Lineare Algebra

Dr. Stefan Kühnlein

Institut für Algebra und Geometrie, Karlsruher Institut für Technologie

September 2012

Vorwort

Die Vorlesung „Lineare Algebra und Analytische Geometrie“ – kurz LA – ist in Karlsruhe für Studierende der Mathematikstudiengänge und der Informatik in den ersten zwei Semestern verpflichtend, für solche der Physik sicher auch hilfreich.

Dabei sind die Vorlesungen für Mathematiker und Informatiker im ersten Semester deckungsgleich, während die Informatiker im zweiten Semester laut Studienordnung die Lineare Algebra nur noch zweistündig zu hören haben.

Dies schlägt sich insofern in diesem Skriptum nieder, als es von einem Dozenten der Vorlesung für Informatiker stammt und in einer ersten Version parallel zu dessen Vorlesung entstand. Trotzdem bietet es den gesamten Standardstoff der Vorlesung für Mathematiker, wie er etwa in der LA-Klausur geprüft wird.

Die Lineare Algebra ist eine mathematische Disziplin, die aus geometrischen Fragestellungen und aus dem Determinanten- und Matrizenkalkül entstand. Die eigentlichen geometrischen Objekte, die dabei studiert wurden, spielen in der Vorlesung in ihrer heutigen Form nicht mehr die zentrale Rolle; von daher ist auch die Analytische Geometrie in diesem Skriptum nicht sehr ausführlich behandelt worden. Ich hoffe, dass trotzdem gelegentlich die Geometrie immer wieder aufleuchtet, denn sie bildet einen Kontrapunkt zur sehr abstrakt vorgehenden algebraischen Sichtweise und ist oft ein guter Ideengeber. Die algebraische Sichtweise ist aber diejenige, die für die Bedeutung der Linearen Algebra in vielen Bereichen der Mathematik, Informatik und Physik entscheidend ist.

Dabei ist es wesentlich, gemeinsame Strukturen zu erkennen, die vielen verschiedenen Phänomenen zugrunde liegen. Diese Strukturen sind es, die in der Algebra thematisiert werden. Unsere Hauptstrukturen in der LA sind Gruppen, Körper und Vektorräume. Ein Vektor ist einfach ein Element eines Vektorraumes, und ohne den Begriff Vektorraum ist der Begriff Vektor sinnlos. Wichtig ist nicht ein einzelner Vektor, sondern die Gesamtheit und das Zusammenspiel aller Elemente eines Vektorraums, das sich in der Form des Additionsgesetzes und der skalaren Multiplikation ausdrückt. Ansonsten möchte ich gerne auf eine Inhaltsangabe für die LA verzichten und vertraue darauf, dass bei der Lektüre des Skriptums klar wird, was die Inhalte desselben sind.

Im Skriptum habe ich versucht, den Vorlesungsstil beizubehalten. Es war mir ein Anliegen, Begriffsbildungen durch Beispiele (ein sehr dehnbarer Begriff übrigens) zu motivieren. Oft wird sich auch ein Argumenttyp an mehreren Stellen des Skriptums finden, damit sich ein gewisser Gewöhnungseffekt einstellen kann. Einige Beispiele, die erst mühsam sind, hätten an späterer Stelle weniger Arbeit erfordert. Das soll auch zeigen, dass es sich lohnt, den umfangreichen Begriffsapparat der Linearen Algebra aufzubauen, auch wenn gerade er für viele Neulinge ein großes Hindernis darstellt. Ich habe auch nicht immer zwischen Definitionen

und Bemerkungen unterschieden, oft bot es sich an, unmittelbar in einer Definition noch ein Argument einzuarbeiten, das zur Klärung hilfreich ist. Andernorts habe ich Begriffe auch innerhalb eines Hilfssatzes definiert.

Die Überschriften, die ich den meisten Definitionen, Bemerkungen und Sätzen gegeben habe, sollen bei der Orientierung hilfreich sein, aber natürlich nicht den Rest der jeweiligen Nummer ersetzen. Im Zweifelsfall gilt immer der Volltext.

Ein Lehrbuch oder den Vorlesungsbesuch zu ersetzen ist nicht das Ziel dieses Skriptums. Das Erste wird oft systematischer vorgehen, beim Zweiten wird man eher erkennen, was wirklich wichtig ist. Auch wird hier eher einmal ein konkretes Beispiel vorgeführt werden. Übrigens ist es nicht möglich, eine mathematische Disziplin zu erlernen, ohne viel zu üben. Hierfür gibt es wieder eigene Veranstaltungen, in denen vieles an Vorlesungsinhalten konkretisiert wird.

Ich habe versucht, die Notation konsequent durchzuhalten. Viele Querverweise sollen das Nachschlagen erleichtern, erzwingen aber auch die sperrige und pedantische Nummerierung.

Schließlich möchte ich es nicht Versäumen, meinen Hörern der LA im akademischen Jahr 2003/04 zu danken, die mich durch ihre Aufnahme des Skriptums darin bestärkt haben, dass es sich lohnt, Energie und Zeit in eine Neuauflage zu stecken. Außerdem haben einige schon damals ein paar versteckte Fehler aufgespürt und mich korrigiert. Dies gelang später auch Prof. Dr. Frank Herrlich und Dr. Hendrik Kasten, denen ich für die Gründlichkeit ihrer Korrekturen danken möchte. Ein paar Fehler sind sicher noch übrig geblieben; diese bitte ich mir anzukreiden und mitzuteilen.

An vielen Stellen des Skriptums sind Ideen mit eingeflossen, die sich vor einigen Jahren bei der Zusammenarbeit mit Prof. Herrlich anlässlich der damaligen LA-Runde ergaben. Auch dafür will ich meinen Dank nicht verhehlen.

Karlsruhe, Oktober 2012 Stefan Kühnlein

Inhaltsverzeichnis

Kapitel 1

Allgemeine Grundlagen

In diesem Kapitel sollen einige Tatsachen und vor allem Ausdrucksweisen sowie Notationen der Logik und der Mengenlehre vermittelt werden. Dabei werden wir den Mengenbegriff nicht problematisieren, also im Bereich der so genannten naiven Mengenlehre verbleiben. Für die Zwecke der Linearen Algebra reicht dies vollkommen aus, manche Leser werden später noch sehen, dass dies nicht alles ist, was die Mengenlehre zu bieten hat.

1.1 Logisches

Die Logik beschäftigt sich mit Aussagen. Das sind Sätze, die entweder wahr oder falsch sind. Fragesätze wie zum Beispiel „Meinst Du, dass es morgen regnet?“ sind keine Aussagen. Auch Befehle wie „Komm sofort her!“ sind keine Aussagen. Beide Beispielsätze haben keinen „Wahrheitswert“.

