Sebastian Thomas

RWTH Aachen, SS 2012
5. April 2012

Vorkurs zur linearen Algebra

Manuskript

Der Vorkurs richtet sich in erster Linie an Studierende der Studiengänge Mathematik (B.Sc., LAB-GyGe oder LAB-BK), die ihr Studium zum Sommersemester 2012 beginnen. Das Ziel ist es, diesen Studierenden den Einstieg in die Vorlesung Lineare Algebra I zu erleichtern.
Es werden die grundlegenden Konzepte der Mathematik wie Mengen, Abbildungen, Relationen sowie einfache algebraische Strukturen behandelt. Es werden keinerlei Vorkenntnisse vorausgesetzt – lediglich eine gewisse Vertrautheit mit den Zahlbereichen aus der Schule ist von Vorteil, um den Beispielen folgen zu können, vgl. etwa Beispiel (1.3).
Für Hinweise auf Fehler und Unklarheiten bin ich dankbar.
Beispiele, Bemerkungen, etc., welche nicht mit einer Nummer versehen sind, wurden nachträglich eingefügt.

Aachen, 5. April 2012
Sebastian Thomas

Inhaltsverzeichnis

1 Mengen

In diesem Abschnitt werden wir Mengen einführen. Hierbei werden wir nicht genau sagen, was eine Menge ist, sondern lediglich, was wir uns hierunter vorstellen und wie wir mit Mengen umgehen. Um Mengen auf einer soliden mathematischen Basis einführen zu können, bedarf es einiger Grundlagen in *mathematischer Logik*, welcher den Rahmen unseres Kurses sprengen würde. Eine solche mathematisch präzise Einführung von Mengen geschieht in einer Vorlesung über *axiomatische Mengenlehre*; an der RWTH Aachen üblicherweise im Rahmen der Vorlesung *Mathematische Logik II* (etwa ab 5. Semester). Für das erfolgreiche Studium der meisten Gebiete der Mathematik genügt jedoch eine Kenntnis über Mengen in einem Rahmen, welcher im Wesentlichen durch diesen Kurs abgedeckt wird (der Rest wird dann in den Anfängervorlesungen vermittelt).
Die durch Anführungsstriche markierten Wörter in diesem Abschnitt werden nicht genauer präzisiert.

Dieses Vorlesungsmanuskript entstand während der Veranstaltung *Vorkurs zur linearen Algebra*; gehalten an der RWTH Aachen im Sommersemester 2012 (26.–30. März 2012).
Vorlesungshomepage: `http://www.math.rwth-aachen.de/~Sebastian.Thomas/teaching/vorkurs_lineare_algebra_12/`

Schreibweisen und Beispiele

(1.1) Vorstellung (Cantor)**.**

(a) Unter einer *Menge* verstehen wir eine „Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen“.

(b) Ist X eine Menge, so bezeichnen wir diejenigen Objekte, die durch X zusammengefasst werden, als die *Elemente* von X. Ist x ein Element von X, so schreiben wir $x \in X$. Ist x kein Element von X, so schreiben wir $x \notin X$.

(c) Mengen X und Y sind gleich, geschrieben $X = Y$, falls sie die gleichen Elemente enthalten, d.h. falls aus $x \in X$ stets $x \in Y$ folgt und falls aus $x \in Y$ stets $x \in X$ folgt.

Im Folgenden werden wir einige Notationen zur Beschreibung von Mengen angeben. In aller Regel erfolgt eine solche Beschreibung durch die Angabe einer „Eigenschaft“, welche die Elemente einer Menge erfüllen, oder durch eine einfache „Aufzählung“ ihrer Elemente. Letzteres wird vor allem bei einer Menge mit „endlich“ vielen Elementen gemacht – etwas unpräzise aber auch bei „unendlich“ vielen Elementen, sofern aus dem Kontext klar ist (bzw. klar sein sollte), welche Objekte aufgezählt werden.
Wir werden gleich zum ersten Mal das Symbol „:=“ sehen, welches bei Definitionen von mathematischen Ausdrücken verwendet wird. Wenn ein *gegebener Ausdruck* y als x *definiert* werden soll, so schreibt man $x := y$; man gibt also dem „bekannten“ Ausdruck y den neuen Namen x.

(1.2) Notation.

(a) Ist X eine Menge bestehend aus genau denjenigen Objekten, die eine gegebene Eigenschaft φ erfüllen, so schreiben wir

$$\{x \mid x \text{ erfüllt } \varphi\} := X.$$

(b) Es sei X eine Menge. Für eine Eigenschaft φ schreiben wir

$$\{x \in X \mid x \text{ erfüllt } \varphi\} := \{x \mid x \in X \text{ und } x \text{ erfüllt } \varphi\}.$$

(c) Es seien $a_1, a_2, a_3, \dots$ gegebene Objekte. Wir schreiben

$$\{a_1, a_2, a_3, \dots\} := \{x \mid x = a_1 \text{ oder } x = a_2 \text{ oder } x = a_3 \text{ oder } \dots\}.$$

Obwohl es sehr natürlich scheint, Mengen durch Eigenschaften zu beschreiben, möchten wir betonen, dass *nicht* jede Eigenschaft eine Menge beschreibt. Vgl. Aufgabe 5. Es ist jedoch stets möglich, Mengen wie in (1.2)(b) zu bilden, d.h. Mengen, deren Elemente alle in einer bereits gegebenen Menge X liegen und zusätzlich eine gegebene Eigenschaft φ erfüllen.

(1.3) Beispiel. Wir wollen davon ausgehen, dass wir wissen, was die folgenden Mengen sind. ([1])

(a) Die *Menge der natürlichen Zahlen* wird mit $\mathbb{N} := \{1, 2, 3, \dots\}$ bezeichnet. Für die *Menge der natürlichen Zahlen mit Null* schreiben wir ferner $\mathbb{N}_0 := \{x \mid x \in \mathbb{N} \text{ oder } x = 0\}$.

(b) Die *Menge der ganzen Zahlen* wird mit $\mathbb{Z} := \{x \mid x \in \mathbb{N} \text{ oder } x = 0 \text{ oder } -x \in \mathbb{N}\}$ bezeichnet.

(c) Die *Menge der rationalen Zahlen* wird mit $\mathbb{Q} := \{x \mid x = \frac{p}{q} \text{ für } p, q \in \mathbb{Z} \text{ mit } q \neq 0\}$ bezeichnet.

(d) Die *Menge der reellen Zahlen* wird mit $\mathbb{R}$ bezeichnet.

(1.4) Beispiel.

(a) Es ist $\{1, 3, 17\} = \{3, 1, 17\} = \{1, 3, 17, 1\}$. Es ist $\{1\} = \{1, 1, 1\} \neq \{1, 2\}$.

(b) Es ist $\{x \mid x \text{ ist eine Primzahl}\}$ eine Menge.

(c) Es ist $\{x \in \mathbb{Z} \mid x \text{ ist gerade}\}$ eine Menge.

(1.5) Definition (leere Menge)**.** Die Menge, welche keine Elemente enthält, heißt *leere Menge* und wird mit $\emptyset$ bezeichnet.

[1] Man kann diese Mengen geeignet aus der leeren Menge, siehe Definition (1.5), konstruieren; dies wollen wir aber in diesem Kurs nicht machen. Um die Konzepte der Mengenlehre einzuführen und die grundlegenden Aussagen zu beweisen, benötigen wir diese Mengen nicht. Sie helfen uns jedoch dadurch, da wir durch sie erläuternde Beispiele angeben können.

Teilmengen

Wir wollen dem Konzept aus Notation (1.2)(b) einen Namen geben:

(1.6) Definition (Teilmenge)**.** Es sei X eine Menge.

(a) Eine Menge U heißt *Teilmenge* von X, falls X alle Elemente von U enthält, d.h. falls aus $u \in U$ stets $u \in X$ folgt. Ist U eine Teilmenge von X, so schreiben wir $U \subseteq X$. Ist U keine Teilmenge von X, so schreiben wir $U \nsubseteq X$.

(b) Eine Teilmenge U von X heißt *echt* (oder *strikt*), falls $U \neq X$ gilt. Ist U eine echte Teilmenge von X, so schreiben wir $U \subset X$.

Man beachte, dass die Teilmengennotation nicht einheitlich ist: Manche Autoren schreiben auch $U \subset X$ anstatt $U \subseteq X$ und $U \subsetneq X$ anstatt $U \subset X$. Da Mathematik von Menschen gemacht wird, sind abweichende Notationen etwas ganz Normales und teilweise auch unvermeidbar. In vielen Bereichen haben sich jedoch Standardnotationen eingebürgert, und in aller Regel versucht man, sich auch an solche Standardnotationen zu halten. (Es wäre zum Beispiel in einem vorliegenden mathematischen Text völlig korrekt, für „U Teilmenge von X“ stets $U\%X$ zu schreiben, sofern man sich in diesem Text vorher auf diese Notation festgelegt hat; ein solcher mathematischer Text wäre jedoch auch für einen geübten Mathematiker nur schwer lesbar.) Wir werden im Folgenden meist nicht mehr auf Alternativnotationen eingehen.

(1.7) Beispiel.

(a) Es ist $\{4, 2, 7, 3\} \subseteq \{1, 2, 3, 4, 5, 6, 7\}$.

(b) Es ist $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$, d.h. es ist $\mathbb{N} \subseteq \mathbb{Z}$ und $\mathbb{Z} \subseteq \mathbb{Q}$ und $\mathbb{Q} \subseteq \mathbb{R}$.

(1.8) Bemerkung. Für Mengen X und Y gilt $X = Y$ genau dann, wenn $X \subseteq Y$ und $Y \subseteq X$ gilt.

Beweis. Dies ist eine Umformulierung von (1.1)(c). □

(1.9) Bemerkung. Für jede Menge X gilt:

(a) Es ist $\emptyset \subseteq X$.

(b) Es ist $X \subseteq X$.

Wir können die Teilmengen einer gegebenen Menge X wieder zu einer Menge zusammenfassen:

(1.10) Definition (Potenzmenge)**.** Für eine Menge X heißt $\mathrm{Pot}(X) := \{U \mid U \subseteq X\}$ die *Potenzmenge* von X.

Beispiel. Es ist $\mathrm{Pot}(\{1\}) = \{\emptyset, \{1\}\}$ und $\mathrm{Pot}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

Weitere Beispiele für Potenzmengen werden wir in Aufgabe 2 sehen.

Mengenoperationen

Als nächstes betrachten wir die sogenannten Mengenoperationen, mit deren Hilfe wir jeweils aus zwei gegebenen Mengen eine neue Menge bilden können.

(1.11) Definition (Schnitt, Vereinigung, Differenz)**.** Es seien X und Y Mengen.

(a) Die Menge

$$X \cap Y := \{x \mid x \in X \text{ und } x \in Y\}$$

heißt *Schnitt* (oder *Durchschnitt*) von X und Y.

(b) Die Menge

$$X \cup Y := \{x \mid x \in X \text{ oder } x \in Y\}$$

heißt *Vereinigung* von X und Y.

(c) Die Menge

$$X \setminus Y := \{x \mid x \in X \text{ und } x \notin Y\}$$

heißt *Differenz* von X und Y.

Hierbei wollen wir betonen, dass das „oder“ in der Mathematik, siehe Definition (1.11)(b), für ein *einschließendes oder* steht, d.h. es gilt „$x \in X$ oder $x \in Y$“ genau dann, wenn x in einer oder beiden Mengen enthalten ist. Wenn wir sagen möchten, dass x in genau einer der beiden Mengen enthalten ist, so betonen wir dies und sagen „entweder $x \in X$ oder $x \in Y$“.

(1.12) Beispiel. Es seien $X := \{1, 2, 3\}$, $Y := \{1, 4\}$. Dann ist $X \cap Y = \{1\}$, $X \cup Y = \{1, 2, 3, 4\}$, $X \setminus Y = \{2, 3\}$ und $Y \setminus X = \{4\}$.

Im Folgenden wollen wir einige Verträglichkeiten der Mengenoperationen untereinander studieren.

(1.13) Bemerkung.

(a) Für alle Mengen X, Y, Z ist $X \cap (Y \cap Z) = (X \cap Y) \cap Z$.

(b) Für alle Mengen X, Y ist $X \cap Y = Y \cap X$.

(c) Für alle Mengen X, Y, Z ist $X \cup (Y \cup Z) = (X \cup Y) \cup Z$.

(d) Für alle Mengen X, Y ist $X \cup Y = Y \cup X$.

(e) Für alle Mengen X, Y, Z ist $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$.

(f) Für alle Mengen X, Y, Z ist $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.

Beweis. Siehe Aufgabe 3. Wir begnügen uns hier mit dem Beweis von (e).

(e) Für alle Mengen X, Y, Z ist

$$\begin{aligned} X \cup (Y \cap Z) &= \{x \mid x \in X \text{ oder } x \in Y \cap Z\} = \{x \mid x \in X \text{ oder } (x \in Y \text{ und } x \in Z)\} \\ &= \{x \mid (x \in X \text{ oder } x \in Y) \text{ und } (x \in X \text{ oder } x \in Z)\} \\ &= \{x \mid x \in X \cup Y \text{ und } x \in X \cup Z\} = (X \cup Y) \cap (X \cup Z). \end{aligned}$$

□

(1.14) Konvention. Da es nach Bemerkung (1.13)(a), (c) bei der iterativen Bildung von Schnitten oder Vereinigungen nicht auf die Klammerung ankommt, lassen wir bei solchen Ausdrücken die Klammern im Folgenden weg.

Die nachstehende Bemerkung besagt, wie wir Schnitte, Vereinigungen und Differenzen von Teilmengen angeben können.

Bemerkung. Es sei X eine Menge und es seien $U, V \subseteq X$.

(a) Es ist $U \cap V = \{x \in X \mid x \in U \text{ und } x \in V\}$.

(b) Es ist $U \cup V = \{x \in X \mid x \in U \text{ oder } x \in V\}$.

(c) Es ist $U \setminus V = \{x \in X \mid x \in U \text{ und } x \notin V\}$.

Beweis. Da $U \subseteq X$ folgt aus $x \in U$ stets $x \in X$, oder, mit anderen Worten, die Aussage $x \in U$ ist äquivalent zur Aussage $x \in X$ und $x \in U$. Analog für V. Damit folgt:

(a) Es ist

$$\begin{aligned} U \cap V &= \{x \mid x \in U \text{ und } x \in V\} = \{x \mid x \in X \text{ und } x \in U \text{ und } x \in V\} \\ &= \{x \in X \mid x \in U \text{ und } x \in V\}. \end{aligned}$$

(b) Es ist

$$\begin{aligned} U \cup V &= \{x \mid x \in U \text{ oder } x \in V\} = \{x \mid (x \in X \text{ und } x \in U) \text{ oder } (x \in X \text{ und } x \in V)\} \\ &= \{x \mid x \in X \text{ und } (x \in U \text{ oder } x \in V)\} = \{x \in X \mid x \in U \text{ oder } x \in V\}. \end{aligned}$$

(c) Es ist

$$\begin{aligned} U \setminus V &= \{x \mid x \in U \text{ und } x \notin V\} = \{x \mid x \in X \text{ und } x \in U \text{ und } x \notin V\} \\ &= \{x \in X \mid x \in U \text{ und } x \notin V\}. \end{aligned}$$

□

(1.15) Proposition (de Morgan'sche Regeln)**.** Es seien eine Menge X und $U, V \subseteq X$ gegeben.

(a) Es ist $X \setminus (U \cap V) = (X \setminus U) \cup (X \setminus V)$.

(b) Es ist $X \setminus (U \cup V) = (X \setminus U) \cap (X \setminus V)$.

Beweis. Siehe Aufgabe 4. □

Geordnete Paare und kartesische Produkte

Schließlich möchten wir noch gerne sogenannte geordnete Paare (x, y) einführen. Dies wollen wir so machen, dass $(x, y) = (x', y')$ genau dann gilt, wenn $x = x'$ und $y = y'$ ist. Wie wir im Folgenden sehen werden, können wir dies unter Zurückführung des Begriffs des geordneten Paares auf den Begriff der Menge, erreichen.

(1.16) Definition (geordnetes Paar (nach Kuratowski))**.**

(a) Für Objekte x, y setzen wir $(x, y) := \{\{x\}, \{x, y\}\}$.

(b) Es sei $n \in \mathbb{N}$. Für Objekte $x_1, \ldots, x_n$ setzen wir rekursiv

$$(x_1, \ldots, x_n) := \begin{cases} x_1, & \text{falls } n = 1, \\ ((x_1, \ldots, x_{n-1}), x_n), & \text{falls } n > 1. \end{cases}$$

(1.17) Proposition. Für Objekte x, x', y, y' gilt $(x, y) = (x', y')$ genau dann, wenn $x = x'$ und $y = y'$ ist.

Beweis. Es seien x, x', y, y' gegeben. Es gelte zunächst $(x, y) = (x', y')$, d.h. $\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}$. Zuerst nehmen wir an, dass $x = y$ ist, also auch $\{x\} = \{x, y\}$. Nach unserer Voraussetzung sind dann aber $\{x'\}, \{x', y'\} \in \{\{x\}, \{x, y\}\} = \{\{x\}\}$, wir haben also auch $\{x'\} = \{x\} = \{x, y\}$ und $\{x', y'\} = \{x\} = \{x, y\}$. Insbesondere folgt $x' \in \{x\}$, also $x' = x$, sowie $y' \in \{x\}$, also $y' = x = y$. Nun nehmen wir noch an, dass $x \neq y$ ist. Dann ist $x \neq x'$ oder $y \neq x'$, also $\{x, y\} \neq \{x'\}$. Es folgt $\{x'\} = \{x\}$ wegen $\{x'\} \in \{\{x\}, \{x, y\}\}$, also $x' \in \{x\}$ und damit $x' = x$ sowie $y \neq x'$. Aus $\{x, y\} \in \{\{x'\}, \{x', y'\}\}$ und $\{x, y\} \neq \{x'\}$ erhalten wir ferner $\{x, y\} = \{x', y'\}$, also $y \in \{x', y'\}$ und schlussendlich $y = y'$ wegen $y \neq x'$. In beiden Fällen haben wir also $x = x'$ und $y = y'$. Gilt umgekehrt $x = x'$ und $y = y'$, so auch $(x, y) = \{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\} = (x', y')$. □

(1.18) Definition (kartesisches Produkt)**.** Es seien X, Y Mengen. Die Menge

$$X \times Y := \{(x, y) \mid x \in X, y \in Y\} := \{z \mid \text{es gibt } x \in X, y \in Y \text{ mit } z = (x, y)\}$$

heißt *kartesisches Produkt* von X und Y.

(1.19) Beispiel. Es ist $\{1, 2\} \times \{3, 4, 5\} = \{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)\}$.

Aufgaben

Aufgabe 1 (Mengenoperation)**.** Es seien $X := \{1, 2, 3\}$, $Y := \{6, 3, 2, 5\}$, $Z := \{5, 3, 1\}$.

(a) Bestimmen Sie $X \cap Y$, $X \cap Z$ und $X \cap Y \cap Z$.

(b) Bestimmen Sie $X \cup Y$, $Y \cup Z$ und $X \cup Y \cup Z$.

(c) Bestimmen Sie $X \cup (Y \cap Z)$ und $X \cap (Y \cup Z)$.

(d) Bestimmen Sie $Y \setminus X$, $Y \setminus Z$, $Z \setminus X$ und $X \setminus (Y \cup Z)$.

(e) Bestimmen Sie $X \times Z$ und $(Z \times X) \setminus (X \times Z)$.

Aufgabe 2 (Potenzmenge)**.** Bestimmen Sie $\mathrm{Pot}(\emptyset)$, $\mathrm{Pot}(\mathrm{Pot}(\emptyset))$ und $\mathrm{Pot}(\mathrm{Pot}(\mathrm{Pot}(\emptyset)))$.

Aufgabe 3 (Rechenregeln für Schnitt und Vereinigung)**.** Zeigen Sie:

(a) Es ist $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ und $X \cup (Y \cup Z) = (X \cup Y) \cup Z$ für alle Mengen X, Y, Z.

(b) Es ist $X \cap Y = Y \cap X$ und $X \cup Y = Y \cup X$ für alle Mengen X, Y.

(c) Es ist $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ und $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ für alle Mengen X, Y, Z.

Aufgabe 4 (de Morgan'sche Regeln)**.** Es sei X eine Menge und es seien $U, V \subseteq X$. Zeigen Sie, dass $X \setminus (U \cap V) = (X \setminus U) \cup (X \setminus V)$ und $X \setminus (U \cup V) = (X \setminus U) \cap (X \setminus V)$ gilt.

