen dient.*
Die bijektiven linearen Abbildungen von $\mathbb{R}^n$ bilden eine Untergruppe $\mathrm{GL}(\mathbb{R}^n)$ *(***generelle lineare Gruppe***) von $S_{\mathbb{R}^n}$.*

Beweis. Als Übung. Beachten Sie, dass die zweite Aussage ganz allgemein für Ringe (mit Eins) gilt: Ist $(R,+,\cdot)$ ein Ring, so ist seine **Einheitengruppe**

$$U(R) := \{a \in R \mid \exists b \in R : ab = ba = 1\}$$

eine Gruppe bezüglich der Multiplikation in R. Dazu müssen Sie nur zeigen, dass die Multiplikation nicht aus $U(R)$ herausführt und Elemente von $U(R)$ multiplikativ Inverse in $U(R)$ besitzen. □

Folgerung 8.21. *Für $n = 2$ gibt es zwei Möglichkeiten für orthogonale Abbildungen, die wir mit Hilfe der Identifikation $\mathbb{R}^2 = \mathbb{C}$ so schreiben können:*
1.) $\alpha_z : \mathbb{C} \to \mathbb{C} : a \mapsto za$ für ein eindeutiges $z \in S^1$. Diese orthogonale Abbildung heißt die **Drehung** *um $\arg(z)$ (vgl. Definition nach Satz 8.11).*
*2.) $\alpha_z \circ \bar{} : \mathbb{C} \to \mathbb{C}$. Diese Abbildung heißt die (Orthogonal-)***Spieglung** *an der Geraden $G(0,w)$ mit $w^2 = z$.*

Beweis. Sei θ eine orthogonale Abbildung von $\mathbb{R}^2 = \mathbb{C}$. Da $1, i$ senkrecht aufeinander stehen und Länge 1 haben, gilt dies auch für $\theta(1), \theta(i)$. Sei $z := \theta(1)$. Dann folgt $z \in S^1$, sagen wir $z = \cos(t) + i\sin(t)$ für ein eindeutiges $t \in [0, 2\pi)$. Da $\theta(i) \in S^1$ auf z senkrecht steht, gibt es nur zwei Möglichkeiten:

$$\theta(i) = -\sin(t) + i\cos(t) = zi \text{ oder } \theta(i) = \sin(t) - i\cos(t) = z \cdot (-i).$$

Wegen der Linearität von θ sieht man im ersten Fall $\theta = \alpha_z$ und im zweiten $\theta = \alpha_z \circ {}^-$. Wir müssen zeigen, dass in beiden Fällen orthogonale Abbildungen vorliegen. Die Linearität ist eine einfache Übungsaufgabe. Weiter:

$$\Phi(\alpha_z(a), \alpha_z(a)) = za\overline{za} = \Phi(a, a)$$

und

$$\Phi(\alpha_z(\overline{a}), \alpha_z(\overline{a})) = z\overline{a}\overline{z\overline{a}} = \Phi(a, a)$$

Im zweiten Fall müssen wir noch den Namen Spieglung an der Geraden $G(0, w)$ rechtfertigen. Wegen $w^2 = z$ haben wir $w \in S^1$ und somit

$$\alpha_z(\overline{w}) = w^2\overline{w} = w$$

d. h. w ist ein Fixpunkt und damit bleibt $G(0, w)$ punktweise fest. Für die beiden Elemente $s \in S^1$, die auf w senkrecht stehen, bleiben nur noch zwei Möglichkeiten: Entweder bleiben beide fest oder sie werden vertauscht. Im ersten Fall läge aber die Identitätsabbildung vor, was nicht sein kann. Also haben wir eine Spieglung. q.e.d.

Bemerkung 8.22. *Die orthogonalen Abbildungen von $\mathbb{R}^2$ bilden eine Gruppe $\mathrm{O}(\mathbb{R}^2) = \mathrm{O}(\mathbb{R}^2, \Phi)$ genannt* **orthogonale Gruppe** *des $\mathbb{R}^2$, von denen die Drehungen eine Untergruppe $\mathrm{SO}(\mathbb{R}^2) = \mathrm{SO}(\mathbb{R}^2, \Phi)$ genannt* **spezielle orthogonale Gruppe** *des $\mathbb{R}^2$. Letztere ist kommutativ und isomorph zu $S^1 \cong \mathbb{R}/2\pi\mathbb{Z}$. Erstere ist nicht kommutativ:*

$$\alpha_z \circ {}^- = {}^- \circ \alpha_{\overline{z}}.$$

Wir wollen genauer verstehen, was der Unterschied ist zwischen der orthogonalen und der speziellen orthogonalen Gruppe. Dazu führen wir den orientierten Flächeninhalt ein. Wenn $n > 2$ ist, spricht man von einem orientierten Volumen. Zur Motivation werfen wir einen kurzen Blick auf den eindimensionalen Fall: Messen wir die Strecke in $\mathbb{R}$ von 0 bis 1 werden wir sagen $1 - 0 = 1$. Messen wir die Strecke von 1 bis 0, so werden wir sagen, dass dies genau so lang ist wie die verschobenen Strecke von 0 bis -1, also $-1 - 0 = -1$. Jedenfalls trägt das Vorzeichen Information. Außerdem haben wir gesehen, dass wir immer von Null aus messen können. Jetzt zur Definition für den zweidimensionalen Fall:

Definition 8.23. *1.) Seien $a, b \in \mathbb{R}^2$. Dann ist das von (a, b) aufgespannte* **Parallelogramm** *$P(a, b)$ durch*

$$P(a, b) := \{sa + tb \mid 0 \leq s, t \leq 1\} \subseteq \mathbb{R}^2$$

gegeben.
2.) Ein **orientierter Flächeninhalt** *oder* **Determinante** *auf $\mathbb{R}^2$ ist eine Abbildung*

$$f : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R} : (a, b) \mapsto f(a, b)$$

mit folgenden Eigenschaften:
a) f ist linear in der ersten Komponente, d. h. $f(sa + ta', b) = sf(a, b) + tf(a', b)$ für alle $s, t \in \mathbb{R}$ und alle $a, a', b \in \mathbb{R}^2$.
b) f ist schiefsymmetrisch, d. h. $f(a, b) = -f(b, a)$ für alle $a, b \in \mathbb{R}^2$.
c.) $f((1, 0), (0, 1)) = 1$.

Satz 8.24. *Ein orientierter Flächeninhalt auf* $\mathbb{R}^2$ *existiert und ist eindeutig. Er ist gegeben durch*

$$f : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R} : (a, b) \mapsto a_1 b_2 - a_2 b_1$$

Beweis. Eindeutigkeit: Da f schiefsymmetrisch ist und linear in der ersten Komponente, ist f auch linear in der zweiten Komponente. Also haben wir

$$\begin{aligned} f(a,b) &= f(a_1(1,0) + a_2(0,1), b) \\ &= a_1 f((1,0), b) + a_2 f((0,1), b) \\ &= a_1 f((1,0), b_1(1,0) + b_2(0,1)) + a_2 f((0,1), b_1(1,0) + b_2(0,1)) \\ &= a_1 b_1 f((1,0),(1,0)) + a_1 b_2 f((1,0),(0,1)) + \\ &\quad + a_2 b_1 f((0,1),(1,0)) + a_2 b_2 f((0,1),(0,1)) \\ &= (a_1 b_2 - a_2 b_1) \underbrace{f((1,0),(0,1))}_{1} \end{aligned}$$

Existenz: Man rechnet nach, dass die angegebene Formel alle 3 Bedingungen erfüllt. q.e.d.

Man wird nun $|f(a, b)|$ als den Flächeninhalt des Parallelogramms definieren. Die folgende Übung bringt die Orientierung, also das Vorzeichen des orientierten Flächeninhaltes, in Verbindung mit dem orientieren Winkel.

Übung: Zeige, $f(1, z) = \sin(\alpha)$ für $z \in S^1$, wo α der orientierte Winkel zwischen 1 und z ist. Wann ist insbesondere der orientierte Flächeninhalt positiv und wann negativ?

Mit dem Begriff des orientierten Flächeninhaltes kann man den Unterschied zwischen Spieglungen und Drehungen klar fassen: Erstere erhalten die Orientierung, letztere ändern sie. Genauer:

Definition 8.25. *Sei* $\theta : \mathbb{R}^2 \to \mathbb{R}^2$ *eine lineare Abbildung. Dann heißt*

$$f_\theta := \frac{f(\theta((1,0)), \theta((0,1)))}{f((1,0),(0,1))}$$

die **orientierte Flächenverzerrung** *von* θ.

Übung: Zeige, dass man statt mit $((1, 0), (0, 1))$ auch andere Paare $(a, b) \in (\mathbb{R}^2)^2$ nehmen kann, um dieselbe orientierte Flächenverzerrung zu bekommen. Welche Bedingung muss (a, b) erfüllen?

Satz 8.26. *Die orientierte Flächenverzerrung einer orthogonalen Abbildung ist* ± 1*, und zwar 1 bei Drehungen und* -1 *bei Spieglungen. Insbesondere ist die orientierte Flächenverzerrung ein surjektiver Homomorphismus* $\mathrm{O}(\mathbb{R}^2) \to (\{\pm 1\}, \cdot)$.

Beweis. Übung. q.e.d.

Kapitel 3

Körper und Ringe konstruktiv

In diesem Kapitel wollen wir einerseits die Existenzbeweise für den Ring der ganzen Zahlen, den Körper der rationalen Zahlen und den Körper der reellen Zahlen behandeln und über Polynome und Restklassenringe sprechen.

9 Ringe, 17. Vorlesung am 10.12.

Lernziel: Konstruktion der ganzen aus den natürliche Zahlen, Umgang mit Äquivalenzklassen in diversen Situationen, erweiterter EUKLIDischer Algorithmus, endliche Restklassenkörper von $\mathbb{Z}$, Polynomringe allgemein, univariate Polynomringe über Körpern mit erweiterten EUKLIDischen Algorithmus und Restklassenkörpern.

9.1 Die ganzen Zahlen

Sei $\mathbb{N}$ die Menge der natürlichen Zahlen. Nach den Peano Axiomen wissen wir:
1) Es gibt eine injektive Abbildung $\nu : \mathbb{N} \to \mathbb{N}$ mit $\mathbb{N} \setminus \nu(\mathbb{N}) = \{1\}$.
2) Ist M eine Teilmenge von $\mathbb{N}$ mit $1 \in M$ und $\nu(M) \subset M$, dann ist $M = \mathbb{N}$.

Aus diesen beiden Axiomen, haben wir die Addition, Multiplikation und die Anordnung auf der Menge der natürlichen Zahlen definiert und ihre wesentlichen Eigenschaften hergeleitet. Wir haben auf gezeigt, dass diese Eigenschaften die Menge der natürlichen Zahlen eindeutig charakterisieren (Satz 5.5).
Warum gibt es aber zunächst einmal die natürlichen Zahlen? Die folgende Definition konstruiert eine Menge, die die Peano-Axiome erfüllt, aus dem Nichts (also der leeren Menge): Wegen Satz 5.5 können wir diese Menge mit der Menge der natürlichen Zahlen identifizieren.

Definition 9.1. *(Skizze) Wir definieren rekursiv eine Menge N mit injektiver Nachfolgerfunktion $\nu : N \to N$ durch $1_N := \{\emptyset\}$ und für $n \in N$ sei $\nu(n) := n \cup \{n\} \in N$.*

Beachten Sie: Die Existenz einer solchen Menge N muss man fordern. Dass dann N die Peano-Axiome erfüllt kann man beweisen vgl. Halmos, "Naive Mengenlehre", Seite 60 ff. Es gilt $\nu(1_N) = \{\emptyset, \{\emptyset\}\}$, $\nu(\nu(1_N)) = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ usw.

Man könnte genausogut mit $0_N := \emptyset$ anfangen und dann $1_N := \emptyset \cup \{\emptyset\} = \{\emptyset\}$ setzen und hätte dann die Menge $\mathbb{N}_0$ aus der leeren Menge konstruiert.

Bemerkung 9.2. *Die Abbildung* $|\ |: N \to \mathbb{N}, n \mapsto |n|$ *ist eine Bijektion mit* $|\nu(n)| = |n| + 1$ *für alle* $n \in N$.

Erinnerung 9.3.

$$\tilde{\mathbb{Z}} := \mathbb{N} \times \mathbb{N}/\sim \ \textit{mit}\ (m,n) \sim (m',n') \Leftrightarrow n + m' = n' + m$$

Dabei wollten wir bei (m,n) *an die Gleichung oder besser Lösung der Gleichung* $x_{(m,n)} + n = m$ *denken.*

Satz 9.4. *1.) Durch*

$$+ : \tilde{\mathbb{Z}} \times \tilde{\mathbb{Z}} \to \tilde{\mathbb{Z}} : ([(m,n)]_\sim, [(s,t)]_\sim) \mapsto [(m+s, n+t)]_\sim$$

ist eine wohldefinierte Addition auf $\tilde{\mathbb{Z}}$ *festgelegt.*
2.) Durch

$$\cdot : \tilde{\mathbb{Z}} \times \tilde{\mathbb{Z}} \to \tilde{\mathbb{Z}} : ([(m,n)]_\sim, [(s,t)]_\sim) \mapsto [(ms+nt, mt+ns)]_\sim$$

ist eine wohldefinierte Multiplikation auf $\tilde{\mathbb{Z}}$ *festgelegt.*
3.) $f : \mathbb{N} \to \tilde{\mathbb{Z}} : n \mapsto [(n+1,1)]_\sim$ *ist injektiv und mit Multiplikation und Addition verträglich.*
4.) $(\tilde{\mathbb{Z}}, +, \cdot)$ *ist ein kommutativer Ring mit Eins, der die natürlichen Zahlen, genauer* $(\mathbb{N}, +, \cdot)$ *enthält. Weiter haben wir eine Totalordnung auf* $\mathbb{Z}$ *definiert durch* $s < t \Leftrightarrow t - s \in \mathbb{N}$*, weche verträglich mit der Addition ist.*

Beweis. Haben Sie i.w. in Übungsblatt 3, Aufgabe 8 gesehen. q.e.d.

Bezeichnungen 9.5. *Statt* $\tilde{\mathbb{Z}}$ *schreiben wir* $\mathbb{Z}$*, statt* $[(m,n)]$ *kurz* $m-n$*, statt* $[(1,1+m)]$ *kurz* $-m$ *und statt* $[(n,n)]$ *kurz* 0 *für alle* $n, m \in \mathbb{N}$*, sodass*

$$\mathbb{Z} = \underbrace{-\mathbb{N}}_{\{-n | n \in \mathbb{N}\}} \uplus \{0\} \uplus \mathbb{N}.$$

Definition 9.6. *Sei* R *ein Ring mit Eins. Die* **Einheitengruppe** R^* *von* R *ist definiert als*

$$R^* := \{r \in R | \exists r' \in R \textit{ mit } rr' = r'r = 1\}$$

Offenbar bildet die Einheitengruppe eine Gruppe bezüglich der Ringmultiplikation. Hier sind einige Beispiele:
Beispiele:
1.) $\mathbb{Z}^* = \{1, -1\}$.
2.) Ist K ein Körper, so gilt $K^* = K - \{0\}$

9.2 Der EUKLIDische Algorithmus für ganze Zahlen

Definition 9.7. *Seien $a, b \in \mathbb{Z}$.*
a) a ist ein **Teiler** *von b (geschrieben $a \mid b$), wenn ein $x \in \mathbb{Z}$ existiert mit mit $ax = b$. Teiler$(b) := \{$Teiler von $b\}$.*
b) Sei $(a, b) \neq (0, 0)$. Eine Zahl $t \in \mathbb{Z}$ heißt ein **größter gemeinsamer Teiler** *von a und b (geschrieben $t = \mathrm{ggT}(a, b)$), falls Teiler$(a) \cap$ Teiler$(b) =$ Teiler(t). Wir setzen $\mathrm{ggT}(0, 0) := 0$.*
c) Sei $t, x, y \in \mathbb{Z}$. Dann heißt $t = xa + yb$ eine **Darstellung** *von t durch a, b. Eine Darstellung von $t := \mathrm{ggT}(a, b)$ durch a, b heißt eine* BÉZOUT**-Identität**[1] *für a, b.*

Bemerkung 9.8. *Seien $a, b, c \in \mathbb{Z}$ und $e, f \in \mathbb{Z}^*$.*
a) $a \mid b \iff ea \mid fb$.
b) $a \mid b \wedge b \mid c \Rightarrow a \mid c$
c) $a \mid b \wedge b \mid a \Rightarrow a \in \{eb \mid e \in \mathbb{Z}^*\}$
d) $a \mid b \wedge a \mid c \Rightarrow a \mid xb + yc$ für alle $x, y \in \mathbb{Z}$
e) Der größte gemeinsame Teiler von a, b ist bis auf Multiplikation mit Einheiten eindeutig bestimmt.

Beweis. Übung. q.e.d.