Im Gegensatz dazu ist ein seltsam anmutender Satz wie „Wenn 2 ungerade ist, dann ist 1 gleich 0.“ eine Aussage. Noch dazu ist diese Aussage wahr, denn die Bedingung, an die der zweite Satzteil geknüpft ist, wird niemals eintreten.

Schlichtere Aussagen sind zum Beispiel die folgenden: „Alle Quadrate sind rund.“ „Draußen regnet es.“ „Ich habe heute Geburtstag.“ Die zwei letzteren Aussagen beziehen sich (direkt oder indirekt) auf einen Zeitpunkt. In der Mathematik werden wir es immer mit Aussagen zu tun haben, deren Wahrheitswert für alle Zeiten ungeändert bleibt (zumindest idealer Weise).

Natürlich ist man nicht unbedingt an jeder einzelnen Aussage für sich interessiert, sondern eher an Zusammenhängen zwischen verschiedenen Aussagen. Die Logik hat einige Möglichkeiten, aus vorhandenen Aussagen neue zu machen, formalisiert. Stellen Sie sich also vor, Sie hätten zwei Aussagen A und B aus einer großen Kiste mit Aussagen herausgezogen und wollten aus diesen neue Aussagen basteln. Dazu gibt es einige einfache Möglichkeiten, die Sie Ihr ganzes Studium

über begleiten werden.

a) Die *Konjunktion* $A \wedge B$: Diese Aussage ist wahr, wenn A und B beide wahr sind, ansonsten ist sie falsch. Oft werden wir auf die symbolische Notation mit dem $\wedge$ verzichten und stattdessen so etwas wie „ A und B “, „sowohl A als auch B “ oder „ A sowie B “ schreiben.

b) Die *Negation* $\neg A$: Diese Aussage ist wahr, wenn A falsch ist und falsch, wenn A wahr ist. Die Negation von „mein Fahrrad ist schwarz“ ist nicht „mein Fahrrad ist weiß“, sondern – entgegen allem Schwarz-Weiß-Denken – „mein Fahrrad ist nicht schwarz“. Die Aussage $A \wedge (\neg A)$, die durch Konjunktion der beiden Aussagen A und $\neg A$ gebildet wird, ist immer falsch. Wahr ist:

$$\boxed{\neg[A \wedge (\neg A)].}$$

c) Die *Disjunktion* $A \vee B$: Diese Aussage ist wahr, wenn A wahr ist oder B wahr ist oder auch beide wahr sind. Sie ist falsch, wenn sowohl A als auch B falsch sind. Wir sagen oft auch „ A oder B “. Im allgemeinen Sprachgebrauch meint man damit oft das ausschließende oder, also das „Entweder - Oder“. In der Mathematik wird das „oder“ immer im nicht ausschließenden Sinn verwendet. Es ist also $A \vee B$ dieselbe Aussage wie $\neg((\neg A) \wedge (\neg B))$. Demnach ist zum Beispiel die Aussage $A \vee (\neg A)$ für jede Aussage A wahr: wenn A wahr ist, ist sie wahr, und wenn A falsch ist, ist ja $\neg A$ wahr und damit auch einer der beiden Partner in $A \vee (\neg A)$ wahr.

An solchen Beispielen sieht man schon, dass es oft sinnvoll ist, in längeren Aussagengefügen die Zutaten durch Klammern zusammenzufassen, sodass die Struktur überhaupt erkennbar ist. So ist zunächst nicht klar, was die Aussage $A \wedge B \vee C$ bedeutet. Dafür gibt es ja die zwei Möglichkeiten

$$(A \wedge B) \vee C \quad \text{bzw.} \quad A \wedge (B \vee C).$$

Wenn A falsch und C wahr ist, dann ist die linke Aussage wahr, aber die rechte falsch.

Die Klammern geben dabei an, in welcher Reihenfolge die Aussagen verknüpft werden.

Bitte lassen Sie sich durch ein langes Klammerngewusel nicht abschrecken, sondern nehmen Sie es als Grundgerüst zur Auflösung einer längeren Aussage!

d) Die *Implikation* $A \Rightarrow B$: „aus A folgt B “, „wenn A wahr ist, so auch B “. Die Implikation ist wahr, wenn entweder A falsch ist oder sowohl A als auch B wahr sind. Dies ist eine Formalisierung der Tatsache, dass die Voraussetzung A die Folgerung B nach sich zieht. Also ist $A \Rightarrow B$ dieselbe Aussage wie $\neg A \vee (A \wedge B)$,

oder auch dieselbe wie $(\neg A) \vee B$. Als Beispiel sei noch einmal der Satz „Wenn 2 ungerade ist, dann ist 1 gleich 0“ benutzt. Auch der Satz „Wenn 2 ungerade ist, dann ist 1 gleich 1“ ist eine wahre Aussage, nicht aber der Satz „Wenn 1 gleich 1 ist, dann ist 2 ungerade.“ Hier ist ja die Voraussetzung wahr, aber die Folgerung falsch.

Eine der wichtigsten Tatsachen der klassischen Logik ist das Widerspruchsprinzip. Es sagt, dass die Aussage $A \Rightarrow B$ dasselbe bedeutet wie die Aussage $(\neg B) \Rightarrow (\neg A)$. Das sieht man am direktesten, wenn man die logischen Verknüpfungen durch ihre Wahrheitstafeln angibt. Dabei stellt man in einer Tabelle die möglichen Wahrheitswerteverteilungen der Aussagen A, B und einer Verknüpfung auf. Beispiele:

$A \wedge B$:

B \ A	w	f
w	w	f
f	f	f

$A \Rightarrow B$:

B \ A	w	f
w	w	w
f	f	w

Machen Sie das für die Aussage $(\neg B) \Rightarrow (\neg A)$, und Sie werden sehen, dass die Wertetabelle dieselbe ist wie für $A \Rightarrow B$. Dies ist die Grundlage dafür, dass in der Mathematik Beweise immer wieder durch Widerspruch geführt werden: wenn die Wahrheit der Implikation $A \Rightarrow B$ zu zeigen ist, dann nimmt man an, B sei falsch, und kann daraus mit etwas Glück folgern, dass dann auch A falsch sein muss. Wenn aber A wie angenommen richtig ist, muss demnach die Annahme, B sei falsch, einen Widerspruch darstellen, also muss B auch wahr sein. Beispiele hierfür werden wir noch häufig zu sehen bekommen.

Hilfreich ist diese Beweistechnik dann, wenn die Annahme der Falschheit von B eine Denkrichtung vorgibt, die man unter der Annahme der Wahrheit von A vielleicht nicht einschlagen würde.