Aufgabe 5 (Russellsche Antinomie)**.** Es sei φ eine Eigenschaft. Wenn es eine Menge gibt, welche aus genau denjenigen Objekten besteht, die φ erfüllen, so sagen wir, *dass die Menge* $\{x \mid x \text{ erfüllt } \varphi\}$ *existiert*. Wenn es keine solche Menge gibt, so sagen wir, *dass* $\{x \mid x \text{ erfüllt } \varphi\}$ *keine Menge ist*.
Zeigen Sie:

(a) Es ist $\{x \mid x \text{ ist eine Menge und } x \notin x\}$ keine Menge.

(b) Für jede Menge X ist $\{x \in X \mid x \text{ ist eine Menge und } x \notin x\} \notin X$.

(c) Es ist $\{x \mid x \text{ ist eine Menge}\}$ keine Menge.

2 Abbildungen

In diesem Abschnitt wollen wir Abbildungen zwischen Mengen einführen. Während Mengen von der Vorstellung her starre Gebilde sind, stellen wir uns unter einer Abbildung eine „Vorschrift“ vor, welche die Elemente einer Menge eindeutig auf gewisse Elemente einer anderen Menge „abbildet“. Wie in der Mathematik allgemein üblich, wollen wir den Abbildungsbegriff auf den Mengenbegriff zurückführen. Oder anders ausgedrückt: wir wollen unsere intuitive Vorstellung von einer Abbildung mit Hilfe von Mengen „modellieren“.

Definition und Beispiele

(2.1) Definition (Abbildung)**.** Eine *Abbildung* (oder *Funktion*) besteht aus Mengen X und Y zusammen mit einer Teilmenge $f \subseteq X \times Y$ so, dass es für jedes $x \in X$ genau ein $y \in Y$ mit $(x, y) \in f$ gibt. Unter Missbrauch der Notation bezeichnen wir sowohl die besagte Abbildung als auch die Teilmenge von $X \times Y$ mit f. Die Menge X wird *Startmenge* (oder *Definitionsbereich*) von f genannt, die Menge Y wird *Zielmenge* (oder *Wertebereich*) von f genannt.
Für eine Abbildung f mit Startmenge X und Zielmenge Y sagen wir auch, dass f eine *Abbildung von X nach Y* ist, und wir schreiben $f\colon X \to Y$. Für $(x, y) \in f$ heißt y das *Bild* (oder *Bildelement*) von x unter f, es heißt x ein *Urbild* (oder *Urbildelement*) von y unter f, und wir schreiben $f(x) := y$ oder $x \mapsto f(x)$.
Für Mengen X und Y bezeichnen wir die *Menge aller Abbildungen von X nach Y* mit

$$\mathrm{Map}(X, Y) := \{f \mid f \text{ ist eine Abbildung von } X \text{ nach } Y\}.$$

Wir betonen, dass in der vorangegangenen Definition $f \neq f(x)$ ist. Während f eine Abbildung angibt, bezeichnet $f(x)$ das Bildelement von x unter f, also ein Element von Y.
Obwohl wir gesagt haben, dass wir Abbildungen auf Mengen zurückführen wollen, haben wir in Definition (2.1) nun den etwas unpräzisen Ausdruck „besteht aus“ verwendet. Dies *könnten* wir präzisieren, indem wir zum Beispiel eine Abbildung als ein Tripel (X, Y, f) definierten, welches die an eine Abbildung geforderten Eigenschaften besitzt (d.h. X ist eine Menge, Y ist eine Menge, es ist $f \subseteq X \times Y$ und für jedes $x \in X$ gibt es genau ein $y \in Y$ mit $(x, y) \in f$). Der Missbrauch, sowohl die gesamte Abbildung als auch die Teilmenge von $X \times Y$ als f zu bezeichnen, würde sich dann als „$f = (X, Y, f)$“ lesen.
Da die Notation (X, Y, f) recht sperrig ist und zudem den Abbildungsgedanken kaum widerspiegelt, hat sich stattdessen die Notation $f\colon X \to Y$ eingebürgert. Ferner ist die Reihenfolge in einem solchen Tripel (X, Y, f)

willkürlich – wir könnten genauso gut eine Abbildung auch stets als (f, X, Y) oder (Y, f, X) notieren; es muss nur einmal festgehalten werden, was die Startmenge, was die Zielmenge und was die Teilmenge des kartesischen Produkts sein soll. Es kommt also nicht wirklich auf die Reihenfolge an (man müsste sich nur ein für alle mal auf eine Reihenfolge einigen und diese dann im Folgenden immer einhalten), sondern nur darauf, dass gegebene Abbildungen $f\colon X \to Y$ und $f'\colon X' \to Y'$ genau dann gleich sind, wenn $X = X'$, $Y = Y'$ und $f = f'$ (als Teilmenge von $X \times Y = X' \times Y'$) gilt.
Es werden noch viele weitere Definitionen dieser Art, in denen ein Objekt definiert wird, welches aus mehreren Einzelobjekten bestehen soll, folgen. Aus den genannten Gründen behilft man sich in einer solchen Definition, die man mit Hilfe von Tupeln modellieren könnte, gerne mit etwas unpräzisen Ausdrücken wie „besteht aus“ oder „zusammen mit“. Durch die jeweils individuell festgelegten Notationen hat man dann stets noch „Zugriff“ auf die einzelnen Bestandteile des definierten Objekts. Nichtsdestotrotz sollte es (und wird es natürlich auch) stets möglich sein, eine solche Definition zu präzisieren.

(2.2) Beispiel.

(a) Es ist $\{1,2,3\} \to \{4,5,6\}$, $1 \mapsto 4$, $2 \mapsto 5$, $3 \mapsto 4$ eine Abbildung.

(b) Es ist $\mathbb{Z} \to \mathbb{Q}$, $x \mapsto 2x^2$ eine Abbildung.

(c) Es gibt keine Abbildung $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(x) \mapsto \sqrt{x}$ für $x \in \mathbb{N}$.

Beweis.

(c) Es ist etwa $\sqrt{2} \notin \mathbb{N}$. □

Im Fall von Beispiel (2.2)(c) sagen wir auch, dass eine solche Abbildung nicht *wohldefiniert* wäre.

Beispiel. Es ist $\mathrm{Map}(\{1,2\},\{3,4\}) = \{(1 \mapsto 3, 2 \mapsto 3), (1 \mapsto 3, 2 \mapsto 4), (1 \mapsto 4, 2 \mapsto 3), (1 \mapsto 4, 2 \mapsto 4)\}$, wobei wir etwa $(1 \mapsto 3, 2 \mapsto 3)$ als Kurzschreibweise für die Abbildung $\{1,2\} \to \{3,4\}$, $1 \mapsto 3$, $2 \mapsto 3$ verwendet haben. ([2])

(2.3) Bemerkung. Es seien $f\colon X \to Y$ und $f'\colon X' \to Y'$ Abbildungen. Genau dann gilt $f = f'$, wenn $X = X'$, $Y = Y'$ und $f(x) = f'(x)$ in Y für alle $x \in X$ ist.

Beweis. Als Teilmenge von $X \times Y$ ist $f = \{(x, f(x)) \mid x \in X\} := \{z \mid \text{es gibt ein } x \in X \text{ mit } z = (x, f(x))\}$, und als Teilmenge von $X' \times Y'$ ist $f' = \{(x', f'(x')) \mid x' \in X'\}$. Nun gilt $f = f'$ als Abbildungen genau dann, wenn $X = X'$, $Y = Y'$ und $f = f'$ als Teilmenge von $X \times Y = X' \times Y'$ ist. Letzteres ist aber äquivalent zu $\{(x, f(x)) \mid x \in X\} = \{(x', f'(x')) \mid x' \in X'\} = \{(x, f'(x)) \mid x \in X\}$. Schließlich sind diese Mengen nach Proposition (1.17) genau dann gleich, wenn $f(x) = f'(x)$ für alle $x \in X$. □

Komposition von Abbildungen

Als nächstes wollen wir gleich mehrere Abbildungen auf einmal betrachten. Haben wir Abbildungen f und g so gegeben, dass die Zielmenge von f gleich der Startmenge von g ist, so können wir diese Abbildungen nacheinander ausführen, d.h. wir können sie komponieren:

(2.4) Definition (Kompositum)**.** Es seien $f\colon X \to Y$ und $g\colon Y \to Z$ Abbildungen. Die Abbildung

$$g \circ f\colon X \to Z,\ x \mapsto g(f(x))$$

heißt *Kompositum* von f und g.

(2.5) Beispiel. Es seien $f\colon \mathbb{N} \to \mathbb{Z}$, $x \mapsto x+1$ und $g\colon \mathbb{Z} \to \mathbb{Q}$, $y \mapsto 2y^2$. Dann ist $g \circ f\colon \mathbb{N} \to \mathbb{Q}$, $x \mapsto 2(x+1)^2$.

Beweis. Für $x \in \mathbb{N}$ ist

$$g(f(x)) = g(x+1) = 2(x+1)^2.$$ □

[2] Start- und Zielmenge der jeweiligen Abbildungen sind ja bereits durch die Bezeichnung $\mathrm{Map}(\{1,2\},\{3,4\})$ festgelegt. Würden wir eine Menge betrachten, deren Elemente Abbildungen mit verschieden Start- und/oder Zielmengen sind, so müssten wir die jeweiligen Start- und Zielmengen der Elemente natürlich angeben.

(2.6) Bemerkung (Assoziativität der Komposition)**.** Für alle Abbildungen $f\colon X \to Y$, $g\colon Y \to Z$, $h\colon Z \to A$ gilt

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

Beweis. Es sind $h \circ (g \circ f)$ und $(h \circ g) \circ f$ Abbildungen von X nach A. Für alle $x \in X$ gilt außerdem

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x).$$

Insgesamt haben wir also $h \circ (g \circ f) = (h \circ g) \circ f$. □

(2.7) Konvention. Da es nach Bemerkung (2.6) bei der iterativen Bildung von Komposita nicht auf die Klammerung ankommt, lassen wir die Klammern im Folgenden weg.

Wir werden nun sehen, dass es möglich ist, für jede Menge X mindestens eine Abbildung $X \to X$ hinzuschreiben, egal welche Element X besitzt.

(2.8) Definition (identische Abbildung)**.** Es sei X eine Menge. Die Abbildung

$$\mathrm{id} = \mathrm{id}_X\colon X \to X,\ x \mapsto x$$

heißt *Identität* (oder *identische Abbildung*) auf X.

(2.9) Bemerkung. Für jede Abbildung $f\colon X \to Y$ gilt

$$f \circ \mathrm{id}_X = \mathrm{id}_Y \circ f = f.$$

Beweis. Es sei $f\colon X \to Y$ eine beliebige Abbildung. Dann haben wir $f \circ \mathrm{id}_X, \mathrm{id}_Y \circ f\colon X \to Y$ und für alle $x \in X$ gilt $f(\mathrm{id}_X(x)) = f(x)$ und $\mathrm{id}_Y(f(x)) = f(x)$. Also ist $f \circ \mathrm{id}_X = f$ und $\mathrm{id}_Y \circ f = f$. □

Schließlich wollen wir zu einer gegebenen Abbildung f solche Abbildungen g betrachten, welche durch Komposition mit f eine Identität liefern. Da die Identität einer Menge, anschaulich gesprochen, mit den Elementen dieser Menge nichts macht, macht g also die Abbildung f „rückgängig“ und umgekehrt.

(2.10) Definition (Invertierbarkeit)**.** Es sei $f\colon X \to Y$ eine Abbildung.

(a) Ein *Inverses* (oder *inverse Abbildung* oder *Umkehrabbildung*) zu f ist eine Abbildung $g\colon Y \to X$, für die $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$ gilt.

(b) Die Abbildung f heißt *invertierbar*, falls es ein Inverses zu f gibt.

(2.11) Beispiel. Es seien $\mathbb{Q}_{>0} := \{x \in \mathbb{Q} \mid x > 0\}$ und $\mathbb{Q}_{<0} := \{x \in \mathbb{Q} \mid x < 0\}$.

(a) Es seien $f\colon \mathbb{Q}_{>0} \to \mathbb{Q}_{<0}$, $x \mapsto -2x$ und $g\colon \mathbb{Q}_{<0} \to \mathbb{Q}_{>0}$, $y \mapsto -\frac{1}{2}y$. Dann ist g eine zu f inverse Abbildung.

(b) Es seien $h\colon \mathbb{Q}_{>0} \to \mathbb{Q}_{<0}$, $x \mapsto -x$ und $k\colon \mathbb{Q}_{<0} \to \mathbb{Q}_{>0}$, $y \mapsto -y$. Dann ist k eine zu h inverse Abbildung.

(c) Die Abbildung $l\colon \mathbb{Q} \to \mathbb{Q}$, $x \mapsto -x$ ist zu sich selbst invers.

Beweis.

(a) Für $x \in \mathbb{Q}_{>0}$ ist

$$g(f(x)) = g(-2x) = -\frac{1}{2}(-2x) = x,$$

und für $y \in \mathbb{Q}_{<0}$ ist

$$f(g(y)) = f(-\frac{1}{2}y) = -2(-\frac{1}{2}y) = y.$$

Folglich ist $g \circ f = \mathrm{id}_{\mathbb{Q}_{>0}}$ und $f \circ g = \mathrm{id}_{\mathbb{Q}_{<0}}$, d.h. es ist g eine zu f inverse Abbildung. □

(2.12) Bemerkung. Es sei $f\colon X \to Y$ eine Abbildung. Dann gibt es höchstens ein Inverses zu f.

Beweis. Es seien $g\colon Y \to X$ und $g'\colon Y \to X$ zu f inverse Abbildungen. Nach Bemerkung (2.9) gilt dann

$$g = g \circ \mathrm{id}_Y = g \circ f \circ g' = \mathrm{id}_X \circ g' = g'. \qquad \square$$

Da wir nun wissen, dass die zu einer gegebenen Abbildung f inverse Abbildung, sofern sie existiert, eindeutig durch f festgelegt ist, können wir ihr eine feste Bezeichnung (in Abhängigkeit von f) geben:

(2.13) Notation. Die zu einer invertierbaren Abbildung $f\colon X \to Y$ gegebene inverse Abbildung bezeichnen wir mit $f^{-1}\colon Y \to X$.

(2.14) Proposition.

(a) Es seien $f\colon X \to Y$ und $g\colon Y \to Z$ invertierbare Abbildungen. Dann ist auch $g \circ f\colon X \to Z$ invertierbar mit

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

(b) Für jede Menge X ist $\mathrm{id}_X\colon X \to X$ eine invertierbare Abbildung mit

$$\mathrm{id}_X^{-1} = \mathrm{id}_X.$$

(c) Es sei $f\colon X \to Y$ eine invertierbare Abbildung. Dann ist auch $f^{-1}\colon Y \to X$ invertierbar mit

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

Beweis.

(a) Da f invertierbar ist, gilt $f^{-1} \circ f = \mathrm{id}_X$ und $f \circ f^{-1} = \mathrm{id}_Y$. Ferner, da g invertierbar ist, gilt $g^{-1} \circ g = \mathrm{id}_Y$ und $g \circ g^{-1} = \mathrm{id}_Z$. Nach Bemerkung (2.9) ist also

$$f^{-1} \circ g^{-1} \circ g \circ f = f^{-1} \circ \mathrm{id}_Y \circ f = f^{-1} \circ f = \mathrm{id}_X,$$
$$g \circ f \circ f^{-1} \circ g^{-1} = g \circ \mathrm{id}_Y \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_Z.$$

Somit ist $g \circ f$ invertierbar mit $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

(b) Für jede Menge X gilt $\mathrm{id}_X \circ \mathrm{id}_X = \mathrm{id}_X$ nach Bemerkung (2.9). Folglich ist id_X invertierbar mit $\mathrm{id}_X^{-1} = \mathrm{id}_X$.

(c) Da $f^{-1}\colon Y \to X$ zu f invers ist, gilt $f^{-1} \circ f = \mathrm{id}_X$ und $f \circ f^{-1} = \mathrm{id}_Y$. Dann ist aber auch $f \circ f^{-1} = \mathrm{id}_Y$ und $f^{-1} \circ f = \mathrm{id}_X$, d.h. es ist f^{-1} invertierbar mit $(f^{-1})^{-1} = f$. $\square$

Injektivität und Surjektivität

Bisher haben wir Abbildungen unter algebraischen Gesichtspunkten studiert, d.h. wir haben Abbildungen komponiert und Eigenschaften der Komposition und der damit verwandten Begriffe wie Identität und Inverses betrachtet. Als nächstes wollen wir Abbildungen mehr unter qualitativen, rein mengentheoretischen Gesichtspunkten betrachten. Wir wollen also Fragen nach dem „Aussehen“ einer Abbildung, d.h. nach ihrem Verhalten gegenüber den Elementen und Teilmengen von Start- und Zielmenge, untersuchen. Der Höhepunkt wird schließlich Satz (2.19) sein, welcher die algebraische und die mengentheoretische Sichtweise miteinander verknüpft.

(2.15) Definition (injektiv, surjektiv)**.** Es sei $f\colon X \to Y$ eine Abbildung.

(a) Wir sagen, dass f *injektiv* (oder eine *Injektion*) ist, falls f verschiedene Elemente aus X auf verschiedene Elemente in Y abbildet, d.h. falls für alle $x, x' \in X$ mit $f(x) = f(x')$ in Y stets $x = x'$ in X folgt.

(b) Wir sagen, dass f *surjektiv* (oder eine *Surjektion*) ist, falls jedes Element aus Y das Bild eines Elementes aus X unter f ist, d.h. falls für alle $y \in Y$ ein $x \in X$ mit $y = f(x)$ existiert.

(c) Wir sagen, dass f *bijektiv* (oder eine *Bijektion*) ist, falls f injektiv und surjektiv ist.

(2.16) Beispiel.

(a) Die Abbildung $f\colon \{1,2,3\} \to \{4,5\}$, $1 \mapsto 4$, $2 \mapsto 4$, $3 \mapsto 5$ ist surjektiv, aber nicht injektiv.

(b) Die Abbildung $f\colon \{1,2\} \to \{4,5,6\}$, $1 \mapsto 4$, $2 \mapsto 5$ ist injektiv, aber nicht surjektiv.

(c) Die Abbildung $f\colon \{1,2,3\} \to \{4,5,6\}$, $1 \mapsto 5$, $2 \mapsto 6$, $3 \mapsto 4$ ist bijektiv.

(d) Die Abbildung $f\colon \{1,2,3\} \to \{4,5,6\}$, $1 \mapsto 5$, $2 \mapsto 6$, $3 \mapsto 5$ ist weder injektiv noch surjektiv.

(2.17) Definition (Bild, Urbild)**.** Es sei $f\colon X \to Y$ eine Abbildung.

(a) Für eine Teilmenge $U \subseteq X$ heißt $f(U) := \{f(u) \mid u \in U\} := \{y \in Y \mid \text{es gibt ein } u \in U \text{ mit } y = f(u)\}$ das *Bild* von U unter f. Ferner heißt $\operatorname{Im} f := f(X)$ das *Bild* von f.

(b) Für eine Teilmenge $V \subseteq Y$ heißt $f^{-1}(V) := \{x \in X \mid f(x) \in V\}$ das *Urbild* von V unter f. Für ein $y \in Y$ heißt ferner $f^{-1}(\{y\})$ die *Faser* von f über y.

Wir möchten betonen, dass die Notation von Urbild und Faser nicht die Existenz einer inversen Abbildung voraussetzt – wir haben es mit einer mehrdeutigen Bezeichnung zu tun.

(2.18) Beispiel. Es sei $f\colon \{1,2,3,4\} \to \{5,6,7,8\}$, $1 \mapsto 5$, $2 \mapsto 7$, $3 \mapsto 5$, $4 \mapsto 8$. Dann ist $f(\{1,2,3\}) = \{5,7\}$, $\operatorname{Im} f = \{5,7,8\}$, $f^{-1}(\{5,8\}) = \{1,3,4\}$, $f^{-1}(\{5\}) = \{1,3\}$.

(2.19) Satz. Es sei $f\colon X \to Y$ eine Abbildung.

(a) Die folgenden Aussagen sind äquivalent.

  (i) Es ist f injektiv.

  (ii) Jede Faser von f besitzt höchstens ein Element.

  (iii) Es ist $X = \emptyset$ oder es gibt eine Abbildung $g\colon Y \to X$ mit $g \circ f = \mathrm{id}_X$.

(b) Die folgenden Aussagen sind äquivalent.

  (i) Es ist f surjektiv.

