MENGEN UND VERKNÜPFUNGEN

Wolfgang Soergel

25. April 2024

Inhaltsverzeichnis

1 Naive Mengenlehre und Kombinatorik

1.1 Mengen

1.1.1. Beim Arbeiten mit reellen Zahlen oder räumlichen Gebilden reicht auf der Schule ein intuitives Verständnis meist aus, und wenn die Intuition in die Irre führt, ist ein Lehrer zur Stelle. Wenn Sie jedoch selbst unterrichten oder etwas beweisen wollen, reicht dieses intuitive Verständnis nicht mehr aus. Im folgenden werden deshalb zunächst der Begriff der reellen Zahlen und der Begriff des Raums zurückgeführt auf Grundbegriffe der Mengenlehre, den Begriff der rationalen Zahlen und elementare Logik. Bei der Arbeit mit diesen Begriffen führt uns die Intuition nicht so leicht in die Irre, wir geben uns deshalb mit einem intuitiven Verständnis zufrieden und verweisen jeden, der es noch genauer wissen will, auf eine Vorlesung über Logik. Wir beginnen mit etwas naiver Mengenlehre, wie sie von Georg Cantor in den Jahren 1874 bis 1897 begründet wurde und von der der berühmte Mathematiker David Hilbert einmal sagte: „Aus dem Paradies, das Cantor uns geschaffen, soll uns niemand vertreiben können“. Natürlich gab es auch vor der Mengenlehre schon hoch entwickelte Mathematik: Beim Tod von Carl Friedrich Gauß im Jahre 1855 gab es diese Theorie noch gar nicht und Fourier fand seine „Fourierentwicklung“ sogar bereits zu Beginn des 19.-ten Jahrhunderts. Er behauptete auch gleich in seiner „Théorie analytique de la chaleur“, daß sich jede beliebige periodische Funktion durch eine Fouriereihe darstellen lasse, aber diese Behauptung stieß bei anderen berühmten Mathematikern seiner Zeit auf Ablehnung und es entstand darüber ein heftiger Disput. Erst in besagtem „Paradies der Mengenlehre“ konnten die Fourier’s Behauptung zugrundeliegenden Begriffe soweit geklärt werden, daß dieser Disput nun endgültig beigelegt ist. Ähnlich verhält es sich auch mit vielen anderen Fragestellungen. Da die Mengenlehre darüber hinaus auch vom didaktischen Standpunkt aus eine äußerst klare und durchsichtige Darstellung mathematischer Sachverhalte ermöglicht, hat sie sich als Grundlage der höheren Mathematik und der Ausbildung von Mathematikern an Universitäten schnell durchgesetzt und ist nun weltweit das „Alphabet der Sprache der Mathematik“. Man wird an Universitäten sogar geradezu dazu erzogen, alle Mathematik in der Sprache der Mengenlehre zu fassen und geometrischen Argumenten keine Beweiskraft zuzugestehen. Ich halte das bei der Ausbildung von Mathematikern auch für angemessen. Bei der Mathematik-Ausbildung im allgemeinen scheint mir dieses Vorgehen dahingegen nicht zielführend: In diesem Kontext sollte man meines Erachtens nicht mit demselben Maß messen, auch ohne alle Mengenlehre geometrisch erklärte Begriffe wie Gerade und Kreis, Ebene und Raum, als wohldefinierte Objekte der Mathematik zulassen und geometrischen Argumenten Beweiskraft zugestehen.

1.1.2. Im Wortlaut der ersten Zeilen des Artikels „Beiträge zur Begründung der transfiniten Mengenlehre (Erster Aufsatz)“ von Georg Cantor, erschienen im Jahre 1895, hört sich die Definition einer Menge so an:

> Unter einer **Menge** verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die **Elemente** von M genannt werden) zu einem Ganzen.

Verbinden wir mit einer Menge eine geometrische Vorstellung, so nennen wir ihre Elemente auch **Punkte** und die Menge selbst einen **Raum**. Ein derartiges Herumgerede ist natürlich keine formale Definition und birgt durchaus verschiedene Fallstricke, vergleiche 1.3.9. Das Ziel dieser Vorlesung ist aber auch nicht eine formale Begründung der Mengenlehre, wie Sie sie in der Logik kennenlernen können. Sie sollen vielmehr die Bedeutung dieser Worte intuitiv erfassen wie ein Kleinkind, das Sprechen lernt: Indem sie mir und anderen Mathematikern zuhören, wie wir mit diesen Worten sinnvolle Sätze bilden, uns nachahmen, und beobachten, welchen Effekt Sie damit hervorrufen. Unter anderem dazu sind die Übungsgruppen da.

Ergänzung 1.1.3. Bei der Entwicklung der Mathematik aus der Umgangssprache durch fortgesetztes Zuspitzen und Umwidmen des Wortschatzes muß ich an den Baron von Münchhausen denken, wie er sich an seinen eigenen Haaren aus dem Sumpf zieht. Schon verblüffend, daß es klappt. Aber bei Kleinkindern, die Sprechen lernen, ist es ja noch viel verblüffender, wie sie die Bedeutung von Worten erfassen, ohne daß man sie ihnen in Worten erklären kann.

Beispiele 1.1.4. Endliche Mengen kann man durch eine vollständige Liste ihrer Elemente in geschweiften Klammern angeben, zum Beispiel in der Form

$$X = \{x_1, x_2, \dots, x_n\}$$

Diese geschweiften Klammern heißen auch **Mengenklammern**. Die Elemente dürfen mehrfach genannt werden und es kommt nicht auf die Reihenfolge an, in der sie genannt werden. Wir haben also $\{1, 1, 2\} = \{2, 1\}$. Die Aussage „x ist Element von X“ wird mit $x \in X$ abgekürzt, ihre Verneinung „x ist nicht Element von X“ mit $x \notin X$. Zum Beispiel gilt $1 \in \{2, 1\}$ und $3 \notin \{2, 1\}$. Es gibt auch die sogenannte **leere Menge** $\emptyset = \{\ \}$, die gar kein Element enthält. Andere Beispiele sind die Mengen

$\mathbb{N} := \{0, 1, 2, \dots\}$ der **natürlichen Zahlen**,

$\mathbb{Z} := \{0, 1, -1, 2, -2, \dots\}$ der **ganzen Zahlen** und

$\mathbb{Q} := \{p/q \mid p, q \in \mathbb{Z},\ q \neq 0\}$ der **rationalen Zahlen**.

Der Name letzterer Menge kommt von lateinisch „ratio“ für „Verhältnis“, der Buchstabe $\mathbb{Q}$ steht für „Quotient“. Man beachte, daß wir auch hier Elemente mehrfach genannt haben, es gilt ja $p/q = p'/q'$ genau dann, wenn $pq' = p'q$. Auf Deutsch bezeichnet man die rationalen Zahlen auch als **Bruchzahlen**, da man sich etwa ein Viertel eines Kekses als den Anteil denken kann, der entsteht, wenn man besagten Keks in vier gleiche Teile zerbricht. Einen Leitfaden zu einem formaleren Aufbau des Zahlensystems können Sie in 2.5.1 finden.

Ergänzung 1.1.5 (**Herkunft des Gleichheitszeichens**). Das Gleichheitszeichen $=$ scheint auf ein 1557 von Robert Recorde publiziertes Buch zurückzugehen und soll andeuten, daß das, was auf der linken und rechten Seite dieses Zeichens steht, so gleich ist wie die beiden Strichlein, die das uns heute so selbstverständliche Gleichheitszeichen bilden. Davor schrieb man statt einem Gleichheitszeichen meist ae für „äquivalent“.