Viele Aussagen sind von der Form „alle X haben die Eigenschaft Y“. In unserer Sprache könnte man das schreiben als

$$(m \text{ ist X}) \Rightarrow (m \text{ hat Y}).$$

Dies lässt sich dann beweisen, indem man zeigt, dass es kein Objekt m gibt, das die Eigenschaft Y nicht hat und trotzdem ein X ist. Dazu braucht man natürlich scharfe Definitionen für Y und X, und genau dies ist eine der großen Stärken der Mathematik. Ein wichtiges sprachliches Mittel hierfür ist die Sprache der Mengenlehre. Bevor wir auf diese eingehen, erklären wir noch, wann zwei Aussagen äquivalent sind.

e) Die *Äquivalenz* $A \iff B$: „A gilt genau dann, wenn B gilt.“ Dies ist genau dann wahr, wenn A und B denselben Wahrheitswert haben. Sie ist eine Kurzschreibweise für

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

Zum Beispiel sind für eine natürliche Zahl n die Aussagen „n ist gerade“ und „$n+1$ ist ungerade“ äquivalent, was Sie alle wissen und was auch leicht bewiesen werden kann.

Wir halten in dieser Notation noch einmal die Grundregel des Widerspruchsbeweises fest:

$$\boxed{(A \Rightarrow B) \iff (\neg B \Rightarrow \neg A).}$$

1.2 Mengen

Wir stellen uns auf den naiven Standpunkt: Eine *Menge* M ist eine Ansammlung von Objekten (was auch immer das ist; Dinge, Aussagen, andere Mengen, Abbildungen), sodass von jedem Objekt x prinzipiell entschieden werden kann, ob es zu M gehört oder nicht.

Statt „x gehört zu M“ schreibt man meistens kurz $x \in M$. Statt „x gehört nicht zu M“ schreibt man entweder (selten) $\neg(x \in M)$ oder meistens $x \notin M$.

Ein wichtiges Beispiel einer Menge ist die leere Menge $\emptyset$[1]. Das ist die Menge, bei der für alle x gilt, dass sie nicht dazu gehören.

$$\boxed{\text{Es gilt für alle } x : x \notin \emptyset.}$$

Man könnte zum Beispiel $\emptyset$ als die Menge aller viereckigen Kreise definieren.

Für viele Leute ist das eine überflüssige Menge. Aber sie ist insofern notwendig, als sie uns immer wieder dazu verhilft, Fallunterscheidungen zu vermeiden, die ohne sie notwendig wären.

Die folgenden Mengen werden wir als bekannt voraussetzen:

$\mathbb{N} = \{1, 2, 3, 4 \dots\}$, die Menge der natürlichen Zahlen.

$\mathbb{N}_0 = \{0, 1, 2, 3, 4 \dots\}$.

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$, die Menge der ganzen Zahlen.

$\mathbb{Q}$, die Menge der rationalen Zahlen, und $\mathbb{R}$, die Menge der reellen Zahlen.

„Kleine“ Mengen können durch die Angabe aller zugehörigen Elemente angegeben werden. Zum Beispiel schreibt man die Menge M, deren Elemente die Zahlen 2, 3, 5 und 7 sind, als $M := \{2, 3, 5, 7\}$.

Dabei bedeutet der **Doppelpunkt** beim Gleichheitszeichen, dass die auf der Seite des Doppelpunktes befindliche Größe durch die Größe auf der anderen Seite definiert wird.

[1] Das sollten Sie nicht mit der Null verwechseln!

Man könnte hier M auch definieren als die Menge aller Primzahlen, die nicht größer als 10 sind. (Eine Primzahl ist eine natürliche Zahl ≥ 2, die sich nicht als Produkt von kleineren natürlichen Zahlen schreiben lässt.)

Eine inhaltliche Charakterisierung der Elemente einer Menge wird umso wichtiger, je komplexer die Menge ist. Man schreibt zum Beispiel in unserem Fall:

$$M := \{n \mid n \text{ ist Primzahl und } 1 \leq n \leq 10\}.$$

In diesem Sinne werden Mengen meistens dadurch angegeben, dass man charakteristische Eigenschaften ihrer Elemente nennt. Zwischen den Zeilen haben wir das eben gesehen bei der Definition der Primzahlen. Um dies aber jetzt noch eleganter aufzuschreiben, brauchen wir ein Symbol, den *Allquantor* $\forall$. Er wird verwendet, um zu sagen, dass für alle Objekte x mit einer bestimmten Eigenschaft eine Aussage $A(x)$ gilt. Statt zum Beispiel zu sagen: „Für jede natürliche Zahl n ist auch $n+1$ eine natürliche Zahl“ schreibt man kurz

$$\forall n \in \mathbb{N} : n + 1 \in \mathbb{N}.$$

Mit dem Allquantor kann man die Menge aller Primzahlen definieren durch

$$\mathbb{P} := \{n \in \mathbb{N} \mid 2 \leq n \wedge \forall a, b \in \mathbb{N} : [(a < n) \wedge (b < n)] \Rightarrow a \cdot b \neq n\}.$$

Wir werden allerdings versuchen, den Inhalt mathematischer Formeln nicht durch eine Überfrachtung mit Notation unkenntlich zu machen. Trotzdem sei an dieser Stelle auch noch auf den *Existenzquantor* $\exists$ hingewiesen, den man verwendet, um zu sagen, dass es mindestens ein Objekt x mit einer speziellen Eigenschaft gibt. Also: statt „es gibt (mindestens) eine Primzahl, die bei Division durch 4 den Rest 1 lässt und bei Division durch 7 den Rest 6“ könnte man zum Beispiel schreiben:

$$\exists p \in \mathbb{P} : [\exists m, n \in \mathbb{N} : p = 4m + 1 \text{ und } p = 7n + 6].$$

Dabei ist gleichzeitig miterklärt, was es heißt, Rest 1 (oder 6) nach Division durch 4 (oder 7) zu lassen. Die Richtigkeit einer solchen Aussage hat man zum Beispiel gezeigt, indem man eine solche Primzahl (etwa $13 = 4 \cdot 3 + 1 = 7 \cdot 1 + 6$) angibt.

Manchmal aber liegen die Dinge so verzwickt, dass man zwar abstrakt zeigen kann, dass es ein x mit der und der Eigenschaft gibt, aber trotzdem kein einziges Beispiel dafür angeben kann. Dann spricht man von einem *reinen Existenzbeweis*. Man kann zum Beispiel zeigen, dass es für beliebige natürliche Zahlen $a < b$ mit größtem gemeinsamen Teiler 1 eine Primzahl gibt, die bei Division durch b den Rest a lässt, kann solch eine Primzahl p jedoch nicht explizit für alle möglichen Wahlen von a und b konstruieren. Für jede feste Wahl von a und b findet sich trotzdem oft sehr schnell eine solche Primzahl (was natürlich noch kein Beweis ist – dieser sieht ganz anders aus).