  (ii) Jede Faser von f besitzt mindestens ein Element.

  (iii) Es gibt eine Abbildung $g\colon Y \to X$ mit $f \circ g = \mathrm{id}_Y$.

(c) Die folgenden Aussagen sind äquivalent.

  (i) Es ist f bijektiv.

  (ii) Jede Faser von f besitzt genau ein Element.

  (iii) Es ist f invertierbar.

Beweis.

(a) Wir zeigen die Äquivalenz von Bedingung (i) und Bedingung (ii) sowie die Äquivalenz von Bedingung (i) und Bedingung (iii).

Es gelte zunächst Bedingung (i), d.h. es sei f injektiv. Ferner sei ein $y \in Y$ beliebig gegeben. Für alle $x, x' \in f^{-1}(\{y\})$ gilt dann $f(x) = y = f(x')$, wegen der Injektivität von f also $x = x'$. Folglich ist $f^{-1}(\{y\})$ entweder leer oder enthält genau ein Element. Da $y \in Y$ beliebig war, gilt also Bedingung (ii).

Nun sei umgekehrt angenommen, dass Bedingung (ii) gilt, d.h. dass jede Faser von f höchstens ein Element enthält. Außerdem seien $x, x' \in X$ mit $f(x) = f(x')$ gegeben. Dann ist $x \in f^{-1}(f(x))$ und $x' \in f^{-1}(f(x'))$, wegen $f(x) = f(x')$ also $x, x' \in f^{-1}(f(x)) = f^{-1}(f(x'))$. Nach unserer Voraussetzung enthält $f^{-1}(f(x)) = f^{-1}(f(x'))$ jedoch höchstens ein Element, und also gilt $x = x'$. Somit ist f injektiv, d.h. es gilt Bedingung (i).

Als nächstes gelte wieder Bedingung (i), d.h. es sei f injektiv. Ferner nehmen wir an, dass $X \neq \emptyset$ ist. Da mit Bedingung (i) auch Bedingung (ii) gilt, enthält jede Faser von f höchstens ein Element. Die Faser auf jedem $y \in \operatorname{Im} f$ ist nach Definition von $\operatorname{Im} f$ jedoch auch nicht leer, d.h. sie enthält also genau ein Element. Mit anderen Worten: Für jedes $y \in \operatorname{Im} f$ gibt es genau ein $g'(y) \in X$ mit $f(g'(y)) = y$. Dies

definiert eine Abbildung $g' \colon \operatorname{Im} f \to X$. Wir wählen ferner eine beliebige Abbildung $g'' \colon Y \setminus \operatorname{Im} f \to X$ (dies ist möglich, da $X \neq \emptyset$) und definieren $g \colon Y \to X$ durch

$$g(y) := \begin{cases} g'(y), & \text{für } y \in \operatorname{Im} f, \\ g''(y), & \text{für } y \in Y \setminus \operatorname{Im} f. \end{cases}$$

Wir erhalten $f(g(f(x))) = f(g'(f(x))) = f(x)$ und somit $g(f(x)) = x$ für $x \in X$ wegen der Injektivät von f. Also ist $g \circ f = \mathrm{id}_X$, d.h. es gilt Bedingung (iii).

Schließlich gelte noch Bedingung (iii), d.h. es sei $X = \emptyset$ oder es existiere eine Abbildung $g \colon Y \to X$ mit $g \circ f = \mathrm{id}_X$. Für alle $x, x' \in X$ mit $f(x) = f(x')$ folgt dann

$$x = g(f(x)) = g(f(x')) = x',$$

d.h. f ist injektiv und es gilt Bedingung (i).

Insgesamt sind alle drei Bedingungen äquivalent.

(b) Wir führen einen Ringschluss, d.h. wir zeigen, dass Bedingung (i) Bedingung (ii) impliziert, dass Bedingung (ii) Bedingung (iii) impliziert, und dass Bedingung (iii) Bedingung (i) impliziert.

Es gelte zunächst Bedingung (i), d.h. es sei f surjektiv. Ferner sei ein $y \in Y$ beliebig gegeben. Da f surjektiv ist, gibt es ein $x \in X$ mit $y = f(x)$, d.h. mit $x \in f^{-1}(\{y\})$. Folglich ist $f^{-1}(\{y\})$ nicht leer, und da $y \in Y$ beliebig war, gilt also Bedingung (ii).

Als nächstes sei angenommen, dass Bedingung (ii) gilt, d.h. dass jede Faser von f mindestens ein Element enthält. Dann gibt es für jedes $y \in Y$ ein $x \in X$ mit $x \in f^{-1}(\{y\})$. Wir wählen uns für jedes $y \in Y$ ein $g(y) \in f^{-1}(\{y\})$ und erhalten so eine Abbildung $g \colon Y \to X$ mit $f(g(y)) = y$ für $y \in Y$, d.h. mit $f \circ g = \mathrm{id}_Y$. Folglich gilt Bedingung (iii).

Schließlich gelte noch Bedingung (iii), d.h. es existiere eine Abbildung $g \colon Y \to X$ mit $f \circ g = \mathrm{id}_Y$. Für alle $y \in Y$ ist dann $f(g(y)) = y$, d.h. $g(y)$ ist ein Urbild von y unter f. Also ist f surjektiv, d.h. es gilt Bedingung (i).

Insgesamt sind alle drei Bedingungen äquivalent.

(c) Siehe Aufgabe 13. □

Aufgaben

Aufgabe 6 (Abbildungen)**.**

(a) Liefert $f := \{(2,3),(1,2)\}$ eine Abbildung von $\{1,2,3\}$ nach $\{1,2,3\}$?

(b) Liefert $f := \{(1,2),(2,3),(3,3)\}$ eine Abbildung von $\{1,2,3\}$ nach $\{2,3,4\}$?

(c) Liefert $f := \{(1,1),(2,3),(3,2)\}$ eine Abbildung von $\{1,2\}$ nach $\{1,3\}$?

(d) Liefert $f := \{(x, x+3) \mid x \in \{1,2,3\}\}$ eine Abbildung von $\{1,2,3\}$ nach $\{4,5,6\}$?

(e) Liefert $f := \{(y+3, y) \mid y \in \{1,2,3\}\}$ eine Abbildung von $\{4,5,6\}$ nach $\{1,2,3\}$?

Aufgabe 7 (Abbildungen)**.** Es sei X eine Menge. Bestimmen Sie $\mathrm{Map}(\emptyset, X)$ und $\mathrm{Map}(X, \emptyset)$.

Aufgabe 8 (Komposita)**.** Bestimmen Sie für folgende Abbildungen $g \circ f$ und/oder $f \circ g$, sofern definiert.

(a) Es seien $f \colon \mathbb{R} \to \mathbb{R}_{\geq 0}$, $x \mapsto (x+1)^2$ und $g \colon \mathbb{R} \to \mathbb{R}$, $y \mapsto y - 1$.

(b) Es seien $f \colon \{1,2,3\} \to \{1,2\}$, $1 \mapsto 1$, $2 \mapsto 1$, $3 \mapsto 2$ und $g \colon \{1,2\} \mapsto \mathbb{N}_0$, $1 \mapsto 0$, $2 \mapsto 100$.

(c) Es seien $f \colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, $n \mapsto (n-1, 2)$ und $g \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(n_1, n_2) \mapsto n_1 + n_2$.

Aufgabe 9 (inverse Abbildung)**.** Zeigen Sie: Es sind $\mathrm{Map}(\{0,1\},\{0,1\}) \to \{0,1,2,3\}$, $b \mapsto b(0) \cdot 2^0 + b(1) \cdot 2^1$ und $\{0,1,2,3\} \to \mathrm{Map}(\{0,1\},\{0,1\})$, $n \mapsto (0 \mapsto n \bmod 2, 1 \mapsto n \operatorname{div} 2)$ zueinander inverse Abbildungen, wobei $n \bmod 2$ den Rest und $n \operatorname{div} 2$ den ganzzahligen Anteil bei Division mit Rest durch 2 bezeichne.

Aufgabe 10 (Injektivität und Surjektivität)**.** Es sei $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$.

(a) Zeigen Sie, dass f weder injektiv noch surjektiv ist.

(b) Finden Sie Teilmengen $U, V \subseteq \mathbb{R}$ mit $f(U) \subseteq V$ so, dass $U \to V$, $x \mapsto f(x)$ injektiv, aber nicht surjektiv ist.

(c) Finden Sie Teilmengen $U, V \subseteq \mathbb{R}$ mit $f(U) \subseteq V$ so, dass $U \to V$, $x \mapsto f(x)$ surjektiv, aber nicht injektiv ist.

(d) Finden Sie Teilmengen $U, V \subseteq \mathbb{R}$ mit $f(U) \subseteq V$ so, dass $U \to V$, $x \mapsto f(x)$ bijektiv ist.

Aufgabe 11 (Injektivität und Surjektivität)**.** Es seien $f\colon X \to Y$ und $g\colon Y \to Z$ Abbildungen. Zeigen oder widerlegen Sie:

(a) Wenn f und g injektiv sind, dann ist $g \circ f$ injektiv. Wenn $g \circ f$ injektiv ist, dann ist f injektiv. Wenn $g \circ f$ injektiv ist, dann ist g injektiv.

(b) Wenn f und g surjektiv sind, dann ist $g \circ f$ surjektiv. Wenn $g \circ f$ surjektiv ist, dann ist f surjektiv. Wenn $g \circ f$ surjektiv ist, dann ist g surjektiv.

(c) Wenn f und g bijektiv sind, dann ist $g \circ f$ bijektiv. Wenn $g \circ f$ bijektiv ist, dann ist f bijektiv. Wenn $g \circ f$ bijektiv ist, dann ist g bijektiv.

Aufgabe 12 (Bild, Urbild)**.** Es seien $X := \{1, 2, 3, 4, 5, 6\}$ und $Y := \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, und es sei $f\colon X \to Y$, $1 \mapsto 2$, $2 \mapsto 2$, $3 \mapsto 2$, $4 \mapsto 5$, $5 \mapsto 8$, $6 \mapsto 8$. Ist f injektiv? Ist f surjektiv? Bestimmen Sie $f(\{1, 2, 5, 6\})$, $f^{-1}(\{2, 8\})$, $f^{-1}(\{2, 3\})$, $f^{-1}(\{5\})$, $f^{-1}(\{9\})$, $f(X)$ und $f^{-1}(Y)$.

Aufgabe 13 (Invertierbarkeit)**.** Es sei $f\colon X \to Y$ eine Abbildung. Zeigen Sie die Äquivalenz der folgenden Aussagen:

(a) Es ist f bijektiv.

(b) Jede Faser von f besitzt genau ein Element.

(c) Es ist f invertierbar.

3 Verknüpfungen

Bisher haben wir lediglich Mengen und Abbildungen zwischen Mengen betrachtet. Die aus der Schule bekannten Mengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ haben jedoch neben der Zusammenfassung ihrer Elemente noch mehr Struktur – wir können etwa Elemente addieren, subtrahieren, etc. oder auch Elemente vergleichen (sagen, wann ein Element „größer“ als ein anderes sein soll).
In diesen und den folgenden Abschnitten wollen wir den ersten Aspekt formalisieren. ([3]) Was passiert also etwa bei der Addition auf der Menge der natürlichen Zahlen $\mathbb{N}$? Wir ordnen natürlichen Zahlen m und n deren Summe $m + n$ zu. Wie wir Zuordnungen mit Hilfe der Sprache der Mengenlehre formalisieren können, haben wir jedoch bereits in Abschnitt 2 über Abbildungen gesehen. Wir müssen also die Abbildung $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(m, n) \mapsto m + n$ betrachten.

Definition und Beispiele

(3.1) Definition (Verknüpfung)**.** Es sei X eine Menge. Eine *Verknüpfung* (oder *binäre algebraische Operation*) ist eine Abbildung $m\colon X \times X \to X$.

Da zu einer gegebenen Menge X der Start- und der Zielbereich einer Verknüpfung auf X eindeutig festgelegt ist ($X \times X$ bzw. X), lassen wir diese Angaben im Folgenden meist weg.

(3.2) Beispiel.

(a) Auf $\mathbb{N}$ haben wir die Verknüpfungen $(x, y) \mapsto x + y$ und $(x, y) \mapsto x \cdot y$.

[3] Der zweite Aspekt (Vergleich von Elementen) wird kurz in Aufgabe 28 angesprochen.

(b) Auf $\mathbb{Z}$ haben wir die Verknüpfungen $(x, y) \mapsto x + y$, $(x, y) \mapsto x - y$ und $(x, y) \mapsto x \cdot y$.

(c) Auf $\mathbb{Q}$ haben wir die Verknüpfungen $(x, y) \mapsto x + y$, $(x, y) \mapsto x - y$ und $(x, y) \mapsto x \cdot y$. Auf $\mathbb{Q} \setminus \{0\}$ haben wir die Verknüpfungen $(x, y) \mapsto x \cdot y$ und $(x, y) \mapsto x : y$.

(d) Es sei X eine Menge. Auf $\mathrm{Map}(X, X)$ haben wir die Verknüpfung $(g, f) \mapsto g \circ f$.

Assoziativität und Kommutativität

Als nächstes wollen wir grundlegende Eigenschaften von Verknüpfungen studieren, die entweder erfüllt sein können, oder nicht. Hierbei orientieren wir uns an den Eigenschaften von Addition und Multiplikation auf den uns bekannten Zahlbereichen, sowie an der Verknüpfung $(g, f) \mapsto g \circ f$ auf $\mathrm{Map}(X, X)$ für eine Menge X, für die wir schon einige Eigenschaften in Abschnitt 2 studiert haben (dort waren wir sogar noch etwas allgemeiner und haben $\mathrm{Map}(Y, Z) \times \mathrm{Map}(X, Y)$, $(g, f) \mapsto g \circ f$ für Mengen X, Y, Z betrachtet).

(3.3) Definition (Assoziativität, Kommutativität)**.** Es sei X eine Menge und m eine Verknüpfung auf X.

(a) Wir sagen, dass m *assoziativ* ist, wenn $m(x, m(y, z)) = m(m(x, y), z)$ für alle $x, y, z \in X$ gilt.

(b) Wir sagen, dass m *kommutativ* ist, wenn $m(x, y) = m(y, x)$ für alle $x, y \in X$ gilt.

(3.4) Beispiel.

(a) Die Verknüpfung $(x, y) \mapsto x + y$ auf $\mathbb{N}$ ist assoziativ und kommutativ.

(b) Es sei X eine Menge. Die Verknüpfung $(g, f) \mapsto g \circ f$ auf $\mathrm{Map}(X, X)$ ist assoziativ, aber im Allgemeinen nicht kommutativ.

Beweis.

(b) Die Verknüpfung ist assoziativ nach Bemerkung (2.6). Um zu zeigen, dass die Verknüpfung im Allgemeinen nicht kommutativ ist, wählen wir $X := \{1, 2\}$ und $f, g \in \mathrm{Map}(X, X)$ mit $f(1) = 2$, $f(2) = 1$, $g(1) = 1$, $g(2) = 1$. Dann ist

$$g(f(1)) = g(2) = 1 \neq 2 = f(1) = f(g(1))$$

und also insbesondere $g \circ f \neq f \circ g$. □

Neutrale und inverse Elemente

(3.5) Definition (neutrales Element)**.** Es sei X eine Menge und m eine Verknüpfung auf X. Ein *neutrales Element* bzgl. m ist ein Element $e \in X$, welches $m(e, x) = x$ und $m(x, e) = x$ für alle $x \in X$ erfüllt.

(3.6) Beispiel.

(a) Es ist 0 ein neutrales Element der Verknüpfung $(x, y) \mapsto x + y$ auf $\mathbb{Z}$.

(b) Für jede Menge X ist id_X ein neutrales Element der Verknüpfung $(g, f) \mapsto g \circ f$ auf $\mathrm{Map}(X, X)$.

(3.7) Bemerkung. Es sei X eine Menge und m eine Verknüpfung auf X. Dann gibt es höchstens ein neutrales Element bzgl. m.

Beweis. Siehe Aufgabe 14(b). □

(3.8) Definition (inverse Elemente)**.** Es sei X eine Menge, m eine Verknüpfung auf X und e ein neutrales Element bzgl. m. Ferner sei ein $x \in X$ gegeben. Ein *inverses Element* zu x bzgl. m ist ein Element $y \in X$, welches $m(y, x) = e$ und $m(x, y) = e$ erfüllt.

(3.9) Beispiel.

(a) Für jedes Element $x \in \mathbb{Z}$ ist $-x$ ein inverses Element zu x bzgl. der Verknüpfung $(x, y) \mapsto x + y$ auf $\mathbb{Z}$.

(b) Es sei X eine Menge und es sei $f \colon X \to X$ eine invertierbare Abbildung im Sinne von Definition (2.10)(b). Dann ist die inverse Abbildung f^{-1} ein inverses Element zu f bzgl. der Verknüpfung $(g, f) \mapsto g \circ f$ auf $\mathrm{Map}(X, X)$.

Der Beweis der folgenden Bemerkung ist analog zum Beweis von (2.12).

(3.10) Bemerkung. Es sei X eine Menge, m eine assoziative Verknüpfung auf X und e ein neutrales Element bzgl. m. Dann gibt es zu jedem $x \in X$ höchstens ein inverses Element bzgl. m.

Beweis. Siehe Aufgabe 14(d). □

(3.11) Definition (Invertierbarkeit)**.** Es sei X eine Menge, m eine Verknüpfung auf X und e ein neutrales Element bzgl. m. Ein $x \in X$ heißt *invertierbar* bzgl. m, falls es ein inverses Element zu x bzgl. m gibt.

(3.12) Beispiel.

(a) Es ist nur 0 bzgl. der Verknüpfung $(x, y) \mapsto x + y$ auf $\mathbb{N}_0$ invertierbar.

(b) Jedes $x \in \mathbb{Z}$ ist bzgl. der Verknüpfung $(x, y) \mapsto x + y$ auf $\mathbb{Z}$ invertierbar.

(c) Es sei X eine Menge. Ein $f \in \mathrm{Map}(X, X)$ ist bzgl. der Verknüpfung $(g, f) \mapsto g \circ f$ invertierbar genau dann, wenn es eine invertierbare Abbildung im Sinne von Definition (2.10)(b) ist.

Aufgaben

Aufgabe 14 (neutrale und inverse Elemente)**.** Es sei X eine Menge und m eine Verknüpfung auf X. Ein *linksneutrales Element* bzgl. m ist ein Element $e \in X$, welches $m(e, x) = x$ für alle $x \in X$ erfüllt. Ein *linksinverses Element* zu x bzgl. m ist ein Element $y \in X$, welches $m(y, x) = e$ für ein neutrales Element e erfüllt. *Rechtsneutrale Elemente* und *rechtsinverse Elemente* sind symmetrisch definiert.

(a) Es sei e ein linksneutrales und e' ein rechtsneutrales Element bzgl. m. Zeigen Sie, dass dann $e = e'$ gilt.

(b) Zeigen Sie, dass es höchstens ein neutrales Element bzgl. m gibt.

(c) Es sei m assoziativ und es sei e ein neutrales Element bzgl. m. Ferner sei $x \in X$ gegeben und es sei y ein linksinverses Element und y' ein rechtsinverses Element zu x bzgl. m. Zeigen Sie, dass dann $y = y'$ gilt.

(d) Es sei m assoziativ und es sei e ein neutrales Element bzgl. m. Zeigen Sie, dass es zu jedem $x \in X$ höchstens ein inverses Element bzgl. m gibt.

Aufgabe 15 (Verknüpfungen)**.** Untersuchen Sie auf $\mathbb{Z}$ die Verknüpfungen $(x, y) \mapsto x + y$, $(x, y) \mapsto x - y$, $(x, y) \mapsto x \cdot y$ auf Assoziativität, Kommutativität, links-/rechtsneutrale Elemente und links-/rechtsinverse Elemente. Untersuchen Sie auf $\mathbb{Q} \setminus \{0\}$ die Verknüpfungen $(x, y) \mapsto x \cdot y$ und $(x, y) \mapsto x : y$ auf Assoziativität, Kommutativität, links-/rechtsneutrale Elemente und links-/rechtsinverse Elemente.

Aufgabe 16 (links-/rechtsinverse Elemente)**.** Bestimmen Sie eine Menge X und ein Element in $\mathrm{Map}(X, X)$, welches ein links-, aber kein rechtsinverses Element bzgl. der Verknüpfung $(g, f) \mapsto g \circ f$ hat.