Bemerkung 9.9. *a) Für $b \in \mathbb{Z}$ sei*

$$|b| := \begin{cases} b & b \geq 0 \\ -b & b < 0 \end{cases}$$

der Absolutbetrag von b (die Einschränkung des reellen Absolutbetrags) und

$$sgn(b) = \begin{cases} 1, & b > 0, \\ 0, & b = 0, \\ -1, & b < 0. \end{cases}$$

Dann ist $|b| = sgn(b) \cdot b$ bzw. $b = sgn(b) \cdot |b|$.
b) Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann gibt es ein $q, r \in \mathbb{Z}$ mit

$$a = qb + r \text{ und } 0 \leq r < |b|.$$

r heißt auch der kleinste nicht negative **Rest** *von a modulo b. Abkürzung: $r = a \bmod b$.*

Algorithmus 9.10. *(*EUKLID*ischer Algorithmus)*
Gegeben: $a, b \in \mathbb{Z}$.
Gesucht: $\mathrm{ggT}(a, b)$ *sowie $x, y \in Z$ 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 $r_0 := |a|, \quad x_0 := 1, \quad y_1 := 0,$
$r_1 := |b|, \quad x_1 := 0, \quad y_1 := 1.$

[1] ÉTIENNE BÉZOUT 1730 - 1783

Für $i \geq 1$ sei q_i definiert durch $r_{i-1} = q_i r_i + r$ mit $0 \leq r < |r_i|$ (vgl. 9.9). Setze nun
$r_{i+1} := \quad r = \quad r_{i-1} - q_i r_i,$
$x_{i+1} := \qquad x_{i-1} - q_i x_i,$
$y_{i+1} := \qquad y_{i-1} - q_i y_i.$
Nach endlich vielen Schritten hat man das erste $n \in \mathbb{N}$ mit $r_{n+1} = 0$.
Dann ist $r_n = \mathrm{ggT}(|a|, |b|) \overset{9.8a)}{=} \mathrm{ggT}(a, b)$ und $r_n = \underbrace{x_n \cdot sgn(a)}_{=:x} \cdot a + \underbrace{y_n \cdot sgn(b)}_{=:y} \cdot b$.

Beweis. Der EUKLIDische Algorithmus bricht nach endlich vielen Schritten ab, da für $i \geq 1$ gilt: $r_i \geq 0$ und $r_{i+1} < r_i$.
Des Weiteren ist $r_n = \mathrm{ggT}(a, b)$, da für $1 \leq i \leq n$ gilt:

$$\mathrm{ggT}(r_{i-1}, r_i) \overset{\text{Übung}}{=} \mathrm{ggT}(r_i, r_{i-1} - q_i r_i) = \mathrm{ggT}(r_i, r_{i+1}).$$

Außerdem ist offensichtlich $\mathrm{ggT}(r_n, 0) = |r_n| = r_n$. Damit ist also gezeigt, dass der EUKLIDische Algorithmus nach endlich vielen Schritten den $\mathrm{ggT}(a, b)$ liefert.
Weiterhin gilt für alle $0 \leq i \leq n$: $r_i = x_i \cdot |a| + y_i \cdot |b|$, denn:

IA Für $i = 0, 1$ gilt die Aussage per Definition von r_i, x_i, y_i.

IV Es sei $2 \leq i \leq n$, und die Behauptung gelte für $i - 1$ und $i - 2$.

IS Dann ist

$$x_i|a| + y_i|b| = (x_{i-2} - q_{i-1}x_{i-1})|a| + (y_{i-2} - q_{i-1}y_{i-1})|b|$$

$$= (x_{i-2}|a| + y_{i-2}|b|) - q_{i-1}(x_{i-1}|a| + y_{i-1}|b|) \overset{IV}{=} r_{i-2} - q_{i-1}r_{i-1} = r_i.$$

Mit 9.9 b) erhalten wir also $r_n = x_n|a| + y_n|b| = (x_n \cdot sgn(a)) \cdot a + (y_n \cdot sgn(b)) \cdot b$. □

Beispiel: $a := 1002$, $b := 912$:

i	r_i	q_i	x_i	y_i
0	1002	–	1	0
1	912	1	0	1
2	90	10	1	−1
3	12	7	−10	11
4	6	2	71	−78
5	0			

Also ist der $\mathrm{ggT}(1002, 912) = 6 = 71 \cdot 1002 - 78 \cdot 912$.
Variante: Berechne nur die r_i und q_i, erhalte so $r_n = \mathrm{ggT}(a, b)$, und ersetze dann rückwärts von $i = n$ bis 2 jedes r_i durch $r_{i-2} - q_{i-1}r_{i-1}$:

$$\mathrm{ggT}(1002, 912) = 6 = 90 - 7 \cdot 12$$

$$= 90 - 7 \cdot (912 - 10 \cdot 90) = 71 \cdot 90 - 7 \cdot 912$$

$$= 71 \cdot (1002 - 912) - 7 \cdot 912 = 71 \cdot 1002 - 78 \cdot 912.$$

Folgerung 9.11. *Seien $a, b \in \mathbb{Z}$. Dann existiert der $ggT(a, b)$ und eine* BÉZOUT*-Identität für a, b.*

Beweis. Der Fall $(a, b) = (0, 0)$ ist klar. Sei oBdA $b \neq 0$. Setze $a_1 := a, a_2 := b$ und definiere wie im EUKLIDischen Algorithmus a_3 durch $|a_3| < |a_2|$ und $a_1 = q_1 a_2 + a_3$ für ein $q_1 \in \mathbb{Z}$ (entweder über den kleinsten postiven Rest oder alternativ über den absolut kleinsten Rest bei der Division). Entsprechend konstruiert man aus a_2, a_3 das nächste Folgenglied a_4 und den Quotienten q_2 bis zum ersten Mal $a_i = 0$.
Behauptung: a_n läßt sich durch a, b darstellen für alle $n < i$.
Dies läßt sich durch Induktion beweisen. Ich gebe nur die Idee: a_1, a_2, a_3 lassen sich offensichtlich durch $a = a_1$ und $b = a_2$ darstellen. Beim Induktionsschritt lässt sich a_{n+1} nach Konstruktion durch a_n, a_{n-1} darstellen. Nach Induktionsannahme lassen sich a_n, a_{n-1} durch a, b darstellen. Setzen wir diese beiden Darststellungen in die von a_{n+1} durch a_n, a_{n-1} ein, so erhalten wir eine Darstellung von a_{n+1}.
An Ende haben wir die gesuchte BÉZOUT-Identität. q.e.d.

Beispiel:
Die FIBONACCI-Folge[2] $F := (1, 1, 2, 3, 5, 8, 13, 21, 34, \cdots)$ mit $F_1 = F_2 = 1$ und $F_{n+1} = F_n + F_{n-1}$ für $n \geq 2$ liefert, wenn man den EUKLIDischen Algorithmus auf zwei hintereinanderliegende Glieder F_n, F_{n-1} anwendet, ungefähr $n - 3$ Schritte im Verfahren bei Division mit nicht negativen kleinsten Resten. Arbeitet man mit absolut kleinsten Resten, so scheint sich das Verfahren auf etwa die Hälfte der Schritte zu reduzieren:

$$\begin{array}{lll}
\underline{34} = 2 \cdot \underline{21} + \underline{(-8)} & \text{also} & \underline{(-8)} = \underline{34} - 2 \cdot \underline{21} \\
\underline{21} = -3 \cdot \underline{(-8)} + \underline{(-3)} & \text{also} & \underline{(-3)} = \underline{21} + 3 \cdot \underline{(-8)} = 3 \cdot \underline{34} - 5 \cdot \underline{21} \\
\underline{-8} = 3 \cdot \underline{(-3)} + \underline{1} & \text{also} & \underline{1} = \underline{-8} - 3 \cdot \underline{(-3)} = -8 \cdot \underline{34} + 13 \cdot \underline{21} \\
\underline{-3} = -3 \cdot \underline{1} + \underline{0} & \text{also} & \underline{0} = \underline{-3} + 3 \cdot \underline{1} = -21 \cdot \underline{34} + 34 \cdot \underline{21}
\end{array}$$

Wir hätten bereits in der vorletzten Zeile aufhören können, weil dort bereits eine BÉZOUT-Identität stand. Indem wir aber Vielfache der letzten Zeile zu der vorletzten addieren, bekommen wir alle BÉZOUT-Identitäten,

$$1 = (-8 - 21x)34 + (13 + 34x)21 \text{ für alle } x \in \mathbb{Z}$$

die den größten gemeinsamen Teiler 1 durch 34 und 21 darstellen. Übrigens ist es interessant zu sehen, dass die früheren FIBONACCI-Zahlen immer wieder bis aufs Vorzeichen als Koeffizienten auftauchen in den Darstellungen.
Weihnachtsübung: Für die Fibonacci Folge (F_n) gilt für alle $n, m \in \mathbb{N}$:
(a) $F_{n+m} = F_{m-1}F_n + F_m F_{n+1}$
(b) F_n teilt F_{nm}.
(c) $\mathrm{ggT}(F_n, F_m) = F_{\mathrm{ggT}(n,m)}$.
Ende der 17. Vorlesung am 10.12.2013

Definition 9.12. *Eine Zahl $p \in \mathbb{Z}$ heißt* **Primzahl**, *falls $p > 1$ und*

$$\textit{für alle } n, m \in \mathbb{Z} \textit{ gilt } p|nm \Rightarrow p|n \textit{ oder } p|m.$$

[2] LEONARDO PISANO FIBONACCI 1170 - 1250

Bemerkung 9.13. $1 < p \in \mathbb{Z}$ *ist eine Primzahl genau dann wenn Teiler*$(p) = \{1, -1, p, -p\}$.

Beweis. $\Rightarrow$ (gilt immer): Sei p eine Primzahl. Es gilt immer Teiler$(p) \supseteq \{1, -1, p, -p\}$. Sei also d ein Teiler von p. Dann gibt es $a \in \mathbb{Z}$ mit $p = da$. Wegen $p \mid p$ folgt also $p \mid d$ (und dann ist $a = \pm 1$, $d = \pm p$) oder $p \mid a$ (und dann ist $d = \pm 1$, $a = \pm p$). $\Leftarrow$ (Hier brauchen wir die BÉZOUT-Identität):
Angenommen $p \nmid n \wedge p \nmid m$. Dann gibt es $a, b, c, d \in \mathbb{Z}$ mit

$$1 = ap + bn \text{ und } 1 = cp + dm.$$

Indem wir diese beiden BÉZOUT-Identitäten miteinander multiplizieren bekommen wir $e, f \in \mathbb{Z}$ mit

$$1 = ep + fnm,$$

also $p \nmid mn$. q.e.d.

Satz 9.14. *Jedes Element $a \neq 0$ von $\mathbb{Z}$ hat eine bis auf Reihenfolge und Vorzeichen eindeutige Produktzerlegung in Primfaktoren.*

Beweis. Sei $a \in \mathbb{Z}, a \neq 0$. Ist $a = 1$, so ist a =leeres Produkt und $-1 = -$leeres Produkt. Sei also Œ$a > 1$. Ist a prim, so sind wir fertig. Anderenfalls existieren $b, c \in \mathbb{Z}$ mit $a = bc$ und $1 < |b|, |c| < |a|$. Faktorisiere die Faktoren weiter. Nach endlich vielen Schritten hat man eine Zerlegung in Primfaktoren. Die Eindeutigkeit dieser Zerlegung folgt mit Bemerkung 9.13. Angenommen $a = p_1 \dots p_s = q_1 \dots q_t$ mit q_i, p_j Primzahlen. Dann gilt $p_1 \mid q_1 \dots q_t$, also gibt es ein i mit $p_1 \mid q_i$. Da q_i prim ist folgt mit Bemerkung 9.13, dass $p_1 = q_i$. Nach Teilen durch p_1 erhalten wir eine kürzere Produktdarstellung. Also folgt durch Induktion über s, dass es eine Bijektion $\sigma : \{1, \dots, s\} \to \{1, \dots, t\}$ gibt mit $p_i = q_{\sigma(i)}$ für alle i. Insbesondere ist $s = t$. □

Man kann nun aus $\mathbb{Z}$ diverse neue Ringe und sogar Körper konstruieren: Dies geht einerseits durch Bereichsvergröberung oder durch Bereichserweiterung von statten. Wir folgen zuerst dem ersten Prinzip.

9.3 Restklassenkörper von $\mathbb{Z}$, 18.Vorlesung am 11.12.

In Bemerkung 6.2 4 hatten wir über Kongruenzrelationen gesprochen, die in der Situation betrachtet werden, wo eine Gruppe G mit einer Untergruppe H gegeben ist. Die Äquivalenzklassen gH mit $g \in G$ hatten wir Restklassen genannt. Im Allgemeinen vererbt die Gruppe ihre Gruppenstruktur nicht auf die Menge der Restklassen, weil $gH \cdot kH := \{st | s \in gH, t \in kH\}$ in den meisten Fällen keine Restklasse nach H ist, sondern die Vereinigung von mehreren Restklassen. Wir wollen ein wichtiges Beispiel studieren, in dem sich nicht nur die Gruppenstruktur auf die Restklassenmenge vererbt, sondern noch viel mehr Struktur erhalten bleibt. Es handelt sich um die additive Gruppe von Ringen und als Untergruppe nimmt man sogenannte Ideale, die sicherstellen, dass die Restklassen vermöge der vertreterweise definierten Addition und Multiplikation wieder einen Ring bilden.

Satz 9.15. *Sei $m \in \mathbb{Z}$. Dann ist*

$$m\mathbb{Z} := \{mn \mid n \in \mathbb{Z}\} \leq (\mathbb{Z}, +),$$

und die zugehörige Kongruenzrelation $\equiv$ oder genauer $\equiv_m$ ist verträglich sowohl mit der Addition als auch mit der Multiplikation von $\mathbb{Z}$, sodass die Restklassen

$$k + m\mathbb{Z} := \{k + mn \mid n \in \mathbb{Z}\}, \qquad k \in \mathbb{Z}$$

bezüglich der vetreterweisen Addition und Multiplikation einen kommutativen Ring $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ mit Eins bilden. Im Falle $m \notin \mathbb{Z}^*$ gilt $1 \neq 0$ in $\mathbb{Z}/m\mathbb{Z}$.

Beweis. Dass $m\mathbb{Z}$ Untergruppe von $(\mathbb{Z}, +)$ ist, ist klar. Wir zeigen die Verträglichkeit der Äquivalenzrelation $\equiv_m$, sowohl mit der Addition als auch mit der Multiplikation. Seien also $k \equiv_m k'$ und $j \equiv j' \pmod m$. Dann behaupten wir: $k + j \equiv_m k' + j'$ und $kj \equiv_m k'j'$.
Zum Beweis: $k \equiv_m k'$ impliziert $m \mid k - k'$ und entsprechend $m \mid j - j'$, sodass m auch die Summe teilt, also $m \mid (k + j) - (k' + j')$, d. h. $k + j \equiv_m k' + j'$,
Zum Produkt: $m \mid k-k'$ impliziert $m \mid j(k-k')$. Entsprechend bekommen wir $m \mid k'(j-j')$, also teilt m auch die Summe, d. h. $m \mid jk - j'k'$, also $kj \equiv_m k'j'$.
Damit sind die vertreterweise definierten Addition und Multiplikation wohldefiniert:

$$[j] + [k] := [j + k] \text{ und } [j][k] := [jk] \ \forall j, k \in \mathbb{Z} \text{ mit } [j] := j + m\mathbb{Z}.$$

Sämtliche Assoziativ-, Kommutativ- und Distributivgesetze vererben sich auf $\mathbb{Z}/m\mathbb{Z}$. Weiter ist [0] das Null- und [1] das Einselement, $-[j] = [-j]$, sodass wirklich ein kommutativer Ring mit Eins vorliegt. q.e.d.

Folgerung 9.16. *$\pi = \pi_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} : j \mapsto j + m\mathbb{Z}$ ist ein surjektiver Ringhomomorphismus, dessen Fasern gerade die Elemente von $\mathbb{Z}/m\mathbb{Z}$ sind.*
Wegen der Division mit Rest gilt $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$.

Diese Ringe haben allerdings gewöhnungsbedürftige Eigentümlichkeiten:
1.) Sei $m = 4$. Dann gilt $(2 + 4\mathbb{Z})^2 = 0$ ohne dass $2 + 4\mathbb{Z}$ gleich Null wäre. (Nilpotentes Element).
2.) $m = 6$. Dann gilt $(4 + 6\mathbb{Z})(3 + 6\mathbb{Z}) = 0$ ohne dass $4 + 6\mathbb{Z}$ oder $3 + 6\mathbb{Z}$ nilpotent wären (nicht nilpotente Nullteiler).
3.) $m = 1001$. Dann ist $12 + 1001\mathbb{Z}$ invertierbar: Wir berechnen eine BÉZOUT-Identität für $12, 1001$:

$$-417 \cdot 12 + 5 \cdot 1001 = 1$$

und wenden π_{1001} an, um

$$[-417][12] = [1]$$

zu erhalten.

Übung: Wie kann man π_3, π_9, π_{11} sehr leicht über die iterierte Quersumme bzw. iterierte alternierenden Quersumme im Dezimalsystem leicht ausrechnen? Z. B. $\pi_{11}(34566) = \pi_{11}(6 - 6 + 5 - 4 + 3) = \pi_{11}(4) = [4]$. Wie kann man π_{10} oder π_{100} bestimmen? Wie kann

man dies zur Kontrolle von Rechnungen mit ganzen Zahlen einsetzen?

Übung: Zeige: Ist $\sim$ eine Äquivalenzrelation auf $\mathbb{Z}$, welche verträglich mit der Addition und Multiplikation von ganzen Zahlen ist, so existiert ein $m \in \mathbb{Z}$ mit $\sim = \equiv_m$.

Wir heben jetzt den wichtigsten Fall in Satz 9.15 heraus, der uns unendlich viele neue Körper beschert.