Ergänzung 1.1.6 (**Diskussion der Notation**). In Texten, in deren Konventionen die Null keine natürliche Zahl ist, verwendet man meist die abweichenden Notationen $\mathbb{N}$ für die Menge $\{1, 2, \ldots\}$ und $\mathbb{N}_0$ für die Menge $\{0, 1, 2, \ldots\}$. Die in diesem Text verwendete Notation $\mathbb{N} = \{0, 1, 2, \ldots\}$ stimmt mit der internationalen Norm ISO 31-11 überein.

1.1.7. Die Bedeutung der Symbole $\mathbb{Z}$ und $\mathbb{Q}$ ist in der Mathematik weitgehend einheitlich. Man verwendet diesen Schrifttypus auch sonst gerne für Symbole, die in ihrer Bedeutung über große Teile der Mathematik hinweg einheitlich verwendet werden. Bei der Bedeutung von $\mathbb{N}$ ist man allerdings nie ganz sicher, ob die Null mitgemeint ist. In den Konventionen dieses Textes gilt $0 \in \mathbb{N}$.

1.1.8. Eine Menge, die nur endlich viele Elemente hat, nennen wir eine **endliche Menge**. Eine präzisere Definition dieses Konzepts wird in [LA1] 4.1.2 gegeben. Wir vereinbaren bereits hier, daß wir auch die leere Menge endlich nennen. Die Zahl der Elemente einer endlichen Menge X nennen wir ihre **Kardinalität** oder **Mächtigkeit** und notieren sie

$$|X|$$

oder $\operatorname{card}(X)$. In der Literatur findet man auch die Notation $\sharp X$. Für endliche Mengen X ist demnach ihre Kardinalität stets eine natürliche Zahl $|X| \in \mathbb{N}$ und $|X| = 0$ ist gleichbedeutend zu $X = \emptyset$. Ist X unendlich, so schreiben wir bis auf weiteres kurzerhand $|X| = \infty$ und ignorieren in unserer Notation, daß auch unendliche Mengen „verschieden groß“ sein können. Für ein Beispiel für „verschieden große unendliche Mengen“ siehe [AN1] 2.5.2 und für eine genauere Diskussion des Begriffs der Kardinalität vergleiche [AL] 5.3.1.

1.2 Teilmengen

Definition 1.2.1. Eine Menge Y heißt **Teilmenge** einer Menge X, wenn jedes Element von Y auch ein Element von X ist. Man schreibt dafür $Y \subset X$ oder $X \supset Y$.

Beispiel 1.2.2. Die leere Menge Teilmenge jeder Menge, in Formeln $\emptyset \subset X$. $\{x\} \subset X$ ist gleichbedeutend zu $x \in X$. Es gilt $\emptyset \subset \{2, 1\} \subset \mathbb{Z} \subset \mathbb{Q}$.

1.2.3 (**Elemente und Teilmengen**). Es ist im Kontext der Mengenlehre wichtig, bei einer Menge X sorgfältig zu unterscheiden zwischen ihren Elementen und ihren Teilmengen. Gegeben ein Element $x \in X$ ist für uns das Element $x \in X$ etwas anderes als die Teilmenge $\{x\} \subset X$, die nur aus dem einzigen Element x besteht. Gegeben eine Menge X mit einer Teilmenge $Y \subset X$ sage ich auch, X **umfaßt** Y. Gegeben ein Element $x \in X$ sage ich, x **gehört zu** X. Andere Sprechweisen möchte ich ungern auf eine so präzise Bedeutung festlegen. Gegeben eine Teilmenge $Y \subset X$ kann man sagen, „Y sei enthalten in X“ oder „Y liege in X“, und gegeben ein Element $x \in X$ kann man auch sagen, „x sei enthalten in X“ oder „x liege in X“. Was genau gemeint ist, gilt es dann aus dem Kontext zu erschließen.

1.2.4 (**Diskussion der Notation**). Gegeben eine Menge X verwenden wir die Schreibweise $Y \subsetneq X$ als Abkürzung für ($Y \subset X$ und $Y \neq X$). Eine von der ganzen Menge verschiedene Teilmenge Y einer Menge X nennen wir auch eine **echte Teilmenge von** X. Bei diesen Notationen folgen wir Cantor und Bourbaki, die sehr viel später festgelegte internationalen Norm ISO 31-11 weicht jedoch davon ab. In der folgenden Tabelle stellen wir diese beiden Konventionen einander gegenüber.

Cantor und Bourbaki	Norm ISO 31-11	Bedeutung
$\subset$	$\subseteq$	ist Teilmenge von
$\subsetneq$	$\subset$	ist echte Teilmenge von

Ich ziehe die Konvention von Cantor und Bourbaki vor, weil ich sie gewohnt bin und weil man sehr oft Teilmengen zu betrachten hat und nur vergleichsweise selten echte Teilmengen. Ich muß jedoch zugeben, daß die in diesem Text gewählte Notation $\subset, \subsetneq$ mit den üblichen Notationen $\leq, <$ für Ungleichungen weniger gut zusammenpaßt als die Konvention nach ISO 31-11.

1.2.5. Oft bildet man neue Mengen als Teilmengen bestehender Mengen. Gebräuchlich ist dazu eine Notation, bei der man zwischen den Mengenklammern hinter einem senkrechten Strich dazuschreibt, welche zusätzliche Eigenschaft die Elemente einer Teilmenge haben sollte, so daß man Teilmengen Y einer Menge

X angeben kann in der Form

$$Y = \{x \in X \mid x \text{ hat eine zusätzlich noch gewisse Eigenschaft}\}$$

Zum Beispiel gilt $\mathbb{N} = \{a \in \mathbb{Z} \mid a \geq 0\}$, lies „die Menge der natürlichen Zahlen ist die Teilmenge der Menge der ganzen Zahlen bestehend aus allen ganzen Zahlen, die ≥ 0 sind", und $\{0, 1\} = \{a \in \mathbb{N} \mid a^2 = a\}$.

Definition 1.2.6. Es ist auch erlaubt, die „Menge aller Teilmengen" einer gegebenen Menge X zu bilden. Sie heißt die **Potenzmenge von** X und wird $\mathcal{P}(X)$ oder $\operatorname{Pot}(X)$ notiert.

Beispiel 1.2.7. Die Potenzmenge $\mathcal{P}(\{1, 2, 3\})$ kann man als die Menge aller möglichen Ausgänge einer Versuchsanordnung interpretieren, bei der man dreimal eine Münze wirft. Dazu mag man etwa jedem Ausgang die Menge der Wurfnummern zuordnet, bei denen Wappen herauskam. So würde etwa dem Ausgang WZW die Teilmenge $\{1, 3\}$ zugeordnet.

1.2.8 (**Kardinalität der Potenzmenge**). Ist X eine endliche Menge, so ist auch ihre Potenzmenge endlich und es gilt die Formel $|\mathcal{P}(X)| = 2^{|X|}$. Für die drei-elementige Menge $X = \{1, 2, 3\}$ besteht ihre Potenzmenge $\mathcal{P}(X)$ zum Beispiel aus $8 = 2^3$ Elementen und wir haben genauer

$$\mathcal{P}(X) = \big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\big\}$$

Die Teilmenge $\{1\} \subset \{1, 2, 3\}$, die nur aus dem Element 1 besteht, ist also ein Element der Potenzmenge $\{1\} \in \mathcal{P}(\{1, 2, 3\})$. Das Element 1 ist dahingegen kein Element der Potenzmenge, sondern ein Element der ursprünglichen Menge $1 \in \{1, 2, 3\}$.