4 Monoide und Gruppen

Als nächstes wollen wir uns davon lösen, Verknüpfungen als eigenständige Objekte zu betrachten. Wir wollen den Standpunkt einnehmen, dass Verknüpfungen fest zu einer Menge dazugehören, und wollen die Menge zusammen mit den Verknüpfungen als eine gemeinsame „algebraische Struktur“ ansehen.
Obwohl wir etwa auf $\mathbb{Q}$ mehrere uns vertraute Verknüpfungen haben, siehe Beispiel (3.2)(c), begnügen wir uns in diesem Abschnitt zunächst mit „einfacheren“ Strukturen und studieren Mengen, die mit einer Verknüpfung versehen sind und einige der in Abschnitt 3 definierten Eigenschaften erfüllen. Mengen, welche mit zwei miteinander verträglichen Verknüpfungen ausgestattet sind, werden dann in Abschnitt 5 studiert.

Monoide und abelsche Monoide

(4.1) Definition ((kommutatives) Monoid)**.**

(a) Ein *Monoid* besteht aus einer Menge M zusammen mit einer assoziativen Verknüpfung m auf M so, dass M ein neutrales Element bzgl. m besitzt. Unter Missbrauch der Notation bezeichnen wir sowohl das besagte Monoid als auch die unterliegende Menge mit M. Die Verknüpfung m wird *Multiplikation* (oder *Monoidverknüpfung*) von M genannt. Das neutrale Element bzgl. der Multiplikation wird auch *Einselement* (oder die *Eins*) von M genannt.

Für ein Monoid M mit Multiplikation m schreiben wir $\cdot = \cdot^M := m$ und $xy = x \cdot y = x \cdot^M y := m(x, y)$ für $x, y \in M$. Für das Einselement von M schreiben wir $1 = 1^M$.

(b) Ein Monoid M heißt *kommutativ*, falls die Multiplikation von M kommutativ ist.

Bei der Festlegung „$\cdot = \cdot^M := m$“ in Definition (4.1)(a) für die Multiplikation eines Monoids handelt es sich um eine Notation, um in einem abstrakt gegebenen Monoid (d.h. ein nicht in einem konkreten Beispiel gegebenes Monoid) einfach von der Verknüpfung sprechen zu können und um diese nicht immer explizit erwähnen zu müssen. In der Regel werden wir also von einem „Monoid M“ anstatt von einem „Monoid M mit Multiplikation m“ sprechen, die Multiplikation als implizit gegeben ansehen und diese dann mit dem Symbol $\cdot$ bezeichnen. Die Bezeichnung $\cdot^M$ werden wir nur dann verwenden, wenn wir explizit darauf hinweisen möchten, dass diese Multiplikation zu M gehört (etwa, wenn wir mehrere Monoide auf einmal betrachten), meistens werden wir jedoch darauf verzichten.
Die Notation „$\cdot$“ (und auch die Bezeichnung „Multiplikation“) ist natürlich von Beispielen motiviert, siehe etwa Beispiel (4.3)(a), (b). Es gibt natürlich auch andere Beispiele, wo die Monoidverknüpfung keine Multiplikation im vertrauten Sinne ist; in diesen konkret gegebenen Beispielen verwenden wir natürlich weiterhin die jeweils vorliegende Notation, die durch das Beispiel mitgebracht wird; siehe insbesondere Beispiel (4.3)(e).
Mit Hilfe der Standardnotation in einem Monoid M lesen sich die *Axiome* eines Monoids, d.h. dessen definierenden Eigenschaften, wie folgt:

- Assoziativität: Für alle $x, y, z \in M$ ist $x(yz) = (xy)z$.
- Einselement: Es existiert ein $e \in M$ mit $ex = xe = x$ für alle $x \in M$. Dieses e ist nach Bemerkung (3.7) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für alle $x \in M$.

Ist M kommutativ, so gilt zusätzlich noch:

- Kommutativität: Für alle $x, y \in G$ ist $xy = yx$.

Für kommutative Monoide haben sich noch andere Bezeichnungen eingebürgert, die natürlich ebenfalls von den Beispielen motiviert sind, siehe etwa Beispiel (4.3)(c), (d).

(4.2) Definition (abelsches Monoid)**.** Ein *abelsches Monoid* ist ein kommutatives Monoid A mit Monoidverknüpfung a. Die Verknüpfung a wird auch *Addition* von A genannt. Das neutrale Element bzgl. der Addition wird auch *Nullelement* (oder die *Null*) von A genannt.
Für ein abelsches Monoid A mit Addition a schreiben wir $+ = +^A := a$ und $x + y = x +^A y := a(x, y)$ für $x, y \in A$. Für das Nullelement von A schreiben wir $0 = 0^A$.

Ein abelsches Monoid ist also strukturell gesehen das Gleiche wie ein kommutatives Monoid; wir verwenden lediglich in abstrakten abelschen Monoiden eine andere Standardnotation: Abstrakte Monoide (die ggf. auch mal kommutativ sein dürfen, aber im Allgemeinen nicht müssen) werden multiplikativ geschrieben, abstrakte abelsche Monoide werden additiv geschrieben.

(4.3) Beispiel.

(a) Es wird $\mathbb{N}$ ein kommutatives Monoid mit Multiplikation $(x, y) \mapsto x \cdot y$ (die uns vertraute Multiplikation der natürlichen Zahlen).

(b) Es wird $\mathbb{Q}$ ein kommutatives Monoid mit Multiplikation $(x, y) \mapsto x \cdot y$. Ebenso wird $\mathbb{Q}\backslash\{0\}$ ein kommutatives Monoid mit Multiplikation $(x, y) \mapsto x \cdot y$.

(c) Es wird $\mathbb{N}$ kein abelsches Monoid mit Addition $(x, y) \mapsto x + y$ (die uns vertraute Addition der natürlichen Zahlen). Aber es wird $\mathbb{N}_0$ ein abelsches Monoid mit Addition $(x, y) \mapsto x + y$.

(d) Es wird $\mathbb{Z}$ ein abelsches Monoid mit Addition $(x, y) \mapsto x + y$.

(e) Es sei X eine Menge. Dann wird $\mathrm{Map}(X, X)$ ein im Allgemeinen nicht-kommutatives Monoid mit Monoidverknüpfung $(g, f) \mapsto g \circ f$.

Gruppen und abelsche Gruppen

In erster Linie haben wir den Begriff des Monoids eingeführt, um mit dessen Hilfe andere, speziellere Strukturen einzuführen, wie etwa im Folgenden den Begriff der Gruppe, siehe Definition (4.6), oder auch den Begriff des Rings in Abschnitt 5.
Bevor wir Gruppen einführen, legen wir noch eine vereinfachte Sprechweise für den Begriff der Invertierbarkeit bzgl. der Monoidverknüpfung in einem gegebenen Monoid fest:

(4.4) Definition (Invertierbarkeit)**.**

(a) Es sei M ein Monoid. Ein Element $x \in M$ heißt *invertierbar*, falls x invertierbar bzgl. $\cdot^M$ ist. Das zu einem invertierbaren Element $x \in M$ bzgl. $\cdot^M$ inverse Element y wird auch das *inverse Element* zu x in M genannt und mit $x^{-1} := y$ bezeichnet.

(b) Es sei A ein abelsches Monoid. Ein Element $x \in A$ heißt *negierbar*, falls x invertierbar bzgl. $+^A$ ist. Das zu einem negierbaren Element $x \in A$ bzgl. $+^M$ inverse Element y wird auch das *negative Element* zu x in A genannt und mit $-x := y$ bezeichnet.

Der Beweis der folgenden Proposition ist analog zum Beweis von Proposition (2.14).

(4.5) Proposition. Es sei M ein Monoid.

(a) Es seien $x, y \in M$ invertierbar. Dann ist auch xy invertierbar und es gilt $(xy)^{-1} = y^{-1}x^{-1}$.

(b) Es ist 1 invertierbar mit $1^{-1} = 1$.

(c) Es sei $x \in M$ invertierbar. Dann ist auch x^{-1} invertierbar mit $(x^{-1})^{-1} = x$.

Beweis. Siehe Aufgabe 17. □

(4.6) Definition ((abelsche) Gruppe)**.**

(a) Eine *Gruppe* ist ein Monoid G, in welchem jedes Element von G invertierbar ist. Die Monoidverknüpfung von G wird auch *Gruppenverknüpfung* von G genannt.

(b) Eine *abelsche Gruppe* ist ein abelsches Monoid A, in welchem jedes Element von A negierbar ist.

Die Axiome einer Gruppe G in Standardnotation lesen sich also wie folgt:

- Assoziativität: Für alle $x, y, z \in G$ ist $x(yz) = (xy)z$.
- Einselement: Es existiert ein $e \in G$ mit $ex = xe = x$ für alle $x \in G$. Dieses e ist nach Bemerkung (3.7) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für alle $x \in G$.
- Inverse Elemente: Für jedes $x \in G$ existiert ein $y \in G$ mit $yx = xy = 1$. Dieses y ist nach Bemerkung (3.10) eindeutig bestimmt und wird mit x^{-1} bezeichnet. Wir haben also $x^{-1}x = xx^{-1} = 1$.

Ist G kommutativ, so gilt zusätzlich noch:

- Kommutativität: Für alle $x, y \in G$ ist $xy = yx$.

Die Axiome einer abelschen Gruppe A sind die einer kommutativen Gruppe, jedoch mit anderer Notation. Es ist eine gute Übung, alle in diesem Abschnitt vorkommenden Aussagen in die additive Notation umzuschreiben, vgl. Aufgabe 22.

(4.7) Konvention. Wegen der Assoziativität der Multiplikation in einem Monoid oder einer Gruppe bzw. der Addition in einer abelschen Gruppe kommt es bei iterativer Bildung nicht auf die Klammerung an. Wir lassen daher im Folgenden die Klammern weg.

Wie von der Menge der ganzen Zahlen $\mathbb{Z}$ bekannt, liefert die Existenz von negativen Elementen eine neue Verknüpfung:

(4.8) Definition (Subtraktion)**.** Es sei A eine abelsche Gruppe. Die Verknüpfung $(x, y) \mapsto x + (-y)$ auf A wird *Subtraktion* von A genannt und mit $-$ bezeichnet. Wir schreiben $x - y := x + (-y)$ für $x, y \in A$.

Wir betonen, dass die Addition einer abelschen Gruppe A ein Teil der Daten von A ist (d.h. A besteht aus der unterliegenden Menge, die unter Missbrauch der Notation ebenfalls mit A bezeichnet wird, und der Addition). Hingegen wird die Subtraktion mit Hilfe der Addition und den inversen Elementen definiert und ist insbesondere somit durch die Daten (unterliegende Menge und Addition) eindeutig festgelegt.
Da Gruppen (multiplikativ geschrieben) im Allgemeinen nicht-kommutativ sind, können wir die analoge Verknüpfung $(x, y) \mapsto \frac{x}{y}$, wie etwa aus dem Beispiel $\mathbb{Q} \setminus \{0\}$ bekannt, nicht immer bilden, da im Allgemeinen $xy^{-1} \neq y^{-1}x$ ist. Lediglich bei Körpern, siehe Definition (5.5), wird diese Notation manchmal verwandt.
Wir betrachten unsere Beispiele aus (4.3) noch einmal und wollen festhalten, welche davon Gruppen bzw. abelsche Gruppen bilden.

(4.9) Beispiel.

(a) Das Monoid $\mathbb{N}$ mit der Multiplikation $(x, y) \to x \cdot y$ ist keine Gruppe.

(b) Das Monoid $\mathbb{Q}$ mit der Multiplikation $(x, y) \to x \cdot y$ ist keine Gruppe. Das Monoid $\mathbb{Q} \setminus \{0\}$ mit der Multiplikation $(x, y) \to x \cdot y$ ist eine kommutative Gruppe.

(c) Das abelsche Monoid $\mathbb{N}_0$ mit der Addition $(x, y) \to x + y$ ist keine abelsche Gruppe.

(d) Das abelsche Monoid $\mathbb{Z}$ mit der Addition $(x, y) \to x + y$ ist eine abelsche Gruppe.

(e) Das Monoid $\mathrm{Map}(X, X)$ für eine Menge X mit der Monoidverknüpfung $(g, f) \mapsto g \circ f$ ist im Allgemeinen keine Gruppe.

Zu Beispiel (4.9)(e) vergleiche man auch Aufgabe 19.
Wir wollen einige einfache Eigenschaften für Gruppen herleiten.

(4.10) Bemerkung. Es sei G eine Gruppe und es seien $g, h, x \in G$ gegeben.

(a) Genau dann gilt $gx = h$, wenn $x = g^{-1}h$ ist.

(b) Genau dann gilt $xg = h$, wenn $x = hg^{-1}$ ist.

Beweis.

(a) Wenn $gx = h$ gilt, dann auch

$$x = 1x = g^{-1}gx = g^{-1}h.$$

Umgekehrt, wenn $x = g^{-1}h$ ist, dann haben wir auch

$$gx = gg^{-1}h = 1h = h.$$

(b) Dies lässt sich analog zu (a) beweisen. □

(4.11) Bemerkung. Es sei G eine Gruppe.

(a) Es seien $g, x, y \in G$ gegeben. Wenn $gx = gy$ oder $xg = yg$ gilt, dann ist $x = y$.

(b) Es seien $g, x \in G$ gegeben. Wenn $gx = g$ oder $xg = g$ gilt, dann ist $x = 1$.

Beweis.

(a) Es gelte $gx = gy$; der andere Fall wird analog bewiesen. Nach Bemerkung (4.10)(a) ist dann

$$x = g^{-1}gy = 1y = y.$$

(b) Es gelte $gx = g$; der andere Fall wird analog bewiesen. Dann haben wir $gx = g1$ und also $x = 1$ nach (a). □

Aufgaben

Aufgabe 17 (Inversionsregeln)**.** Es sei M ein Monoid. Zeigen Sie:

(a) Es seien $x, y \in M$ invertierbar. Dann ist auch xy invertierbar und es gilt $(xy)^{-1} = y^{-1}x^{-1}$.

(b) Es ist 1 invertierbar mit $1^{-1} = 1$.

(c) Es sei $x \in M$ invertierbar. Dann ist auch x^{-1} invertierbar mit $(x^{-1})^{-1} = x$.

Aufgabe 18 (Gruppenaxiome)**.** Zeigen Sie: Die Menge der ganzen Zahlen $\mathbb{Z}$ wird zu einer kommutativen Gruppe mit Gruppenverknüpfung $(m, n) \mapsto m + n - 1$.

Aufgabe 19 (symmetrische Gruppe)**.** Nach Beispiel (4.9)(e) ist $\mathrm{Map}(X, X)$ zusammen mit der Verknüpfung $(g, f) \mapsto g \circ f$ im Allgemeinen keine Gruppe. Finden Sie eine geeignete Teilmenge S von $\mathrm{Map}(X, X)$ so, dass S mit der auf S *eingeschränkten* Verknüpfung $S \times S \to S$, $(g, f) \mapsto g \circ f$ eine Gruppe wird.

Aufgabe 20 (Linksmultiplikation)**.** Es seien eine Gruppe G und ein $g \in G$ gegeben. Zeigen Sie, dass die Abbildung $G \to G$, $x \mapsto gx$ bijektiv ist.

Aufgabe 21 (kommutative Gruppen)**.** Es sei G eine Gruppe. Für $g \in G$ sei $g^2 := gg$. Zeigen Sie:

(a) Es ist G kommutativ genau dann, wenn $(gh)^2 = g^2h^2$ für alle $g, h \in G$ gilt.

(b) Wenn $g^2 = 1$ für alle $g \in G$ gilt, dann ist G kommutativ.

(c) Wenn $g = g^{-1}$ für alle $g \in G$ gilt, dann ist G kommutativ.

Aufgabe 22 (abelsche Gruppen)**.** Reformulieren Sie die Aussagen aus Abschnitt 4 für abelsche Gruppen (d.h. übersetzen Sie alles in die additive Schreibweise). Beginnen Sie mit den Axiomen.

5 Ringe und Körper

Als nächstes wollen wir algebraische Strukturen betrachten, deren unterliegende Mengen mit zwei Verknüpfungen versehen sind.

Ringe

(5.1) Definition ((kommutativer) Ring)**.**

(a) Ein *Ring* (genauer *unitärer Ring* oder *Ring mit Einselement*) besteht aus einer Menge R zusammen mit Verknüpfungen a und m auf R so, dass folgendes gilt.

(i) Es wird R eine abelsche Gruppe mit Addition a.

(ii) Es wird R ein Monoid mit Multiplikation m.

(iii) Es gelten die *Distributivgesetze*: Für alle $x, y, z \in R$ ist $m(x, a(y, z)) = a(m(x, y), m(x, z))$ und $m(a(x, y), z) = a(m(x, z), m(y, z))$.

Die Verknüpfung a wird *Addition* von R, die Verknüpfung m wird *Multiplikation* von R genannt.

(b) Ein Ring R heißt *kommutativ*, falls die Multiplikation von R kommutativ ist.

Wir betonen, dass wir die in Definition (4.2) bzw. Definition (4.1)(a) eingeführten Notationen für die Addition in einem abelschen Monoid (und also auch in einer abelschen Gruppe) bzw. für die Multiplikation in einem Monoid auch für Ringe weiterhin verwenden. Die Axiome eines Rings R in Standardnotation lesen sich also wie folgt:

- Assoziativität der Addition: Für alle $x, y, z \in R$ ist $x + (y + z) = (x + y) + z$.
- Nullelement: Es existiert ein $n \in R$ mit $n+x = x+n = x$ für alle $x \in R$. Dieses n ist nach Bemerkung (3.7) eindeutig bestimmt und wird mit 0 bezeichnet. Wir haben also $0 + x = x + 0 = x$ für alle $x \in R$.

- Negative Elemente: Für jedes $x \in R$ existiert ein $y \in R$ mit $y + x = x + y = 0$. Dieses y ist nach Bemerkung (3.10) eindeutig bestimmt und wird mit $-x$ bezeichnet. Wir haben also $(-x) + x = x + (-x) = 0$.
- Kommutativität der Addition: Für alle $x, y \in R$ ist $x + y = y + x$.
- Assoziativität der Multiplikation: Für alle $x, y, z \in R$ ist $x(yz) = (xy)z$.
- Einselement: Es existiert ein $e \in R$ mit $ex = xe = x$ für alle $x \in R$. Dieses e ist nach Bemerkung (3.7) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für alle $x \in R$.
- Distributivität: Für alle $x, y, z \in R$ ist $x(y + z) = (xy) + (xz)$ und $(x + y)z = (xz) + (yz)$.

Ist R kommutativ, so gilt zusätzlich noch:

- Kommutativität der Multiplikation: Für alle $x, y \in R$ ist $xy = yx$.

Ebenso verwenden wir die Notationen und Begriffe aus Definition (4.4) und Definition (4.8). Ferner betonen wir, dass natürlich alle Aussagen über (abelsche) Gruppen für die einem Ring unterliegende abelsche Gruppe bestehend aus der unterliegenden Menge zusammen mit der Addition des Rings, sowie alle Aussagen über Monoide für das einem Ring unterliegende Monoid bestehend aus der unterliegenden Menge zusammen mit der Multiplikation des Rings, gültig bleiben.

Konvention. In Ringen lassen wir die Klammern um Produkte meistens weg, d.h. es gelte *Punkt- vor Strichrechnung*.

(5.2) Beispiel.

(a) Es wird $\mathbb{N}$ kein Ring mit Addition $(x, y) \mapsto x + y$ und Multiplikation $(x, y) \mapsto xy$ (die uns vertraute Addition und die uns vertraute Multiplikation der natürlichen Zahlen).

(b) Es wird $\mathbb{Z}$ ein kommutativer Ring mit Addition $(x, y) \mapsto x + y$ und Multiplikation $(x, y) \mapsto xy$.

(c) Es wird $\mathbb{Q}$ ein kommutativer Ring mit Addition $(x, y) \mapsto x + y$ und Multiplikation $(x, y) \mapsto xy$.

(5.3) Beispiel. Es wird $\mathbb{R} \times \mathbb{R}$ ein kommutativer Ring mit *komponentenweiser* Addition und Multiplikation, d.h. mit Addition $((a_1, a_2), (b_1, b_2)) \mapsto (a_1 + b_1, a_2 + b_2)$ und Multiplikation $((a_1, a_2), (b_1, b_2)) \mapsto (a_1 b_1, a_2 b_2)$.

Beweis. Siehe Aufgabe 25(a). □

Wir werden in diesem Kurs keine nichtkommutativen Ringe mit Einselement betrachten. Bereits zu Beginn der linearen Algebra werden wir allerdings mit dem Ring der quadratischen Matrizen über einem Körper (oder über einem kommutativen Ring mit Einselement) das erste Beispiel eines nichtkommutativen Rings kennenlernen.