Satz 9.17. *Sei $p \in \mathbb{N}$ eine Primzahl. Dann gibt es bis auf Isomorphie genau einen Körper $\mathbb{F}_p$ von p Elementen, nämlich $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

Beweis. Existenz: Wir zeigen, dass $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist. Zu diesem Zweck brauchen wir nur zu zeigen, dass $0 \neq [j] \in \mathbb{Z}/p\mathbb{Z}$ invertierbar ist. Da $p \nmid j$ und p prim ist, haben wir $1 = \mathrm{ggT}(i, p)$ und bekommen eine BÉZOUT-Identität für j, p: Es existieren $x, y \in \mathbb{Z}$ mit

$$xj + yp = 1,$$

sodass $[x] = [j]^{-1}$.
Eindeutigkeit: (Dies haben Sie schon in der Übung gesehen)
Sei F ein Körper mit p Elementen. Offenbar (vgl. Bemerkung 6.5) hat man einen Ringhomomorphismus

$$f := \mathbb{Z} \to F : i \mapsto i \cdot 1.$$

Da $(F, +)$ eine Gruppe von p Elementen ist, würde eine Untergruppe entweder nur 1 oder p Elemente haben, weil keine anderen Teiler von p existieren und alle Restklassen nach einer Untergruppe gleich viele Elemente enthalten. Also ist f surjektiv und $f^{-1}(\{0_F\}) = p\mathbb{Z} \subseteq \mathbb{Z}$. Aus dem Distributivgesetz in F folgt, dass F nur eine Multiplikation zulässt. Es folgt dass

$$\overline{f} : \mathbb{Z}/p\mathbb{Z} \to F, [j] \mapsto f(j)$$

ein wohldefinierter Ringisomorphismus ist. q.e.d.

Übung: Zeige $|(\mathbb{Z}/p^n\mathbb{Z})^*| = (p-1)p^{n-1}$ für jede Primzahl p und jede natürliche Zahl n.

9.4 Der Polynomring über einem Körper, 19.Vorlesung am 17.12.

Bemerkung 9.18. *Sei R ein kommutativer Ring mit 1 (z.B. ein Körper). Die Menge der* **endlichen Folgen**

$$(R^{\mathbb{N}_0})_{endl} := \{(a_0, \ldots, a_n) \mid n \in \mathbb{N}_0, a_i \in R \text{ für alle } i \in \{0, \ldots, n\}\}$$

wird mit komponentenweiser Addition zu einer abelschen Gruppe $(R^{\mathbb{N}_0}_{endl}, +)$. Wir definieren eine Multiplikation $\cdot : R^{\mathbb{N}_0}_{endl} \times R^{\mathbb{N}_0}_{endl} \to R^{\mathbb{N}_0}_{endl}$ durch

$$(a_0, \ldots, a_n)(b_0, \ldots, b_m) := (c_0, \ldots, c_{m+n}), \text{ wobei } c_k := \sum_{i+j=k} a_i b_j \in R.$$

Dann wird $(R^{\mathbb{N}_0}_{endl}, +, \cdot)$ zu einem kommutativen Ring mit $1 = (1, 0, \ldots, 0)$. $(R^{\mathbb{N}_0}_{endl}, +, \cdot)$ heißt der **Polynomring** *über R. Anstelle von $(R^{\mathbb{N}_0}_{endl}, +, \cdot)$ schreibt man auch $R[x]$ und für $(a_0, \ldots, a_n) \in R[x]$ das* **Polynom** $p = a_n x^n + \ldots + a_1 x^1 + a_0$.

Der Beweis ist elementares Nachrechnen. Der Polynomring ist ein Spezialfall einer allgemeineren Konstruktion, dem Halbgruppenring, die ich unten näher spezifiziere. Die Multiplikation ergibt sich aus dem Distributivgesetz und der Vorschrift $x^n x^m = x^{n+m}$, wie Sie es aus der Schule gewöhnt sind.

Bemerkung 9.19. *(a) Zwei Polynome sind gleich, genau dann wenn alle ihre Koeffizienten übereinstimmen.*
(b) Die Abbildung $R \to R[x], a \mapsto a = (a, 0, \ldots, 0)$ ist ein injektiver Ringhomomorphismus vermöge dem wir R als Teilring von $R[x]$ ansehen.

Definition 9.20. *Sei K ein Körper.*
1.) Ist $r \in K$, so heißt

$$\epsilon_r : K[x] \to K : p = p(x) = \sum_{i=0}^{n} a_i x^i \to p(r) := \sum_{i=0}^{n} a_i r^i$$

der zu r gehörige **Einsetzungshomomorphismus**.
2.) Für $p = p(x) \in K[x]$ heißt

$$\tilde{p} : K \to K : r \mapsto p(r)$$

die von p induzierte **Polynomfunktion**.

Übung: Zeige für $p = p(x) \in K[x]$ und $r \in K$ sind äquivalent:
1.) r ist **Nullstelle** von $\tilde{p}$, d. h. $\tilde{p}(r) = 0$.
2.) r ist **Wurzel** von p, d. h. $\epsilon_r(p) = 0$.
3.) $x - r$ teilt $p(x)$ in $K[x]$, d. h. $(x - r) \mid p(x)$.
Zu 3.) berechne man

$$(a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0) : (x - r) =$$
$$a_n x^{n-1} + (a_n r + a_{n-1}) x^{n-2} + \ldots + (a_n r^{n-1} + a_{n-1} r^{n-2} + \ldots + a_1) x \text{ mit Rest } p(r).$$

Später werden wir sehen, dass wir nicht nur Zahlen in Polynome einsetzen können sondern noch viel kompliziertere Elemente aus diversen Ringen. Wir belassen es hier bei den Körperelementen aus K und betrachten den Fall, wo wir das einzusetzende Körperelement noch variabel lassen.

Satz 9.21. *Sei K ein Körper. Dann ist K^K mit der werteweisen Addition und Multiplikation, also $f + g : K \to K : r \mapsto f(r) + g(r)$ und $fg : K \to K : r \mapsto f(r)g(r)$, ein kommutativer Ring mit Eins. Weiter ist*

$$K[x] \to K^K : p \mapsto \tilde{p}$$

ein Ringhomomorphismus. Das Bild dieses Homomorphismus besteht aus allen Polynomfunktionen von K.

Beweis. Wir müssen zeigen $\widetilde{p+q} = \tilde{p} + \tilde{q}$ und $\widetilde{pq} = \tilde{p}\tilde{q}$ für alle $p = \sum_i a_i x^i, q = \sum_i b_i x^i \in K[x]$. Für $r \in K$ gilt:

$$\begin{aligned}(\widetilde{p+q})(r) &= \sum_i (a_i + b_i) r^i \\ &= \sum_i a_i r^i + \sum_i b_i r^i \\ &= \tilde{p}(r) + \tilde{q}(r) \\ &= (\tilde{p} + \tilde{q})(r)\end{aligned}$$

Da r geliebig war, ist somit $\widetilde{p+q} = \tilde{p} + \tilde{q}$ gezeigt. Ebenso folgt $\widetilde{pq} = \tilde{p}\tilde{q}$ aus:

$$\begin{aligned}(\widetilde{pq})(r) &= \sum_i (\sum_k (a_k b_{i-k}) r^i \\ &= \sum_k a_k r^k \sum_j b_j r^j \\ &= \tilde{p}(r)\tilde{q}(r) \\ &= (\tilde{p}\tilde{q})(r)\end{aligned}$$

q.e.d.

Beispiel: $\mathbb{F}_2[x] \to \mathbb{F}_2^{\mathbb{F}_2}$ ist surjektiv aber nicht injektiv. Da in $\mathbb{F}_2$ für alle Elemente a gilt, dass $a^2 + a = 0$ ist, haben das Nullpolynom $0 \in \mathbb{F}_2[x]$ und $p := x^2 + x \in \mathbb{F}_2[x]$ dasselbe Bild in $\mathbb{F}_2^{\mathbb{F}_2}$, $\tilde{p}(a) = 0$ für alle $a \in \mathbb{F}_2$.

9.5 Der EUKLIDische Algorithmus für Polynomringe über Körpern

Wir wollen uns davon überzeugen, dass der Polynomring $K[x]$ über einem Körper K vielerlei Ähnlichkeit mit dem Ring $\mathbb{Z}$ der ganzen Zahlen hat und insbesondere einen EUKLIDischen Algorithmus zulässt. Diese Tatsache hat viele wichtige Konsequenzen. Zuerst muss man sich fragen, wie man die Division mit Rest überträgt, insbesondere, wie man sieht, dass der Rest wirklich "kleiner" geworden ist. Im folgenden bezeichnet K immer einen Körper.

Definition 9.22. *Sei $p(x) := a_n x^n + \ldots + a_0 \in K[x]$ mit $a_n \neq 0$. Dann heißt n der* **Grad von $p(x)$.**

Der Grad ist also für jedes Polynom $\neq 0$ definiert und liefert unmittelbar die folgenden Einsichten:

Bemerkung 9.23. *1.) $p, q \in K[x] - \{0\}$. Dann gilt:* $\mathrm{Grad}(pq) = \mathrm{Grad}(p) + \mathrm{Grad}(q)$.
2.) Insbesondere ist $K[x]^* = K^*$ und $K[x]$ hat keine Nullteiler $\neq 0$. Ein Polynom vom Grad n heißt **normiert**, *falls der* **führende Koeffizient**, *also der Koeffizient von x^n, gleich Eins ist.*

Beispiel. In $(\mathbb{Z}/4\mathbb{Z})[x]$ gilt $\mathrm{Grad}((2x^2+1)(2x+2)) = \mathrm{Grad}(2x+2) = 1$. Teil 1) benutzt also wesentlich, dass ein Körper keine Nullteiler hat.

Definition 9.24. *Seien $p, q \in K[x]$. Wir sagen p teilt q ($p \mid q$), falls es ein Polynom $a \in K[x]$ gibt mit $q = ap$. Teiler$(q) := \{p \in K[x] \mid p \mid q\}$ ist die Menge der Teiler von q.*
Ein Polynom $t \in K[x]$ heißt **größter gemeinsamer Teiler** *von p und q, $t = \mathrm{ggT}(p,q)$, falls Teiler$(q) \cap$ Teiler$(p) =$ Teiler(t).*
Ein Polynom p heißt **irreduzibel**, *falls Teiler$(p) = K[x]^* \cup pK[x]^*$.*

Klar: $a \in$Teiler$(p) \Rightarrow \mathrm{Grad}(a) <= \mathrm{Grad(p)}$.

Übung: Ein Polynom in $K[x]$ vom Grad 2 oder 3 ist genau dann irreduzibel, wenn es keine Nullstellen in K hat. Wie steht es mit Polynomen vom Grad 4?

Lemma 9.25. *(Division mit Rest in $K[x]$) Seien $a, b \in K[x] - \{0\}$ mit $m := \mathrm{Grad}(b)$. Dann gibt es eindeutige $q, r \in K[x]$ mit $r = 0$ oder $\mathrm{Grad}(r) < m$ und $a = qb + r$*

Beweis. Existenz: Wenn $a = 0$ oder $n := \mathrm{Grad}(a) < m$ ist nicht zu zeigen. Anderenfalls kann man sehr leicht den Grad von $a = a_n x^n + \ldots + a_0$ um mindestens eins erniedrigen: Ersetze a durch $a - a_n/b_m x^{n-m} b$. Nach maximal $n - m$ Schritten summiert man die Vorfaktoren von b zu q auf und hat die Existenz von q und r.
Eindeutigkeit: Sei $a = q'b + r'$ eine weitere Identität mit den obigen Eigenschaften. Dann folgt durch Differenzenbildung:

$$0 = (q - q')b + (r - r').$$

Im Falle $q \neq q'$ folgt $b \mid r - r'$, was aber aus Gradgründen nicht möglich ist. q.e.d.

Durch dieses Lemma wird nun vieles möglich, was wir bereits beim Ring $\mathbb{Z}$ der ganzen Zahlen gesehen hatten:

Folgerung 9.26. *Sei K ein Körper. Für den Polynomring $K[x]$ gilt:*
1.) In $K[x]$ hat man einen erweiterten Euklid*ischen Algorithmus.*
2.) Insbesondere hat jedes Polynom eine bis auf Reihenfolge der Faktoren eindeutige multiplikative Zerlegung in normierte irreduzible (=prime) Polynome und eine Einheit.
3.) Ist $p = p(x) \in K[x]$ vom Grad ≥ 1, dann bilden die Restklassen

$$[r] := r + pK[x] := \{r + ps \mid s \in K[x]\}$$

unter der vertreterweise definierten Addition und Multiplikation eine Restklassenring $K[x]/pK[x]$. Ist $n = \mathrm{Grad}(p)$, so liefert die Division mit Rest für jede Klasse in $K[x]/pK[x]$ einen eindeutigen Vertreter vom Grad $< n$,

$$K[x]/pK[x] = \{[q] \mid q \in K[x], q = 0 \text{ oder } \mathrm{Grad}(q) < n\}.$$

$K[x]/pK[x]$ ist genau dann ein Körper, wenn p irreduzibel ist. In diesem Fall enthält $F := K[x]/pK[x]$ den Grundkörper K als Teilkörper, und $[x] \in F$ ist eine Wurzel von $p(x)$.

Beweis. Alles geht analog zum Fall der ganzen Zahlen.
1.) Mit der Division mit Rest erhalten Sie einen Euklidischen Algorithmus, der wie bei $\mathbb{Z}$ eine BÉZOUT-Identität $\mathrm{ggT}(p,q) = ap + bq$ mit $a, b \in K[x]$ konstruiert.
2.) Primelemente sind Polynome p mit der Eigenschaft $p \mid ab \Rightarrow p \mid a \ \vee p \mid b$. Dass prim und irreduzibel in $K[x]$ dasselbe bedeuten, überträgt sich sehr leicht mit der BÉZOUT-Identität.
3.) Einzelheiten lassen wir als Übung. Nur eins ist neu:
K ist eingebettet in F und es gilt $p([x]) = [p(x)] = 0$. q.e.d.

Beispiel (Von oben.) Es gilt $\mathbb{F}_2[x]/(x^2+x)\mathbb{F}_2[x] \cong \mathbb{F}_2^{\mathbb{F}_2}$. Wir definieren dazu $\varphi : \mathbb{F}_2[x]/(x^2+x)\mathbb{F}_2[x]$ durch $\varphi([p]) = \widetilde{p}$. Dann ist φ wohldefiniert, da für $[p] = [q]$ gilt, dass $(x^2+x) \mid (p-q)$ also $q = p + a(x^2+x)$ und somit $\widetilde{q} = \widetilde{p} + \widetilde{a}\widetilde{x^2+x} = \widetilde{p}$ da $\widetilde{x^2+x}$ die Nullfunktion ist. Da das Rechnen im Restklassenring vertreterweise erfolgt und $\widetilde{\ } : \mathbb{F}_2[x] \to \mathbb{F}_2^{\mathbb{F}_2}$ ein Ringhomomorphismus ist, folgt auch dass φ ein Ringhomomorphismus ist. Die Bijektivität zeigt man z.B. durch Angabe der Umkehrfunktion

$$\varphi^{-1} : \mathbb{F}_2^{\mathbb{F}_2}, f \mapsto [(f(1) + f(0))x + f(0)].$$

Beispiel (Algebraische Konstruktion von $\mathbb{C}$ aus $\mathbb{R}$)
$x^2 + 1 \in \mathbb{R}[x]$ ist irreduzibel, also ist $\mathbf{C} := \mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ ein Körper.

$$\varphi : \mathbb{R}[x]/(x^2+1)\mathbb{R}[x] \cong \mathbb{C}, [ax+b] \mapsto ai + b$$

ist ein Körperisomorphismus. Es gilt für $a, b, c, d \in \mathbb{R}$:

$$[ax+b]\cdot[cx+d] = [acx^2+(ad+bc)x+bd] = ac[x]^2+(ad+bc)[x]+bd[1] = (bd-ac)[1]+(ad+bc)[x]$$

Übung: Sei $x^2+ax+b \in \mathbb{R}[x]$ irreduzibel, also $a^2-4b < 0$. Zeige $\mathbb{R}[x]/(x^2+ax+b)\mathbb{R}[x] \cong \mathbb{C}$.

Beispiel (Der Körper mit vier Elementen)
$x^2 + x + 1 \in \mathbb{F}_2[x]$ ist irreduzibel. Also ist $\mathbb{F}_4 := \mathbb{F}_2[x]/(x^2+x+1)\mathbb{F}_2[x]$ ein Körper mit Elementen

$$\mathbb{F}_4 = \{0, 1, \omega := [x], \omega + 1\}$$

Es gilt $\omega^2 = \omega + 1$.

Lemma 9.27. *Ist $p(x) \in \mathbb{Q}[x]$ vom Grad $n > 0$ und normiert mit ganzzahligen Koeffizienten, so gilt: Jede rationale Wurzel von $p(x)$ liegt bereits in $\mathbb{Z}$ und teilt $p(0)$.*

Beweis. Sei $a/b \in \mathbb{Q}$ Wurzel von $p(x)$ mit $a \in \mathbb{Z}$ und $b \in \mathbb{Z} - \{0\}$ teilerfremd. Dann ist $p(a/b) = 0$, also auch $b^{n-1}p(a/b) = 0$, also $b \mid a^n$, d. h. $b = \pm 1$ und $a/b \in \mathbb{Z}$. Sei also oBdA $b = 1$ und $a \in \mathbb{Z}$ Nullstelle von $p(x)$. Schreibe $p(x) = xq(x)+p(0)$. Durch Einsetzen von a folgt, dass $aq(a) = -p(0)$, also a ein Teiler von $p(0)$ ist. q.e.d.