Definition 1.2.1 (Teilmenge, Mengengleichheit)

Eine Menge N heißt *Teilmenge* der Menge M, falls alle ihre Elemente auch in M liegen:

$$\forall x : (x \in N \Rightarrow x \in M).$$

Dann schreibt man $N \subseteq M$ oder $M \supseteq N$.

Zwei Mengen sind *gleich*, wenn sie sich gegenseitig als Teilmengen enthalten. In Zeichen:

$$M = N : \Longleftrightarrow \ (M \subseteq N \wedge N \subseteq M).$$

Wie für Aussagen, so gibt es auch für Mengen Bastelanleitungen zum Herstellen neuer Mengen.

Definition 1.2.2 (Durchschnitt, Vereinigung, Produkt, Tupel)

Für zwei Mengen A und B treffen wir die folgenden Definitionen.

a) Der *Durchschnitt* $A \cap B$ ist definiert als

$$A \cap B := \{x \mid x \in A \text{ und } x \in B\}.$$

b) Die *Vereinigung* $A \cup B$ ist definiert als

$$A \cup B := \{x \mid x \in A \text{ oder } x \in B\}.$$

c) Die *Differenzmenge* $A \setminus B$ ist definiert als

$$A \setminus B := \{x \mid x \in A \text{ und } x \notin B\}.$$

d) Das *kartesische Produkt* $A \times B$ ist definiert als die Menge aller geordneten Paare mit einem ersten Eintrag aus A und einem zweiten aus B. In Zeichen:

$$A \times B := \{(a, b) | a \in A \text{ und } b \in B\}.$$

e) Für positives $k \in \mathbb{N}$ setzen wir

$$A^k := \{(a_1,\ a_2,\ \ldots,\ a_k) \mid \forall i :\ a_i \in A\}$$

und nennen die Elemente von A^k auch k*-Tupel* in A. Später werden wir die Elemente von A^k oft als „Spalten“ schreiben, also als

$$(a_1\ a_2\ \ldots\ a_k)^\top := \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix}.$$

Dabei steht das Symbol $^\top$ für die *Transposition*, siehe 4.1.11.

All das kann man noch etwas wilder treiben und beliebig viele Mengen schneiden oder vereinigen. Bevor wir das erklären, führen wir noch die *Potenzmenge* $\mathcal{P}(M)$ ein. Das ist die Menge, deren Elemente die Teilmengen von M sind:

$$\mathcal{P}(M) := \{x \mid x \subseteq M\}.$$

Zum Beispiel gilt

$$\mathcal{P}(\{0,1,2\}) = \big\{\emptyset, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\big\}.$$

Wichtig ist hierbei, dass $M \in \mathcal{P}(M)$ immer gilt, aber $M \subseteq \mathcal{P}(M)$ in aller Regel falsch ist. Das hängt eng damit zusammen, dass man zwischen $\in$ und $\subseteq$ streng unterscheiden muss.

$$\boxed{\emptyset \subseteq \emptyset, \text{ aber } \emptyset \notin \emptyset.}$$

Nun sei eine nichtleere Menge I gegeben, und für jedes $i \in I$ eine Menge M_i. Dann setzt man

$$\bigcap_{i\in I} M_i := \{x \mid \forall i \in I : x \in M_i\} \text{ und } \bigcup_{i\in I} M_i := \{x \mid \exists i \in I : x \in M_i\}.$$

Dies sind die naheliegenden Verallgemeinerungen der Durchschnitte und Vereinigungen zweier Mengen.

Manchmal liegt der Spezialfall vor, dass (die sogenannte *Indexmenge*) I selber schon eine Teilmenge von $\mathcal{P}(M)$ ist für eine Menge M. Dann hat man die Mengen

$$\bigcap_{i\in I} i, \quad \bigcup_{i\in I} i$$

als Durchschnitt und Vereinigung, auch wenn dies etwas gewöhnungsbedürftig aussieht.

Als letzte Notation führen wir noch eine Schreibweise für die Anzahl der Elemente einer Menge ein.

Definition 1.2.3 (Mächtigkeit)

Die Anzahl der Elemente einer Menge M nennt man die *Mächtigkeit* oder auch die *Kardinalität* von M. Wir schreiben dafür $|M|$ oder auch $\#M$.

Beispiel 1.2.4 (Prinzip der vollständigen Induktion)

Eine Teilmenge $S \subseteq \mathbb{N}$, die nicht leer ist, enthält mindestens ein Element n. Da es nur endlich viele natürliche Zahlen gibt, die kleiner sind als n, gibt es auch

in S nur endlich viele solcher Zahlen, also enthält S ein kleinstes Element s_0. Wenn nun für jedes $n \in$ S gilt, dass auch $n+1$ in S liegt, dann ist

$$\{s_0, s_0+1, s_0+2, \dots\} \subseteq S,$$

und da es sonst keine natürlichen Zahlen gibt, die größer sind als s_0, gilt hier sogar

$$\{s_0, s_0+1, s_0+2, \dots\} = S.$$

Das begründet das Prinzip der *vollständigen Induktion.* Um zu zeigen, dass eine von $n \in \mathbb{N}$ abhängige Aussage $A(n)$ für alle natürlichen Zahlen n ab einer gegebenen natürlichen Zahl N gilt, setzt man

$$S := \{n \in \mathbb{N} \mid n \geq N \text{ und } A(n) \text{ wahr}\}.$$

Nun hat man also noch zu zeigen, dass

$$N \in S \text{ und } \forall n : (n \in S) \Rightarrow (n+1 \in S).$$

Wir werden später Beispiele hierfür sehen.

1.3 Abbildungen

Wir machen erst eine Art Absichtserklärung und sagen, was wir uns unter einer Abbildung f zwischen zwei Mengen M und N vorstellen: Es soll eine „Vorschrift“ sein, die jedem $m \in M$ ein $n \in N$ zuordnet. Da wir nicht wissen, wie der Begriff „Vorschrift“ definiert werden soll, müssen wir das anders angehen und definieren etwas weniger eingänglich:

Definition 1.3.1 (Abbildung)

Eine *Abbildung* f zwischen zwei Mengen M und N ist eine Teilmenge $f \subseteq M \times N$, sodass für alle $m \in M$ genau ein $n \in N$ existiert, sodass $(m,n) \in f$. Für dieses n schreibt man kurz $n = f(m)$.

M heißt der *Definitionsbereich* von f, N heißt der *Wertebereich*. Die Menge aller Abbildungen von M nach N bezeichnen wir mit $\mathrm{Abb}(M,N)$. Auch die Notation N^M ist gebräuchlich.