(5.4) Proposition. Es sei R ein Ring.

(a) Für $a \in R$ ist $a0 = 0a = 0$.

(b) Für $a \in R$ ist $(-1)a = a(-1) = -a$.

(c) Für $a, b \in R$ gilt $(-a)(-b) = ab$.

Beweis. Siehe Aufgabe 23. □

Körper

(5.5) Definition (Körper)**.** Ein *Körper* ist ein kommutativer Ring K, in welchem $0 \neq 1$ gilt und in welchem jedes Element von $K \setminus \{0\}$ invertierbar (bzgl. der Multiplikation $\cdot^K$) ist.

Wir fassen nun noch einmal alle Axiome, welche in einem Körper K gelten, zusammen.

- Assoziativität der Addition: Für alle $x, y, z \in K$ ist $x + (y + z) = (x + y) + z$.
- Nullelement: Es existiert ein $n \in K$ mit $n+x = x+n = x$ für alle $x \in K$. Dieses n ist nach Bemerkung (3.7) eindeutig bestimmt und wird mit 0 bezeichnet. Wir haben also $0 + x = x + 0 = x$ für alle $x \in K$.

- Negative Elemente: Für jedes $x \in K$ existiert ein $y \in K$ mit $y + x = x + y = 0$. Dieses y ist nach Bemerkung (3.10) eindeutig bestimmt und wird mit $-x$ bezeichnet. Wir haben also $(-x) + x = x + (-x) = 0$.
- Kommutativität der Addition: Für alle $x, y \in K$ ist $x + y = y + x$.
- Assoziativität der Multiplikation: Für alle $x, y, z \in K$ ist $x(yz) = (xy)z$.
- Einselement: Es existiert ein $e \in K$ mit $ex = xe = x$ für alle $x \in K$. Dieses e ist nach Bemerkung (3.7) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für alle $x \in K$.
- Inverse Elemente: Es ist $0 \neq 1$. Für jedes $x \in K \setminus \{0\}$ existiert ein $y \in K$ mit $yx = xy = 1$. Dieses y ist nach Bemerkung (3.10) eindeutig bestimmt und wird mit x^{-1} bezeichnet. Wir haben also $x^{-1}x = xx^{-1} = 1$.
- Kommutativität der Multiplikation: Für alle $x, y \in K$ ist $xy = yx$.
- Distributivität: Für alle $x, y, z \in R$ ist $x(y + z) = (xy) + (xz)$ und $(x + y)z = (xz) + (yz)$.

(5.6) Beispiel. Es wird $\mathbb{Q}$ ein Körper mit Addition $(x, y) \mapsto x + y$ und Multiplikation $(x, y) \mapsto xy$ (die uns vertraute Addition und die uns vertraute Multiplikation der rationalen Zahlen).

(5.7) Lemma. Es sei K ein Körper und $a, b \in K$. Wenn $ab = 0$ gilt, dann ist $a = 0$ oder $b = 0$.

Beweis. Siehe Aufgabe 24. □

(5.8) Korollar. Es sei K ein Körper. Dann wird $K \setminus \{0\}$ eine kommutative Gruppe mit der vom Körper eingeschränkten Multiplikation.

Beweis. Nach Lemma (5.7) ist $xy \neq 0$ für alle $x, y \in K \setminus \{0\}$. Wir erhalten also eine eingeschränkte Verknüpfung $(K \setminus \{0\}) \times (K \setminus \{0\}) \to K \setminus \{0\}$, $(x, y) \mapsto xy$. Die Gruppenaxiome folgen aus den entsprechenden Körperaxiomen für die Multiplikation. □

Aufgaben

Aufgabe 23 (Rechenregeln in Ringen)**.** Es sei R ein Ring. Zeigen Sie:

(a) Für alle $a \in R$ ist $0 \cdot a = a \cdot 0 = 0$.

(b) Für alle $a \in R$ ist $(-1)a = a(-1) = -a$.

(c) Für alle $a, b \in R$ gilt $(-a)(-b) = ab$.

Aufgabe 24 (Nullteilerfreiheit)**.** Es sei K ein Körper und $a, b \in K$. Zeigen Sie: Wenn $ab = 0$ gilt, dann ist $a = 0$ oder $b = 0$.

Aufgabe 25 (Ringstrukturen auf $\mathbb{R} \times \mathbb{R}$)**.**

(a) Zeigen Sie, dass $\mathbb{R} \times \mathbb{R}$ zu einem kommutativen Ring mit Addition $((a_1, a_2), (b_1, b_2)) \mapsto (a_1 + b_1, a_2 + b_2)$ und Multiplikation $((a_1, a_2), (b_1, b_2)) \mapsto (a_1 b_1, a_2 b_2)$ wird. Ist $\mathbb{R} \times \mathbb{R}$ mit dieser Struktur ein Körper? (Hinweis: Aufgabe 24.)

(b) Zeigen Sie, dass $\mathbb{R} \times \mathbb{R}$ zu einem kommutativen Ring mit Addition $((a_1, a_2), (b_1, b_2)) \mapsto (a_1 + b_1, a_2 + b_2)$ und Multiplikation $((a_1, a_2), (b_1, b_2)) \mapsto (a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1)$ wird. Ist $\mathbb{R} \times \mathbb{R}$ mit dieser Struktur ein Körper?

6 Äquivalenzrelationen und Quotientenmengen

In diesem Abschnitt kehren wir zu rein mengentheoretischen Betrachtungen zurück. Unser Ziel ist es, den Begriff der (absoluten) Gleichheit von Objekten abzuschwächen und zu formalisieren, was wir unter einer „Gleichheit unter einem gewissen Gesichtspunkt“ verstehen. Hierzu dient der Begriff der Äquivalenzrelation. In Abschnitt 8 werden wir die in diesem und dem folgenden Abschnitt eingeführten Konzepte anwenden, um eine ganze Serie von neuen Beispielen von Ringen und Körpern zu konstruieren.

Relationen

Äquivalenzrelationen sind spezielle Relationen, welche wir nun zunächst einführen werden.

(6.1) Definition (Relation)**.** Es sei X eine Menge. Eine *Relation* (genauer *binäre Relation*) auf X ist eine Teilmenge $r \subseteq X \times X$. Falls $(x, y) \in r$, so sagen wir, *dass x bzgl. r in Relation zu y steht* und schreiben $x\ r\ y$.

(6.2) Beispiel.

(a) Für $m, n \in \mathbb{N}$ gelte $m < n$ genau dann, wenn es ein $p \in \mathbb{N}$ mit $n = p + m$ gibt. Die Relation $<$ auf $\mathbb{N}$ ist die übliche *Striktordnung* auf den natürlichen Zahlen und als Teilmenge von $\mathbb{N} \times \mathbb{N}$ gegeben ist durch $\{(m, n) \in \mathbb{N} \times \mathbb{N} \mid \text{es existiert ein } p \in \mathbb{N} \text{ mit } n = p + m\}$.

(b) Für $m, n \in \mathbb{N}$ gelte $m \mid n$, lies m *teilt* n, genau dann, wenn ein $q \in \mathbb{N}$ existiert mit $n = qm$. Die Relation $\mid$ auf $\mathbb{N}$ wird *Teilbarkeitsrelation* (oder *Teilbarkeit*) auf $\mathbb{N}$ genannt und ist als Teilmenge von $\mathbb{N} \times \mathbb{N}$ gegeben durch $\{(m, n) \in \mathbb{N} \times \mathbb{N} \mid \text{es existiert ein } q \in \mathbb{N} \text{ mit } n = qm\}$.

(c) Auf jeder Menge X haben wir folgende Relation: Für $x, y \in X$ gelte $x = y$ genau dann, wenn x und y gleich sind. Wir nennen $=$ die *Gleichheitsrelation* (oder *Gleichheit*) auf X, welche wir mit $=$ bezeichnen werden. Als Teilmenge von $X \times X$ ist $=$ gegeben durch $= = \{(x, x) \mid x \in X\}$.

(d) Auf jeder Menge X haben wir die *Allrelation*, welche als Teilmenge von $X \times X$ durch $\{(x, y) \mid x, y \in X\} = X \times X$ gegeben ist.

Wie in Beispiel (6.2) schon angedeutet, ist es üblich, Relationen durch Angabe der Eigenschaft, welche für die in Relation stehenden Elemente erfüllt ist, zu definieren. Dies ist äquivalent zur Angabe der Teilmenge des kartesischen Produkts und meistens etwas leserlicher.

(6.3) Definition (Transitivität, Reflexivität, Symmetrie)**.** Es sei X eine Menge und r eine Relation auf X.

(a) Wir sagen, dass r *transitiv* ist, falls für $x, y, z \in X$ aus $x\ r\ y$ und $y\ r\ z$ stets $x\ r\ z$ folgt.

(b) Wir sagen, dass r *reflexiv* ist, falls für $x \in X$ stets $x\ r\ x$ gilt.

(c) Wir sagen, dass r *symmetrisch* ist, falls für $x, y \in X$ aus $x\ r\ y$ stets $y\ r\ x$ folgt.

(6.4) Beispiel.

(a) Die übliche Striktordnung $<$ auf den natürlichen Zahlen ist transitiv, aber nicht reflexiv und nicht symmetrisch.

(b) Die Teilbarkeitsrelation $\mid$ auf den natürlichen Zahlen ist transitiv und reflexiv, aber nicht symmetrisch.

(c) Für jede Menge X ist die Gleichheitsrelation $=$ auf X transitiv, reflexiv und symmetrisch.

Beweis.

(a) Es seien $m, n, p \in \mathbb{N}$ mit $m < n$ und $n < p$ gegeben. Dann gibt es $q, r \in \mathbb{N}$ mit $n = q + m$ und $p = r + n$. Es folgt $p = r + n = r + q + m$, also $m < p$. Folglich ist $<$ transitiv.

Für kein $m \in \mathbb{N}$ gibt es ein $p \in \mathbb{N}$ mit $m = p + m$, d.h. es gilt $m < m$ für kein $m \in \mathbb{N}$. Insbesondere ist $<$ nicht reflexiv.

Es seien $m, n \in \mathbb{N}$ mit $m < n$ gegeben. Dann gibt es ein $p \in \mathbb{N}$ mit $n = p + m$. Gäbe es ein $q \in \mathbb{N}$ mit $m = q + n$, so wäre $m = q + n = q + p + m$ im Widerspruch zu Beispiel (4.3)(c). Folglich gilt $n < m$ nicht. Insbesondere ist $<$ nicht symmetrisch.

(b) Siehe Aufgabe 28(a). □

Äquivalenzrelationen

(6.5) Definition (Äquivalenzrelation)**.** Es sei X eine Menge. Eine *Äquivalenzrelation* auf X ist eine Relation auf X, welche transitiv, reflexiv und symmetrisch ist.

(6.6) Beispiel.

(a) Für $m, n \in \mathbb{Z}$ gelte $m\ c\ n$ genau dann, wenn $m = n$ oder $m = -n$ ist. Dann ist c eine Äquivalenzrelation auf $\mathbb{Z}$.

(b) Es ist $c := \{(1,1),(2,2),(3,3),(4,4),(1,2),(2,1),(1,4),(4,1),(2,4),(4,2)\}$ eine Äquivalenzrelation auf $\{1,2,3,4\}$.

(c) Für jede Menge X ist die Gleichheitsrelation auf X eine Äquivalenzrelation auf X.

Beweis.

(a) Es seien $m, n, p \in \mathbb{Z}$ mit $m\ c\ n$ und $n\ c\ p$ gegeben. Dann gilt $m = n$ oder $m = -n$, sowie $n = p$ oder $n = -p$. Wir erhalten

$$m = \left.\begin{cases} n, & \text{falls } m = n, \\ -n, & \text{falls } m = -n \end{cases}\right\} = \left.\begin{cases} p, & \text{falls } m = n,\ n = p, \\ -p, & \text{falls } m = n,\ n = -p, \\ -p, & \text{falls } m = -n,\ n = p, \\ -(-p), & \text{falls } m = -n,\ n = -p \end{cases}\right\}$$
$$= \begin{cases} p, & \text{falls } m = n,\ n = p \text{ oder } m = -n,\ n = -p, \\ -p, & \text{falls } m = n,\ n = -p \text{ oder } m = -n,\ n = -p. \end{cases}$$

Also ist $m = p$ oder $m = -p$, und damit $m\ c\ p$. Folglich ist c transitiv. □

Die bzgl. einer Äquivalenzrelation in Relationen stehenden Elemente wollen wir nun zu Teilmengen zusammenfassen:

(6.7) Definition (Äquivalenzklasse)**.** Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Für $x \in X$ heißt $[x] = [x]_c := \{\tilde{x} \in X \mid \tilde{x}\ c\ x\}$ die *Äquivalenzklasse* von x in X bzgl. c, und es heißt x ein *Repräsentant* von $[x]_c$.

(6.8) Beispiel.

(a) Für $m, n \in \mathbb{Z}$ gelte $m\ c\ n$ genau dann, wenn $m = n$ oder $m = -n$ ist. Dann ist $[m]_c = \{m, -m\}$ für alle $m \in \mathbb{Z}$.

(b) Es sei c gegeben wie in Beispiel (6.6)(b). Dann ist $[1]_c = [2]_c = [4]_c = \{1,2,4\}$ und $[3]_c = \{3\}$.

(c) Es sei X eine Menge. Dann ist $[x]_= = \{x\}$ für alle $x \in X$.

(6.9) Proposition. Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben.

(a) Für $x \in X$ ist $x \in [x]_c$.

(b) Für $x, y \in X$ sind die folgenden Aussagen äquivalent:

(i) Es ist $[x]_c = [y]_c$.
(ii) Es ist $[x]_c \subseteq [y]_c$.
(iii) Es gilt $x\ c\ y$.

Beweis.

(a) Da c reflexiv ist, haben wir $x\ c\ x$ und damit $x \in [x]$ für alle $x \in X$.

(b) Es seien $x, y \in X$ gegeben.

Wenn $[x] \subseteq [y]$ gilt, dann haben wir $x \in [x] \subseteq [y]$ nach (a) und somit $x \; c \; y$. Es sei also umgekehrt angenommen, dass $x \; c \; y$ gilt. Für alle $\tilde{x} \in [x]$ haben wir $\tilde{x} \; c \; x$, die Transitivität von c liefert also $\tilde{x} \; c \; y$, d.h. $\tilde{x} \in [y]$. Folglich ist $[x] \subseteq [y]$.

Es ist also $[x] \subseteq [y]$ genau dann, wenn $x \; c \; y$ gilt; wir haben also die Äquivalenz von Aussage (ii) und Aussage (iii) gezeigt. Nun ist aber c symmetrisch, d.h. aus $x \; c \; y$ folgt $y \; c \; x$, und folglich folgt aus $[x] \subseteq [y]$ bereits $[y] \subseteq [x]$ und damit $[x] = [y]$. Da $[x] = [y]$ aber stets $[x] \subseteq [y]$ impliziert, sind folglich auch Aussage (i) und Aussage (ii) äquivalent.

Insgesamt haben wir die Äquivalenz der drei Aussagen bewiesen. □

Quotientenmengen

Als nächstes wollen wir die Äquivalenzklassen bzgl. einer Äquivalenzrelation wieder zu einer Menge zusammenfassen:

(6.10) Definition (Quotientenmenge)**.** Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Die *Menge aller Äquivalenzklassen in X bzgl. c* bezeichnen wir mit

$$X/c := \{[x]_c \mid x \in X\}.$$

Wir nennen X/c auch die *Quotientenmenge* (oder den *Quotienten*) von X bzgl. c und $\mathrm{quo} = \mathrm{quo}^{X/c} \colon X \to X/c$, $x \mapsto [x]_c$ die *Quotientenabbildung* von X/c.

Beispiel. Es sei c gegeben wie in Beispiel (6.6)(b). Dann ist

$$\{1,2,3,4\}/c = \{[1],[2],[3],[4]\} = \{[1],[3]\}.$$

Unter der Quotientenmenge einer Menge X bzgl. einer Äquivalenzrelation c auf X stellen wir uns eine Art „Vergröberung“ der Menge X vor. Diejenigen Elemente in X, welche in X nur äquivalent bzgl. c sind, werden über die Quotientenabbildung zu gleichen Elementen in der Quotientenmenge.

(6.11) Proposition. Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben.

(a) Es ist $X/c = \{\mathrm{quo}(x) \mid x \in X\}$.

(b) Für $x, y \in X$ ist $\mathrm{quo}(x) = \mathrm{quo}(y)$ in X/c genau dann, wenn $x \; c \; y$ in X gilt.

Beweis.

(a) Nach Definition (6.10) ist

$$X/c = \{[x]_c \mid x \in X\} = \{\mathrm{quo}(x) \mid x \in X\}.$$

(b) Es seien $x, y \in X$ gegeben. Nach Definition (6.10) ist $\mathrm{quo}(x) = [x]_c$, wir haben also $\mathrm{quo}(x) = \mathrm{quo}(y)$ in X/c genau dann, wenn $[x]_c = [y]_c$ in X/c. Letzteres ist nach Proposition (6.9)(b) aber äquivalent zu $x \; c \; y$ in X. □

Proposition (6.11) gibt uns eine abstrakte Beschreibung von X/c für eine Menge X und eine Äquivalenzrelation c auf X. Man beachte, dass in dieser Beschreibung keine Aussage mehr über die genaue Beschaffenheit der Elemente von X/c, welche ja selbst Teilmengen von X waren, getroffen wird. Elemente sind von der Form $\mathrm{quo}(x)$ für $x \in X$, und wir haben eine Charakterisierung, wann $\mathrm{quo}(x) = \mathrm{quo}(y)$ für $x, y \in X$ gilt (nämlich genau dann, wenn $x \; c \; y$). Umso beachtlicher ist es, dass für fast alle Anwendungszwecke diese theoretische Beschreibung von X/c in Abhängigkeit von X und c genügt; d.h. für fast alle Aspekte genügen uns diese zwei formalen Eigenschaften, und es ist egal, wie das Element $\mathrm{quo}(x)$ von X/c für $x \in X$ „im Einzelnen aussieht“. Wir werden, nichtsdestotrotz, im Folgenden meistens der kürzeren und damit lesefreundlicheren Notation $[x]$ den Vorzug geben.

(6.12) Korollar. Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Die Quotientenabbildung $\mathrm{quo} \colon X \to X/c$ ist surjektiv.

Beweis. Nach Proposition (6.11)(a) ist $X/c = \{\mathrm{quo}(x) \mid x \in X\} = \mathrm{Im}\,\mathrm{quo}$, d.h. $\mathrm{quo} \colon X \to X/c$ ist surjektiv. □

Aufgaben

Aufgabe 26 (Relationen)**.**

(a) Finden Sie eine Relation auf $\{1,2,3\}$, die transitiv, aber weder reflexiv noch symmetrisch ist.

(b) Finden Sie eine Relation auf $\{1,2,3\}$, die reflexiv, aber weder transitiv noch symmetrisch ist.

(c) Finden Sie eine Relation auf $\{1,2,3\}$, die symmetrisch, aber weder transitiv noch reflexiv ist.

Aufgabe 27 (Bildgleichheit)**.** Es sei $f\colon X \to Y$ eine Abbildung.

(a) Es sei c eine Äquivalenzrelation auf Y. Für $x, \tilde{x} \in X$ gelte $x\ c_f\ \tilde{x}$ genau dann, wenn $f(x)\ c\ f(\tilde{x})$ gilt. Zeigen Sie, dass c_f eine Äquivalenzrelation auf X ist.

(b) Was sind die Äquivalenzklassen bzgl. $=_f$ (wobei $=_f$ wie in (a) definiert sei)?

Aufgabe 28 (Ordnungsrelationen)**.** Es sei X eine Menge. Eine Relation r auf X heißt *antisymmetrisch*, falls für $x, y \in X$ aus $x\ r\ y$ und $y\ r\ x$ stets $x = y$ folgt. Eine (*partielle*) *Ordnungsrelation* auf X ist eine Relation auf X, welche transitiv, reflexiv und antisymmetrisch ist. Zeigen Sie:

(a) Die Teilbarkeitsrelation $\mid$ auf $\mathbb{N}$ ist eine Ordnungsrelation auf $\mathbb{N}$.

(b) Die Teilmengenrelation $\subseteq$ auf $\mathrm{Pot}(X)$ ist eine Ordnungsrelation auf $\mathrm{Pot}(X)$.