Beispiel. Da 1 und -1 keine Nullstellen von $x^3 + x + 1 \in \mathbb{Q}[x]$ sind, ist dieses Polynom irreduzibel. Wir wollen $[x^2 + x - 1]^{-1} \in \mathbb{Q}[x]/(x^3 + x + 1)\mathbb{Q}[x]$, welches nach der Übungsaufgabe ein Körper ist, berechnen:

$$\begin{aligned} \underline{x^3 + x + 1} &= (-1 + x)\underline{(x^2 + x - 1)} + \underline{3x} \\ \underline{x^2 + x - 1} &= 1/3(x + 1)\underline{3x} - \underline{1} \end{aligned}$$

woraus man durch Einsetzen eine BÉZOUT-Identität erhält, deren Koeffizient von x^2+x-1 den Vertreter der inversen Restklasse liefert.
Weihnachten !!

9.6 Der Polynomring als Halbgruppenring.

(wird weggelassen)
In diesem Abschnitt wollen wir ein Verfahren kennenlernen, wie man aus einem Monoid M, z. B. $(\mathbb{Z}_{\geq 0}, +)$, und einen kommutativen Ring R mit Eins einen neuen Ring RM, den sogenannten Monoidring oder Halbgruppenring RM, konstruiert.

Definition 9.28. *Sei $(M, \cdot)$ eine Halbgruppe mit Eins und R ein kommutativer Ring mit Eins.*
1.) Für $f \in R^M$ heißt

$$\{a \in M \mid f(a) \neq 0\}$$

der **Träger** *von f.*
2.) R^M ist eine kommutative Gruppe vermöge der werteweisen Addition:

$$+ : R^M \times R^M \to R^M : (f, g) \mapsto f + g$$

mit

$$f + g : M \to R : m \mapsto f(m) + g(m).$$

3.) Auf R^M haben wir eine äußere Verknüpfung mit R, die ebenfalls werteweise definiert ist:

$$R \times R^M \to R^M : (r, f) \mapsto rf$$

mit

$$rf : M \to R : m \mapsto r \cdot f(m).$$

4.) Für $m \in M$ sei

$$x(m) : M \to R : a \mapsto \begin{cases} 1 & \text{falls } a = m \\ 0 & \text{falls } a \neq m \end{cases}$$

Ist M additiv geschrieben, so schreiben wir x^m statt $x(m)$.
5.) R_e^M bestehe aus allen Elementen von R^M mit endlichem Träger.

Offenbar gilt:

Bemerkung 9.29. *1.) R_e^M ist eine Untergruppe von R^M, abgeschlossen unter Multiplikation mit Elementen von R.*
2.) Für jedes $m \in M$ gilt $x(m) \in R_e^M$.
3.) Jedes Element $f \in R_e^M$ kann eindeutig als sogenannte **Linearkombination** *der $x(m)$ mit m im Träger von f und Koeffizienten aus R geschrieben werden:*

$$f = \sum_{m \in M} f(m)x(m).$$

Man beachte, dass alle bis auf endlich viele Summanden Null sind, so dass die Summation eigentlich über den Träger von f statt M geht.

Satz 9.30. *Sei $(M,\cdot)$ eine Halbgruppe mit Eins und R ein kommutativer Ring mit $1 \neq 0$. Dann ist der Halbgruppenring RM von M über R definiert als die abelsche Gruppe $(R_e^M,+)$ mit der Multiplikation*

$$R_e^M \times R_e^M \to R_e^M : (g,f) \mapsto f \cdot g$$

mit

$$(f \cdot g)(k) := \sum_{(m,n)\in M\times M, m\cdot n=k} f(m)g(n).$$

Also insgesondere $x(m_1)x(m_2) = x(m_1m_2)\ \forall m_1,m_2 \in M$.
1.) RM ist ein Ring mit Eins (mit äußerer Verknüpfung mit R).
2.) Die Abbildung

$$x : M \to RM : m \mapsto x(m)$$

ist injektiv und multiplikativ, also

$$x(m_1m_2) = x(m_1)x(m_2)\ \forall m_1,m_2 \in M$$

(sodass man M in RM wiederfindet). Insbesondere ist $x(1)$ das Einselement von RM und RM ist genau dann kommutativ, wenn M kommutativ ist.

Beweis. 1.) Die Multiplikation ist wohldefiniert und distributiv, wie man sofort sieht. Darüberhinaus ist sie R-bihomogen, d. h. für $r \in R$ ind $f,g \in RM$ gilt:

$$(rf)\cdot g = r(f\cdot g) = f\cdot(rg).$$

Daher und weil jedes Element R-Linearkombination endlich vieler $x(m)$ ist, reduziert sich das Assoziativgesetz der Multiplikation auf die Assoziativität der Produkte der $x(m)$:

$$x(m_1)(x(m_2)x(m_3) = (x(m_1)x(m_2))x(m_3)\ \forall m_1,m_2,m_3 \in M.$$

Dies ist aber klar nach Defintion der $x(m)$ wegen der Assoziativität von M: Beide Seiten sind gleich $x(m_1m_2m_3)$. Der Rest ist jetzt klar. q.e.d.

Beispiele.
1.) Den Polynomring $R[x]$ erhält man, indem man als Halbgruppe $\mathbb{N}_0 = (\mathbb{Z}_{\geq 0},+)$ wählt.
2.) Der Gruppenring von $(\mathbb{Z},+)$ über R wird mit $R[x,x^{-1}]$ bezeichnet. Er besteht aus (endlichen) R-Linearkombinationen von

$$\ldots, x^{-2}, x^{-1}, 1 = x^0, x = x^1, x^2, x^3, \ldots$$

und heißt der **Ring der** Laurent**-Polynome**[3] in einer Variablen x über R.
3.) Der Gruppenring $\mathbb{Z}C_6$ einer zyklischen Gruppe $C_6 := \{1,x,x^2,\ldots,x^5,x^6=1,\ldots\}$ über $\mathbb{Z}$ besteht also aus den $\mathbb{Z}$-Linearkombinationen von $1,x,\ldots,x^5$ (eigentlich müssten wir $1,x(x),x(x^2),\ldots$ schreiben, aber wir sind nicht zur Umständlichkeit verpflichtet, solange wir vor Augen haben, dass wir nicht im Polynomring sind) und gerechnet wird in den Exponenten modulo 6.

[3] Pierre Alphonse Laurent 1813 – 1854

4.) Sei $M := \mathbb{N}_0 \times \mathbb{N}_0$ mit der komponentenweisen Addition. Dann besteht RM aus den R-Linearkombinationen der $x^{(a,b)}$ mit $(a,b) \in \mathbb{N}_0 \times \mathbb{N}_0$. Statt $x^{(a,b)}$ schreibt man auch $x_1^a x_2^b$. Man nennt den Halbgruppenring auch **Polynomring** $R[x_1, x_2]$ in zwei Variablen x_1, x_2. Man sieht sofort, dass

$$R[x_1][x_2] \to R[x_1, x_2] : \sum_j (\sum_i a_{ij} x_1^i) x_2^j \mapsto \sum_{(i,j)} a_{ij} x^{(i,j)}$$

ein Ringisomorphismus ist, weshalb wir die beiden Ringe auch identifizieren.
5.) Wie würde man den Ring $R[x_1^{\pm 1}, x_2^{\pm 1}]$ der LAURENT-Polynome in zwei Variablen auffassen?

10 Quotientenkörper, 20. Vorlesung am 7.1.14

Lernziele: Rationaler Zahlkörper und rationaler Funktionenkörper als Beispiele der Quotientenkörperbildung, Normalformen der Elemente in diesen Körpern, Anordnung des rationalen Zahlkörpers

10.1 Konstruktion der rationalen aus den ganzen Zahlen

Beim Übergang von $\mathbb{N}$ nach $\mathbb{Z}$ wollten wir Gleichungen der Form $x + a = b$ mit $a, b \in \mathbb{N}$ lösen, kürzten diese Gleichungen als (a, b) ab und sahen zwei Gleichungen als äquivalent an, wenn begründeter Verdacht bestand, dass sie dieselbe Lösung haben sollten. Die Äquivalenzklassen waren dann die Lösungen. Es ließen sich Normalformen herstellen und Rechenoperationen definieren. Dasselbe Programm wollen wir jetzt als Konstruktion des Körpers $\mathbb{Q}$ der rationalen Zahlen aus dem Ring $\mathbb{Z}$ der ganzen Zahlen absolvieren. Die Gleichungen, die wir dieses Mal lösen wollen sind

$$bx = a \text{ mit } b \in \mathbb{Z} - \{0\}, a \in \mathbb{Z},$$

die wir wiederum als (a, b) abkürzen wollen.

Definition 10.1. *(***Rationale Zahlen***) 1.) Auf*

$$M := \mathbb{Z} \times \mathbb{Z}_{\neq 0} = \{(a, b) \mid a \in \mathbb{Z} \text{ und } b \in \mathbb{Z} - \{0\}\}$$

sei die Äquivalenzrelation $\sim$ gegeben durch

$$(a, b) \sim (c, d) \text{ genau dann wenn } ad = bc.$$

Die Äquivalenzklasse $[(a, b)]_\sim$ wird mit $\frac{a}{b}$ bezeichnet.
2.) Äquivalenzklassen werden addiert und multipliziert wie folgt:

$$[(a, b)] + [(c, d)] = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = [(ad + bc, bd)]$$

und

$$[(a, b)] \cdot [(c, d)] = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = [(ac, bd)].$$

Wir müssen zeigen, dass dies wohldefinierte Verknüpfungen sind, also nicht von der Wahl des Vertreters $(a,b) \in \frac{a}{b}$ abhängen.

Lemma 10.2. *1.) $\sim$ ist eine Äquivalenzrelation auf M.*
2.) Die Addition und Multiplikation der Äquivalenzklassen ist wohldefiniert. d. h. ist unabhängig von den gewählten Vertretern.
3.) Es gibt einen eindeutigen Vertreter (a,b) einer jeden Äquivalenzklasse mit $b \in \mathbb{N}$ und $\mathrm{ggT}(a,b) = 1$. *Man sagt dann, a/b ist durchgekürzt oder in* **Normalform***(, was etwas unscharf ist, weil man sich ja auf das Paar (a,b) beziehen sollte innerhalb der Äquivalenzklasse a/b).*

Beweis. 1.) $\sim$ ist symmetrisch und reflexiv (leichte Übung). Für die Transitivität benötigen wir eine Eigenschaft des Rings $\mathbb{Z}$: Er ist **nullteilerfrei**, d.h. aus $ab = 0$ folgt $a = 0$ oder $b = 0$.
Sei also $(a,b) \sim (c,d)$ und $(c,d) \sim (e,f)$. Dann gilt $ad = bc$ und $cf = de$. Also auch

$$adf = cbf = bde \Rightarrow d(af - be) = 0 \overset{d\neq 0}{\Rightarrow} af = be.$$

2.) Sei $(a,b) \sim (a',b')$ und $(c,d) \sim (c',d')$. Dann ist also $ab' = a'b$ und $cd' = c'd$. Dann gilt auch $(ac, bd) \sim (a'c', b'd')$, denn

$$acb'd' = (ab')(cd') = (a'b)(c'd) = a'c'bd$$

und ebenso (Übung) $(ad + bc, bd) \sim (a'd' + b'c', b'd')$.
3.) Die Existenz ist klar, läuft unter dem Stichwort kürzen und kann mit Hilfe des Euklidischen Algorithmus durchgeführt werden. Die Eindeutigkeit ergibt sich aus der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$: Sei $a/b = c/d$ mit $a, c \in \mathbb{Z}$ und $b, d \in \mathbb{N}$, sodass $\mathrm{ggT}(a,b) = \mathrm{ggT}(c,d) = 1$. Dann gilt $ad = bc$. Wegen der eindeutigen Primfaktorzerlegung folgt dann $a|c$ und $c|a$. D. h. a und c unterscheiden sich nur durch eine Einheit als Faktor. Ebenso b und d. Da zudem $b, d \in \mathbb{N}$ folgt $b = d$ und damit auch $a = c$. q.e.d.

Man beachte die Idee der Normalformen: Hat man sie, so ist der schwierige Vergleich von Äquivalenzklassen auf Gleichheit auf den einfachen Vergleich der Gleichheit von Elementen reduziert.

Satz 10.3. *Sei $\mathbb{Q} := M/\sim$ die Menge der Äquivalenzklassen. Dann gilt:*
1.) $(\mathbb{Q}, +, \cdot)$ ist ein Körper, genannt der Körper der rationalen Zahlen.
2.) $\iota : \mathbb{Z} \to \mathbb{Q} : a \mapsto \frac{a}{1}$ ist ein injektiver Ringhomomorphismus, sodass wir in Zukunft $a \in \mathbb{Z}$ mit $a/1 \in \mathbb{Q}$ identifizieren, also $\mathbb{Z}$ als Teilring von $\mathbb{Q}$ auffassen.
3.) $P := \{\frac{a}{b} \mid a, b \in \mathbb{N}\}$ ist eine Anordnung auf $\mathbb{Q}$, sodass $(\mathbb{Q}, P)$ ein angeordneter Körper ist. Die zugehörige Totalordung $<$ setzt die Ordnung auf $\mathbb{Z}$ fort.

Beweis. Addition und Multiplikation sind wohldefiniert, wie wir schon in Lemma 10.2 gesehen haben. Assoziativität und Kommutativität der Multiplikation ergeben sich direkt aus den entsprechenden Gesetzen für die Multiplikation in $\mathbb{Z}$. Das Einselement ist $\frac{1}{1}$ und für $a \neq 0$ ist

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

Assoziativität und Kommutativität der Addition ergeben sich auch direkt aus der Kommutativität und Assoziativität der Addition in $\mathbb{Z}$, weil man oEdA denselben Nenner für die involvierten Elemente annehmen kann. Das Nullelement ist $0 = \frac{0}{1}$ und das additiv Inverse ist $-(\frac{a}{b}) = \frac{-a}{b}$. Zum Distributivgesetz seien $a, b, c \in \mathbb{Z}, d, e, f \in \mathbb{N}$.

$$\left(\frac{a}{d} + \frac{b}{e}\right)\frac{c}{f} = \frac{ae+db}{ed}\frac{c}{f} \overset{dist\mathbb{Z}}{=} \frac{aec+dbc}{edf}.$$

Umgekehrt ergibt sich

$$\frac{a}{d}\frac{c}{f} + \frac{b}{e}\frac{c}{f} = \frac{ac}{df} + \frac{bc}{ef} = \frac{acef+bcdf}{edff} = \frac{ace+bcd}{edf}.$$

Man kann auch Œ $d = e$ annehmen, dann ist der Beweis sofort auf das Distributivgesetz in $\mathbb{Z}$ zurückgeführt.
3.) Übung. q.e.d.

Bemerkung 10.4. *Der* **Absolutbetrag** *auf* $\mathbb{Q}$ *ist die Funktion* $|\cdot| : \mathbb{Q} \to \mathbb{Q}_{>=0}$ *definiert durch*

$$\left|\frac{a}{b}\right| := \frac{|a|}{|b|} \in \mathbb{Q} \text{ für alle } a, b \in \mathbb{Z}, b \neq 0.$$

Er setzt den Absolutbetrag der ganzen Zahlen fort und definiert einen **Abstand** *zwischen zwei rationalen Zahlen* s, t*:*

$$d(s,t) := |s-t| = |t-s|.$$

Dieser Abstand ist eine **Metrik***, so dass* $(\mathbb{Q}, d)$ *ein metrischer Raum ist.*

Übung: Zwischen je zwei verschiedenen rationalen Zahlen liegen unendlich viele weitere rationale Zahlen, d. h. für $a, b \in \mathbb{Q}$ mit $a < b$ ist

$$\{c \in \mathbb{Q} |\ a < c < b\}$$

unendlich. Man beschreibe das Wachstum der Folge

$$a_n := |\{c \in \frac{1}{n}\mathbb{Z} |\ a < c < b\}|.$$

10.2 Konstruktion der rationalen Funktionen aus den Polynomen

Wir wollen schauen, was von der Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ wird, wenn man sie auf den Polynomring $K[x]$ über einem Körper K anwendet. Wir lassen die Beweise als Übungsaufgaben.

Definition 10.5. *(***Rationale Funktionen***) 1.) Auf*

$$M := K[x] \times K[x]_{\neq 0} = \{(a,b) \mid a \in K[x] \text{ und } b \in K[x] - \{0\}\}$$

sei die Äquivalenzrelation $\sim$ gegeben durch durch

$$(a,b) \sim (c,d) \text{ genau dann wenn } ad = bc.$$

Die Äquivalenzklasse $[(a,b)]_\sim$ wird mit $\frac{a}{b}$ bezeichnet.
2.) Äquivalenzklassen können addiert und multipliziert werden wie folgt:

$$[(a,b)] + [(c,d)] = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = [(ad+bc, bd)]$$

und

$$[(a,b)] \cdot [(c,d)] = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = [(ac, bd)].$$

Lemma 10.6. *1.) $\sim$ ist eine Äquivalenzrelation auf M.*
2.) Die Addition und Multiplikation der Äquivalenzklassen ist wohldefiniert. d. h. ist unabhängig von den gewählten Vertretern.
3.) Es gibt einen eindeutigen Vertreter (a,b) einer jeden Äquivalenzklasse mit $b \in K[x] - \{0\}$ normiert und $\mathrm{ggT}(a,b) = 1$.