Satz 1.2.9 (**Bedeutung der Binomialkoeffizienten**). *Gegeben natürliche Zahlen $n, k \in \mathbb{N}$ gibt der Binomialkoeffizient $\binom{n}{k}$ die Zahl der k-elementigen Teilmengen einer n-elementigen Menge an. In Formeln ausgedrückt haben wir unter der Annahme $|X| = n$ also*

$$|\{Y \subset X \mid |Y| = k\}| = \tbinom{n}{k}$$

Beweis. Vollständige Induktion über n. Für $n = 0$ gilt die Aussage, denn eine nullelementige Menge hat genau eine k-elementige Teilmenge falls $k = 0$ und keine k-elementige Teilmenge falls $k \geq 1$. Nehmen wir nun an, die Aussage sei für ein n schon bewiesen. Eine $(n + 1)$-elementige Menge X schreiben wir als $X = M \cup \{x\}$ mit dem gleich in 1.3.1 formal eingeführten Vereingungszeichen $\cup$, wo M eine n-elementige Menge ist und $x \notin M$. Ist $k = 0$, so gibt es genau eine k-elementige Teilmenge von $M \cup \{x\}$, nämlich die leere Menge. Ist $k \geq 1$, so gibt es in $M \cup \{x\}$ nach Induktionsannahme genau $\binom{n}{k}$ k-elementige Teilmengen, die x nicht enthalten. Die k-elementigen Teilmengen dahingegen, die x enthalten, ergeben sich durch Hinzunehmen von x aus den $(k-1)$-elementigen Teilmengen von M, von denen es gerade $\binom{n}{k-1}$ gibt. Insgesamt hat $M \cup \{x\}$ damit also genau $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ Teilmengen mit genau k Elementen. □

1.2.10. Wieder scheint mir dieser Beweis in der für vollständige Induktion typischen Weise undurchsichtig. Ich ziehe deshalb den in [EIN] 1.1.19 gegebenen weniger formellen Beweis vor. Man kann auch diesen Beweis formalisieren und verstehen als Spezialfall der sogenannten „Bahnformel“, vergleiche [LA2] 5.2.3.

1.2.11 (**Variante zum Beweis der binomischen Formel**). Wir geben nun die versprochene präzise Formulierung unseres ersten Beweises der binomischen Formel [EIN] 1.1.23. Wir rechnen dazu

$$(a+b)^n = \sum_{Y \subset \{1,2,\ldots,n\}} a^{|Y|} b^{n-|Y|}$$

Die rechte Seite soll hier in Verallgemeinerung der in [EIN] 1.1.8 eingeführten Notation bedeuten, daß wir für jede Teilmenge Y von $\{1, 2, \ldots, n\}$ den angegebenen Ausdruck $a^{|Y|} b^{n-|Y|}$ nehmen und alle diese Ausdrücke aufsummieren. Dann fassen wir gleiche Summanden zusammen und erhalten mit 1.2.9 die binomische Formel.

Übungen

Übung 1.2.12. Es gilt $\sum_k \binom{n}{k} = 2^n$.

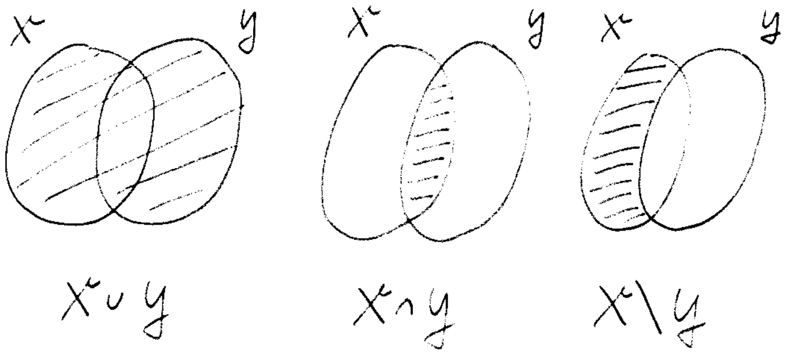
Übung 1.2.13. Man zeige $(a+b+c)^n = \sum_{i+j+k=n} \frac{n!}{i!j!k!} a^i b^j c^k$.

1.3 Mengenoperationen

Definition 1.3.1. Wir erinnern, daß wir $:=$ als Abkürzung für „ist definiert als“ verwenden und daß „oder“ in der Mathematik stets das „nichtausschließende oder“ meint. Gegeben zwei Mengen X, Y können wir unter anderem auf folgende Weisen neue Mengen bilden:

1. Die **Vereinigung** $X \cup Y := \{z \mid z \in X \text{ oder } z \in Y\}$, zum Beispiel ist $\{1, 2\} \cup \{2, 3\} = \{1, 2, 3\}$;

2. Den **Schnitt** oder auch **Durchschnitt** $X \cap Y := \{z \mid z \in X \text{ und } z \in Y\}$, zum Beispiel ist $\{1, 2\} \cap \{2, 3\} = \{2\}$;



Van-de-Ven-Diagramme für Vereinigung, Schnitt und Differenz

3. Die **Differenz** $X \backslash Y := \{z \in X \mid z \notin Y\}$, zum Beispiel haben wir $\{1,2\} \backslash \{2,3\} = \{1\}$. Man schreibt statt $X \backslash Y$ auch $X - Y$. Ist Y eine Teilmenge von X, so heißt $X \backslash Y$ das **Komplement** von Y in X oder ausführlicher die **Komplementmenge**;

4. Das **Produkt** $X \times Y := \{(x,y) \mid x \in X,\ y \in Y\}$ oder ausführlicher **kartesische Produkt**. Es gilt also $(x,y) = (x',y')$ genau dann, wenn gilt $x = x'$ und $y = y'$. Zum Beispiel haben wir

$$\{1,2\} \times \{1,2,3\} = \{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3)\}$$

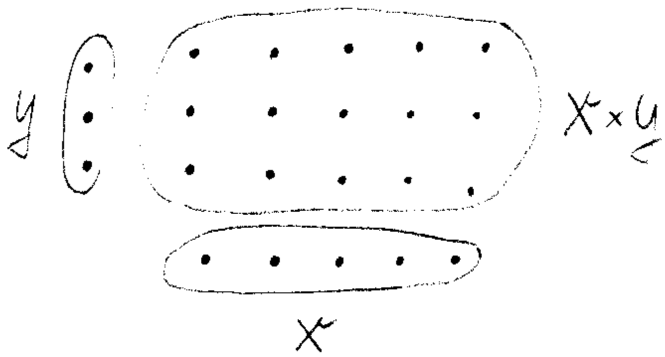
   Oft benutzt man für das Produkt $X \times X$ einer Menge X mit sich selbst die Abkürzung $X^2 := X \times X$ und nennt das die Menge aller **angeordneten Paare** von Elementen von X.

1.3.2. Eine gute Anschauung für die ersten drei Operationen liefern die sogenannten **van-de-Ven-Diagramme**, wie sie die nebenstehenden Bilder zeigen. Sie sind allerdings nicht zu genau zu hinterfragen, denn ob die Punkte auf einem Blatt Papier im Sinne von Cantor „bestimmte wohlunterschiedene Objekte unserer Anschauung“ sind, scheint mir nicht ohne weiteres so klar. Wenn man jedoch jedes der schraffierten Gebiete im Bild als die Menge aller darin liegenden Kreuzungspunkte auf einem dazugedachten Millimeterpapier auffaßt und keine dieser Kreuzungspunkte auf den Begrenzungslinien liegen, so können sie wohl schon als eine Menge im Cantor'schen Sinne angesehen werden.

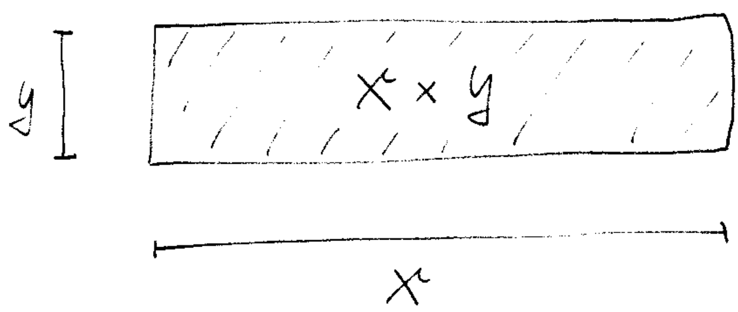
1.3.3. Zwei Teilmengen einer gegebenen Menge, die kein gemeinsames Element haben, heißen **disjunkt**. Äquivalent dazu ist die Bedingung, daß ihr Schnitt die leere Menge ist.