7 Kongruenzrelationen und Quotientenringe

In diesem Abschnitt wollen wir die Menge der Äquivalenzklassen in einem Ring R bzgl. einer gegebenen Äquivalenzrelation c wieder zu einem Ring machen, und zwar so, dass wir repräsentantenweise rechnen können. Wir wollen also, dass in R/c die Gleichung $[x]+[y] = [x+y]$ gilt, analog für die Multiplikation. Um dies zu erreichen, muss für $(x,y), (\tilde{x},\tilde{y}) \in R \times R$ mit $([x],[y]) = ([\tilde{x}],[\tilde{y}])$ in $R/c \times R/c$ stets $[x+y] = [\tilde{x}+\tilde{y}]$ gelten. Nun ist aber $[x] = [\tilde{x}]$ genau dann, wenn $x\ c\ \tilde{x}$ ist, etc.; d.h. es muss notwendigerweise aus $x\ c\ \tilde{x}$ und $y\ c\ \tilde{y}$ stets $x+y\ c\ \tilde{x}+\tilde{y}$ folgen.

Kongruenzrelationen

Unsere Überlegungen führen uns auf den Begriff der Kongruenzrelation – eine Äquivalenzrelation auf der unterliegenden Menge eines Rings, welche verträglich mit der Ringstruktur ist.

(7.1) Definition (Kongruenzrelation)**.** Es sei R ein Ring. Eine *Kongruenzrelation* (genauer, eine *Kongruenzrelation von Ringen*) auf R ist eine Äquivalenzrelation c auf R, welche folgende Bedingungen erfüllt.

(a) Für alle $x, \tilde{x}, y, \tilde{y} \in R$ mit $x\ c\ \tilde{x}$ und $y\ c\ \tilde{y}$ gilt $x+y\ c\ \tilde{x}+\tilde{y}$.

(b) Es ist $0\ c\ 0$.

(c) Für alle $x, \tilde{x} \in R$ mit $x\ c\ \tilde{x}$ gilt $-x\ c\ -\tilde{x}$.

(d) Für alle $x, \tilde{x}, y, \tilde{y} \in R$ mit $x\ c\ \tilde{x}$ und $y\ c\ \tilde{y}$ gilt $xy\ c\ \tilde{x}\tilde{y}$.

(e) Es ist $1\ c\ 1$.

Eine Äquivalenzklasse bzgl. einer Kongruenzrelation wird auch *Kongruenzklasse* genannt.

Ein Beispiel für eine Kongruenzrelation werden wir in Abschnitt 8 sehen.
Wir haben Kongruenzrelationen etwas redundant definiert, im Allgemeinen folgen Bedingung (b) und Bedingung (e) in Definition (7.1) aus der Reflexivität und Bedingung (c) aus Bedingung (a) (siehe Beweis zu Proposition (7.2)). Wir sind nur am Spezialfall eines kommutativen Rings interessiert und kriegen hierfür sogar ein noch einfacheres Kriterium:

(7.2) Proposition. Es sei R ein kommutativer Ring und es sei c eine Äquivalenzrelation auf R. Genau dann ist c eine Kongruenzrelation auf R, wenn für $x, y, \tilde{y} \in R$ mit $y\ c\ \tilde{y}$ stets $x+y\ c\ x+\tilde{y}$ und $xy\ c\ x\tilde{y}$ gilt.

Beweis. Wenn c eine Kongruenzrelation auf R ist, dann gilt für $x, y, \tilde{y} \in R$ mit $y \; c \; \tilde{y}$ insbesondere $x + y \; c \; x + \tilde{y}$ und $xy \; c \; x\tilde{y}$ wegen der Reflexivität von c.
Es gelte also umgekehrt für $x, y, \tilde{y} \in R$ mit $y \; c \; \tilde{y}$ stets $x + y \; c \; x + \tilde{y}$ und $xy \; c \; x\tilde{y}$. Wir zeigen, dass c eine Kongruenzrelation ist. Hierzu seien zunächst $x, \tilde{x}, y, \tilde{y} \in R$ mit $x \; c \; \tilde{x}$ und $y \; c \; \tilde{y}$ gegeben. Da Addition und Multiplikation in R kommutativ sind, gilt dann

$$x + y \; c \; x + \tilde{y} = \tilde{y} + x \; c \; \tilde{y} + \tilde{x} = \tilde{x} + \tilde{y},$$
$$xy \; c \; x\tilde{y} = \tilde{y}x \; c \; \tilde{y}\tilde{x} = \tilde{x}\tilde{y},$$

d.h. es gelten Bedingung (a) und Bedingung (d) aus Definition (7.1). Ferner gilt

$$-x = (-x) + 0 = (-x) + \tilde{x} + (-\tilde{x}) \; c \; (-x) + x + (-\tilde{x}) = 0 + (-\tilde{x}) = -\tilde{x}$$

nach Bedingung (a) aus Definition (7.1) ([4]), und wir haben $0 \; c \; 0$ und $1 \; c \; 1$ wegen der Reflexivität von c. Insgesamt ist also c tatsächlich eine Kongruenzrelation auf R. □

Quotientenringe

Wie angekündigt können wir den Quotienten R/c für einen gegebenen Ring R und eine Kongruenzrelation c zu einem Ring machen:

(7.3) Proposition. Es sei R ein Ring und c eine Kongruenzrelation auf R. Dann wird R/c ein Ring mit Addition und Multiplikation gegeben durch

$$[x] + [y] = [x + y],$$
$$[x] \, [y] = [xy]$$

für $x, y \in R$. Es ist $0 = [0]$ und $1 = [1]$. Für $x \in R$ ist $-[x] = [-x]$, und falls x invertierbar ist, so ist $[x]^{-1} = [x^{-1}]$. Wenn R kommutativ ist, dann ist R/c kommutativ.

Beweis. Für $x, \tilde{x}, y, \tilde{y} \in R$ gilt $[x] = [\tilde{x}]$ bzw. $[y] = [\tilde{y}]$ genau dann, wenn $x \; c \; \tilde{x}$ bzw. $y \; c \; \tilde{y}$. Da c eine Kongruenzrelation ist, haben wir in diesem Fall dann aber $x + y \; c \; \tilde{x} + \tilde{y}$ sowie $xy \; c \; \tilde{x}\tilde{y}$, also $[x + y] = [\tilde{x} + \tilde{y}]$ und $[xy] = [\tilde{x}\tilde{y}]$. Wir erhalten somit wohldefinierte Verknüpfungen

$$+ \colon R/c \times R/c \to R/c, \; ([x], [y]) \mapsto [x + y],$$
$$\cdot \colon R/c \times R/c \to R/c, \; ([x], [y]) \mapsto [xy]$$

auf R/c. Wir verifizieren die Ringaxiome:

- Für alle $x, y, z \in R$ ist

  $$[x] + ([y] + [z]) = [x] + [y + z] = [x + (y + z)] = [(x + y) + z] = [x + y] + [z] = ([x] + [y]) + [z].$$

  Folglich ist $+$ assoziativ.

- Für alle $x \in R$ ist

  $$[0] + [x] = [0 + x] = [x]$$

  sowie analog $[x] + [0] = [x]$. Folglich ist $[0]$ neutrales Element bzgl. $+$.

- Es sei $x \in R$. Dann ist

  $$[-x] + [x] = [(-x) + x] = [0]$$

  sowie analog $[x] + [-x] = [0]$. Folglich ist $[-x]$ ein zu $[x]$ inverses Element bzgl. $+$.

- Für alle $x, y \in R$ ist

  $$[x] + [y] = [x + y] = [y + x] = [y] + [x].$$

  Folglich ist $+$ kommutativ.

[4] Alternativ können wir unter Benutzung von Proposition (5.4)(b) auch $-x = (-1)x \; c \; (-1)\tilde{x} = -\tilde{x}$ schließen.

- Die Axiome für die Multiplikation werden analog zu denen der Addition nachgewiesen.
- Für alle $x, y, z \in R$ ist

$$[x]([y]+[z]) = [x][y+z] = [x(y+z)] = [xy+xz] = [xy]+[xz] = [x][y]+[x][z]$$

sowie analog $([x]+[y])[z] = [x][z]+[y][z]$.

Insgesamt ist also R/c ein Ring mit Addition $+$ und Multiplikation $\cdot$. □

(7.4) Definition (Quotientenring)**.** Es sei R ein Ring und c eine Kongruenzrelation auf R. Der Ring R/c mit Addition und Multiplikation gegeben wie in Proposition (7.3) wird *Quotientenring* (oder *Faktorring*) von R modulo c genannt.

8 Restklassenringe

In diesem Abschnitt wollen wir schließlich die allgemeine Konstruktion eines Quotientenrings anwenden, um einen Quotientenring vom Ring der ganzen Zahlen $\mathbb{Z}$ zu konstruieren.

Kongruenz von ganzen Zahlen

(8.1) Definition (Kongruenz modulo n)**.** Es sei $n \in \mathbb{Z}$. Für $x, y \in \mathbb{Z}$ gelte $x \equiv_n y$ genau dann, wenn es ein $p \in \mathbb{Z}$ gibt mit $x = pn + y$.

(8.2) Beispiel. Es ist $1 \equiv_7 8$, $3 \equiv_7 10$, $2 \equiv_7 9$, $2 \equiv_7 16$, $2 \equiv_7 -5$, $16 \equiv_7 -5$.

(8.3) Erinnerung. Für $n \in \mathbb{N}$, $x \in \mathbb{Z}$ gibt es eindeutig bestimmte $q \in \mathbb{Z}$, $r \in \{0, \ldots, n-1\}$ mit $x = qn + r$. Man nennt q den *ganzzahligen Anteil* und r den *Rest* bei *Division mit Rest durch* n und schreibt $x \operatorname{div} n := q$ und $x \bmod n := r$. (Vgl. Aufgabe 9).

(8.4) Bemerkung. Es sei $n \in \mathbb{N}$. Für alle $x \in \mathbb{Z}$ ist $x \equiv_n x \bmod n$.

Beweis. Für alle $x \in \mathbb{Z}$ gilt $x = (x \operatorname{div} n)\, n + (x \bmod n)$ nach Division mit Rest, also $x \equiv_n (x \bmod n)$. □

(8.5) Proposition. Für alle $n \in \mathbb{Z}$ ist $\equiv_n$ eine Kongruenzrelation auf $\mathbb{Z}$.

Beweis. Wir zeigen zunächst, dass $\equiv_n$ eine Äquivalenzrelation ist. Hierzu seien $x, y, z \in \mathbb{Z}$ mit $x \equiv_n y$ und $y \equiv_n z$ gegeben. Dann gibt es $p, q \in \mathbb{Z}$ mit $x = pn + y$ und $y = qn + z$. Es folgt

$$x = pn + y = pn + qn + z = (p+q)n + z,$$

also $x \equiv_n z$. Folglich ist $\equiv_n$ transitiv. Für alle $x \in \mathbb{Z}$ ist $x = 0n + x$, also $x \equiv_n x$, d.h. $\equiv_n$ ist reflexiv. Schließlich seien $x, y \in \mathbb{Z}$ mit $x \equiv_n y$ gegeben. Dann gibt es ein $p \in \mathbb{Z}$ mit $x = pn + y$. Es folgt $y = (-p)n + x$, also $y \equiv_n x$. Folglich ist $\equiv_n$ symmetrisch. Insgesamt ist $\equiv_n$ also eine Äquivalenzrelation.
Um zu zeigen, dass $\equiv_n$ sogar eine Kongruenzrelation ist, zeigen wir die beiden Bedingungen aus Proposition (7.2). Hierzu seien $x, y, \tilde{y} \in \mathbb{Z}$ mit $y \equiv_n \tilde{y}$ gegeben. Dann gibt es ein $p \in \mathbb{Z}$ mit $y = pn + \tilde{y}$. Es folgt $x + y = x + pn + \tilde{y} = pn + (x + \tilde{y})$ und $xy = x(pn + \tilde{y}) = (xp)n + (x\tilde{y})$, also $x + y \equiv_n x + \tilde{y}$ und $xy \equiv_n x\tilde{y}$. Mit Proposition (7.2) folgt nun, dass $\equiv_n$ eine Kongruenzrelation auf $\mathbb{Z}$ ist. □

Rechnen in Restklassenringen

Aus Proposition (8.5) folgt nun, dass die Quotientenmenge $\mathbb{Z}/\equiv_n$ mit repräsentantenweiser Addition und Multiplikation ein kommutativer Ring wird.

(8.6) Definition (Restklassenring)**.** Es sei $n \in \mathbb{Z}$. Der Quotientenring $\mathbb{Z}/n := \mathbb{Z}/\equiv_n$ heißt *Restklassenring* von $\mathbb{Z}$ modulo n. Für $x \in \mathbb{Z}$ heißt die Kongruenzklasse $[x]_{\equiv_n}$ auch die *Restklasse* von x modulo n.

Der Restklassenring $\mathbb{Z}/n$ wird in der Literatur oft auch als $\mathbb{Z}/n\mathbb{Z}$ bezeichnet und leicht anders konstruiert; bei dieser alternativen Konstruktion spielt dann die Teilmenge $n\mathbb{Z} = \{np \mid p \in \mathbb{Z}\}$ eine Rolle.

(8.7) Konvention. Es sei $n \in \mathbb{Z}$. Für $x \in \mathbb{Z}$ schreiben wir unter Missbrauch der Notation meistens kurz x anstatt $[x]$ für die Restklasse von x modulo n, und sagen dann immer dazu, sobald x als Element von $\mathbb{Z}/n$ anzusehen ist. ([5])

Mit Konvention (8.7) gilt für $x, y \in \mathbb{Z}$ also $x = y$ in $\mathbb{Z}/n$ genau dann, wenn $x \equiv_n y$ in $\mathbb{Z}$.

(8.8) Beispiel. In $\mathbb{Z}/7$ ist $1 = 8$, $3 = 11$, $2 = 5$. Es gilt $5 + 4 = 9 = 2$, $3 \cdot 4 = 12 = 5$, $13 \cdot 13 = (-1) \cdot (-1) = 1$.

Die Bezeichnung Restklasse bzw. Restklassenring kommt daher, dass jedes Element in $\mathbb{Z}/n$ für $n \in \mathbb{N}$, also jede Restklasse modulo n, durch den Rest eines beliebigen Repräsentanten bei Division mit Rest durch n repräsentiert wird:

Bemerkung. Es sei $n \in \mathbb{N}$. Für alle $x \in \mathbb{Z}$ ist $x = x \bmod n$ in $\mathbb{Z}/n$.

Beweis. Dies folgt aus Bemerkung (8.4) und Proposition (6.9)(b). □

(8.9) Bemerkung. Für $n \in \mathbb{N}$ ist

$$\mathbb{Z}/n = \{0, \dots, n-1\}.$$

Beweis. Für $x \in \mathbb{Z}$ ist $x \bmod n \in \{0, \dots, n-1\}$, vgl. Erinnerung (8.3). □

Manchmal nennt man $\{0, \dots, n-1\}$, aufgefasst als Teilmenge von $\mathbb{Z}$, auch das *Standardrepräsentantensystem* für $\mathbb{Z}/n$.

Algebraische Struktur

Per Konstruktion ist $\mathbb{Z}/n$ für $n \in \mathbb{Z}$ ein kommutativer Ring. Es stellt sich die Frage, für welche $n \in \mathbb{Z}$ dieser kommutative Ring ein Körper ist.

(8.10) Satz. Für $n \in \mathbb{Z}$ ist $\mathbb{Z}/n$ genau dann ein Körper, wenn n eine Primzahl ist.

Beweis. Siehe Aufgabe 32(b). □

Aufgaben

Aufgabe 29 (Rechnen in $\mathbb{Z}/n$)**.**

(a) Berechnen Sie $17 + 23 + 40 - 8$ und $2 \cdot (-3) \cdot 15$ und $6^{1000000}$ in $\mathbb{Z}/7$.

(b) Berechnen Sie $(-8) + 13 - 2 + 5$ und $4 \cdot 3 \cdot 5$ und 9^{14} in $\mathbb{Z}/8$.

(c) Ist $3^{2016} = 3^{2012}$ in $\mathbb{Z}/80$?

Aufgabe 30 (Nullteiler in $\mathbb{Z}/n$)**.**

(a) Finden Sie $n \in \mathbb{N}$, $x, y \in \mathbb{Z}$ mit $x \neq 0$ und $y \neq 0$ in $\mathbb{Z}/n$, aber $xy = 0$ in $\mathbb{Z}/n$.

(b) Es seien $p, q \in \mathbb{N}$ mit $p > 1$ und $q > 1$. Zeigen Sie, dass $\mathbb{Z}/pq$ kein Körper ist. (Hinweis: Lemma (5.7).)

Aufgabe 31 (Inverse in $\mathbb{Z}/n$)**.**

(a) Bestimmen Sie die Inversen der invertierbaren Elemente in $\mathbb{Z}/11$.

(b) Es sei $a \in \mathbb{Z}$ so, dass a^2 in $\mathbb{Z}/12$ invertierbar ist. Ist dann auch a invertierbar?

Aufgabe 32 (Invertierbarkeit in $\mathbb{Z}/n$)**.** Es sei $n \in \mathbb{N}$.

(a) Es sei $x \in \mathbb{Z}$. Zeigen Sie, dass x genau dann invertierbar in $\mathbb{Z}/n$ ist, wenn $\gcd(x, n) = 1$ ist.
Hinweis: Sie dürfen ohne Beweis benutzen, dass es $a, b \in \mathbb{Z}$ gibt mit $\gcd(x, n) = ax + bn$.

(b) Zeigen Sie, dass $\mathbb{Z}/n$ genau dann ein Körper ist, wenn n eine Primzahl ist.

[5] Es ist üblich, in einem beliebigen Ring $2 := 1 + 1$, $3 := 2 + 1$, etc. zu definieren, wobei hier 1 das Einselement des Rings bezeichne. Da in $\mathbb{Z}/n$ jedoch $1 = 1^{\mathbb{Z}/n} = [1^{\mathbb{Z}}]$ ist, entspricht dies genau unserer Konvention.

A Addenda

In diesem Anhang erarbeiten wir noch einige Konzepte und Sätze, welche gut zu den Themen des Vorkurses gepasst hätten, auf welche jedoch aus Zeitgründen verzichtet werden musste.

Familien

Zunächst wollen wir noch einen anderen Blick auf Abbildungen werfen.

(A.1) Definition (Familie)**.** Es seien I und X Mengen. Eine *Familie* in X über I ist eine Teilmenge $x \subseteq I \times X$ so, dass es für alle $i \in I$ genau ein $y \in X$ mit $(i, y) \in x$ gibt. Die Menge I wird *Indexmenge* von x genannt, ihre Elemente heißen *Indizes* (oder *Stellen*) von x. Für $(i, y) \in x$ heißt y die *Komponente* von x an der Stelle i, wir schreiben $x_i := y$.
Für eine Familie x in X über I schreiben wir auch $(x_i)_{i \in I} := x$.
Die *Menge aller Familien in X über I* bezeichnen wir mit

$$X^I := \{x \mid x \text{ ist eine Familie in } X \text{ über } I\}.$$

Eine Familie in X über I ist also im Wesentlichen dasselbe wie eine Abbildung von I nach X; bei Abbildungen fassen wir lediglich noch Start- und Zielmenge als Bestandteile auf, bei Familien nicht.
Die folgende Bemerkung zeigt, dass Familien geordnete Paare verallgemeinern, vgl. Proposition (1.17).

(A.2) Bemerkung. Es seien I und X Mengen. Für $x, y \in X^I$ gilt $x = y$ genau dann, wenn $x_i = y_i$ für alle $i \in I$ ist.

Beweis. Dies folgt aus Bemerkung (2.3). □

Allgemeine Schnitte und Vereinigungen

In Definition (1.11)(a), (b) haben wir gesehen, wie wir den Schnitt von zwei Mengen bilden können. Nun wollen wir den Schnitt über Familien (von Mengen) und Mengen (von Mengen) definieren.

(A.3) Definition (Schnitt)**.**

(a) Es sei I eine nicht-leere Menge und X eine Familie über I so, dass X_i für jedes $i \in I$ eine Menge ist. Die Menge

$$\bigcap X = \bigcap_{i \in I} X_i := \{x \mid x \in X_i \text{ für alle } i \in I\}$$

heißt *Schnitt* (oder *Durchschnitt*) von X.

(b) Es sei $\mathcal{X}$ eine nicht-leere Menge so, dass jedes $X \in \mathcal{X}$ eine Menge ist. Die Menge

$$\bigcap \mathcal{X} := \bigcap_{X \in \mathcal{X}} X$$

heißt *Schnitt* (oder *Durchschnitt*) von $\mathcal{X}$.