Eine Abbildung ist also „eigentlich“ der aus der Schule bekannte Funktionsgraph. Es ist in der Tat schwierig, die Absichtserklärung anders zu präzisieren. Wenn einmal die präzise Definition gemacht ist, schreibt man dafür dann doch wieder

$$f : M \longrightarrow N,\ m \mapsto f(m)$$

oder auch etwas verkürzend

$$M \ni m \mapsto f(m) \in N.$$

Wie gesagt: $f(m)$ ist <u>das</u> Element von N, für das $(m, f(m)) \in f$ gilt.

Definition 1.3.2 (Gleichheit von Abbildungen, Identität)

a) Zwei Abbildungen $f, g : M \longrightarrow N$ sind *gleich*, wenn für alle $m \in M$ die Gleichheit $f(m) = g(m)$ gilt. Das bedeutet gerade, dass die entsprechenden Teilmengen von $M \times N$ gleich sind.

b) Die Abbildung $\mathrm{Id}_M : M \longrightarrow M$, die durch

$$\forall m \in M : \mathrm{Id}_M(m) := m$$

definiert ist, heißt die *Identität auf* M.

Zum Beispiel sind die zwei reellwertigen Abbildungen f und g, die auf $\{0, 1, -1\}$ durch

$$f(x) := 0 \quad \text{und} \quad g(x) := x^3 - x$$

definiert sind, gleich, auch wenn sie zunächst verschieden angegeben werden. Es gibt ja nur drei erlaubte Argumente, und für diese sieht man leicht, dass f und g dieselben Werte annehmen.

Wenn zwei Abbildungen $f : M \longrightarrow N$ und $g : N \longrightarrow O$ vorliegen, so kann man diese Abbildungen zusammensetzen (man sagt auch verknüpfen, komponieren oder hintereinander ausführen) und damit eine neue Abbildung $g \circ f$ (sprich: „g nach f“) von M nach O definieren. Erst einmal machen wir das formal als Graph, wie es die Definition einer Abbildung verlangt:

Definition 1.3.3 (Komposition von Abbildungen)

In der eben beschriebenen Situation ist die *Komposition* $g \circ f$ definiert durch

$$g \circ f := \{(m, o) \in M \times O | \exists n \in N : (m, n) \in f \text{ und } (n, o) \in g\}.$$

Da n hier das eindeutig festliegende $n = f(m)$ ist und $o = g(n)$, auch durch n, und damit durch m eindeutig festgelegt wird, ist klar, dass diese Menge wieder die Eigenschaften aus der Definition einer Abbildung besitzt. Es gilt

$$(g \circ f)(m) = g(f(m)).$$

Wenn $f : M \longrightarrow N$, $g : N \longrightarrow O$ und $h : O \longrightarrow P$ Abbildungen sind, so kann man auf zwei Arten die Hintereinanderausführung bilden:

$$(h \circ g) \circ f \quad \text{oder } h \circ (g \circ f).$$

Es ist offensichtlich, dass beide Möglichkeiten zum selben Ergebnis führen:

$$\begin{aligned} \forall m \in M : \quad & ((h \circ g) \circ f)(m) \\ = \; & (h \circ g)(f(m)) = h(g(f(m))) = h((g \circ f)(m)) \\ = \; & (h \circ (g \circ f))(m). \end{aligned}$$

Dabei wird in jedem Schritt nur die Definition von $\circ$ benutzt. Das begründet das folgende

Fazit 1.3.4 (Assoziativität der Komposition von Abbildungen)

$$\boxed{(h \circ g) \circ f = h \circ (g \circ f)}$$

Bemerkung 1.3.5 (Urbild und Bild)

Nun wenden wir uns wieder einer einzelnen Abbildung $f : M \longrightarrow N$ zu. Zu dieser Abbildung gibt es eine Abbildung zwischen den Potenzmengen

$$f^{-1} : \mathcal{P}(N) \longrightarrow \mathcal{P}(M), \text{ wobei } f^{-1}(B) := \{m \in M | f(m) \in B\}.$$

Man nennt $f^{-1}(B)$ das *Urbild der Teilmenge* $B \subseteq N$ *unter* f.

Wenn zum Beispiel f die Abbildung ist, die jeder Studentin ihren Geburtstag zuordnet (eine kalenderwertige Abbildung auf der Menge der Studentinnen sozusagen), dann ist $f^{-1}(\{29.\text{ Februar } 1996\})$ eben die Menge aller Studentinnen, die an diesem Tag Geburtstag hatten. Und $f^{-1}(\{29.\text{ Februar } 1997\})$ ist die leere Menge.

Oft wird man statt $f^{-1}(\{a\})$ die kürzere Notation $f^{-1}(a)$ benutzen, auch wenn dies formal nicht ganz korrekt ist.

Für eine Abbildung $f : M \longrightarrow N$ und eine Teilmenge $A \subseteq M$ bezeichnen wir mit $f(A) := \{f(a) \mid a \in A\} \subseteq N$ die Menge aller Funktionswerte von f auf der Menge A. Diese Menge heißt auch das *Bild von* A *unter* f.

Es gibt einige Eigenschaften von f, für die man sich interessieren sollte.

Definition 1.3.6 (injektiv, surjektiv, bijektiv)

a) Eine Abbildung $f : M \longrightarrow N$ heißt *injektiv*, wenn für alle $m_1, m_2 \in M$ gilt :

$$[f(m_1) = f(m_2)] \Rightarrow [m_1 = m_2].$$

Das bedeutet, dass man m eindeutig daran erkennen kann, was $f(m)$ ist. Noch anders gesagt ist f injektiv, wenn für alle $n \in N$ gilt:

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

Also: es gibt <u>höchstens</u> ein m mit $f(m) = n$.

b) f heißt *surjektiv*, wenn $f(M) = N$ gilt, also wenn für jedes $n \in N$ gilt:

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

Also: es gibt <u>mindestens</u> ein m mit $f(m) = n$. Oder auch:

$$\forall n \in N : f^{-1}(\{n\}) \neq \emptyset.$$

c) Die Abbildung f heißt *bijektiv*, wenn sie sowohl injektiv als auch surjektiv ist. Also: für jedes $n \in N$ gibt es <u>genau</u> ein $m \in M$ mit $f(m) = n$.

Beispiel 1.3.7 Die Menge M hat dann und nur dann genau n Elemente, wenn es eine Bijektion zwischen M und $\{1, 2, 3, \ldots, n\} \subseteq \mathbb{N}$ gibt. Solch eine Bijektion tut ja nichts anderes, als die Elemente aus M durchzunummerieren.