1.3.4 (**Mehrdeutigkeiten mit dem Komma als Trenner**). Die Verwendung des Kommas als Trenner ist hier problematisch, da $(1,2)$ nun zweierlei bedeuten kann: Zum einen ein Element des kartesischen Produkts $\mathbb{N} \times \mathbb{N}$, zum anderen aber auch den eingeklammerten Dezimalbruch $1{,}2$. Was im Einzelfall gemeint ist, gilt es aus dem Kontext zu erschließen. In diesem Text werden Dezimalbrüche nur selten vorkommen. In deutschen Schulbüchern verwendet man für angeordnete Paare meist die abweichende Notation $(x|y)$, um auch Paare von Dezimalbrüchen unmißverständlich notieren zu können.

1.3.5 (**Diskussion der Terminologie**). Die Bezeichnung als „Schnitt“ kommt wohl her von der Vorstellung des Schnitts zweier Geraden, wenn man sie als Teilmengen der Ebene denkt und diese hinwiederum als ein Blatt Papier, das man längs der einen Gerade entzweischneiden kann. Der Punkt, an dem die andere Gerade entzweigeschnitten wird, ist dann der Schnittpunkt und der Schnitt unserer beiden Geraden besteht genau aus diesem einen Punkt.



Anschauliche Darstellung des Produkts einer Menge mit fünf und einer Menge mit drei Elementen. Hier wird ein Paar (x, y) dargestellt durch einen Punkt, der über x und neben y liegt.



Dies Bild muß anders interpretiert werden als das Vorherige. Die Mengen X und Y sind nun zu verstehen als die Mengen der Punkte der vertikalen und horizontalen Geradensegmente und ein Punkt des Quadrats meint das Element $(x, y) \in X \times Y$, das in derselben Höhe wie $y \in Y$ senkrecht über $x \in X$ liegt.

1.3.6 (**Mengenlehre und das Bilden von Begriffen**). Wir werden in unserer naiven Mengenlehre die ersten drei Operationen „Vereinigung“, „Schnitt“ und „Differenz“ aus 1.3.1 nur auf Teilmengen einer gemeinsamen Obermenge anwenden, die uns in der einen oder anderen Weise bereits zur Verfügung steht. Die Potenzmenge und das kartesische Produkt dahingegen benutzen wir, um darüber hinaus neue Mengen zu erschaffen. Diese Konstruktionen erlauben es, im Rahmen der Mengenlehre so etwas wie Abstraktionen zu bilden: Wenn wir uns etwa die Menge T aller an mindestens einem Tag der Weltgeschichte lebenden oder gelebt habenden Tiere als eine Menge im Cantor'schen Sinne denken, so würden wir Konzepte wie „männlich“ oder „Hund“ oder „Fleischfresser“ formal als Teilmengen dieser Menge alias als Elemente von $\mathcal{P}(T)$ formalisieren. Das Konzept „ist Kind von“ würde dahingegen formalisiert als eine Teilmenge $K \subset T \times T$ des kartesischen Produkts unserer Menge T mit sich selbst alias als ein Element $K \in \mathcal{P}(T \times T)$, nämlich als die Teilmenge

$$K := \{(x, y) \in T \times T \mid x \text{ ist Kind von } y\}$$

1.3.7. Für das Rechnen mit Mengen überlegt man sich die folgenden Regeln, die ich gleich mit ihren üblichen Bezeichnungen angebe:

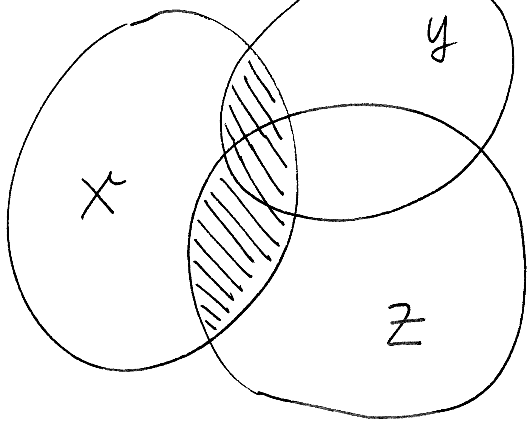
Assoziativgesetze:	$X \cap (Y \cap Z)$	$=$	$(X \cap Y) \cap Z$
	$X \cup (Y \cup Z)$	$=$	$(X \cup Y) \cup Z$
Distributivgesetze:	$X \cup (Y \cap Z)$	$=$	$(X \cup Y) \cap (X \cup Z)$
	$X \cap (Y \cup Z)$	$=$	$(X \cap Y) \cup (X \cap Z)$
de Morgan'sche Regeln:	$X \backslash (Y \cup Z)$	$=$	$(X \backslash Y) \cap (X \backslash Z)$
	$X \backslash (Y \cap Z)$	$=$	$(X \backslash Y) \cup (X \backslash Z)$
Komplement der Differenzmenge:	$X \backslash (X \backslash Y)$	$=$	$X \cap Y$

Eine gute Anschauung für diese Regeln liefern die van-de-Ven-Diagramme, wie die nebenstehenden Bilder zeigen. Das liegt daran, daß alle acht möglichen Lagen in Bezug auf unsere drei Mengen in diesen Diagrammen als Flächen zu sehen sind.

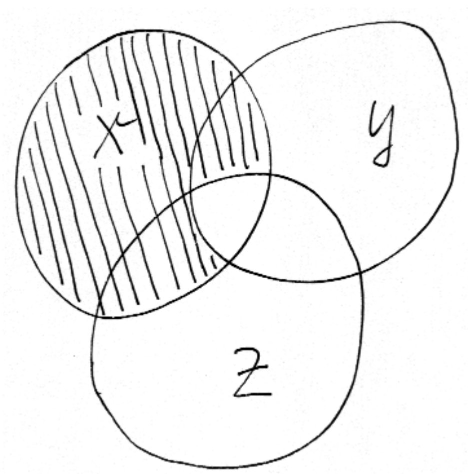
1.3.8. Ich zeige beispielhaft die Regel $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$. Es reicht, statt der Gleichheit die beiden Inklusionen $\subset$ und $\supset$ zu zeigen.

Ich beginne mit $\subset$. Sicher gilt $(Y \cap Z) \subset Y$, also auch $X \cup (Y \cap Z) \subset X \cup Y$. Ebenso zeigt man $X \cup (Y \cap Z) \subset X \cup Z$ und damit folgt schon mal $\subset$.

Bleibt noch $\supset$ zu zeigen. Das will mir nur durch Betrachtung von Elementen gelingen. Gegeben $a \in (X \cup Y) \cap (X \cup Z)$ gilt entweder $a \in X$ oder $a \notin X$. Falls $a \in X$ haben wir eh $a \in X \cup (Y \cap Z)$. Falls $a \notin X$ folgt aus $a \in (X \cup Y) \cap (X \cup Z)$