In Definition (A.3)(b) haben wir für eine Menge $\mathcal{X}$ die Familie $(X)_{X \in \mathcal{X}}$ betrachtet, also die Familie $Y = (Y_X)_{X \in \mathcal{X}}$ mit $Y_X = X$ für alle $X \in \mathcal{X}$.

(A.4) Beispiel. Wir definieren eine Familie X in $\mathbb{Z}$ über $\mathbb{N}$ durch $X_d := \{n \in \mathbb{Z} \mid d \mid n\} = \{n \in \mathbb{Z} \mid d \text{ teilt } n\}$ für $d \in \mathbb{N}$. Dann ist $\bigcap X = \{0\}$.

Die folgende Bemerkung zeigt den Zusammenhang zwischen Definition (A.3)(a) und Definition (1.11)(a).

(A.5) Bemerkung. Für jede Familie X über $\{1, 2\}$ gilt $\bigcap X = X_1 \cap X_2$.

Der Begriff des Schnitts über Familien ist allgemeiner als der des Schnitts über Mengen, da in einer Familie Komponenten auch doppelt vorkommen dürfen. Hier ist der Zusammenhang:

(A.6) Bemerkung. Es sei I eine nicht-leere Menge und X eine Familie über I so, dass X_i für jedes $i \in I$ eine Menge ist. Dann gilt

$$\bigcap X = \bigcap \{X_i \mid i \in I\}.$$

Analog zum Schnitt können wir Vereinigungen von Familien und Mengen definieren:

(A.7) Definition (Vereinigung)**.**

(a) Es sei I eine Menge und X eine Familie über I so, dass X_i für jedes $i \in I$ eine Menge ist. Die Menge

$$\bigcup X = \bigcup_{i \in I} X_i := \{x \mid x \in X_i \text{ für ein } i \in I\}$$

heißt *Vereinigung* von X.

(b) Es sei $\mathcal{X}$ eine Menge so, dass jedes $X \in \mathcal{X}$ eine Menge ist. Die Menge

$$\bigcup \mathcal{X} := \bigcup_{X \in \mathcal{X}} X$$

heißt *Vereinigung* von $\mathcal{X}$.

(A.8) Beispiel. Wir definieren eine Familie X in $\mathbb{Z}$ über $\mathbb{N}$ durch $X_d := \{n \in \mathbb{Z} \mid d \mid n\} = \{n \in \mathbb{Z} \mid d \text{ teilt } n\}$ für $d \in \mathbb{N}$. Dann ist $\bigcup X = \mathbb{Z}$.

(A.9) Bemerkung. Für jede Familie X über $\{1, 2\}$ gilt $\bigcup X = X_1 \cup X_2$.

(A.10) Bemerkung. Es sei I eine nicht-leere Menge und X eine Familie über I so, dass X_i für jedes $i \in I$ eine Menge ist. Dann gilt

$$\bigcup X = \bigcup \{X_i \mid i \in I\}.$$

Allgemeine kartesische Produkte

Als nächstes verallgemeinern wir kartesische Produkte.

(A.11) Definition (kartesisches Produkt)**.**

(a) Es sei I eine Menge und X eine Familie über I so, dass X_i für jedes $i \in I$ eine Menge ist. Die Menge

$$\bigtimes X = \bigtimes_{i \in I} X_i := \{(x_i)_{i \in I} \mid x_i \in X_i \text{ für } i \in I\}$$

heißt *kartesisches Produkt* von X.

(b) Es sei $\mathcal{X}$ eine Menge so, dass jedes $X \in \mathcal{X}$ eine Menge ist. Die Menge

$$\bigtimes \mathcal{X} := \bigtimes_{X \in \mathcal{X}} X$$

heißt *kartesisches Produkt* von $\mathcal{X}$.

Die folgende Bemerkung zeigt den Zusammenhang zwischen Definition (A.11)(a) und Definition (1.18).

(A.12) Bemerkung. Es sei X eine Familie über $\{1, 2\}$. Wir haben zueinander inverse Abbildungen

$$X_1 \times X_2 \to \bigtimes X,\ (x_1, x_2) \mapsto (x_i)_{i \in \{1,2\}},$$
$$\bigtimes X \to X_1 \times X_2,\ x \mapsto (x_1, x_2),$$

eine Bijektion.

Wir können also im Folgenden annehmen, dass geordnete Paare immer Familien über $\{1,2\}$ sind, und verwenden hierfür die Schreibweisen aus Definition (1.16)(a) und Definition (1.18). Wir können außerdem allgemeinere *n-Tupel* als Familien über $\{1,\dots,n\}$ einführen und benötigen nicht die Rekursion aus Definition (1.16)(b), sowie die Schreibweise $X_1 \times \ldots \times X_n := \times_{i\in\{1,\dots,n\}} X_i$ für ein n-Tupel $X = (X_1,\dots,X_n)$. Den Begriff des geordneten Paares nach KURATOWSKI brauchen wir also nur, um allgemeinere Familien einführen zu können.

(A.13) Bemerkung. Es ist

$$X^I = \bigtimes_{i\in I} X.$$

Beweis. Wir haben

$$X^I := \{x \mid x \text{ ist eine Familie in } X \text{ über } I\} = \{(x_i)_{i\in I} \mid x_i \in X \text{ für } i \in I\} = \bigtimes_{i\in I} X. \qquad \square$$

In Bemerkung (A.13) haben wir für eine Menge X also die Familie $(X)_{i\in I}$ betrachtet, also die Familie $Y = (Y_i)_{i\in I}$ mit $Y_i = X$ für alle $i \in I$.

Disjunkte Vereinigungen

Wir wollen den Begriff der disjunkten Vereinigung einführen, d.h. Vereinigungen von Mengen, welche sich paarweise nicht schneiden.

(A.14) Definition (Disjunktheit)**.**

(a) Es sei I eine Menge und X eine Familie über I so, dass X_i für jedes $i \in I$ eine Menge ist. Wir sagen, dass X *disjunkt* ist, falls $X_i \cap X_j = \emptyset$ für alle $i,j \in I$ mit $i \neq j$ gilt.

(b) Es sei $\mathcal{X}$ eine Menge so, dass jedes $X \in \mathcal{X}$ eine Menge ist. Wir sagen, dass $\mathcal{X}$ *disjunkt* ist, falls $(X)_{X\in\mathcal{X}}$ disjunkt ist.

(A.15) Definition (disjunkte Vereinigung)**.**

(a) Es sei I eine Menge und X eine Familie über I so, dass X_i für jedes $i \in I$ eine Menge ist. Falls X disjunkt ist, so sagen wir, dass $\bigcup X$ eine *disjunkte Vereinigung* von X ist, und schreiben

$$\dot{\bigcup} X = \dot{\bigcup_{i\in I}} X_i := \bigcup X.$$

(b) Es sei $\mathcal{X}$ eine Menge so, dass jedes $X \in \mathcal{X}$ eine Menge ist. Falls $\mathcal{X}$ disjunkt ist, so sagen wir, dass $\bigcup \mathcal{X}$ eine *disjunkte Vereinigung* von $\mathcal{X}$ ist, und schreiben

$$\dot{\bigcup} \mathcal{X} := \bigcup \mathcal{X}.$$

Wir können Vereinigungen auch künstlich disjunkt machen (vgl. Aufgabe 33(b)):

(A.16) Definition (disjunkte Vereinigung)**.**

(a) Es sei I eine Menge und X eine Familie über I so, dass X_i für jedes $i \in I$ eine Menge ist. Die Menge

$$\bigsqcup X = \bigsqcup_{i\in I} X_i := \dot{\bigcup_{i\in I}} X_i^{\{i\}}$$

heißt (*äußere*) *disjunkte Vereinigung* von X.

(b) Es sei $\mathcal{X}$ eine Menge so, dass jedes $X \in \mathcal{X}$ eine Menge ist. Die Menge

$$\bigsqcup \mathcal{X} := \bigsqcup_{X\in\mathcal{X}} X$$

heißt (*äußere*) *disjunkte Vereinigung* von $\mathcal{X}$.

Restriktion von Abbidungen

In diesem Abschnitt werden wir kurz aufzeigen, dass Teilmengen Anlass zu Abbildungen geben.

(A.17) Bemerkung. Es sei $f\colon X \to Y$ eine Abbildung.

(a) Für alle Teilmengen U, U' von X mit $U \subseteq U'$ gilt $f(U) \subseteq f(U')$.

(b) Für alle Teilmengen V, V' von Y mit $V \subseteq V'$ gilt $f^{-1}(V) \subseteq f^{-1}(V')$.

Beweis.

(a) Es seien Teilmengen U, U' von X mit $U \subseteq U'$ gegeben. Ferner sei ein $v \in f(U)$ gegeben. Dann ist $v = f(u)$ für ein $u \in U$. Da aber $U \subseteq U'$, ist insbesondere $u \in U'$ und also $v = f(u) \in f(U')$. Folglich ist $f(U) \subseteq f(U')$.

(b) Es seien Teilmengen V, V' von Y mit $V \subseteq V'$ gegeben. Ferner sei ein $u \in f^{-1}(V)$ gegeben. Dann ist $f(u) \in V$, wegen $V \subseteq V'$ also auch $f(u) \in V'$ und damit $u \in f^{-1}(V')$. Folglich ist $f^{-1}(V) \subseteq f^{-1}(V')$. □

(A.18) Definition (Restriktion)**.** Es sei $f\colon X \to Y$ eine Abbildung. Für $U \subseteq X$ und $V \subseteq Y$ mit $f(U) \subseteq V$ heißt

$$f|_U^V\colon U \to V,\ u \mapsto f(u)$$

die *Restriktion* (oder *Einschränkung*) von f bzgl. U und V.
Für $U \subseteq X$ setzen wir

$$f|_U := f|_U^Y.$$

Für $V \subseteq Y$ mit $\operatorname{Im} f \subseteq V$ setzen wir

$$f|^V := f|_X^V.$$

(A.19) Bemerkung. Für jede Abbildung $f\colon X \to Y$ ist

$$f|_X^Y = f|_X = f|^Y = f.$$

(A.20) Proposition. Es seien Abbildungen $f\colon X \to Y$ und $g\colon Y \to Z$ gegeben.

(a) Für $U \subseteq X$, $V \subseteq Y$, $W \subseteq Z$ mit $f(U) \subseteq V$ und $g(V) \subseteq W$ gilt $(g \circ f)(U) \subseteq W$ und

$$(g \circ f)|_U^W = g|_V^W \circ f|_U^V.$$

(b) Für $U \subseteq X$, $V \subseteq Y$ mit $f(U) \subseteq V$ gilt

$$(g \circ f)|_U = g|_V \circ f|_U^V.$$

(c) Für $U \subseteq X$ gilt

$$(g \circ f)|_U = g \circ f|_U.$$

(d) Für $V \subseteq Y$, $W \subseteq Z$ mit $\operatorname{Im} f \subseteq V$ und $g(V) \subseteq W$ gilt

$$(g \circ f)|^W = g|_V^W \circ f|^V.$$

(e) Für $W \subseteq Z$ mit $\operatorname{Im} g \subseteq W$ gilt

$$(g \circ f)|^W = g|^W.$$

Beweis.

(a) Da $f(U) \subseteq V$ ist $g(f(U)) \subseteq g(V)$ nach Bemerkung (A.17)(a), und da $g(V) \subseteq W$ folgt schließlich

$$(g \circ f)(U) = g(f(U)) \subseteq g(V) \subseteq W.$$

Für alle $u \in U$ gilt aber

$$(g \circ f)|_U^W(u) = (g \circ f)(u) = g(f(u)) = g|_V^W(f|_U^V(u)) = (g|_V^W \circ f|_U^V)(u),$$

es ist also $(g \circ f)|_U^W = g|_V^W \circ f|_U^V$.

(b) Da $g(V) \subseteq Z$ ist

$$(g \circ f)|_U = (g \circ f)|_U^Z = g|_V^Z \circ f|_U^V = g|_V \circ f|_U^V$$

nach (a).

(c) Da $f(U) \subseteq Y$ ist

$$(g \circ f)|_U = g|_Y \circ f|_U^Y = g \circ f|_U$$

nach (b).

(d) Da $f(X) = \operatorname{Im} f \subseteq V$ ist

$$(g \circ f)|^W = (g \circ f)|_X^W = g|_V^W \circ f|_X^V = g|_V^W \circ f|^V$$

nach (a).

(e) Da $\operatorname{Im} f \subseteq Y$ und $g(Y) = \operatorname{Im} f \subseteq W$ ist

$$(g \circ f)|^W = g|_Y^W \circ f|^Y = g|^W \circ f$$

nach (d). □

(A.21) Bemerkung. Es sei $f\colon X \to Y$ eine Abbildung. Für $U \subseteq X$ ist $f(U) = \operatorname{Im}(f|_U)$.

Beweis. Für $U \subseteq X$ ist

$$f(U) = \{f(u) \mid u \in U\} = \{f|_U(u) \mid u \in U\} = \operatorname{Im}(f|_U).$$ □

(A.22) Definition (Inklusion)**.** Es sei X eine Menge und $U \subseteq X$. Die Abbildung $\operatorname{inc} = \operatorname{inc}^U := \operatorname{id}_X|_U\colon U \to X$ heißt *Inklusion* (oder *Inklusionsabbildung*) von U in X.

(A.23) Bemerkung. Es sei eine Abbildung $f\colon X \to Y$ und Teilmengen $U \subseteq X$ und $V \subseteq Y$ mit $f(U) \subseteq V$ gegeben. Dann gilt

$$\operatorname{inc}^V \circ f|_U^V = f \circ \operatorname{inc}^U.$$

Beweis. Nach Proposition (A.20)(b), (c) und Bemerkung (2.9) ist

$$\operatorname{inc}^V \circ f|_U^V = \operatorname{id}_Y|_V \circ f|_U^V = (\operatorname{id}_Y \circ f)|_U = (f \circ \operatorname{id}_X)|_U = f \circ \operatorname{id}_X|_U = f \circ \operatorname{inc}^U.$$ □

Redundanz der Gruppenaxiome

Wir wollen zeigen, dass die Axiome einiger algebraischer Strukturen, welche wir in Abschnitt 4 betrachtet haben, etwas redundant sind (und damit auch diejenigen aus Abschnitt 5). Hierzu müssen wir die Begriffe „neutrales Element“ und „inverses Element“ bzgl. einer gegebenen Verknüpfung etwas verallgemeinern; vgl. auch Aufgabe 14.

(A.24) Definition (links-/rechtsneutrales Element)**.** Es sei X eine Menge und m eine Verknüpfung auf X.

(a) Ein *linksneutrales Element* bzgl. m ist ein Element $e \in X$, welches $m(e, x) = x$ für alle $x \in X$ erfüllt.

(b) Ein *rechtsneutrales Element* bzgl. m ist ein Element $e \in X$, welches $m(x, e) = x$ für alle $x \in X$ erfüllt.

(A.25) Bemerkung. Es sei X eine Menge und m eine Verknüpfung auf X. Ein Element $e \in X$ ist neutral bzgl. m genau dann, wenn es links- und rechtsneutral bzgl. m ist.

(A.26) Bemerkung. Es sei A eine Menge und a eine assoziative und kommutative Verknüpfung auf A.

(a) Wenn es ein linksneutrales Element e bzgl. a gibt, dann wird A zu einem abelschen Monoid mit Addition $+^A = a$.

(b) Wenn es ein rechtsneutrales Element e bzgl. a gibt, dann wird A zu einem abelschen Monoid mit Addition $+^A = a$.

Beweis.

(a) Es sei $e \in A$ ein linksneutrales Element bzgl. a. Dann gilt $a(e, x) = x$ für alle $x \in A$. Da aber a kommutativ ist, gilt folglich auch $a(x, e) = a(e, x) = x$ für alle $x \in A$, d.h. e ist auch rechtsneutrales Element und damit neutrales Element bzgl. a. Somit wird A zu einem abelschen Monoid mit Addition a.

(b) Dies lässt sich analog zu (a) beweisen. □

(A.27) Definition (links-/rechtsinverse Elemente)**.** Es sei X eine Menge und m eine Verknüpfung auf X. Ferner seien $e, x \in X$ gegeben.

(a) Ein *linksinverses Element* zu x bzgl. m und e ist ein Element $y \in X$, welches $m(y, x) = e$ erfüllt. Ist e ein neutrales Element bzgl. m, so nennen wir ein linksinverses Element zu x bzgl. m und e auch einfach ein *linksinverses Element* zu x bzgl. m.

(b) Ein *rechtsinverses Element* zu x bzgl. m und e ist ein Element $y \in X$, welches $m(x, y) = e$ erfüllt. Ist e ein neutrales Element bzgl. m, so nennen wir ein rechtsinverses Element zu x bzgl. m und e auch einfach ein *rechtsinverses Element* zu x bzgl. m.

(A.28) Bemerkung. Es sei X eine Menge, m eine Verknüpfung auf X und e ein neutrales Element bzgl. m. Ferner sei ein $x \in X$ gegeben. Ein Element $y \in X$ ist ein inverses Element zu x bzgl. m genau dann, wenn es links- und rechtsinvers zu x bzgl. m ist.

Im folgenden Lemma werden wir sehen, dass die Gruppenaxiome auch im nicht-kommutativen Fall redundant sind.

(A.29) Lemma. Es sei G eine Menge und m eine assoziative Verknüpfung auf G.

(a) Wenn es ein linksneutrales Element e bzgl. m und für alle $x \in G$ ein linksinverses Element bzgl. m und e gibt, dann wird G zu einer Gruppe mit Multiplikation $\cdot^G = m$.

(b) Wenn es ein rechtsneutrales Element e bzgl. m und für alle $x \in G$ ein rechtsinverses Element bzgl. m und e gibt, dann wird G zu einer Gruppe mit Multiplikation $\cdot^G = m$.

Beweis.

(a) Es sei $e \in G$ ein linksneutrales Element in G bzgl. m und es sei $x \in G$ ein beliebiges Element. Ferner sei $y \in G$ ein linksinverses Element zu x bzgl. m und e und es sei $z \in G$ ein linksinverses Element zu y bzgl. m und e. Dann gilt $m(e, x) = x$, $m(e, y) = y$, $m(y, x) = e$ und $m(z, y) = e$ und es folgt

$$\begin{aligned} m(x, y) &= m(m(e, x), y) = m(m(m(z, y), x), y) = m(m(z, m(y, x)), y) = m(m(z, e), y) \\ &= m(z, m(e, y)) = m(z, y) = e, \end{aligned}$$

d.h. y ist auch ein rechtsinverses Element von x bzgl. m und e. Außerdem gilt

$$m(x, e) = m(x, m(y, x)) = m(m(x, y), x) = m(e, x) = x$$

und da $x \in G$ beliebig gewählt war, ist e somit auch ein rechtsneutrales Element in G bzgl. m. Folglich ist e ein neutrales Element bzgl. m und zu jedem Element $x \in G$ existiert ein inverses Element bzgl. m, d.h. es wird G zu einer Gruppe mit Multiplikation m.

(b) Dies lässt sich analog zu (a) beweisen. □

(A.30) Korollar. Es sei A eine Menge und a eine assoziative und kommutative Verknüpfung auf A.

(a) Wenn es ein linksneutrales Element e bzgl. a und für alle $x \in A$ ein linksinverses Element bzgl. a und e gibt, dann wird A zu einer abelschen Gruppe mit Addition $+^A = a$.

(b) Wenn es ein rechtsneutrales Element e bzgl. a und für alle $x \in A$ ein rechtsinverses Element bzgl. a und e gibt, dann wird A zu einer abelschen Gruppe mit Addition $+^A = a$.

Universelle Eigenschaft der Quotientenmenge

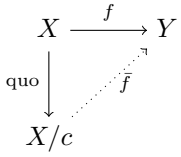
Wir wollen zeigen, dass für eine gegebene Äquivalenzrelation c auf einer Menge X gewisse Abbildungen über den Quotienten X/c faktorisieren.

(A.31) Proposition. Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben.

(a) Für jede Menge Y und jede Abbildung $f\colon X \to Y$ mit $f(x) = f(\tilde{x})$ für alle $x, \tilde{x} \in X$ mit $x\ c\ \tilde{x}$ existiert genau eine Abbildung $\bar{f}\colon X/c \to Y$ mit $f = \bar{f} \circ \mathrm{quo}$, gegeben durch

$$\bar{f}([x]_c) = f(x)$$

für $x \in X$.



(b) Es sei $f\colon X \to Y$ eine Abbildung mit $f(x) = f(\tilde{x})$ für alle $x, \tilde{x} \in X$ mit $x\ c\ \tilde{x}$ und es sei $\bar{f}\colon X/c \to Y$ die eindeutige Abbildung mit $f = \bar{f} \circ \mathrm{quo}$. Dann ist $\mathrm{Im}\,\bar{f} = \mathrm{Im}\,f$.