Um noch eine etwas andere Sichtweise auf diese Eigenschaften von Abbildungen zu bekommen, geben wir ein anderes Kriterium für Injektivität und Surjektivität an.

Satz 1.3.8 (Injektivität und Surjektivität)

Es sei $f : M \longrightarrow N$ eine Abbildung zwischen den Mengen M und N, und M sei nicht leer. Dann gelten die folgenden Aussagen:

a) (f *ist injektiv*) $\iff$ ($\exists g : N \longrightarrow M$ *mit* $g \circ f = \mathrm{Id}_M$).
b) (f *ist surjektiv*) $\iff$ ($\exists h : N \longrightarrow M$ *mit* $f \circ h = \mathrm{Id}_N$).
c) (f *ist bijektiv*) $\iff$ (*es gibt* g *und* h *wie in* a) *und* b)).

In diesem Fall gilt außerdem $g = h$.

Beweis. [2] a) „$\Longrightarrow$“ Wir nehmen zunächst an, f sei injektiv. Zu zeigen ist die Existenz einer Abbildung g mit den gewünschten Eigenschaften. Um diese zu konstruieren wählen wir zunächst ein $m_0 \in M$, was geht, da M nicht leer ist. Dann setzen wir für $n \in N$

$$g(n) := \begin{cases} m & \text{falls } n = f(m) \in f(M), \\ m_0 & \text{falls } n \notin f(M). \end{cases}$$

Diese Abbildung ist sinnvoll definiert: für alle $n \in f(M)$ gibt es genau ein $m \in M$ mit $f(m) = n$, denn f ist injektiv. Nun rechnet man nach

$$\forall m \in M : (g \circ f)(m) = g(f(m)) = m,$$

also $g \circ f = \mathrm{Id}_M$ nach Definition der identischen Abbildung.

„$\Longleftarrow$“ Nun gibt es nach Voraussetzung ein g wie im Satz, und wir müssen daraus folgern, dass f injektiv ist. Wenn aber $m_1, m_2 \in M$ Elemente mit $f(m_1) = f(m_2)$ sind, dann folgt

$$\begin{aligned} m_1 &= \mathrm{Id}_M(m_1) = (g \circ f)(m_1) = g(f(m_1)) \\ &\overset{f(m_1)=f(m_2)}{=} g(f(m_2)) = (g \circ f)(m_2) = \mathrm{Id}_M(m_2) = m_2. \end{aligned}$$

Also ist f injektiv.

[2] Um eine Äquivalenz zweier Aussagen zu zeigen, zeigt man oft, dass die eine die andere impliziert und umgekehrt. Dies wird – wie hier im Beweis – oft dadurch kenntlich gemacht, dass man den Äquivalenzpfeil in zwei Implikationpfeile zerlegt und eben einmal „$\Longrightarrow$“ zeigt, das ist die Implikation von links nach rechts, und dann auch noch „$\Longleftarrow$“, die andere Implikation.

b) „$\Longrightarrow$“ Hier ist f zunächst als surjektiv vorausgesetzt. Wir wählen für jedes $n \in N$ ein $m \in M$ mit $f(m) = n$ und nennen dieses gewählte m geschickter Weise $h(n)$.[3] Damit ist eine Abbildung $h : N \longrightarrow M$ ausgewählt, und es gilt für alle $n \in N$:

$$(f \circ h)(n) = f(h(n)) = n$$

nach Wahl von $h(n)$: $f \circ h = \mathrm{Id}_N$.

„$\Longleftarrow$“ Nun nehmen wir an, wir hätten eine Abbildung h von N nach M mit $f \circ h = \mathrm{Id}_N$. Dann gilt wieder für jedes $n \in N$:

$$n = (f \circ h)(n) = f(h(n)),$$

also $h(n) \in f^{-1}(\{n\})$ und damit ist f surjektiv, da n beliebig war.

c) Nach Definition ist f genau dann bijektiv, wenn es sowohl in- als auch surjektiv ist. Nach den Teilen a) und b) (die ja schon bewiesen sind!) ist das äquivalent zur Existenz von g und h. Nur $g = h$ ist noch zu zeigen. Wir benutzen nun das Assoziativitätsgesetz (Fazit 1.3.4) für die Hintereinanderausführung von Abbildungen und sehen, dass gilt:

$$g = g \circ \mathrm{Id}_N = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{Id}_M \circ h = h.$$

$\bigcirc$

Definition/Bemerkung 1.3.9 (Umkehrabbildung)

Falls f bijektiv ist, so heißt die Abbildung g aus Satz 1.3.8 die *Umkehrabbildung von* f.

Die Abbildung g ist eindeutig durch f festgelegt. Die Teile a) und b) aus dem Satz zeigen außerdem, dass dann g auch wieder injektiv und surjektiv ist, also bijektiv. Statt g schreibt man meistens f^{-1}.

Es gilt

$$\forall m \in M : f^{-1}(f(m)) = m,$$

und da f surjektiv ist, liegt damit $f^{-1}(n)$ für alle $n \in N$ fest: es gibt genau eine Umkehrabbildung.

VORSICHT: Jetzt muss man natürlich aufpassen, dass man die Umkehrabbildung nicht mit der Urbildabbildung f^{-1} von vorhin (1.3.5) verwechselt.

Das wird uns nie Probleme bereiten: wenn f nicht bijektiv ist, gibt es die Umkehrabbildung gar nicht. Und wenn f bijektiv ist, so gilt für alle $n \in N$

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

wobei links die Urbildabbildung gemeint ist und rechts die Umkehrabbildung.

[3] Hier benutzen wir das so genannte Auswahlaxiom. Das soll hier nicht problematisiert werden.

Bemerkung 1.3.10 (noch einmal Tupel)

Die Menge aller k-Tupel in der Menge A aus 1.2.2 kann man sich auch denken als die Menge aller Abbildungen von $\{1, \ldots, k\}$ nach A. Die Vorschrift, die dem Tupel $(a_1, \ldots, a_k)$ die Abbildung $[i \mapsto a_i] \in \mathrm{Abb}(\{1, \ldots, k\}, A)$ zuordnet, ist eine Bijektion zwischen A^k und $\mathrm{Abb}(\{1, \ldots, k\}, A)$. Dies gibt uns die Möglichkeit, auch A^0 noch einen Sinn zu geben:

$$A^0 = \mathrm{Abb}(\emptyset, A).$$

Diese Menge hat genau ein Element, denn es gibt genau eine Teilmenge von $\emptyset \times A = \emptyset$, und diese Teilmenge erfüllt die Bedingung aus der Definition von Abbildungen (1.3.1).