$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$

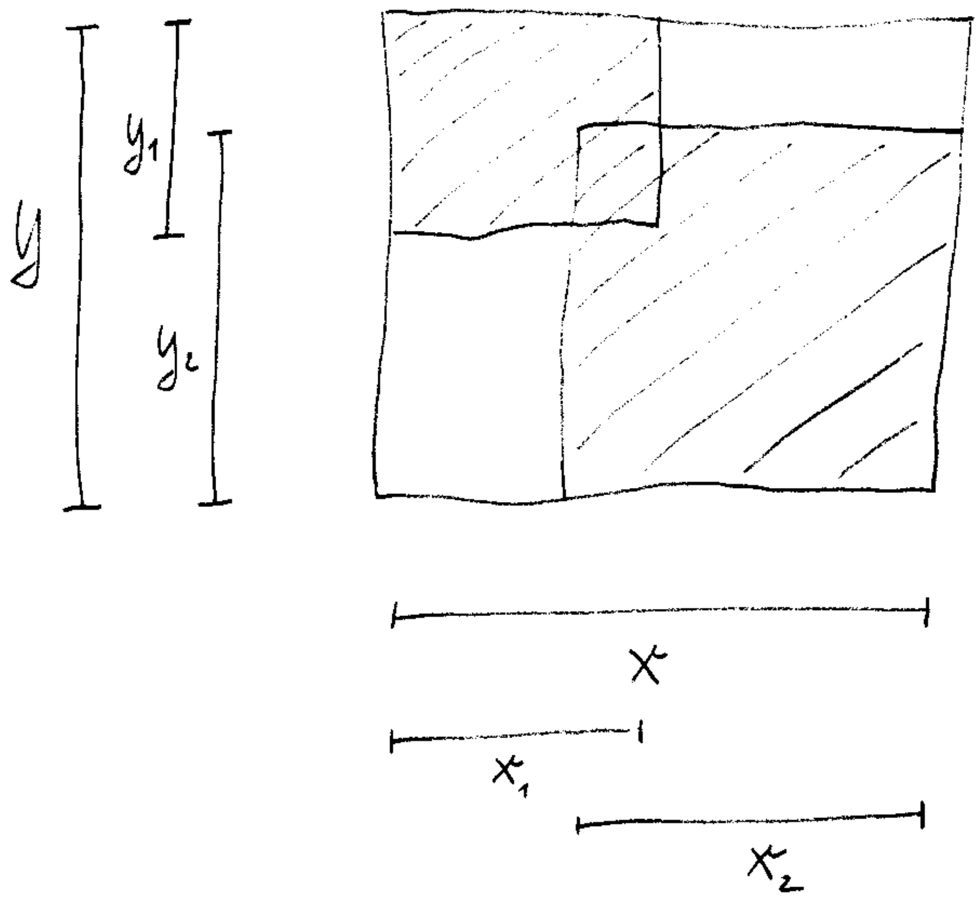


$X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$

erst $a \in (X \cup Y)$ und dann $a \in Y$ und weiter erst $a \in (X \cup Z)$ und dann $a \in Z$, also $a \in Y \cap Z \subset X \cup (Y \cap Z)$. Wir haben somit gezeigt, daß jedes Element a von $(X \cup Y) \cap (X \cup Z)$ auch zu $X \cup (Y \cap Z)$ gehört. Damit folgt die behauptete Inklusion $\supset$.

Ergänzung 1.3.9 (**Das Russell'sche Paradoxon**). Ich will nicht verschweigen, daß der in diesem Abschnitt dargestellte naive Zugang zur Mengenlehre durchaus begriffliche Schwierigkeiten mit sich bringt: Zum Beispiel darf die Gesamtheit $\mathcal{M}$ aller Mengen nicht als Menge angesehen werden, da wir sonst die „Menge aller Mengen, die sich nicht selbst als Element enthalten", gegeben durch die formelhafte Beschreibung $\mathcal{N} = \{A \in \mathcal{M} \mid A \notin A\}$, bilden könnten. Für diese Menge kann aber weder $\mathcal{N} \in \mathcal{N}$ noch $\mathcal{N} \notin \mathcal{N}$ gelten. Diese Art von Schwierigkeiten kann erst ein formalerer Zugang klären und auflösen, bei dem man unsere naiven Vorstellungen durch Ketten von Zeichen aus einem wohlbestimmten endlichen Alphabet ersetzt und unsere Vorstellung von Wahrheit durch die Verifizierbarkeit vermittels rein algebraischer „erlaubter Manipulationen" solcher Zeichenketten, die in „Axiomen" festgelegt werden. Diese Verifikationen kann man dann durchaus auch einer Rechenmaschine überlassen, so daß wirklich auf „objektivem" Wege entschieden werden kann, ob ein „Beweis" für die „Richtigkeit" einer unserer Zeichenketten in einem vorgegebenen axiomatischen Rahmen stichhaltig ist. Allerdings kann in derartigen Systemen von einer Zeichenkette algorithmisch nur entschieden werden, ob sie eine „sinnvolle Aussage" ist, nicht aber, ob sie „bewiesen" werden kann. Noch viel stärker zeigt der Unvollständigkeitssatz von Gödel, daß es in einem derartigen axiomatischen Rahmen, sobald er reichhaltig genug ist für eine Beschreibung des Rechnens mit natürlichen Zahlen, stets sinnvolle Aussagen gibt derart, daß entweder sowohl die Aussage als auch ihre Verneinung oder aber weder die Aussage noch ihre Verneinung bewiesen werden können. Mit diesen und ähnlichen Fragestellungen beschäftigt sich die Logik.

Vorschau 1.3.10 (**Weitere Konstruktionen der Mengenlehre**). Um mich nicht dem Vorwurf auszusetzen, während des Spiels die Spielregeln ändern zu wollen, sei bereits hier erwähnt, was noch hinzukommen soll. Die einzigen grundlegenden Konstruktionen, die noch fehlen, sind das Bilden der „disjunkten Vereinigung" und des „kartesischen Produkts" zu einer „beliebigen Mengenfamilie" in [LA2] 7.7.17 und [LA2] 7.7.7. In [AN1] **??** besprechen wir weiter Schnitt und Vereinigung einer „beliebigen Familie von Teilmengen einer gegebenen Menge". In [LA1] 1.9 werden einige weniger offensichtliche Argumentationen im Zusammenhang mit dem sogenannten „Zorn'schen Lemma" erläutert, die meines Erachtens bereits an den Rand dessen gehen, was man in unserem informellen Rahmen der naiven Mengenlehre als Argumentation noch vertreten kann. In [LA1] 4.1 wird die Konstruktion der natürlichen Zahlen im Rahmen der Mengenlehre diskutiert, insbesondere geben wir erst dort eine formale Definition des Begriffs einer



Aus $X = X_1 \cup X_2$ und $Y = Y_1 \cup Y_2$ folgt noch lange nicht
$X \times Y = (X_1 \times Y_1) \cup (X_2 \times Y_2)$

endlichen Menge. Sicher ist es in gewisser Weise unbefriedigend, das Fundament des Hauses der Mathematik erst fertigzustellen, wenn bereits erste Stockwerke stehen und bewohnt sind. Andererseits will ich aber auch vermeiden, daß Sie mir auf einem gewaltigen Fundament, das die ganze Mathematik tragen kann, im ersten Winter(semester) jämmerlich erfrieren.

1.3.11 (**Der Sinn von Genauigkeit und sorgfältiger Sprache**). Ich könnte mir gut vorstellen, daß verschiedene meiner Leser denken, diese ganze Pedanterie sei doch eigentlich überflüssig und jetzt sollten wir doch einfach mal fröhlich losrechnen wie das in der Schule ja auch sehr gut ging. Ich will hier erklären, warum Pedanterie in diesem Zusammenhang wichtig ist. Viele von Ihnen werden wissen, wie man mit einem einfachen Blatt Papier zum Mond kommt: 42-mal Falten und draufsteigen, das war's schon. So ähnlich ist es in der Mathematik: Etwas völlig Banales wie die naive Mengenlehre wird in den etwa dreißig Vorlesungsdoppelstunden des Wintersemesters jedes Mal von neuem gefaltet und wenn Sie dann am Ende des Wintersemesters zurückblicken, kann Ihnen schon leicht schwindlig werden. Das funktioniert mit wirklichem Papier nur eingeschränkt, aber wenn man sehr festes und glattes „Gedankenpapier" nimmt, und solches Gedankenpapier ist eben gerade die Mengenlehre, dann klappt es verblüffend gut. Man muß dazu aber mit der Herstellung dieses Gedankenpapiers ebenso wie beim Falten sorgfältig sein bis zur Pedanterie, denn auch die kleinste Ungeschicklichkeit vervielfacht sich bei diesem Vorgehen mit derselben Schnelligkeit wie die gedankliche Höhe und bringt, eh man sich's versieht, alles zum Einsturz.