Satz 10.7. *Sei $K(x) := M/\sim$ die Menge der Äquivalenzklassen. Dann gilt:*
1.) $(K(x), +, \cdot)$ ist ein Körper, genannt der Körper der rationalen Funktionen.
2.) $\iota : K[x] \to K(x) : p \mapsto \frac{p}{1}$ ist ein injektiver Ringhomomorphismus, sodass wir in Zukunft $p \in K[x]$ mit $p/1 \in K(x)$ identifizieren, also $K[x]$ als Teilring von $K(x)$ auffassen.

Da wir keine Anordnung auf $K[x]$ haben, können wir sie auch nicht fortsetzen. Man kann sich jedoch fragen, was mit dem Grad passiert.

Bemerkung 10.8. *Die Abbildung*

$$\mathrm{Grad} : K(x) - \{0\} \to \mathbb{Z} : \frac{a}{b} \mapsto \mathrm{Grad}(a) - \mathrm{Grad}(b)$$

setzt die Gradabbildung von $K[x]$ fort. Sie ist multiplikativ und erfüllt die Ungleichung

$$\mathrm{Grad}(a+b) \leq \max(\mathrm{Grad}(a), \mathrm{Grad}(b)) \qquad \forall a, b \in K(x).$$

Es fragt sich, ob eine rationale Funktion auch eine Abbildung $K \to K$ induziert, ähnlich wie bei den Polynomen. Die Antwort lautet beinahe, denn der Definitionsbereich ist nicht mehr K sondern hängt vom Nenner ab.

Übung: Man diskutiere Begriffe wie Polstelle und hebbare Lücke der induzierten Abbildungen rationaler Funktionen von $K - A \to K$, wo A eine (von der Situation abhängige) endliche Teilmenge von K ist und $K \in \{\mathbb{R}, \mathbb{C}\}$.

11 Der Körper der reellen Zahlen. Am 21. und 28.1., 22. und 23. Vorlesung

Lernziele: Konstruktion des reellen Zahlkörpers aus rationalen CAUCHY-Folgen, Dezimalbruchentwicklung, Grenzwerte von Folgen, rationale Zahlen und periodische Dezimalbrüche,

Wir hatten bereits früher gesehen, dass der Körper $\mathbb{Q}$ zwar angeordnet ist, aber nicht ordnungsvollständig, also nicht notwendig ein Supremum für eine nach oben beschränkte Menge enthält. Z. B. haben rationale CAUCHY-Folgen nicht unbedingt einen rationalen Grenzwert. Wir werden in gewohnter Manier aus unseren Wünschen eine Konstruktion machen, die die Wünsche erfüllt.

11.1 Der Ring der rationalen CAUCHY-Folgen.

Erinnerung 11.1. *Sei M eine Menge und R ein Ring. Dann bildet die Menge der Abbildungen R^M von M nach R einen Ring durch bildweise Addition und Multiplikation*

$$\begin{aligned}(f+g)(m) &:= f(m)+g(m)\\ (f\cdot g)(m) &:= f(m)\cdot g(m)\end{aligned}$$

für alle $f,g\in R^M, m\in M$.

Definition 11.2. *1.) Eine rationale Folge $(a_n)_{n\in\mathbb{N}}\in\mathbb{Q}^{\mathbb{N}}$ heißt* **CAUCHY-Folge**, *falls es für alle $\epsilon\in\mathbb{Q},\epsilon>0$ ein $N\in\mathbb{N}$ gibt, so dass*

$$|a_n-a_m|<\epsilon \text{ für alle } n,m\geq N.$$

2.) Eine rationale Folge $(a_n)_{n\in\mathbb{N}}\in\mathbb{Q}^{\mathbb{N}}$ heißt **Nullfolge** *falls es für alle $\epsilon\in\mathbb{Q},\epsilon>0$ ein $N\in\mathbb{N}$ gibt, so dass*

$$|a_n|<\epsilon \text{ für alle } n\geq N.$$

Lemma 11.3. *Jede Nullfolge ist eine CAUCHY-Folge.*

Beweis. Sei $(a_n)_{n\in\mathbb{N}}$ eine Nullfolge und $\epsilon>0$. Dann gibt es $N\in\mathbb{N}$ mit $|a_n|<\frac{1}{2}\epsilon$ für alle $n\geq N$. Dann ist für $n,m\geq N$

$$|a_n-a_m|\leq|a_n|+|a_m|\leq\epsilon.$$

q.e.d.

Lemma 11.4. *(CAUCHY-Folgen sind beschränkt.) Sei $(a_n)_{n\in\mathbb{N}}$ eine CAUCHY-Folge. Dann ist auch $(|a_n|)_{n\in\mathbb{N}}$ eine CAUCHY-Folge, und es gibt ein $S\in\mathbb{Q}$ mit $|a_n|\leq S$ für alle $n\in\mathbb{N}$.*

Beweis. Es ist $|a_n|-|a_m|\leq|a_n-a_m|$ da $|a_n|\leq|a_n-a_m|+|a_m|$ nach der Dreiecksungleichung. Ebenso gilt $|a_m|-|a_n|\leq|a_n-a_m|$ also ist mit $(a_n)_{n\in\mathbb{N}}$ auch $(|a_n|)_{n\in\mathbb{N}}$ eine CAUCHY-Folge. Zu $\epsilon>0$ gibt es also ein $N\in\mathbb{N}$ mit $||a_n|-|a_m||<\epsilon$ für alle $n,m\geq N$. Setzt man $s:=|a_N|+\epsilon$ so gilt für $n\geq N$, dass

$$|a_n|\leq||a_n|-|a_N||+|a_N|\leq\epsilon+|a_N|\leq s$$

also $|a_n|\leq S:=\max\{|a_1|,\ldots,|a_{N-1}|,s\}$ für alle $n\in\mathbb{N}$. q.e.d.

Satz 11.5. *Die Menge aller rationalen* CAUCHY*-Folgen bildet bezüglich komponentenweiser Addition und Multiplikation einen Ring* $\mathcal{C}(\mathbb{Q})$.

Beweis. Wir wissen schon, dass $\mathbb{Q}^N$, die Menge aller rationalen Folgen, einen Ring bzgl. komponentenweiser Addition und Multiplikation bildet. Es genügt also zu zeigen, dass $\mathcal{C}(\mathbb{Q})$ ein Teilring ist, also 0 und 1 enthält (klar, da konstante Folgen CAUCHY-Folgen sind), und Summe und Produkt von CAUCHY-Folgen wieder CAUCHY-Folgen sind: Seien $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ zwei CAUCHY-Folgen, und $\epsilon > 0$. Dann gibt es ein $N \in \mathbb{N}$ mit

$$|a_n - a_m| < \frac{\epsilon}{2} \text{ und } |b_n - b_m| < \frac{\epsilon}{2} \text{ für alle } n, m \geq N.$$

Für diese $n, m \geq N$ ist dann aber auch

$$|(a_n + b_n) - (a_m + b_m)| \leq |a_n - a_m| + |b_n - b_m| < \epsilon.$$

Nach Lemma 11.4 gibt es ein $0 < S \in \mathbb{Q}$ mit $|a_n| \leq S$ und $|b_n| \leq S$ für alle $n \in \mathbb{N}$. Sei $N \in \mathbb{N}$ so gewählt, dass

$$|a_n - a_m| < \frac{\epsilon}{2S} \text{ und } |b_n - b_m| < \frac{\epsilon}{2S} \text{ für alle } n, m \geq N.$$

Dann ist für $n, m \geq N$

$$\begin{aligned} |a_n b_n - a_m b_m| &= |a_n(b_n - b_m) + b_m(a_n - a_m)| \\ &\leq |a_n||b_n - b_m| + |b_m||a_n - a_m| \\ &< S\epsilon/(2S) + S\epsilon/(2S) = \epsilon \end{aligned}$$

q.e.d.

Spätestens jetzt ist die Marschroute klar: Stellen wir uns vor, dass wir $\mathbb{R}$ schon haben, dann sollte

$$\mathcal{C}(\mathbb{Q}) \to \mathbb{R} : (a_n) \mapsto \lim_{n\to\infty} a_n$$

ein surjektiver Ringhomomorphismus sein mit den Nullfolgen als Faser über Null. Dies gibt uns eine Konstruktionsmöglichkeit von $\mathbb{R}$, wenn wir es noch nicht haben. Zunächst ein vorbereitendes Lemma.

Lemma 11.6. *Sei* $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}(\mathbb{Q})$ *eine* CAUCHY*-Folge, die keine Nullfolge ist. Dann gibt es ein* $s > 0$ *und ein* $N \in \mathbb{N}$ *sodass entweder* $a_n \geq s$ *für alle* $n \geq N$ *oder* $a_n \leq -s$ *für alle* $n \geq N$

Beweis. Da $(a_n)_{n\in\mathbb{N}}$ keine Nullfolge ist, gibt es ein $\epsilon > 0$ so dass für alle $N \in \mathbb{N}$ ein $n = n(\epsilon, N) \geq N$ existiert mit $|a_n| \geq \epsilon$. Da $(a_n)_{n\in\mathbb{N}}$ eine CAUCHY-Folge ist, gibt es zu diesem ϵ ein $N' \in \mathbb{N}$ mit $|a_n - a_m| < \frac{1}{4}\epsilon$ für alle $n, m \geq N'$. Setze $n_0 := n(\epsilon, N')$. Nun gilt aber für $m \geq N'$

$$|a_m - a_{n_0}| < \frac{1}{4}\epsilon, \text{ d. h. } -\frac{1}{4}\epsilon < a_m - a_{n_0} < \frac{1}{4}\epsilon$$

also

$$a_{n_0} - \frac{1}{4}\epsilon < a_m < a_{n_0} + \frac{1}{4}\epsilon.$$

Setze $s := |a_{n_0}| - \frac{1}{4}\epsilon$ ($> \frac{3}{4}\epsilon$). Im Falle $a_{n_0} < 0$ nehmen wir die rechte Ungleichung und bekommen $a_m < -s$. Im Falle $a_{n_0} > 0$ nehmen wir die linke Ungleichung und bekommen $a_m > s$. q.e.d.

11.2 Definition der reellen Zahlen

Definition 11.7. *Auf der Menge $\mathcal{C}(\mathbb{Q})$ der* Cauchy*-Folgen in $\mathbb{Q}$ sei die Äquivalenzrelation $\sim$ gegeben durch*

$$(a_n)_{n\in\mathbb{N}} \sim (b_n)_{n\in\mathbb{N}} \Leftrightarrow (a_n - b_n)_{n\in\mathbb{N}} \text{ ist eine Nullfolge .}$$

Es ist sehr leicht zu sehen, dass $\sim$ eine Äquivalenzrelation definiert. Genauso wie bei den Kongruenzrelationen $\equiv_n$ auf $\mathbb{Z}$ bzw. $\equiv_f$ auf $K[X]$ wollen wir zeigen, dass diese Äquivalenzrelation mit Multiplikation und Addition verträglich ist, die vertreterweise Multiplikation und Addition also eine Ringstruktur auf der Menge der Äquivalenzklassen definiert. Dieser so erhaltene Ring ist dann der Körper der reellen Zahlen.

Lemma 11.8. *Seien $a := (a_n)_{n\in\mathbb{N}}$, $a' := (a'_n)_{n\in\mathbb{N}}$, $b := (b_n)_{n\in\mathbb{N}}$, $b' := (b'_n)_{n\in\mathbb{N}}$ rationale* Cauchy*-Folgen mit $a \sim a'$ und $b \sim b'$. Dann ist auch*

$$ab \sim a'b' \text{ und } a + b \sim a' + b'.$$

Beweis. Für die Summe ist dies recht leicht. Also betrachten wir hier nur das Produkt. Wir müssen zeigen, dass $(a_n b_n - a'_n b'_n)_{n\in\mathbb{N}}$ eine Nullfolge ist. Da a und b' beides Cauchy-Folge sind, gibt es ein $S \in \mathbb{Q}$ mit $|a_n| < S$ und $|b'_n| < S$ für alle $n \in \mathbb{N}$. Sei $\epsilon > 0$. Da $a - a'$ und $b - b'$ Nullfolgen sind, gibt es ein $N \in \mathbb{N}$ mit $|a_n - a'_n| < \epsilon/(2S)$ und $|b_n - b'_n| < \epsilon/(2S)$ für alle $n \geq N$. Für diese n ist dann

$$\begin{aligned} |a_n b_n - a'_n b'_n| &= |a_n(b_n - b'_n) + b'_n(a_n - a'_n)| \\ &\leq |a_n||b_n - b'_n| + |b'_n||a_n - a'_n| \\ &< S\epsilon/(2S) + S\epsilon/(2S) \leq \epsilon. \end{aligned}$$

q.e.d.

Satz 11.9. *Die Menge der Äquivalenzklassen von* Cauchy*-Folgen bildet einen Körper*

$$\mathbb{R} := \{[(a_n)_{n\in\mathbb{N}}]_\sim \mid (a_n)_{n\in\mathbb{N}} \in \mathcal{C}(\mathbb{Q})\}$$

den **Körper der reellen Zahlen**. *Man schreibt üblicherweise $\lim_{n\to\infty} a_n$ statt $[(a_n)_{n\in\mathbb{N}}]_\sim$.*

Beweis. Nach Lemma 11.8 und Satz 11.5 ist $\mathbb{R}$ mit vertreterweiser Addition und Multiplikation ein kommutativer Ring mit Eins $= [(1)_{n\in\mathbb{N}}]_\sim$, das Nullelement ist die Klasse der Nullfolgen. Es ist noch zu zeigen, dass die Klasse jeder Cauchy-Folge, die keine Nullfolge ist, ein multiplikativ Inverses besitzt. Sei also $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}(\mathbb{Q})$ keine Nullfolge. Dann gibt

es nach Lemma 11.6 ein $N \in \mathbb{N}$ und ein $s > 0$ mit $|a_n| \geq s$ für alle $n \geq N$. Insbesondere ist für diese n das Folgenglied $a_n \neq 0$ und es hat daher in $\mathbb{Q}$ ein multiplikativ Inverses. Definiere die Folge $a' \in \mathbb{Q}^{\mathbb{N}}$ durch

$$a'_n := \begin{cases} 1 & n < N \\ a_n^{-1} & n \geq N. \end{cases}$$

Dann ist $(a'_n)_{n\in\mathbb{N}}$ eine CAUCHY-Folge (Übung) und es gilt

$$[a]_\sim [a']_\sim = [(1)_{n\in\mathbb{N}}]_\sim$$

denn die Folge $(a_n a'_n - 1)_{n\in\mathbb{N}}$ ist eine Nullfolge, da ihre Folgenglieder für $n \geq N$ alle gleich 0 sind. q.e.d.

Übung: Zeige, dass man $\mathbb{Q}$ als Teilkörper von $\mathbb{R}$ auffassen kann, indem man jede rationale Zahl mit der Äquivalenzklasse der zugehörigen konstanten Folge identifiziert. Zeige weiter, dass $\lim_{n\to\infty} : \mathcal{C}(\mathbb{Q}) \to \mathbb{R}$ ein surjektiver Ringhomomorphismus ist.

11.3 Anordnung, Abstand, Betrag.

Hier ist unsere Anordnung von $\mathbb{R}$:

Definition 11.10. *$P_\mathbb{R} \subseteq \mathbb{R}$ bestehe aus allen $\alpha := [(a_n)_{n\in\mathbb{N}}]_\sim$ für die ein $\epsilon \in \mathbb{Q}$, $\epsilon > 0$ existiert und ein $N \in \mathbb{N}$ mit $a_n \geq \epsilon$ für alle $n \geq N$.*

Aus Lemma 11.6 bekommt man direkt $\mathbb{R} = -P_\mathbb{R} \uplus \{0\} \uplus P_\mathbb{R}$, so dass nun mit wenig Aufwand aus der Tatsache, dass $\mathbb{Q}$ ein geordneter Körper ist, $\mathbb{R}$ als angeordneten Körper erhält. (Vergl. Definition 7.1.)

Folgerung 11.11. *$(\mathbb{R}, +.\cdot, P_\mathbb{R})$ ist ein angeordneter Körper, welcher $(\mathbb{Q}, +, \cdot, P)$ als angeordneten Teilkörper enhält, wobei $P = P_\mathbb{R} \cap \mathbb{Q}$ die gewöhnliche Anordnung von $\mathbb{Q}$ ist.*

Die zugehörige Totalordnung auf $\mathbb{R}$ wird natürlich wieder mit $<$ bezeichnet. Unser Hauptziel ist nun, die Ordnungsvollstängikeit von $\mathbb{R}$ zu zeigen. Der Weg dahin wird uns einige Einsichten liefern, die für sich genommen wichtig sind. Zunächst ist der Abolutbetrag wie bei den rationalen Zahlen definiert:

Definition 11.12. *1.) Der* **Absolutbetrag** *auf $\mathbb{R}$ ist*

$$|\ \ | : \mathbb{R} \to \mathbb{R}_{\geq 0} : \alpha \mapsto |\alpha| := \begin{cases} \alpha & \alpha \geq 0 \\ -\alpha & \alpha < 0 \end{cases}$$

2.) Der **Abstand** *$d(\alpha, \beta)$ zweier reeller Zahlen α, β ist*

$$d(\alpha, \beta) := |\alpha - \beta|.$$

Übung: Dieser Abstand ist eine **Metrik**, d.h. es gilt für alle $\alpha, \beta, \gamma \in \mathbb{R}$
1.) $d(\alpha, \beta) \geq 0$ und $d(\alpha, \beta) = 0 \Leftrightarrow \alpha = \beta$.
2.) $d(\alpha, \beta) = d(\beta, \alpha)$.
3.) $d(\alpha, \beta) + d(\beta, \gamma) \geq d(\alpha, \gamma)$.