Definition 1.3.11 (Einschränkung einer Abbildung)

Es seien $f : M \longrightarrow N$ eine Abbildung und T eine Teilmenge von M. Dann heißt die Abbildung

$$f|_T : T \longrightarrow N, \quad t \mapsto f(t)$$

die *Einschränkung* oder auch *Restriktion von f nach T*. Man merkt sich hier im Symbol der Abbildung den künstlich verkleinerten Definitionsbereich.

Wenn $M = N$ gilt und $f(T) \subseteq T$, dann bezeichnet man mit $f|_T$ oft auch die Abbildung von T nach T, die durch f gegeben ist; siehe z.B. Definition 7.2.1.

1.4 Relationen

Definition 1.4.1 (Relationen)

Es sei M eine beliebige Menge. Eine (zweistellige) *Relation* auf M ist eine Teilmenge $R \subseteq M \times M$.

Statt $(x, y) \in R$ schreibt man zumeist kürzer xRy.

Beispiel 1.4.2

a) Für jede Menge M ist die Relation $R := \{(m, m) | m \in M\}$ die Gleichheitsrelation auf M:

$$\forall x, y \in M : \; xRy \iff x = y.$$

b) Für das Intervall $M = [0, 1] \subseteq \mathbb{R}$ sei $S := \{(x, y) | x \leq y\}$. Das ist die Kleinergleich–Relation.

Nun interessiert man sich in aller Regel nicht für alle Relationen, sondern nur für solche, die günstige Eigenschaften haben. Für uns von besonderem Interesse sind die folgenden Eigenschaften.

Definition 1.4.3 (Eigenschaften von Relationen)

Es sei $R \subseteq M \times M$ eine Relation. Dann heißt R

- *reflexiv*, wenn für alle $x \in M$ gilt: $(x, x) \in R$.
- *symmetrisch*, wenn für alle $x, y \in M$ gilt:

$$xRy \iff yRx.$$

- *antisymmetrisch*, wenn für alle $x, y \in M$ gilt:

$$[xRy \text{ und } yRx] \Longrightarrow x = y.$$

- *transitiv*, wenn für alle $x, y, z \in M$ gilt:

$$[xRy \text{ und } yRz] \Longrightarrow xRz.$$

Es ist sicher instruktiv, für jeden dieser Begriffe Relationen zu haben, die ihn erfüllen und auch solche, die dies nicht tun.

Die Gleichheitsrelation (Bsp. 1.4.2) ist reflexiv, symmetrisch und transitiv. Die Relation $\leq$ in Beispiel 1.4.2 ist antisymmetrisch. Sie ist auch nicht symmetrisch, aber reflexiv. (Die $<$-Relation wäre nicht reflexiv.)

Beide aber sind transitiv. Eine Relation, die nicht transitiv ist, ist zum Beispiel die folgende Relation U („Ungleichheit“) auf der Menge $\{0, 1\}$:

$$U := \{(0, 1), (1, 0)\}.$$

Es gilt ja $0U1$ und $1U0$, und Transitivität würde verlangen, dass aus diesen beiden auch $0U0$ folgt, was aber nicht stimmt.

Definition 1.4.4 (Äquivalenzrelation)

Eine Relation R auf der Menge M heißt eine *Äquivalenzrelation*, wenn sie reflexiv, symmetrisch und transitiv ist.

Beispiel 1.4.5 (Kongruenz)

a) Die Gleichheit ist eine Äquivalenzrelation auf jeder Menge M.

b) Die $\leq$-Relation auf $[0, 1]$ aus obigem Beispiel ist keine Äquivalenzrelation, denn sie ist nicht symmetrisch (z.B. gilt $0 \leq 1$ aber nicht $1 \leq 0$).

c) Nun sei $M = \mathbb{Z}$ und n eine natürliche Zahl.

Dann definieren wir die Relation $\equiv_n$ durch

$$x \equiv_n y \iff (x - y) \text{ ist teilbar durch } n.$$

Dabei heißt „teilbar durch n“, dass für eine geeignete ganze Zahl k die Gleichheit $x - y = k \cdot n$ gilt.

Jetzt weisen wir nach, dass dies eine Äquivalenzrelation ist. Der Nachweis besteht aus drei Schritten.

Reflexivität: Für alle $x \in \mathbb{Z}$ gilt

$$x - x = 0 = 0 \cdot n.$$

Also ist $x \equiv_n x$.

Symmetrie: Für alle $x, y \in \mathbb{Z}$ gilt:

$$\begin{aligned} x \equiv_n y &\implies \exists k \in \mathbb{Z} : x - y = k \cdot n \\ &\implies \exists k \in \mathbb{Z} : y - x = (-k) \cdot n \\ &\implies y \equiv_n x. \end{aligned}$$

Transitivität: Für alle $x, y, z \in \mathbb{Z}$ gilt:

$$\begin{aligned} (x \equiv_n y \wedge y \equiv_n z) &\implies \exists k, l \in \mathbb{Z} : x - y = k \cdot n \wedge y - z = l \cdot n \\ &\implies x - z = (x - y) + (y - z) = (k + l) \cdot n \\ &\implies x \equiv_n z. \end{aligned}$$

Oft schreibt man übrigens statt $x \equiv_n y$ lieber $x \equiv y \pmod{n}$ und sagt dafür: x und y sind *kongruent modulo* n. Diese Relation und ihre weitläufige Verwandtschaft ist in vielen Teilen der Mathematik, speziell auch in der (linearen) Algebra, von großer Bedeutung. Außerdem braucht man sie in vielen Anwendungen, zum Beispiel in der Kryptographie.

Äquivalenzrelationen gehen Hand in Hand mit einer Zerlegung der Menge M in disjunkte Teilmengen. Das heißt, dass man M als Vereinigung von Teilmengen schreibt, von denen jeweils zwei verschiedene die leere Menge als Schnitt haben. Um diesen Zusammenhang zu präzisieren machen wir die folgende Definition. Dabei benutzen wir die übliche Notation $\sim$ für eine beliebige Äquivalenzrelation (anstelle des Buchstaben R aus Definition 1.4.1).

Definition 1.4.6 (Äquivalenzklassen)

Es sei $\sim$ eine Äquivalenzrelation auf der Menge M. Dann heißt für $x \in M$ die Teilmenge

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

die *Äquivalenzklasse von* x (bezüglich $\sim$).

Wir erhalten den folgenden Satz.