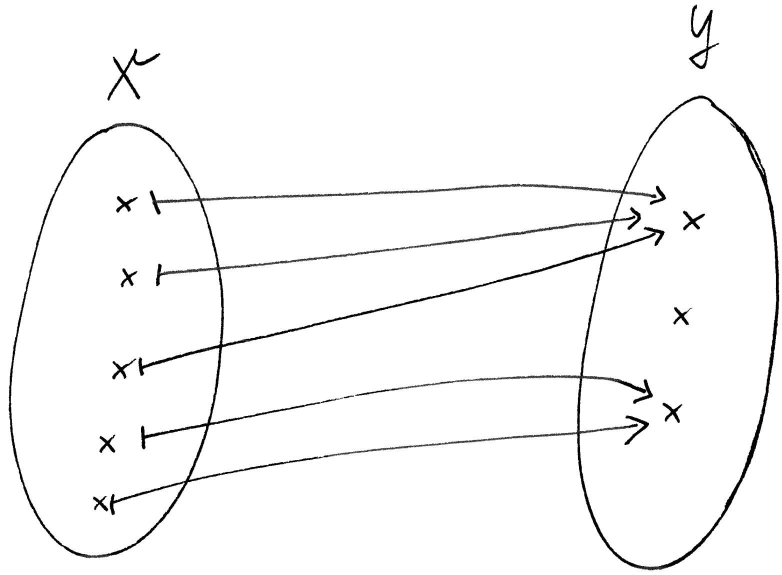
Übungen

Übung 1.3.12. Sind X und Y endliche Mengen, so gilt für die Kardinalitäten $|X \times Y| = |X| \cdot |Y|$ und $|X \cup Y| = |X| + |Y| - |X \cap Y|$.

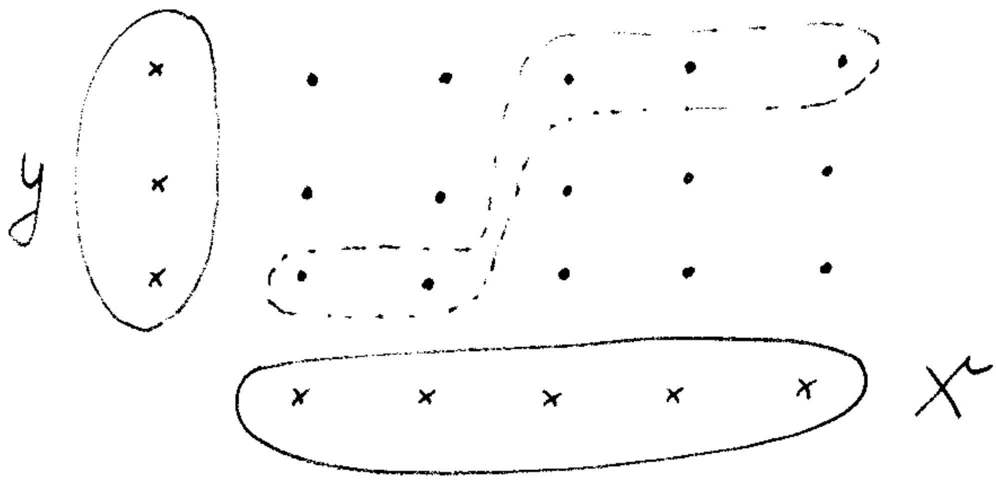
1.4 Abbildungen

Definition 1.4.1. Seien X, Y Mengen. Eine **Abbildung** $f : X \to Y$ ist eine Zuordnung, die jedem Element $x \in X$ genau ein Element $f(x) \in Y$ zuordnet, das **Bild** von x unter f, auch genannt der **Wert** von f an der Stelle x. Man spricht dann auch vom **Auswerten** der Funktion f an der Stelle x oder vom **Einsetzen** von x in f und schreibt manchmal abkürzend $f(x) = fx$.

1.4.2. Wem das zu vage ist, der mag die alternative Definition vorziehen, nach der eine **Abbildung** $f : X \to Y$ eine Teilmenge $f \subset X \times Y$ ist derart, daß es für jedes $x \in X$ genau ein $y \in Y$ gibt mit $(x, y) \in f$. Dies eindeutig bestimmte y schreiben wir dann $f(x)$ und sind auf einem etwas formaleren Weg wieder an



Eine Abbildung einer Menge mit fünf in eine mit drei Elementen



Der Graph der oben angegebenen Abbildung, wobei das X oben mit dem X hier identifiziert wurde durch „Umkippen nach Rechts“

demselben Punkt angelangt. In unseren Konventionen nennen wir besagte Teilmenge den **Graphen von** f und notieren sie mit dem Symbol Γ (sprich: Gamma), einem großen griechischen G, und schreiben

$$\Gamma(f) := \{(x, f(x)) \mid x \in X\} \subset X \times Y$$

Definition 1.4.3. Ist $f : X \to Y$ eine Abbildung, so nennen wir X ihren **Definitionsbereich** und Y ihren **Wertebereich**. Zwei Abbildungen nennen wir gleich, wenn sie denselben Definitionsbereich X, denselben Wertebereich Y und dieselbe Abbildungsvorschrift $f \subset X \times Y$ haben.

1.4.4 (**Die Notationen $\to$ und $\mapsto$**). Wir notieren Abbildungen oft in der Form

$$\begin{array}{rccc} f : & X & \to & Y \\ & x & \mapsto & f(x) \end{array}$$

und in verschiedenen Verkürzungen dieser Notation. Zum Beispiel sprechen wir von „einer Abbildung $\mathbb{N} \to \mathbb{N}$ von der Menge der natürlichen Zahlen in sich selber“ oder „der Abbildung $n \mapsto n^3$ von der Menge der natürlichen Zahlen in sich selber“. Wir benutzen unsere zwei Arten von Pfeilen $\to$ und $\mapsto$ auch im allgemeinen in derselben Weise.

Beispiel 1.4.5. Für jede Menge X haben wir die **identische Abbildung** oder **Identität**

$$\begin{array}{rccc} \mathrm{id} = \mathrm{id}_X : & X & \to & X \\ & x & \mapsto & x \end{array}$$

Ein konkreteres Beispiel für eine Abbildung ist das Quadrieren

$$\begin{array}{rccc} q : & \mathbb{Z} & \to & \mathbb{Z} \\ & n & \mapsto & n^2 \end{array}$$

Beispiel 1.4.6. Gegeben zwei Mengen X, Y erklärt man die **Projektionsabbildungen** oder **Projektionen** $\mathrm{pr}_X : X \times Y \to X$ beziehungsweise $\mathrm{pr}_Y : X \times Y \to Y$ durch die Vorschrift $(x, y) \mapsto x$ beziehungsweise $(x, y) \mapsto y$. In manchen Zusammenhängen notiert man sie auch abweichend pr_1 und pr_2 für die „Projektion auf die erste beziehungsweise zweite Komponente“.

Definition 1.4.7. Sei $f : X \to Y$ eine Abbildung.

1. Gegeben eine Teilmenge $A \subset X$ erklären wir das **Bild von A unter f**, eine Teilmenge $f(A) \subset Y$, durch

$$f(A) := \{y \in Y \mid \text{Es gibt } x \in A \text{ mit } f(x) = y\}$$

2. Gegeben eine Teilmenge $B \subset Y$ erklären wir das **Urbild von B unter f**, eine Teilmenge von $f^{-1}(B) \subset X$, durch

$$f^{-1}(B) := \{x \in X \mid f(x) \in B\}$$

1.4.8. Das Bild von ganz X nennen wir das **Bild von f** und notieren es $\operatorname{im}(f) := f(X)$. Das Kürzel im steht für französisch und englisch **image**.