11.4 Rationale Zahlen als reelle Zahlen.

Wir wollen nun sehen, wie $\mathbb{Q}$ in $\mathbb{R}$ eingebettet ist.

Lemma 11.13. *Für jedes $\epsilon \in \mathbb{R}$ mit $\epsilon > 0$ gibt es ein $b \in \mathbb{N}$ mit $\frac{1}{b} < \epsilon$.*

Beweis. Sei $\epsilon = [(e_n)_{n\in\mathbb{N}}] > 0$. Dann ist $(e_n)_{n\in\mathbb{N}}$ keine Nullfolge und es gibt nach Lemma 11.6 ein $0 < s = \frac{a}{b} \in \mathbb{Q}$ mit $a \geq 2$ und ein $N \in \mathbb{N}$ mit $e_n \geq s$ für alle $n \geq N$. Dann ist aber $\epsilon - \frac{1}{b} = [(e_n - \frac{1}{b})_{n\in\mathbb{N}}] > 0$. q.e.d.

Übung: Zeige Lemma 11.13 ist äquivalent zum ARCHIMEDischen Axiom: Für jedes $r \in \mathbb{R}$ existiert ein $n \in \mathbb{N}$ mit $r < n$.

Satz 11.14. *$\mathbb{Q}$ liegt dicht in $\mathbb{R}$, d.h. für jedes $\alpha = [(a_n)_{n\in\mathbb{N}}]$ und jedes $\epsilon \in \mathbb{R}$, $\epsilon > 0$ gibt es ein $a \in \mathbb{Q}$ mit $|\alpha - a| < \epsilon$.*

Beweis. Wegen Lemma 11.13 gibt es ein $e \in \mathbb{Q}$ mit $0 < e < \epsilon$. Da $(a_n)_{n\in\mathbb{N}}$ eine rationale CAUCHY-Folge ist, gibt es ein $N \in \mathbb{N}$ mit $|a_n - a_m| < e$ für alle $n, m \geq N$. Setze $a := a_N$. q.e.d.

Es ist nun instruktiv, einen zweiten Beweis dieser Tatsache zu geben, der gleichzeitig eine (fast) normierte CAUCHY-Folge in jeder Äquivalenzklasse aussucht und unter dem Namen Dezimalbruchentwicklung bekannt ist.

Beispiel 11.15. *(**Dezimalbruchdarstellung reeller Zahlen**)*
1.) Sei $z \in \mathbb{N}_0^{\mathbb{N}}$ eine Folge mit $z_i \in \{0, 1, \ldots, 9\}$ für $i \geq 2$. Dann ist $a \in \mathbb{Q}^{\mathbb{N}}$ definiert durch

$$a_1 := z_1, a_{i+1} = a_i + \frac{z_{i+1}}{10^i}$$

offenbar eine CAUCHY-Folge, denn

$$a_i = \sum_{j=1}^{i} \frac{z_j}{10^{j-1}} \text{ und } |a_i - a_{i+k}| \leq \frac{9}{10^i} \sum_{j=0}^{k-1} 10^{-j} < \frac{1}{10^{i-1}}.$$

Leider ist die so definierte Abbildung

$$\{z \in \mathbb{N}_0^{\mathbb{N}} | z_i \in \{0, 1, \ldots, 9\} \text{ für } i \geq 2\} \to \mathbb{R}_{\geq 0} :$$
$$z \mapsto \sum_{i=1}^{\infty} \frac{z_i}{10^{i-1}} := \lim_{k\to\infty} \sum_{i=1}^{k} \frac{z_i}{10^{i-1}} =: z_1, z_2 z_3 z_4 \ldots$$

nicht injektiv, denn z. B.

$$\sum_{i=1}^{\infty} \frac{9}{10^i} = 1$$

hat sowohl die Folge $z = (0, 9, 9, 9, 9, 9, \ldots)$ *also auch* $z := (1, 0, 0, 0, 0, \ldots)$ *im Urbild.*
2.) Die obige Abbildung ist aber surjektiv. Um eine Rechstinverse zu konstruieren, brauchen wir die GAUSS**-Klammer***:*

$$\lfloor\ \rfloor : \mathbb{R} \to \mathbb{Z} : a \mapsto \max\{k \in \mathbb{Z} \mid k \leq a\} = z \in \mathbb{Z} \text{ mit } z \leq a < z + 1.$$

Die gesuchte Rechtsinverse heißt **Dezimalbruchentwicklung** *und ist gegeben durch*

$$\mathbb{R}_{\geq 0} \to \mathbb{N}_0^{\mathbb{N}} : a \mapsto (\lfloor \zeta_1 \rfloor, \lfloor \zeta_2 \rfloor, \lfloor \zeta_3 \rfloor, \ldots)$$

mit $\zeta_1 := a$ *und* $\zeta_{i+1} := 10(\zeta_i - \lfloor \zeta_i \rfloor)$ *für* $i \geq 1$*. Wir lassen es als Übungsaufgabe zu zeigen, dass diese Abbildung rechtsinvers zu der aus 1.) ist. Dies liefert sowohl einen normierten Vertreter in jeder* $\sim$*-Klasse von rationalen* CAUCHY*-Folgen als auch einen alternativen Beweis von Satz 11.14.*

Beispiel. $\frac{1}{9} = 0,\overline{1}$, wie man durch schriftliche Division sieht und mithilfe der geometrischen Reihe

$$\frac{1}{1-x} = \sum_{i=0}^{\infty} x^i$$

beweist, denn es ist

$$0,\overline{1} = \sum_{i=1}^{\infty} 10^{-i} = \frac{1}{1 - 1/10} - 1 = \frac{10}{9} - 1 = \frac{1}{9}.$$

Ebenso ergibt sich $\frac{1}{11} = 0,\overline{09}$.
Umgekehrt findet man

$$0,\overline{081} = 81 \sum_{i=1}^{\infty} 1000^{-i} = \frac{81}{999} = \frac{3}{37}.$$

11.5 Ordnungsvollständigkeit des reellen Zahlkörpers.

Definition 11.16. *1.) Eine reelle Folge* $(\alpha_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ *heißt* CAUCHY**-Folge** *falls es für alle* $\epsilon \in \mathbb{R}, \epsilon > 0$ *ein* $N \in \mathbb{N}$ *gibt, so dass*

$$|\alpha_n - \alpha_m| < \epsilon \text{ für alle } n, m \geq N.$$

2.) Eine reelle Folge $(\alpha_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ *heißt* **konvergent** *gegen* $\beta \in \mathbb{R}$*, falls es für alle* $\epsilon \in \mathbb{R}, \epsilon > 0$ *ein* $N \in \mathbb{N}$ *gibt, so dass*

$$|\beta - \alpha_n| < \epsilon \text{ für alle } n \geq N.$$

Satz 11.17. *(***Vollständigkeitssatz***) Jede* CAUCHY*-Folge reeller Zahlen konvergiert gegen eine reelle Zahl.*

Beweis. Sei $(\alpha_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ eine reelle CAUCHY-Folge. Für jedes $n \in \mathbb{N}$ wählen wir ein $a_n \in \mathbb{Q}$ mit $|\alpha_n - a_n| < \frac{1}{n}$. Dann ist $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}(\mathbb{Q})$, denn es gilt

$$|a_n - a_m| \leq |a_n - \alpha_n| + |\alpha_n - \alpha_m| + |\alpha_m - a_m| < \frac{1}{n} + |\alpha_n - \alpha_m| + \frac{1}{m}.$$

Sei $\beta := [(a_n)_{n\in\mathbb{N}}]_\sim \in \mathbb{R}$. Dann konvergiert $(\alpha_n)_{n\in\mathbb{N}}$ gegen β, da

$$|\beta - \alpha_n| \leq |\beta - a_n| + |a_n - \alpha_n|$$

beliebig klein wird für große n. q.e.d.

Jetzt können wir für unseren konstruierten Körper $\mathbb{R}$ das Axiom der oberen Grenze verifizieren.

Hauptsatz 11.18. $\mathbb{R}$ *ist ordnungsvollständig. d. h. jede nach oben beschränkte Teilmenge* $M \neq \emptyset$ *von* $\mathbb{R}$ *hat ein Supremum* $\sup(M)$*, also eine kleinste obere Schranke. Insbesondere existiert ein angeordneter ordnungsvollständiger Körper, vgl. Def. 7.5.*

Beweis. Unser Beweis ist im Geiste der Dezimalbruchentwicklung, wie in Beispiel 11.15 dargestellt. Sei $\emptyset \neq M \subseteq \mathbb{R}$ nach oben beschränkt durch $b \in \mathbb{R}$. Wir können oBdA annehmen, dass M ein positives Element enthält. Die halboffenen Intervalle

$$[a, a+1) := \{x \in \mathbb{R} \mid a \leq x < a+1\}$$

mit $a \in \mathbb{N}_0$ partitionieren $\mathbb{R}_{\geq 0} = \dot{\cup}_{a\in\mathbb{N}_0}\ [a, a+1)$. Insbesondere gibt es ein eindeutiges größtes $z_1 \in \mathbb{N}_0$ mit $M \cap [z_1, z_1+1) \neq \emptyset$. Beachte $M \cap [z_1+1, z_1+2) = \emptyset$. Alsdann gibt es ein eindeutiges größtes $z_2 \in \{0, 1, \ldots, 9\} = -1 + \underline{10}$ mit i

$$M \cap [z_1 + z_2/10, z_1 + (z_2+1)/10) \neq \emptyset.$$

(Beachte diese 10 Intervalle bilden eine Partition von $[z_1, z_1+1)$.)
Weiter gibt es ein eindeutiges größtes $z_3 \in -1 + \underline{10}$ mit

$$M \cap [z_1 + z_2/10 + z_3/10^2, z_1 + z_2/10 + (z_3+1)/10^2) \neq \emptyset$$

etc. Die formale rekursive Definition lassen wir als Übung. Jedenfalls bekommen wir eine rationale CAUCHY-Folge $a = (a_n)_{n\in\mathbb{N}}$ mit $a_n = \sum_{i=1}^n z_i 10^{1-i}$ mit einem Grenzwert $s := [a]_\sim \in \mathbb{R}$. Es ist klar, dass keine obere Schranke kleiner als irgendeine der Teilsummen $a_n = \sum_{i=1}^n z_i/10^{i-1}$ ist. Andererseits ist klar, dass für jedes n das Element $10^{1-n} + \sum_{i=1}^n z_i 10^{1-i}$ eine obere Schranke für M ist. Aber

$$\lim_{n\to\infty} \sum_{i=1}^n z_i 10^{1-i} = \lim_{n\to\infty} (10^{1-n} + \sum_{i=1}^n z_i 10^{1-i}),$$

sodass $[a]_\sim = \lim_{n\to\infty} \sum_{i=1}^n z_i 10^{1-i} = \sup(M)$ gilt. q.e.d.

Nach dem Existenzsatz bleibt noch die Frage nach der Eindeutigkeit, die wir nur skizzieren, aber die Einzelheiten sprengen nicht den Rahmen einer Übungsaufgabe.

Hauptsatz 11.19. *Sei $(K, +, \cdot, P)$ ein ordnungsvollständiger angeordneter Körper. Dann gibt es genau einen ordnungstreuen Körperisomorphismus $\varphi : K \to \mathbb{R}$.*

Beweis. K ist angeordnet, also ist die Abbildung $\mathbb{N} \to K, n \mapsto 1+\ldots+1$ (n Summanden) nach Lemma 7.3 injektiv. Somit ist auch $\mathbb{Q} \hookrightarrow K$, $\frac{a}{b} \mapsto ab^{-1}$ injektiv und K enthält die rationalen Zahlen als Teilkörper. Wegen $n < n+1$ für alle $n \in \mathbb{N}$, ist die Anordnung auf $\mathbb{Q}$ genau die Einschränkung der Anordnung von K auf $\mathbb{Q}$. Man sieht, dass $\mathbb{Q}$ dicht in K liegt, denn wie bei den reellen Zahlen partitionieren die Intervalle $(n, n+1]$ mit $n \in \mathbb{N}_0$ die Menge P. Ist $\alpha \in P$ beliebig so gibt es ein eindeutiges $n \in \mathbb{N}_0$ mit $\alpha \in (n, n+1]$, also $\alpha - n \in (0, 1] = \dot{\cup}_{i=1}^{10} (\frac{i-1}{10}, \frac{i}{10}]$. Wie bei der Zifferndarstellung reeller Zahlen konstruieren wir eine Folge $(a_k = n + \sum_{i=1}^{k} z_i 10^{-i}) \in \mathbb{Q}^{\mathbb{N}}$ mit $|\alpha - a_k| \leq 10^{-k}$. Da 10^{-k} beliebig klein wird, können wir also α durch rationale Zahlen (a_k) beliebig genau approximieren.
Aus der Ordnungsvollständigkeit folgt, dass K vollständig ist. Insbesondere hat jede rationale CAUCHY-Folge a einen eindeutigen Grenzwert in K, den wir mit ${}_K\lim a$ bezeichnen. Der offensichtliche surjektive Ringhomomorphismus

$$\mathcal{C}(\mathbb{Q}) \to K : a \to {}_K\lim a$$

induziert das Inverse des gesuchten ordnungstreuen Körperisomorphismus $\varphi : K \to \mathbb{R}$;

$$\mathbb{R} \to K : \lim a \mapsto {}_K\lim a,$$

und dieser ist auch offenbar der einzig mögliche Isomorphismus, der die Anordnung und damit die Grenzwerte erhält. q.e.d.

12 Kettenbrüche, letzte Vorlesung am 3.2.

12.1 Kettenbrüche und gute Approximationen

Definition 12.1. *(Kettenbruchentwicklung) Sei $\alpha > 0$ eine reelle Zahl. Wir ordnen α rekursiv eine Folge $\alpha_0, \alpha_1, \ldots$ von reellen Zahlen und $a_0, a_1, \ldots$ von natürlichen Zahlen zu (wobei $a_0 = 0$ zugelassen ist) vermöge*

$$\alpha_0 := \alpha, a_0 := \lfloor \alpha_0 \rfloor, \alpha_{n+1} := \frac{1}{\alpha_n - a_n}, a_{n+1} := \lfloor \alpha_{n+1} \rfloor$$

für $n \in \mathbb{N}_0$ solange $a_n \neq \alpha_n$ ist. Es gilt dann

$$\alpha = [a_0, a_1, \ldots, a_n, \alpha_{n+1}] = a_0 + \frac{1}{a_1 + \ldots + \frac{1}{a_n + \frac{1}{\alpha_{n+1}}}}.$$

$[a_0, \ldots, a_n]$ heißt der n-te **Näherungsbruch** *von α, die Folge $[a_0, a_1, a_2, \ldots]$ die* **Kettenbruchentwicklung** *von α und α_n die n-te* **Restzahl**. *Die Kettenbruchentwicklung von α heißt* **endlich**, *falls $\alpha = [a_0, \ldots, a_n]$ für ein n, also $\alpha_n = a_n \in \mathbb{Z}$.*

Beispiel: $\frac{315}{273} = [1, 6, 2]$, denn

$$\begin{array}{rcrcl} 315 & = & 273 & + & 42 \\ 273 & = & 6 \cdot 42 & + & 21 \\ 42 & = & 2 \cdot 21 & & \end{array}$$

und

$$\left\lfloor \left(\frac{315}{273} - 1 \right)^{-1} \right\rfloor = \left\lfloor \left(\frac{315-273}{273} \right)^{-1} \right\rfloor = \left\lfloor \frac{273}{42} \right\rfloor = 6$$

bzw.

$$\left\lfloor \left(\frac{273}{42} - 6 \right)^{-1} \right\rfloor = \left\lfloor \left(\frac{273-6\cdot 42}{42} \right)^{-1} \right\rfloor = \left\lfloor \frac{42}{21} \right\rfloor = 2.$$

Satz 12.2. *Die Kettenbruchentwicklung von $\alpha \in \mathbb{R}_{>0}$ ist genau dann endlich, wenn $\alpha \in \mathbb{Q}$.*

Beweis. Bricht die Kettenbruchentwicklung von α ab, so liegt $\alpha = [a_0, a_1, \ldots, a_n] \in \mathbb{Q}$, da alle $a_i \in \mathbb{N}$ liegen.
Ist $\alpha = \frac{a}{b}$ in $\mathbb{Q}$ so erhält man die Kettenbruchentwicklung von α, indem man den Euklidischen Algorithmus auf (a, b) anwendet ($a > b > 0$). Dieser ist endlich, also auch die Kettenbruchentwicklung:
Ist nämlich $a = qb + r$, so ist $q = \lfloor \frac{a}{b} \rfloor$ und

$$\left(\frac{a}{b} - q \right)^{-1} = \frac{b}{a-qb} = \frac{b}{r}$$

so dass die Kettenbruchentwicklung und der Euklidische Algorithmus die gleiche Rekursion liefern. q.e.d.

Satz 12.3. *Für $n \in \mathbb{N}$ seien $A_n, B_n \in \mathbb{N}$ mit $\mathrm{ggT}(A_n, B_n) = 1$, so dass $\frac{A_n}{B_n} = [b_0, b_1, \ldots, b_n]$ der n-te Näherungsbruch einer Kettenbruchentwicklung ist. Dann gilt:*
(a) $A_0 = b_0$, $B_0 = 1$, $A_1 = b_1 A_0 + 1$, $B_1 = b_1 B_0$, und für $n \geq 2$:
$A_n = b_n A_{n-1} + A_{n-2}$, $B_n = b_n B_{n-1} + B_{n-2}$.
(b) $A_n B_{n-1} - A_{n-1} B_n = (-1)^{n-1}$.