Satz 1.4.7 (Zerlegung in Äquivalenzklassen)
Es sei M eine Menge.

a) Für jede Äquivalenzrelation $\sim$ auf M sind die Äquivalenzklassen bezüglich $\sim$ nicht leer und es gilt

$$M = \bigcup_{x \in M} [x]_\sim.$$

Außerdem gilt für alle $x, y \in M$

$$[x]_\sim \cap [y]_\sim = \emptyset \text{ oder } [x]_\sim = [y]_\sim.$$

b) Ist umgekehrt $\mathcal{S} \subseteq \mathcal{P}(M)$ ein System von Teilmengen von M, sodass $\emptyset \notin \mathcal{S}$ gilt sowie

$$M = \bigcup_{A \in \mathcal{S}} A \quad \text{und} \quad \forall A, B \in \mathcal{S} : [A \cap B = \emptyset \text{ oder } A = B],$$

dann gibt es eine Äquivalenzrelation $\sim$ auf M, für die $\mathcal{S}$ die Menge aller Äquivalenzklassen ist, das heißt:

$$\mathcal{S} = \{[x]_\sim \mid x \in M\}.$$

Beweis. a) Da für jedes $x \in M$ wegen der Reflexivität von $\sim$ insbesondere auch $x \in [x]_\sim$ gilt, ist $[x]_\sim \neq \emptyset$, und es folgt außerdem $M = \bigcup_{x \in M} [x]_\sim$. Wenn $[x]_\sim \cap [y]_\sim \neq \emptyset$ gilt, dann gibt es ein Element z in $[x]_\sim \cap [y]_\sim$. Für dieses gilt $x \sim z$ und $y \sim z$, und wegen Symmetrie und Transitivität folgt $x \sim y$. Wiederum Symmetrie und Transitivität implizieren dann, dass für alle $m \in M$ gilt: $x \sim m \iff y \sim m$. Also sind die Äquivalenzklassen $[x]_\sim$ und $[y]_\sim$ gleich.

b) Wir definieren die Relation $\sim$ durch

$$x \sim y :\iff \exists A \in \mathcal{S} : x \in A \text{ und } y \in A.$$

Dies ist eine Äquivalenzrelation, denn sie ist

- reflexiv, weil M die Vereinigung aller $A \in \mathcal{S}$ ist, also für jedes $x \in M$ ein $A \in \mathcal{S}$ existiert mit $x \in A$.
- symmetrisch: klar.
- transitiv, weil aus $x, y \in A$ und $y, z \in B$ für $A, B \in \mathcal{S}$ folgt, dass $A \cap B$ nicht leer ist (denn y liegt im Schnitt), also $A = B$ und damit auch $x, z \in A$.

Es ist klar, dass für $x \in M$ die Äquivalenzklasse von x bezüglich $\sim$ gerade diejenige Menge $A \in \mathcal{S}$ ist, für die $x \in A$. Also gilt

$$\mathcal{S} \supseteq \{[x]_\sim \mid x \in M\}.$$

Umgekehrt ist jedes $A \in \mathcal{S}$ nicht leer, enthält also ein $x \in M$, und damit ist $A = [x]_\sim$. Das zeigt

$$\mathcal{S} \subseteq \{[x]_\sim \mid x \in M\}.$$

Also sind diese zwei Mengensysteme gleich. ◯

Beispiel 1.4.8 (noch einmal die Kongruenz)

Zur Illustration betrachten wir den Fall der Äquivalenzrelation $\equiv_n$ (Kongruenz modulo n) aus dem letzten Beispiel 1.4.5. Die Äquivalenzklasse von $x \in \mathbb{Z}$ ist die Menge aller $y \in \mathbb{Z}$, für die $x - y$ durch n teilbar ist, also die Menge aller y, die nach Division durch n denselben Rest lassen wie x nach Division durch n. Offensichtlich ist das

$$\{x + kn | k \in \mathbb{Z}\} = [x]_{\equiv_n}.$$

Wenn n nicht gerade 0 ist, so gibt es genau n Äquivalenzklassen, nämlich

$$[0]_{\equiv_n}, [1]_{\equiv_n}, \ldots, [n-1]_{\equiv_n}.$$

Der Rest von x nach Division durch n ist ja eine nicht negative Zahl kleiner als n, und zwei verschiedene solcher Zahlen sind nicht kongruent modulo n.

Betrachten wir noch den **Spezialfall** $n = 2$, so bekommen wir zwei Äquivalenzklassen: die Menge der geraden Zahlen und die der ungeraden Zahlen.

Die Klassenbildung aus dem letzten Satz verallgemeinert also einen Typus der Unterscheidung, der uns allen vertraut ist.

Wir wollen noch eine wichtige Konstruktion für Äquivalenzrelationen angeben:

Hilfssatz 1.4.9 (Abbildungen und Äquivalenzrelationen)

Es sei $f : M \longrightarrow N$ eine Abbildung. Dann wird durch

$$x \sim y :\Longleftrightarrow f(x) = f(y)$$

eine Äquivalenzrelation auf M definiert, und die Äquivalenzklasse von x ist $f^{-1}(f(x))$.

Den einfachen *Beweis* können Sie selbst als Übungsaufgabe durchführen. Die Eigenschaften einer Äquivalenzrelation werden sehr leicht auf die entsprechenden Eigenschaften der Gleichheitsrelation zurückgeführt.

Bemerkung 1.4.10 (Quotientenbildung)

Jede Äquivalenzrelation auf M lässt sich aus der Konstruktion des letzten Hilfssatzes gewinnen, wenn man nur N und f richtig wählt. Konkreter sei $\sim$ irgendeine Äquivalenzrelation auf M. Wähle $N := \mathcal{P}(M)$ die Potenzmenge von M und setze

$$f(x) := [x]_\sim.$$

Dann rechnet man leicht nach, dass man aus f durch die Konstruktion des letzten Hilfssatzes die alte Relation $\sim$ zurückgewinnt.

Dies ist das Prinzip, das der so genannten Quotientenbildung zu Grunde liegt, auf das wir noch des öfteren zu sprechen kommen werden. Sie werden hoffentlich im Laufe der Zeit feststellen, dass dieses Prinzip eines der fundamentalsten Prinzipien der Mathematik ist. Genauer nennt man das Bild von f

$$f(M) = \{[x]_\sim | x \in M\} =: M/_\sim$$

die *Quotientenmenge von M nach der Äquivalenzrelation $\sim$* . Diese Quotientenmenge wird oft benutzt, um Abbildungen $g : M \longrightarrow P$, die die Bedingung

$$\forall x, y \in M : x \sim y \Longrightarrow g(x) = g(y)$$

erfüllen, zu schreiben als

$$g = \widetilde{g} \circ f,$$

wobei die Abbildung $\widetilde{g} : M/_\sim \longrightarrow P$ definiert ist durch

$$\widetilde{g}([x]_\sim) := g(x).$$

Das ist sinnvoll, da g ja auf $[x]_\sim$ konstant ist.

Oft ist es sogar so, dass man nicht an M interessiert ist, sondern M nur braucht um die eigentlich viel interessantere Menge $M/_\sim$ hinzuschreiben, die man anders nicht in den Griff bekommt.