Beispiel 1.4.9. Für unsere Abbildung $q : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto n^2$ des Quadrierens von eben könnten wir die Menge aller Quadratzahlen schreiben als

$$q(\mathbb{Z}) = \{a^2 \mid a \in \mathbb{Z}\}$$

Ebenso wäre $\{2a \mid a \in \mathbb{N}\}$ eine mögliche formelmäßige Darstellung der Menge aller geraden natürlichen Zahlen, und $\{ab \mid a, b \in \mathbb{N}, a \geq 2, b \geq 2\}$ wäre eine formelmäßige Darstellung der Menge aller natürlichen Zahlen, die nicht prim und auch nicht Null oder Eins sind.

1.4.10. Eine Abbildung, deren Bild aus höchstens einem Element besteht, nennen wir eine **konstante Abbildung**. Eine Abbildung, deren Bild aus genau einem Element besteht, nennen wir eine **einwertige Abbildung**. Eine einwertige Abbildung ist also eine konstante Abbildung mit nichtleerem Definitionsbereich.

1.4.11 (**Konstanten und konstante Abbildungen**). Gegeben ein festes $c \in Y$ schreiben wir oft auch kurz c für die konstante Abbildung $X \to Y$ gegeben durch $x \mapsto c$ für alle $x \in X$. Damit verbunden ist die Hoffnung, daß aus dem Kontext klar wird, ob im Einzelfall die Abbildung $c : X \to Y$ oder das Element $c \in Y$ gemeint sind.

1.4.12. Gegeben eine Abbildung $f : X \to Y$ ist formal f^{-1} eine Abbildung $f^{-1} : \mathcal{P}(Y) \to \mathcal{P}(X)$ in der Gegenrichtung auf den Potenzmengen. Besteht B nur aus einem Element x, so schreiben wir auch $f^{-1}(x)$ statt $f^{-1}(\{x\})$ und nennen diese Menge die **Faser von f über x** oder **bei** x. Das Quadrieren q aus 1.4.9 hat etwa die Faser $q^{-1}(1) = \{1, -1\}$ bei 1 und die Faser $q^{-1}(-1) = \emptyset$ bei -1.

1.4.13 (**Diskussion der Notation**). Die Notation $f^{-1}(B)$ für das Urbild einer Menge unter einer Abbildung führt leicht zu Verwirrung, da man a^{-1} aus der Schule als alternative Notation für den Bruch $a^{-1} = 1/a$ gewohnt ist. Diese beiden Notationen sind nur entfernt verwandt und werden beide in der Mathematik durchgehend verwendet. Was im Einzelfall gemeint ist, gilt es aus dem Kontext zu erschließen.

1.5 Verknüpfung von Abbildungen

Definition 1.5.1. Sind drei Mengen X, Y, Z gegeben und dazwischen Abbildungen $f : X \to Y$ und $g : Y \to Z$, so definieren wir die **Verknüpfung** unserer

Abbildungen f und g, eine Abbildung $g \circ f : X \to Z$, durch die Vorschrift

$$\begin{array}{rccc} g \circ f : & X & \to & Z \\ & x & \mapsto & g(f(x)) \end{array}$$

1.5.2 (**Diskussion der Notation**). Die Notation $g \circ f$, sprich „g nach f“, für „erst f, dann g“ ist gewöhnungsbedürftig, erklärt sich aber durch die offensichtliche Formel $(g \circ f)(x) = g(f(x))$. Ich sage, $g \circ f$ entstehe aus g durch **Vorschalten von** f und aus f durch **Nachschalten von** g. Oft kürzt man auch $g \circ f$ mit gf ab. Mit dieser Abkürzung muß man jedoch sorgsam umgehen, da im Fall von zwei Abbildungen f, g von derselben Menge in einen Zahlbereich, etwa $f, g : X \to \mathbb{Q}$, der Ausdruck fg vielmehr für die Abbildung $x \mapsto f(x)g(x)$ reserviert ist, das sogenannte „punktweise Produkt“ unserer beiden Funktionen.

Beispiel 1.5.3. Betrachten wir zusätzlich zum Quadrieren $q : \mathbb{Z} \to \mathbb{Z}$ die Abbildung $t : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x + 1$, so gilt $(q \circ t)(x) = (x + 1)^2$ aber $(t \circ q)(x) = x^2 + 1$.

Definition 1.5.4. Sei $f : X \to Y$ eine Abbildung.

1. f heißt **injektiv** oder eine **Injektion**, wenn aus $x \neq x'$ folgt $f(x) \neq f(x')$. Gleichbedeutend ist die Forderung, daß es für jedes $y \in Y$ höchstens ein $x \in X$ gibt mit $f(x) = y$. Injektionen schreibt man oft $\hookrightarrow$.

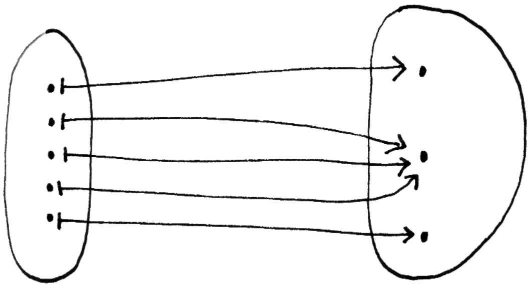
2. f heißt **surjektiv** oder eine **Surjektion**, wenn es für jedes $y \in Y$ mindestens ein $x \in X$ gibt mit $f(x) = y$. Surjektionen schreibt man manchmal $\twoheadrightarrow$.

3. f heißt **bijektiv** oder eine **Bijektion**, wenn f injektiv und surjektiv ist. Gleichbedeutend ist die Forderung, daß es für jedes $y \in Y$ genau ein $x \in X$ gibt mit $f(x) = y$. Bijektionen schreibt man oft $\xrightarrow{\sim}$.

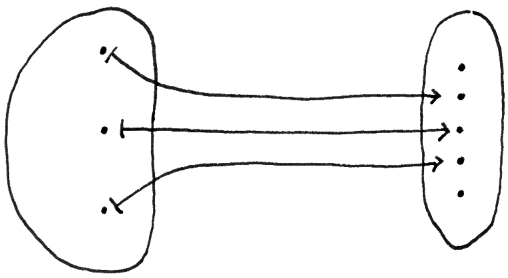
1.5.5. Ist $X \subset Y$ eine Teilmenge, so ist die **Einbettung** oder **Inklusion** $i : X \to Y$, $x \mapsto x$ stets injektiv. Ist $g : Y \to Z$ eine Abbildung und $X \subset Y$ eine Teilmenge, so nennen wir die Verknüpfung $g \circ i$ von g mit der Inklusion auch die **Einschränkung** von g auf X und notieren sie

$$g \circ i =: g|X = g|_X : X \to Z$$

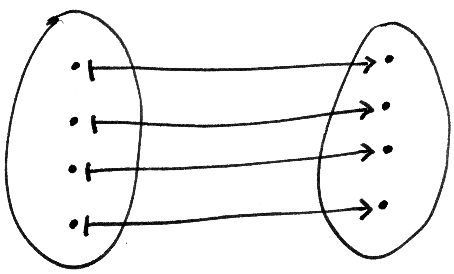
Oft bezeichnen wir eine Einschränkung aber auch einfach mit demselben Buchstaben g in der Hoffnung, daß der Leser aus dem Kontext erschließen kann, welche Abbildung genau gemeint ist. Das ist nicht ganz unproblematisch: So ist etwa unsere Abbildung $q : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto n^2$ nicht injektiv, ihre Restriktion zu einer Abbildung $q : \mathbb{N} \to \mathbb{Z}$ ist aber durchaus injektiv.