Beweis. (a) Induktion über n. $n = 0, 1$ Klar.
Induktionsschluss:

$$\frac{A_{n+1}}{B_{n+1}} = \frac{b_{n+1}A_n + A_{n-1}}{b_{n+1}B_n + B_{n-1}} = \frac{(b_n + b_{n+1}^{-1})A_{n-1} + A_{n-2}}{(b_n + b_{n+1}^{-1})B_{n-1} + B_{n-2}} \overset{IV}{=} [b_0, b_1, \ldots, b_n + b_{n+1}^{-1}] = [b_0, b_1, \ldots, b_n, b_{n+1}]$$

wobei wir im letzten Schritt die Induktionsvoraussetzung benutzen.
(b) Folgt aus (a) mit Induktion über n, denn es ist

$$A_n B_{n-1} - A_{n-1} B_n = (b_n A_{n-1} + A_{n-2}) B_{n-1} - A_{n-1}(b_n B_{n-1} + B_{n-2}) = A_{n-2} B_{n-1} - A_{n-1} B_{n-2}.$$

Für $n = 1$ ist (b) klar durch Einsetzen. q.e.d.

Satz 12.4. *Sei $\alpha = [b_0, b_1, b_2, \ldots] \in \mathbb{R}_{>0}$ eine Kettenbruchentwicklung. Dann ist*

$$0 \leq (-1)^n (\alpha - \frac{A_n}{B_n}) < \frac{1}{B_n B_{n+1}} \leq \frac{1}{B_n^2}.$$

Beweis.

$$\alpha = \lim_{n\to\infty} \frac{A_n}{B_n} = \frac{A_n}{B_n} + \left(\frac{A_{n+1}}{B_{n+1}} - \frac{A_n}{B_n}\right) + \left(\frac{A_{n+2}}{B_{n+2}} - \frac{A_{n+1}}{B_{n+1}}\right) + \dots$$

$$= \frac{A_n}{B_n} + (-1)^n \frac{1}{B_n B_{n+1}} - (-1)^n \left(\frac{1}{B_{n+1}B_{n+2}} - \frac{1}{B_{n+2}B_{n+3}} + \dots\right).$$

Also ist

$$0 \le (-1)^n \left(\alpha - \frac{A_n}{B_n}\right) = \frac{1}{B_n B_{n+1}} - \left(\frac{1}{B_{n+1}B_{n+2}} - \frac{1}{B_{n+2}B_{n+3}} + \dots\right) \le \frac{1}{B_n B_{n+1}}$$

da B_n monoton steigend ist. Wegen $B_{n+1} \ge B_n$ erhält man die letzte Ungleichung. q.e.d.

Bemerkung 12.5. *Sei $\alpha \in \mathbb{R}_{>0}$ nicht rational und $\frac{A_n}{B_n}$ der n-te Näherungsbruch in der Kettenbruchentwicklung von α. Dann ist*

$$\frac{A_0}{B_0} < \frac{A_2}{B_2} < \frac{A_4}{B_4} < \dots < \alpha < \dots < \frac{A_5}{B_5} < \frac{A_3}{B_3} < \frac{A_1}{B_1}.$$

Bemerkung 12.6. *Eine rationale Zahl $\frac{a}{b}$ heißt* **gute Approximation** *für $\alpha \in \mathbb{R}_{>0}$, falls für alle $\frac{c}{d} \in \mathbb{Q}$ mit $\frac{c}{d} \ne \frac{a}{b}$ und $0 < d < b$ gilt*

$$|d\alpha - c| > |b\alpha - a|.$$

Dann gilt: Jede gute Approximation von α kommt als Näherungsbruch in der Kettenbruchentwicklung von α vor.

Beweis. Sei $\frac{a}{b}$ eine gute Approximation für $\alpha \in \mathbb{R}_{>0}$, $a, b \in \mathbb{N}$ und $\alpha = [a_0, a_1, a_2, \dots]$ die Kettenbruchentwicklung von α. Angenommen $\frac{a}{b} \notin \{\frac{A_k}{B_k} \mid k \in \mathbb{N}_0\}$ (sonst ist nichts zu zeigen).
Dann ist $\frac{a}{b} \ge a_0$, denn

$$1 > \alpha - a_0 \ge |b\alpha - a| \ge \alpha - \frac{a}{b}.$$

Weiter ist $\frac{a}{b} \le \frac{A_1}{B_1}$ denn sonst ist $\frac{a}{b} > \frac{A_1}{B_1} > \alpha$ und daher

$$|b\alpha - a| = b\left|\alpha - \frac{a}{b}\right| > b\left|\frac{A_1}{B_1} - \frac{a}{b}\right| \ge^{4} b\frac{1}{B_1 b} = \frac{1}{B_1} = \frac{1}{a_1}$$

aber es ist $|\alpha - a_0| \le \frac{1}{a_1}$ ein Widerspruch dazu, dass $\frac{a}{b}$ eine gute Approximation ist. Also gibt es ein $k \in \mathbb{N}$, so dass $\frac{a}{b}$ zwischen dem $k-1$-ten und dem $k+1$-ten Näherungsbruch liegt. Dann ist also

$$\frac{1}{B_k B_{k-1}} = \left|\frac{A_k}{B_k} - \frac{A_{k-1}}{B_{k-1}}\right| > \left|\frac{a}{b} - \frac{A_{k-1}}{B_{k-1}}\right| \ge \frac{1}{bB_{k-1}}$$

[4] da der 2. Faktor ein Bruch $\ne 0$ mit Nenner $B_1 b$ ist

und somit $b > B_k$, wobei wieder bei der letzten Ungleichung benutzt wurde, dass $\frac{a}{b} \neq \frac{A_{k-1}}{B_{k-1}}$. Da $\frac{a}{b}$ zwischen dem $k-1$-ten und dem $k+1$-ten Näherungsbruch liegt ist α weiter entfernt von $\frac{a}{b}$ als der $k+1$-te Näherungsbruch und daher

$$\left|\alpha - \frac{a}{b}\right| \geq \left|\frac{A_{k+1}}{B_{k+1}} - \frac{a}{b}\right| \geq \frac{1}{bB_{k+1}}$$

also nach Multiplikation mit b: $|b\alpha - a| \geq \frac{1}{B_{k+1}}$. Wegen Satz 12.4 ist aber $|B_k\alpha - A_k| \leq \frac{1}{B_{k+1}}$ also $|B_k\alpha - A_k| \leq |b\alpha - a|$ was wegen $b > B_k$ ein Widerspruch ist zu der Tatsache, dass $\frac{a}{b}$ eine gute Approximation ist. q.e.d.

12.2 Periodische Kettenbrüche und quadratische Gleichungen.

Beispiel: Wir wollen die Kettenbruchentwicklung von $\sqrt{2}$ bestimmen, also die der positiven Lösung $x \in \mathbb{R}$ mit $x^2 = 2$. Es ist

$$x^2 = 2 \Leftrightarrow (x-1)(x+1) = 1 \Leftrightarrow (x-1) = \frac{1}{x+1}$$

Also ist

$$x = 1 + \frac{1}{1+x} = 1 + \frac{1}{2 + \frac{1}{1+x}} = [1, 2, 1+x] = [1, 2, 2, 1+x] = \ldots = [1, 2, 2, 2, \ldots] = [1, \overline{2}].$$

Satz 12.7. *(ohne Beweis) Sei $\alpha \in \mathbb{R}$, $\alpha > 1$. Die Kettenbruchentwicklung von α wird nach einer eventuellen Vorperiode periodisch, genau dann wenn α eine rationale quadratische Gleichung erfüllt.*

Lemma 12.8. *(Euler) Hat $\alpha > 0$ eine periodische Kettenbruchentwicklung, so gibt es $a, b \in \mathbb{Q}$ mit $\alpha^2 + a\alpha + b = 0$.*

Beweis. Wir können Œ annehmen, dass die Kettenbruchentwicklung von α rein periodisch ist, also keine Vorperiode hat, da dies durch Addition rationaler Zahlen und ggf. Invertieren erreicht werden kann (vergleiche Tutorium). Sei also $\alpha = [\overline{b_0, \ldots, b_k}] = [b_0, \ldots, b_k, \alpha]$ und $\frac{A_n}{B_n} = [b_0, \ldots, b_n]$ für $n = k-1$ und $n = k$, die Näherungsbrüche. Dann ist

$$\alpha = [b_0, \ldots, b_k, \alpha] = \frac{\alpha A_k + A_{k-1}}{\alpha B_k + B_{k-1}}$$

und somit

$$B_k\alpha^2 + (B_{k-1} - A_k)\alpha - A_{k-1} = 0.$$

□

Beispiel. Sei $\alpha = [\overline{1}] = [1, 1, \ldots]$. Dann gilt $\alpha = 1 + \frac{1}{\alpha}$, also $\alpha^2 - \alpha - 1 = 0$. Mithilfe von quadratischer Ergänzung findet man $\alpha = \frac{1+\sqrt{5}}{2}$, der goldene Schnitt.

12.3 Die Kettenbruchentwicklung der Eulerschen Zahl.

In der Analysis Vorlesung haben Sie die Euler'sche Zahl kennengelernt

$$e = \sum_{k=0}^{\infty} \frac{1}{k!} \sim 2,7182818286$$

Berechnet man die Kettenbruchentwicklung von e, so findet man $e = [2,1,2,1,1,4,1,1,6,\ldots] = [1,0,1,1,2,1,1,4,1,1,\ldots]$, was die Vermutung nahelegt, dass

$$e = [2,1,\{2\lambda,1,1\}_{\lambda=1}^{\infty}] = [1,\{2\lambda,1,1\}_{\lambda=0}^{\infty}]$$

gilt.

Satz 12.9. *Sei $(a_i)_{i\in\mathbb{N}_0}$ definiert durch $a_{3i} = a_{3i+2} = 1$, $a_{3i+1} = 2i$ für $i \in \mathbb{N}_0$ und $\frac{p_n}{q_n} := [a_0, a_1, \ldots, a_n]$ der n-te Näherungsbruch ($n \neq 1$). Dann ist $e = [a_0, a_1, a_2, \ldots] = \lim_{n\to\infty} \frac{p_n}{q_n}$.*

Bemerkung 12.10. *Es gilt $p_0 = 1, p_1 = 1, p_2 = 2$, $q_0 = 1, q_1 = 0, q_2 = 1$ und für $n \geq 1$ ist*

$$\begin{aligned} p_{3n} &= p_{3n-1} + p_{3n-2}, & q_{3n} &= q_{3n-1} + q_{3n-2}, \\ p_{3n+1} &= 2np_{3n} + p_{3n-1}, & q_{3n+1} &= 2nq_{3n} + q_{3n-1}, \\ p_{3n+2} &= p_{3n+1} + p_{3n}, & q_{3n+2} &= q_{3n+1} + q_{3n} \end{aligned}$$

Lemma 12.11. *Setze*

$$A_n := \int_0^1 \frac{x^n(x-1)^n}{n!} e^x dx,\ B_n := \int_0^1 \frac{x^{n+1}(x-1)^n}{n!} e^x dx,\ C_n := \int_0^1 \frac{x^n(x-1)^{n+1}}{n!} e^x dx$$

Dann gilt für $n \geq 0$: $A_n = q_{3n}e - p_{3n}$, $B_n = p_{3n+1} - q_{3n+1}e$ und $C_n = p_{3n+2} - q_{3n+2}e$.

Beweis. Wegen der Rekursionsformeln für p_n und q_n in Bemerkung 12.10 genügt es
$A_0 = \int_0^1 e^x dx = e^x \,|_0^1 = e - 1 = q_0 e - p_0$,
$B_0 = \int_0^1 xe^x dx = (xe^x - e^x) \,|_0^1 = 1 = p_1 - q_1 e$,
$C_0 = \int_0^1 (x-1)e^x dx = B_0 - A_0 = 2 - e = p_2 - q_2 e$.
zu beachten und die Rekursionsformeln

(a) $A_n = -B_{n-1} - C_{n-1}$

(b) $B_n = -2nA_n + C_{n-1}$

(c) $C_n = B_n - A_n$

zu beweisen um dann das Lemma mit vollständiger Induktion folgern zu können. Die dritte Formel (c) ergibt sich direkt aus Bemerkung 12.10.
Um (a) zu zeigen, also $A_n + B_{n-1} + C_{n-1} = 0$ berechnen wir

$$\frac{d}{dx}\left(\frac{x^n(x-1)^n}{n!}e^x\right) = \frac{x^n(x-1)^n}{n!}e^x + \frac{x^n(x-1)^{n-1}}{(n-1)!}e^x + \frac{x^{n-1}(x-1)^n}{(n-1)!}e^x$$

mit der Produktregel. Also ist

$$A_n + B_{n-1} + C_{n-1} = \left(\frac{x^n(x-1)^n}{n!} e^x \right) |_0^1 = 0.$$

Für (b), also $B_n + 2nA_n - C_{n-1} = 0$ berechnen wir analog

$$\frac{d}{dx}\left(\frac{x^n(x-1)^{n+1}}{n!} e^x \right) = \frac{x^{n+1}(x-1)^n}{n!} e^x + 2n \frac{x^n(x-1)^n}{(n)!} e^x - \frac{x^{n-1}(x-1)^n}{(n-1)!} e^x$$

wobei hier einige Zwischenschritte fehlen. q.e.d.

Beweis. (Von Satz 12.9) Es gilt $\lim_{n\to\infty} A_n = 0$, $\lim_{n\to\infty} B_n = 0$ und $\lim_{n\to\infty} C_n = 0$, also $\lim_{n\to\infty} q_n e - p_n = 0$ und somit (da $q_n \geq 1$ für $n \geq 2$) $\lim_{n\to\infty} \frac{p_n}{q_n} = e$. q.e.d.

Kapitel 4

Ergänzungen und Wiederholung

13 Gleichungssysteme, Einschub am 14.1.2014, 21. Vorl.

13.1 Fasern einer Abbildung

Was ist ein Gleichungssystem? Was bedeutet es, ein Gleichungssystem zu lösen? Zunächst eine ganz allgemeine Bemerkung zum allgemeinen Verständnis auch im Sinne unserer Philosophie, dass wir Abbildungen als Hauptelement unserer Sprache benutzen wollen.

Bemerkung 13.1. *Seien M, N Mengen und $f : M \to N$ eine Abbildung. Für jedes $n \in N$ ist das zu f und n gehörige* **Gleichungssystem** *gegeben durch*

$$f(m) = n,$$

und seine **Lösungsmenge** *ist gerade die Faser $f^{-1}(\{n\})$.*

Übung: Seien $f, g : M \to N$ Abbildungen. Wie kann man das „verallgemeinerte Gleichungssytem“ $f(m) = g(m)$ als Gleichungssystem im obigen Sinne auffassen mit derselben Lösungsmenge?

Also das Lösen von Gleichungssystemen kann aufgefasst werden als spezielle Untersuchung von Abbildungen. Oftmals sind dies besonders wichtige Untersuchungen mit vielfältigen Anwendungen. Wir wollen einige wichtige Beispiele studieren.

Beispiel 13.2. *1.) Sei $p(x) \in \mathbb{R}[x] - \{0\}$ vom Grad n. Dann hat das zu $\tilde{p}, 0$ gehörige Gleichungssystem höchstens n Lösungen. Für jede Lösung $a \in \mathbb{R}$ gilt nämlich $x - a | p(x)$, sodass*

$$\prod_{a, p(a)=0} (x - a) \ \mid \ p(x),$$

und ein Vergleich der Grade die Behauptung in Evidenz setzt.
2.) Sei $p(x) \in \mathbb{C}[x] - \{0\}$ vom Grad n. Dann hat das zu $\tilde{p}, 0$ gehörige Gleichungssystem höchstens n Lösungen, in der Regel sogar n. Denn $\mathbb{C}$ ist **algebraisch abgeschlossen**, *d.*

h. jedes Polynom hat eine Wurzel, zerfällt also multiplikativ in Linearfaktoren.
3.) Sei K ein Körper und $K[x,y] := K[x][y]$ der Polynomring in zwei Variablen (der Polynomring vom (Polynom-)Ring $K[x]$). $p = p(x,y) = \sum_{i\in\mathbb{N}_0^2} a_i x^{i_1} \cdot y^{i_2} \in K[x,y]$. Dann induziert p eine Abbildung

$$\tilde{p} : K^2 \to K : s = (s_1, s_2) \mapsto p(s) := p(s_1, s_2) := \sum_{i\in\mathbb{N}_0^2} a_i s_1^{i_1} \cdot s_2^{i_2}.$$

Allgemeiner sei $p = (p_1, \ldots, p_m) \in K[x,y]^m$ für ein $m \in \mathbb{N}$. Dann induziert p eine Abbildung

$$\tilde{p} : K^2 \to K^m : s \mapsto (p_1(s), \ldots, p_m(s))$$

Das zu $\tilde{p}$ und $b \in K^m$ gehörige Gleichungssystem

$$p_1(s) = b_1, \ldots, p_m(s) = b_m$$

heißt **polynomial**. *Z.B. $K = \mathbb{R}$, $x^2 + y^2 = 1,\ x + 3y = 1$. Man rechnet leicht nach, dass dieses Gleichungssystem genau 2 Lösungen hat, die man als Schnittpunkte von einem Kreis und einer Gerade finden kann.*

13.2 Die Substitutionsmethode

Definition 13.3. *1. Sei K ein Körper und $n \in \mathbb{N}$. Wir definieren den* **Polynomring in n Veränderlichen** *rekursiv über*

- *(a) ist $n = 1$, so haben wir den Polynomring bereits in Bemerkung (9.18) definiert, Bezeichnung: $K[x_1]$,*
- *(b) ist $n > 1$, so definiere den Polynomring in n Veränderlichen als Polynomring zum Ring $K[x_1, \ldots, x_{n-1}]$, dem Polynomring in $n-1$ Veränderlichen $x_1, \ldots, x_{n-1}$, Bezeichnung: $K[x_1, \ldots, x_n] := K[x_1, \ldots, x_{n-1}][x_n]$ mit Veränderlichen $x_1, \ldots, x_n$.*

2. *Sei $p \in K[x_1, \ldots, x_n]$. Dann existieren* **Koeffizienten** *$a_i \in K$ für alle $i \in \mathbb{N}_0$, wobei nur endlich viele $\neq 0$ sind, und es gilt*

$$p = \sum_{i\in\mathbb{N}_0^n} a_i x_1^{i_1} \cdots x_n^{i_n}.$$

3. *Für $i \in \mathbb{N}_0^n$ definiere $|i| := i_1 + \ldots + i_n$. Ist $p \neq 0$ so heißt das größte $|i|$ mit $a_i \neq 0$ der (Total-)***Grad** *von p und wird mit $\mathrm{Grad}(p)$ bezeichnet.*

Wir wollen jetzt eine Methode kennenlernen, die für polynomiale Gleichungssysteme, deren zugehörigen Polynome allesamt Grad 1 haben, die Lösungsmenge bestimmt. Solche Gleichungssysteme heißen auch linear. Aber manchmal funktioniert die Methode auch für etwas allgemeinere polynomiale Gleichungssysteme. Grundlage der Methode ist die folgende Bemerkung.