Beweis.

(a) Es seien eine Menge Y und eine Abbildung $f\colon X \to Y$ mit $f(x) = f(\tilde{x})$ für alle $x, \tilde{x} \in X$ mit $x\ c\ \tilde{x}$ gegeben. Für $x, x' \in X$ mit $[x]_c = [x']_c$ gilt $x\ c\ x'$ nach Proposition (6.9)(b) und somit $f(x) = f(x')$. Folglich haben wir eine wohldefinierte Abbildung $\bar{f}\colon X/c \to Y$, $[x] \mapsto f(x)$. Wegen

$$f(x) = \bar{f}([x]_c) = \bar{f}(\mathrm{quo}(x))$$

für $x \in X$ gilt $f = \bar{f} \circ \mathrm{quo}$.

Ist umgekehrt $g\colon X/c \to Y$ eine beliebige Abbildung mit $f = g \circ \mathrm{quo}$, so folgt notwendigerweise

$$g([x]_c) = g(\mathrm{quo}(x)) = f(x)$$

für $x \in X$.

Insgesamt gibt es also genau eine Abbildung $\bar{f}\colon X/c \to Y$ mit $f = \bar{f} \circ \mathrm{quo}$.

(b) Nach Proposition (6.11)(a) haben wir

$$\mathrm{Im}\,\bar{f} = \{\bar{f}(z) \mid z \in X/c\} = \{\bar{f}(\mathrm{quo}(x)) \mid x \in X\} = \{f(x) \mid x \in X\} = \mathrm{Im}\,f. \qquad \square$$

(A.32) Korollar. Es sei X eine Menge und c eine Äquivalenzrelation auf X. Dann ist

$$\mathrm{Map}(X/c, Y) \to \{f \in \mathrm{Map}(X, Y) \mid f(x) = f(\tilde{x}) \text{ für alle } x, \tilde{x} \in X \text{ mit } x\ c\ \tilde{x}\},\ g \mapsto g \circ \mathrm{quo}$$

eine wohldefinierte Bijektion.

Beweis. Es sei

$$M := \{f \in \mathrm{Map}(X, Y) \mid f(x) = f(\tilde{x}) \text{ für alle } x, \tilde{x} \in X \text{ mit } x\ c\ \tilde{x}\}.$$

Für alle Abbildungen $g\colon X/c \to Y$ ist $g(\mathrm{quo}(x)) = g(\mathrm{quo}(\tilde{x}))$ für alle $x, \tilde{x} \in X$ mit $x\ c\ \tilde{x}$ nach Proposition (6.11)(b), d.h. es ist $g \circ \mathrm{quo} \in M$. Folglich erhalten wir eine wohldefinierte Abbildung

$$\Phi\colon \mathrm{Map}(X/c, Y) \to M,\ g \mapsto g \circ \mathrm{quo}.$$

Nach Proposition (A.31)(a) gibt es für jedes $f \in M$ genau ein $\bar{f} \in \mathrm{Map}(X/c, Y)$ mit $f = \bar{f} \circ \mathrm{quo}$, d.h. Φ ist eine Bijektion. $\square$

Der Homomorphiesatz für Mengen

In Proposition (A.31) sind wir von einer Menge X und einer Äquivalenzrelation c auf X ausgegangen und haben Aussagen über gewisse Abbildungen $X \to Y$ getroffen. Nun beschreiten wir den umgekehrten Weg, d.h. wir zeigen, dass jede Abbildung $f\colon X \to Y$ Anlass zu einer Äquivalenzrelation gibt.

(A.33) Definition (Bildgleichheit)**.** Es sei $f\colon X \to Y$ eine Abbildung. Für $x, \tilde{x} \in X$ gelte $x =_f \tilde{x}$ genau dann, wenn $f(x) = f(\tilde{x})$ ist. Die Relation $=_f$ heißt *Bildgleichheit* bzgl. f.

(A.34) Bemerkung. Für jede Abbildung $f\colon X \to Y$ ist $=_f$ eine Äquivalenzrelation auf X.

Beweis. Dies folgt aus Aufgabe 27(a) und Beispiel (6.6)(c). □

Die folgende Bemerkung besagt insbesondere, dass sich jede Äquivalenzrelation als Bildgleichheit bzgl. einer geeigneten Abbildung realisieren lassen.

(A.35) Bemerkung. Es sei X eine Menge. Für jede Äquivalenzrelation c auf X gilt

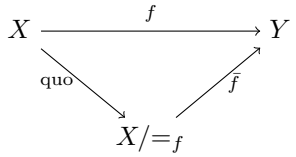
$$c = =_{\mathrm{quo}^{X/c}}.$$

Beweis. Es sei c eine Äquivalenzrelation auf X und es seien $x, x' \in X$ gegeben. Genau dann gilt $x =_{\mathrm{quo}^{X/c}} x'$, wenn $\mathrm{quo}^{X/c}(x) = \mathrm{quo}^{X/c}(x')$ ist, und letzteres ist äquivalent zu $x\, c\, x'$ nach Proposition (6.11)(b). □

(A.36) Satz (Homomorphiesatz für Mengen)**.** Es sei $f\colon X \to Y$ eine Abbildung. Dann haben wir eine induzierte Abbildung $\bar{f}\colon X/{=_f} \to Y$, $\mathrm{quo}(x) \mapsto f(x)$, welche $f = \bar{f} \circ \mathrm{quo}$ erfüllt. Es ist $\bar{f}$ injektiv und $\operatorname{Im} \bar{f} = \operatorname{Im} f$. Insbesondere ist

$$\bar{f}|^{\operatorname{Im} f}\colon X/{=_f} \to \operatorname{Im} f$$

eine Bijektion.



Beweis. Für $x, x' \in X$ gilt $x =_f x'$ nach Definition von $=_f$ genau dann, wenn $f(x) = f(x')$ ist. Nach Proposition (A.31)(a) ist also $\bar{f}\colon X/{=_f} \to Y$, $\mathrm{quo}(x) \mapsto f(x)$ eine wohldefinierte Abbildung mit $f = \bar{f} \circ \mathrm{quo}$. Ferner ist $\operatorname{Im} \bar{f} = \operatorname{Im} f$ nach Proposition (A.31)(b).
Um zu zeigen, dass $\bar{f}$ injektiv ist, seien $x, x' \in X$ mit $\bar{f}(\mathrm{quo}(x)) = \bar{f}(\mathrm{quo}(x'))$ in Y gegeben. Wegen $f = \bar{f} \circ \mathrm{quo}$ haben wir also $f(x) = f(x')$, was aber äquivalent zu $x =_f x'$ ist. Nach Proposition (6.11)(b) ist dies aber wiederum äquivalent zu $\mathrm{quo}(x) = \mathrm{quo}(x')$. Also ist $\bar{f}$ in der Tat injektiv. □

(A.37) Korollar. Für jede Abbildung $f\colon X \to Y$ existiert eine Surjektion p und eine Injektion i mit

$$f = i \circ p.$$

Beweis. Dies folgt aus Satz (A.36) und Korollar (6.12). □

Der Hauptsatz über Äquivalenzrelationen

In diesem Abschnitt wollen wir den mengentheoretischen Aspekt von Quotientenmengen etwas genauer beleuchten: Jede Äquivalenzrelation c auf einer Menge X partitioniert (also unterteilt) via X/c die Menge X in Teilmengen, nämlich in die Elemente von X/c. Gehen wir umgekehrt von einer Unterteilung von X in Teilmengen aus, so liefert uns dies wiederum eine Äquivalenzrelation, indem wir zwei Elemente als äquivalent betrachten, wenn sie im gleichen Teil der Unterteilung liegen. Der Hauptsatz über Äquivalenzrelationen (A.39) besagt, dass sich diese Konstruktionen gegenseitig umkehren.
Zunächst präzisieren wir den Begriff der Unterteilung einer Menge:

(A.38) Definition (Partition)**.** Es sei X eine Menge. Eine *Partition* von X ist eine Teilmenge $\mathcal{P}$ von $\mathrm{Pot}(X)$ so, dass $\emptyset \notin \mathcal{P}$ und

$$X = \dot{\bigcup} \mathcal{P}.$$

Für $x \in X$ heißt das eindeutige $P \in \mathcal{P}$ mit $x \in P$ der *Teil* von x in X bzgl. $\mathcal{P}$; wir schreiben $[x] = [x]_{\mathcal{P}} := P$.

(A.39) Satz (Hauptsatz über Äquivalenzrelationen)**.** Es sei X eine Menge. Wir haben zueinander inverse Abbildungen

$$X/{-}\colon \{c \mid c \text{ ist Äquivalenzrelation auf } X\} \to \{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } X\},\ c \mapsto X/c,$$
$$=_{q_-}\colon \{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } X\} \to \{c \mid c \text{ ist Äquivalenzrelation auf } X\},\ \mathcal{P} \mapsto =_{q_{\mathcal{P}}},$$

wobei für eine Partition $\mathcal{P}$ von X die Abbildung $q_{\mathcal{P}}\colon X \to \mathcal{P}$ gegeben sei durch $q_{\mathcal{P}}(x) = [x]_{\mathcal{P}}$.

Beweis. Es sei zunächst eine Äquivalenzrelation c gegeben. Dann haben wir $X/c = \{[x]_c \mid x \in X\}$. Für alle $K \in X/c$ gibt es also ein $x \in X$ mit $K = [x]_c$, und nach Proposition (6.9)(a) schließen wir, dass $x \in [x]_c = K$. Insbesondere ist $K \neq \emptyset$ für alle $K \in X/c$ und damit $\emptyset \notin X/c$. Da ferner

$$x \in [x]_c \subseteq \bigcup_{y \in X} [y]_c = \bigcup \{[y]_c \mid y \in X\} = \bigcup X/c$$

für $x \in X$ gilt, haben wir folglich

$$X = \bigcup X/c.$$

Um die Disjunktheit dieser Vereinigung zu zeigen, seien $K, L \in \bigcup X/c$ mit $K \cap L \neq \emptyset$ gegeben. Ferner seien $x, y, z \in X$ mit $K = [x]_c$, $L = [y]_c$ und $z \in K \cap L$ gegeben. Da $z \in K = [x]_c$ folgt $z\ c\ x$, und da $z \in L = [y]_c$ folgt $z\ c\ y$. Nun ist aber c nach Aufgabe 37 euklidisch, wir erhalten also $x\ c\ y$ und somit $K = [x]_c = [y]_c = L$ nach Proposition (6.9)(b).
Wir haben also gezeigt, dass X/c für jede Äquivalenzrelation c auf X eine Partition von X ist, mit $[x]_{X/c} = [x]_c$ für alle $x \in X$. Folglich haben wir eine wohldefinierte Abbildung

$$X/{-}\colon \{c \mid c \text{ ist Äquivalenzrelation auf } X\} \to \{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } X\},\ c \mapsto X/c.$$

Umgekehrt ist für jede Partition $\mathcal{P}$ von X die Bildgleichheit $=_{q_{\mathcal{P}}}$ von $q_{\mathcal{P}}\colon X \to \mathcal{P}$, $x \mapsto [x]_{\mathcal{P}}$ eine Äquivalenzrelation nach Bemerkung (A.34). Folglich haben wir auch eine wohldefinierte Abbildung

$$=_{q_-}\colon \{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } X\} \to \{c \mid c \text{ ist Äquivalenzrelation auf } X\},\ \mathcal{P} \mapsto =_{q_{\mathcal{P}}}.$$

Es bleibt zu zeigen, dass sich $X/{-}$ and $=_{q_-}$ gegenseitig invertieren. Ist eine Partition $\mathcal{P}$ von X gegeben, so haben wir

$$\begin{aligned}[x]_{=_{q_{\mathcal{P}}}} &= \{y \in X \mid y =_{q_{\mathcal{P}}} x\} = \{y \in X \mid q_{\mathcal{P}}(y) = q_{\mathcal{P}}(x)\} = \{y \in X \mid [y]_{\mathcal{P}} = [x]_{\mathcal{P}}\} = \{y \in X \mid y \in [x]_{\mathcal{P}}\} \\ &= [x]_{\mathcal{P}}\end{aligned}$$

für $x \in X$. Somit gilt

$$X/{=_{q_{\mathcal{P}}}} = \{[x]_{=_{q_{\mathcal{P}}}} \mid x \in X\} = \{[x]_{\mathcal{P}} \mid x \in X\} = \mathcal{P}$$

für alle Partitionen $\mathcal{P}$ von X, d.h. es ist $X/{-} \circ =_{q_-} = \mathrm{id}_{\{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } X\}}$. Nach Proposition (6.9)(b) gilt umgekehrt

$$\begin{aligned}=_{q_{X/c}} &= \{(x, y) \mid q_{X/c}(x) = q_{X/c}(y)\} = \{(x, y) \mid [x]_{X/c} = [y]_{X/c}\} = \{(x, y) \mid [x]_c = [y]_c\} = \{(x, y) \mid x\ c\ y\} \\ &= c\end{aligned}$$

für jede Äquivalenzrelation c auf X, d.h. es ist $=_{q_-} \circ X/{-} = \mathrm{id}_{\{c \mid c \text{ ist Äquivalenzrelation auf } X\}}$. Insgesamt sind $X/{-}$ und $=_{q_-}$ zueinander inverse Abbildungen. □

Aufgaben

Aufgabe 33 (Projektionen, Einbettungen)**.** Es sei I eine Menge und X eine Familie über I so, dass X_i für jedes $i \in I$ eine Menge ist.

(a) Für $i \in I$ heißt $\mathrm{pr}_i \colon \times X \to X_i$, $(x_i)_{i\in I} \mapsto x_i$ die *Projektion* an die Stelle i von $\times X$. Zeigen Sie:

(i) Für $x \in \times X$ gilt $x = (\mathrm{pr}_i(x))_{i\in I}$.

(ii) Für $x, y \in \times X$ ist $x = y$ genau dann, wenn $\mathrm{pr}_i(x) = \mathrm{pr}_i(y)$ für alle $i \in I$ ist.

(iii) Für jede Menge Y und jede Familie $(f_i)_{i\in I}$ so, dass f_i für jedes $i \in I$ eine Abbildung $f_i \colon Y \to X_i$ ist, gibt es genau eine Abbildung $f \colon Y \to \times X$ mit $f_i = \mathrm{pr}_i \circ f$ für alle $i \in I$.

(b) Für $i \in I$ sei $\mathrm{emb}_i \colon X_i \to \bigsqcup X$ definiert wie folgt: Für $x \in X_i$ sei $\mathrm{emb}_i(x) \in X_i^{\{i\}}$ diejenige Familie mit $(\mathrm{emb}_i(x))_i = x$. Für $i \in I$ heißt emb_i die *Einbettung* an die Stelle i von $\bigsqcup X$. Zeigen Sie:

(i) Es ist $\bigsqcup X = \{\mathrm{emb}_i(x) \mid x \in X_i,\ i \in I\}$.

(ii) Für $i, j \in I$, $x \in X_i$, $y \in X_j$ gilt $\mathrm{emb}_i(x) = \mathrm{emb}_j(y)$ genau dann, wenn $i = j$ und $x = y$ ist.

(iii) Für jede Menge Y und jede Familie $(f_i)_{i\in I}$ so, dass f_i für jedes $i \in I$ eine Abbildung $f_i \colon X_i \to Y$ ist, gibt es genau eine Abbildung $f \colon \bigsqcup X \to Y$ mit $f_i = f \circ \mathrm{emb}_i$ für alle $i \in I$.

Aufgabe 34 (kartesisches Produkt, disjunkte Vereinigung)**.** Es sei I eine Menge und X eine Familie über I so, dass X_i für jedes $i \in I$ eine Menge ist. Zeigen Sie, dass im Allgemeinen $\times X \neq \times \{X_i \mid i \in I\}$ und $\bigsqcup X \neq \bigsqcup \{X_i \mid i \in I\}$ ist.

Aufgabe 35 (Bild, Urbild)**.** Es sei $f \colon X \to Y$ eine Abbildung. Zeigen Sie:

(a) Für alle $U \subseteq X$ gilt $U \subseteq f^{-1}(f(U))$.

(b) Für alle $V \subseteq Y$ gilt $f(f^{-1}(V)) \subseteq V$.

(c) Für alle $U \subseteq X$ gilt $f(U) = f(f^{-1}(f(U)))$.

(d) Für alle $V \subseteq Y$ gilt $f^{-1}(f(f^{-1}(V))) = f^{-1}(V)$.

Aufgabe 36 (direktes Produkt)**.** Es seien Gruppen G_1 und G_2 gegeben. Zeigen Sie, dass $G_1 \times G_2$ zu einer Gruppe mit Multiplikation $((x_1, x_2), (y_1, y_2)) \mapsto (x_1 y_1, x_2 y_2)$ wird. Zeigen Sie weiter, dass $G_1 \times G_2$ kommutativ ist, falls G_1 und G_2 kommutativ sind.

Aufgabe 37 (Äquivalenzrelationen)**.** Es sei X eine Menge und r eine Relation auf X. Wir sagen, dass r *euklidisch* ist, falls für $x, x', x'' \in X$ aus $x\ r\ x''$ und $x'\ r\ x''$ stets $x\ r\ x'$ folgt. Zeigen Sie: Genau dann ist r eine Äquivalenzrelation auf X, wenn r reflexiv und euklidisch ist.

Aufgabe 38 (Ordnungsrelationen und Injektivität)**.** Es sei $f \colon X \to Y$ eine Abbildung, es sei o eine Ordnungsrelation auf X und es sei p eine Ordnungsrelation auf Y. Zeigen Sie: Wenn für $x, x' \in X$ aus $f(x)\ p\ f(x')$ stets $x\ o\ x'$ folgt, dann ist f injektiv.

Aufgabe 39 (Homomorphiesatz für Mengen anschaulich)**.** Es sei B die Menge aller Briefe, die an einem Tag bei der Aachener Post abgegeben werden, und es sei A die Menge aller Städte und Dörfer auf der Erde. Weiter sei $z \colon B \to A$ diejenige Abbildung, welche jedem Brief $b \in B$ seinen Zielort $z(b) \in A$ zuordnet. Wie profitiert die Post vom Homomorphiesatz?

Aufgabe 40 (Homomorphiesatz für Mengen)**.** Es sei $f \colon \mathbb{Z}/8 \to \mathbb{Z}/8$, $x \mapsto x^2$. Bestimmen Sie $(\mathbb{Z}/8)/{=_f}$ sowie die Quotientenabbildung $\mathrm{quo} \colon \mathbb{Z}/8 \to (\mathbb{Z}/8)/{=_f}$ und die eindeutige Abbildung $\bar{f} \colon (\mathbb{Z}/8)/{=_f} \to \mathbb{Z}/8$ mit $f = \bar{f} \circ \mathrm{quo}$.

Aufgabe 41 (ganze und rationale Zahlen)**.**

(a) Für $(m, s), (n, t) \in \mathbb{N}_0 \times \mathbb{N}_0$ gelte $(m, s) \equiv (n, t)$ genau dann, wenn $m + t = n + s$ ist. Zeigen Sie:

(i) Zeigen Sie, dass $\equiv$ eine Äquivalenzrelation auf $\mathbb{N}_0 \times \mathbb{N}_0$ ist und dass $(\mathbb{N}_0 \times \mathbb{N}_0)/{\equiv} \to \mathbb{Z}$, $[(m, s)] \mapsto m - s$ eine wohldefinierte Bijektion ist.

Hinweis: Homomorphiesatz für Mengen.

(ii) Definieren Sie eine Verknüpfung a auf $(\mathbb{N}_0 \times \mathbb{N}_0)/\equiv$ so, dass $(\mathbb{N}_0 \times \mathbb{N}_0)/\equiv$ eine abelsche Gruppe mit Addition a wird und so, dass es eine injektive Abbildung $l\colon \mathbb{N}_0 \to (\mathbb{N}_0 \times \mathbb{N}_0)/\equiv$ mit $l(m+n) = a(l(m), l(n))$ für alle $m, n \in \mathbb{N}_0$ gibt.

(b) Finden Sie eine Äquivalenzrelation auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ so, dass es eine Bijektion von der zugehörigen Quotientenmenge zu $\mathbb{Q}$ gibt.

Sebastian Thomas
Lehrstuhl D für Mathematik
RWTH Aachen University
Templergraben 64
52062 Aachen
Germany
sebastian.thomas@math.rwth-aachen.de
http://www.math.rwth-aachen.de/~Sebastian.Thomas/