Bemerkung 13.4. *Sei K ein Körper und $e := x_n - p(x_1, \ldots, x_{n-1}) \in K[x_1, \ldots, x_n]$ mit $p(x_1, \ldots, x_{n-1}) \in K[x_1, \ldots, x_{n-1}]$.*
1.) Dann definiert

$$\sigma_e : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_{n-1}] : \\ q(x_1, \ldots, x_n) \mapsto q(x_1, \ldots, x_{n-1}, p(x_1, \ldots, x_{n-1}))$$

einen surjektiven Ringhomomorphismus.
2.) Sei $g = (g_1, \ldots, g_m) \in K[x_1, \ldots, x_n]^m$ mit $g_1 = e$. Setze $h := (\sigma_e(g_2), \ldots, \sigma_e(g_m)) \in K[x_1, \ldots, x_{n-1}]^{m-1}$. Dann gilt für die Lösungsmengen

$$\tilde{g}^{-1}(\{\underbrace{(0, \ldots, 0)}_{m}\}) = \{(b_1, \ldots, b_{n-1}, p(b)) | b = (b_1, \ldots, b_{n-1}) \in \tilde{h}^{-1}(\{\underbrace{(0, \ldots, 0)}_{m-1}\}).$$

Beispiel 13.5. *Wir wollen das Gleichungssystem*

$$\begin{aligned} x_1 + x_2 + x_3 + 1 &= 0 \\ x_2 + x_3 + 2\,x_4 + 3 &= 0 \\ x_1 + x_3 + x_4 + 4 &= 0 \end{aligned}$$

lösen. Also in der obigen Terminologie:

$$g := (x_1 + x_2 + x_3 + 1, x_2 + x_3 + 2\,x_4 + 3, x_1 + x_3 + x_4 + 4).$$

Wir eliminieren x_4 aus der letzten Gleichung:

$$x_4 = -x_1 - x_3 - 4$$

und setzen in die erste und zweite Gleichung ein. (Da die erste kein x_4 enthält, bleibt sich unverändert. Wir erhalten

$$h := (x_1 + x_2 + x_3 + 1, x_2 - x_3 - 2\,x_1 - 5).$$

Wir eliminieren x_3 aus der letzten neuen Gleichung:

$$x_3 = x_2 - 2\,x_1 - 5$$

und setzen in die erste neue Gleichung ein:

$$k := (-x_1 + 2\,x_2 - 4).$$

Diese Gleichung können wir nach x_2 auflösen:

$$x_2 = 1/2\,x_1 + 2.$$

Setzen wir dies in die Gleichung für x_3 ein, wo wird auch x_3 durch s_1 alleine ausgedrückt.

$$x_3 = -3/2\,x_1 - 3.$$

In den ersten Ausdruck für x_4 eingestzt, erhalten wir auch x_4 durch s_1 alleine ausgedrückt (Normalerweise hätte man auch noch den Ausdruck für x_2 dort einsetzen müssen.):

$$x_4 = 1/2\, x_1 - 1.$$

Zusammenfassend stellen wir fest, dass wir eine Bijektion zwischen der Lösungsmenge und dem Körper K haben, über den die einzige Voraussetzung ist, das $2 \neq 0$ gilt. Die Abbildung von K auf die Lösungsmenge nennt man auch eine Parametrisierung der Lösungsmenge. Wären wir bereit gewesen, nach x_2 statt nach x_1 aufzulösen, hätten wir keine Beschränkung für den Körper gehabt.

Manchmal hat man Glück und kann auch polynomiale Gleichungssysteme mit dieser Methode behandeln, wo nicht sämtliche Gleichungen den Grad 1 haben:

Beispiel 13.6. *(Fortsetzung)*

$$\begin{aligned} x^2 + y^2 &= 1 \\ x + 3y &= 1 \end{aligned}$$

Wir eliminieren x aus der zweiten Gleichung: $x = 1-3y$ und setzen in die erste Gleichung ein und erhalten eine quadratische Gleichung für t, also $-6t + 10t^2 = 0$. Man sieht, das mam genau zwei Lösungen hat:

$$t = 0 \text{ und } t = \frac{2}{3}.$$

Setzt man diese beiden Lösungen in die Gleichung für x ein, so hat man das System gelöst. Dies kann man geometrisch so ausdrücken, dass der Einheitskreis von der Geraden $x + 3y = 1$ zwei mal geschnitten wird.

13.3 Lineare-affine Geometrie

Weiter sei K ein Körper. Wir wollen lineare Gleichungssysteme in drei Veränderlichen x, y, z geometrisch interpretieren.

Definition 13.7. *Eine Ebene E in K^3 ist gegeben durch die Lösungsmenge $\tilde{g}^{-1}(\{0\})$ für ein $g \in K[x, y, z]$ vom Grad 1.*

Übung: Zeige, dass jede Ebene das beschreibende Polynom bis auf K-Vielfache eindeutig bestimmt. Zeige weiter, dass die Gleichung nach mindestens einer der Variablen x, y, z aufgelöst werden kann und dass somit die Ebene durch den K^2 parametrisiert werden kann.

Satz 13.8. *Zwei verschiedene Ebenen $E_1, E_2 \subseteq K^3$ haben entweder keine gemeinsamen Punkte oder der Durchschnitt lässt sich durch K parametrisieren. Der erste Fall tritt genau dann auf, wenn $a_1, a_2 \in K$ existieren, sodass $a_1 g_1 + a_2 g_2 \in K^*$ gilt, wobei g_i eine beschreibende Gleichung für E_i ist. Im ersten Fall sagt man, die beiden Ebenen sind* **parallel***; im zweiten Fall sagt man, die beiden Ebenen schneiden sich in einer* **Gerade***n.*

Beweis. Sei die Ebene E_i gegeben durch $\widetilde{g_i}^{-1}((0,0,0))$ mit $g_i \in K[x,y,z]$, für $i = 1,2$. Definiere $g := (g_1, g_2) \in K[x,y,z]^2$ und damit gilt $E_1 \cap E_2 = \widetilde{g}^{-1}((0,0,0))$. Schreibe $g_i = a_i x + b_i y + c_i z + d_i$ mit $a_i, b_i, c_i, d_i \in K$, für $i = 1,2$. Wir können g_2 nach einer Variablen auflösen, o.B.d.A. nach z, also o.B.d.A. $c_2 = 1$. Definiere $e := g_2 = z - p$ mit $p := -a_2 x - b_2 y - d_2$. Dann ist $\sigma_e(g_1) = a_1 x + b_1 y + c_1(-a_2 x - b_2 y - d_2) + d_1 = (a_1 - c_1 a_2)x + (b_1 - c_1 b_2)y + (d_1 - c_1 d_2)$ und

$$\widetilde{g}^{-1}((0,0,0)) = \{(k_1, k_2, -a_2 k_1 - b_2 k_2 - d_1) \mid \sigma_e(g_1)((k_1,k_2)) = 0\}.$$

Es können folgende Fälle auftreten:

1. $\sigma_e(g_1) = 0$, dann folgt $g_1 - c_1 g_2 = 0$, also $E_1 = E_2$.
2. $\mathrm{Grad}(\sigma_e(g_1)) = 0$, d.h. $g_1 - c_1 g_2 \in K^*$ und E_1, E_2 sind parallel.
3. $\mathrm{Grad}(\sigma_e(g_1)) = 1$ und $\widetilde{g}^{-1}((0,0,0))$ beschreibt eine Gerade.

q.e.d.

Es ist klar, dass eine Gerade viele Ebenenpaare hat, deren Schnitt sie ist. Wir fragen, wie der Schnitt einer Geraden mit einer Ebene aussehen kann.

Satz 13.9. *Der Durchschnitt einer Geraden mit einer Ebene im K^3 ist entweder leer, die Gerade oder aus einem Punkt bestehend. Im ersten Fall sagt man, dass die Gerade und die Ebene (schwach)* **parallel** *sind.*

Beweis. Übung q.e.d.

Der letzte Satz schließt auch die Analyse des Durchschnittes dreier Ebenen mit ein. Der Normalfall ist also, dass diese drei Ebenen sich in genau einem Punkt scheiden. Alle anderen Fälle sind recht speziell. Wir beenden den Abschnitt mit der Analyse eines Geradenpaares in K^3.

Satz 13.10. *Liegen zwei verschiedene Geraden im K^3 in einer Ebene, so gibt es zwei Möglichkeiten: Entweder sie haben leeren Schnitt, in welchem Fall sie parallel heißen, oder sie schneiden sich in genau einem Punkt. Gibt es keine Ebene, die die zwei Geraden enthält, so heißen die beiden Geraden* **windschief** *zueienander. Sie liegen dann in unterschiedlichen Ebenen einer eindeutig bestimmten Ebenenschar von parallelen Ebenen.*

Beweis. Übung q.e.d.

Es sei darauf hingewiesen, dass die Betrachtungen dieses Abschnittes für jeden Körper gültig sind.

Index

Äquivalenzklasse, 30
Äquivalenzklassen, 31
Äquivalenzrelation, 30
    Bildgleichheit, 30
überabzählbar, 21
Ähnlichkeit, 75
Äquivalenz, 9
äquivalent, 7
Archimedisches Axiom, 58
Bézout-Identität, 79
Cauchy-Schwarz-Ungleichung, 68
Cauchy-Folge, 95, 100
Gauss-Klammer, 100
Peano-Axiome, 34
Russellsche Antinomie, 12
Euklidischer Algorithmus, 80

Kongruenzsatz, 75

Abbildung, 17
    auf, 27
    eineindeutig, 27
    Identität, 20
    injektiv, 27
    inverse, 19
    Komposition, 26
    Linksinverses, 27
    natürliche, 31
    Rechtsinverses, 27
    surjektiv, 27
    Transversale, 31
    Vertreterabbildung, 31
abelsche Gruppe, 50
Absolutbetrag, 58, 63, 93, 98
Abstand, 58, 64, 93, 98
abzählbar, 21
Abzählfunktion, 21
Algorithmus
    Euklidischer Algorithmus, 80
Allgemeines Assoziativgesetz, 42
Allgemeines Distributivgesetz, 53
Allgemeines Kommutativgesetz, 43
angeordneter Körper, 56
Anordnung, 56
antisymmetrisch, 40
Argument, 66
Assoziativität, 26
Assoziativität der Disjunktion, 8
Assoziativität der Konjunktion, 8
Assoziativität der Vereinigung, 14
Assoziativität des Durchschittes, 14

Betrag, 63
Bijektion, 19
bijektiv, 19
Bild, 17
Bildgleichheit, 30
Binomialkoeffizient, 46
Binomischer Lehrsatz, 54

Cantorschen Diagonalverfahren, 24
Cantorschen Diagonalverfahren., 22
charakteristische Funktion, 18

Darstellung, 79
Definitionsbereich, 17
Determinante, 71
Dezimalbruchdarstellung reeller Zahlen, 99
Dezimalbruchentwicklung, 100
direkte Produkt, 59
disjunkt, 21, 31
Disjunktion, 8
Diskriminante, 60
Distributivgesetz, 52
Distributivität der Disjunktion gegenüber der Konjunktion, 8
Distributivität der Konjunktion gegenüber der Disjunktion, 8

Distributivität der Vereinigung gegenüber dem Schnitt, 14
Distributivität des Schnittes gegenüber der Vereinigung, 14
Drehung, 70
Dreiecksungleichung, 63
Durchschnitt, 12

Einbettung, 26
Eindeutigkeit der natürlichen Zahlen, 36
eineindeutig, 27
Einheitengruppe, 79
Einschränkung, 23
Einsetzungshomomorphismus, 88
Element, 11
endlich, 21

führende Koeffizient, 89
Fakultät, 45
Faser, 19
Folge
    endliche, 23
Funktion, 17
    charakteristische, 18

generelle lineare Gruppe, 70
geordnetes Paar, 15
Geraden, 69
gleich, 11
größter gemeinsamer Teiler, 79
Gruppe, 50
    abelsche, 50
    kommutative, 50

Halbgruppe, 50
Halbgruppe mit Eins, 50
Homomorphismus, 59

Identität, 20
Identitätsabbildung, 20
imaginäre Achse, 63
Imaginärteil, 63
Implikation, 8, 9
injektiv, 27
inverse Abbildung, 19
inverses Element, 50
Isometrie, 74
Isomorphismus, 59

Körper der reellen Zahlen, 97
Körper, 52, 55
kartesisches Produkt, 15
Klassen, 31
    Äquivalenzklassen, 31
Kleiner-Relation, 39
kommutative Gruppe, 50
kommutativen Ring mit Eins, 52
Kommutativität der Disjunktion, 8
Kommutativität der Konjunktion, 8
Kommutativität der Vereinigung, 14
Kommutativität des Durchschnittes, 14
Komplement , 13
komplexe Konjugation, 62
komplexe Zahlkörper, 61
Komposition, 26
Kongruenzrelation, 51
Konjunktion, 8
Kontraposition, 10
konvergent, 100

Längenfunktion, 68
leere Menge, 11
linear, 69
Linearkombination, 85
Linksinverses, 27
Logarithmus, 59

Menge
    Differenzmenge, 13
    Durchschnitt, 12
    Partition, 31
    Potenzmenge, 12
    Vereinigung, 13
    Vertretermenge, 31
Menge aller reellen Zahlen, 20
Menge der ganzen Zahlen, 20
Menge der natürlichen Zahlen, 20
Menge der rationalen Zahlen, 20
Metrik, 58, 93, 98
metrischer Raum, 69, 74
Minimum, 39
Monoid, 50
monoton, 60

Multiplikation mit Skalaren, 67

natürliche Abbildung, 31
Nebenklassen, 51
Normalform, 92
normiert, 89
Nullfolge, 95
Nullstelle, 88

ordnungsvollständig, 57
orientierte Flächenverzerrung, 72
orientierte Winkel, 65
orientierter Flächeninhalt, 71
orthogonal, 69
orthogonale Gruppe, 71

Parallelogramm, 71
partielle Ordung, 40
Partition, 31
    Menge, 31
Polarzerlegung, 64, 66
Polynom, 86
Polynomfunktion, 88
Polynomring, 86, 87
Potenz, 37
Potenzieren, 44
Potenzmenge, 12
Primzahl, 82
Prinzip des kleinsten Verbrechers, 40
Produkt, 42, 43
    kartesisches, 15
Produktfolge, 42

Quadratsumme, 68
Quadratwurzel, 60

Rationale Funktionen, 93
Rationale Zahlen, 91
Realteil, 63
Rechtsinverses, 27
reelle Achse, 63
reeller Zahlkörper, 57
reflexiv, 30
Reihe, 42
Rekursion, 36
Relation, 30
    Äquivalenzrelation, 30
    reflexiv, 30
    symmetrisch, 30
    transitiv, 30
Rest, 80
Restklassen, 51
Ring, 52
Ring der Laurent-Polynome, 87
Ringschluss, 10

senkrecht, 69
spezielle orthogonale Gruppe, 71
Spieglung, 70
Standardskalarprodukt, 68
Strecken, 69
Streckung, 51, 67
Summe, 42
Supremum, 57
surjektiv, 27
symmetrisch, 30
symmetrische Differenz, 15
symmetrische Gruppe, 45, 51

Teiler, 79
Teilmenge, 11
total geordnet, 39
Träger, 85
transitiv, 30
Transitivität, 10
Translation, 51, 67, 73
Transversale, 31

Umkehrfunktion, 19
unendlich, 21
Untergruppe, 51

Vereinigung, 13
Verneinung, 7
Verneinung der Disjunktion, 9
Verneinung der Konjunktion, 9
Vertreter, 31
Vertreterabbildung, 31
Vertretermenge, 31
vollständige Induktion, 35
Vollständigkeitssatz, 100

Wahrheitstafel, 8
Wahrheitswert, 7

Wertebereich, 17
Widerspruchsbeweis, 10
Winkel, 69
winkeltreue, 73
wohlgeordnet, 39
Wurzel, 88