Eine Surjektion



Eine Injektion



Eine Bijektion

1.5.6 (**Surjektion auf das Bild**). Ist $f : X \to Y$ eine Abbildung, so ist die Abbildung $f : X \to f(X)$, $x \mapsto f(x)$ stets surjektiv. Der Leser möge entschuldigen, daß wir hier zwei verschiedene Abbildungen mit demselben Symbol f bezeichnet haben. Das wird noch öfter vorkommen. Überhaupt ignorieren wir, gegeben Mengen X, Y und eine Teilmenge $Z \subset Y$, im folgenden meist den Unterschied zwischen einer „Abbildung von X nach Y, deren Bild in Z enthalten ist" und einer „Abbildung von X nach Z".

Beispiele 1.5.7. Unsere Abbildung $q : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto n^2$ ist weder injektiv noch surjektiv. Die Identität $\mathrm{id} : X \to X$ ist stets bijektiv. Sind X und Y endliche Mengen, so gibt es genau dann eine Bijektion von X nach Y, wenn X und Y dieselbe Kardinalität haben, in Formeln $|X| = |Y|$.

Satz 1.5.8. *Seien $f : X \to Y$ und $g : Y \to Z$ Abbildungen.*

1. *Ist $g \circ f$ injektiv, so ist f injektiv;*

2. *Sind g und f injektiv, so auch $g \circ f$;*

3. *Genau dann ist g injektiv, wenn für beliebige Abbildungen $f_1, f_2 : X \to Y$ aus $g \circ f_1 = g \circ f_2$ schon folgt $f_1 = f_2$.*

Beweis. Übung. Besonders elegant ist es, zunächst die letzte Aussage zu zeigen, und dann die vorderen Aussagen ohne weitere Betrachtung von Elementen zu folgern. $\square$

1.5.9 (**Universelle Eigenschaft von Injektionen**). Sei $i : Y \hookrightarrow X$ eine injektive Abbildung und $\varphi : Z \to X$ eine beliebige Abbildung. Genau dann gibt es eine Abbildung $\tilde{\varphi} : Z \to Y$ mit $i \circ \tilde{\varphi} = \varphi$, wenn gilt $\mathrm{im}(\varphi) \subset \mathrm{im}(i)$. Nach dem Vorhergehenden ist diese Abbildung $\tilde{\varphi}$ dann sogar eindeutig bestimmt.

Satz 1.5.10. *Seien $f : X \to Y$ und $g : Y \to Z$ Abbildungen.*

1. *Ist $g \circ f$ surjektiv, so ist g surjektiv;*

2. *Sind g und f surjektiv, so auch $g \circ f$;*

3. *Genau dann ist f surjektiv, wenn für beliebige Abbildungen $g_1, g_2 : Y \to Z$ aus $g_1 \circ f = g_2 \circ f$ schon folgt $g_1 = g_2$.*

Beweis. Übung. Besonders elegant ist es, zunächst die letzte Aussage zu zeigen, und dann die vorderen Aussagen ohne weitere Betrachtung von Elementen zu folgern. $\square$

1.5.11 (**Universelle Eigenschaft von Surjektionen**). Sei $s : X \twoheadrightarrow Y$ eine surjektive Abbildung und $\varphi : X \to Z$ eine beliebige Abbildung. Offensichtlich gibt es genau dann eine Abbildung $\bar{\varphi} : Y \to Z$ mit $\bar{\varphi} \circ s = \varphi$, wenn φ auf den Fasern von s konstant ist. Nach dem Vorhergehenden ist diese Abbildung $\bar{\varphi}$ dann sogar eindeutig bestimmt. Diese Erkenntnis ist insbesondere für die Algebra relevant.

1.5.12. Ist $f : X \xrightarrow{\sim} Y$ eine bijektive Abbildung, so ist offensichtlich die Menge $\{(f(x), x) \in Y \times X \mid x \in X\}$ im Sinne von 1.4.2 eine Abbildung oder, vielleicht klarer, der Graph einer Abbildung $Y \to X$. Diese Abbildung in die Gegenrichtung heißt die **Umkehrabbildung** oder **Umkehrfunktion** auch die **inverse Abbildung** zu f und wird mit $f^{-1} : Y \to X$ bezeichnet. Offensichtlich ist mit f auch f^{-1} eine Bijektion.

1.5.13 (**Diskussion der Notation**). Mit dem vorhergehenden haben wir schon eine dritte mögliche Bedeutung für das Symbol f^{-1} kennengelernt. Was im Einzelfall gemeint ist, gilt es aus dem Kontext zu erschließen.

Beispiel 1.5.14. Die Umkehrabbildung unserer Bijektion $t : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x + 1$ ist die Abbildung $t^{-1} : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x - 1$.

Satz 1.5.15 (Bedeutung der Fakultät). *Sind X und Y zwei Mengen mit je n Elementen, so gibt es genau $n!$ bijektive Abbildungen $f : X \xrightarrow{\sim} Y$.*

Beweis. Sei $X = \{x_1, \ldots, x_n\}$. Wir haben n Möglichkeiten, ein Bild für x_1 auszusuchen, dann noch $(n - 1)$ Möglichkeiten, ein Bild für x_2 auszusuchen, und so weiter, bis schließlich nur noch 1 Element von Y als mögliches Bild von x_n in Frage kommt. Insgesamt gibt es also $n(n-1)\cdots 1 = n!$ Möglichkeiten für f. Da wir $0! = 1$ vereinbart hatten, stimmt unser Satz auch für $n = 0$. □

Übungen

Übung 1.5.16. Gegeben eine Bijektion $f : X \to Y$ ist $g = f^{-1}$ die einzige Abbildung $g : Y \to X$ mit $f \circ g = \mathrm{id}_Y$. Ebenso ist auch $h = f^{-1}$ die einzige Abbildung $h : Y \to X$ mit $h \circ f = \mathrm{id}_X$.

Ergänzende Übung 1.5.17. Gegeben endliche Mengen X, Y gibt es genau $|Y|^{|X|}$ Abbildungen von X nach Y und unter diesen Abbildungen sind genau $|Y|(|Y| - 1)(|Y| - 2) \ldots (|Y| - |X| + 1)$ Injektionen.

Übung 1.5.18. Sind Abbildungen $f : X \to Y$ und $g : Y \to Z$ gegeben, so haben wir $(g \circ f)(A) = g(f(A))$ für jede Teilmenge $A \subset X$ und umgekehrt auch $(g \circ f)^{-1}(C) = f^{-1}(g^{-1}(C))$ für jede Teilmenge $C \subset Z$.

Ergänzende Übung 1.5.19. Sei X eine Menge mit n Elementen und seien natürliche Zahlen $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$ gegeben mit $n = \alpha_1 + \ldots + \alpha_r$. Man zeige: Es gibt genau $n!/(\alpha_1! \cdots \alpha_r!)$ Abbildungen $f : X \to \{1, \ldots, r\}$, die jedes i genau α_i-mal als Wert annehmen, in Formeln

$$\frac{n!}{\alpha_1! \cdots \alpha_r!} = \operatorname{card}\{f \mid |f^{-1}(i)| = \alpha_i \text{ für } i = 1, \ldots r\}$$

Ergänzung 1.5.20. Manche Autoren bezeichnen die Zahlen aus der vorherigen Übung 1.5.19 als **Multinomialkoeffizienten** und verwenden die Notation

$$\binom{n}{\alpha_1; \ldots; \alpha_r} := \frac{n!}{\alpha_1! \cdots \alpha_r!}$$

Mich überzeugt diese Notation nicht, da sie im Gegensatz zur Notation für Binomialkoeffizienten nichts kürzer macht.

Ergänzende Übung 1.5.21. Man zeige die Formel

$$(x_1 + \ldots + x_r)^n = \sum_{\alpha_1 + \ldots + \alpha_r = n} \frac{n!}{\alpha_1! \cdots \alpha_r!} x_1^{\alpha_1} \cdots x_r^{\alpha_r}$$

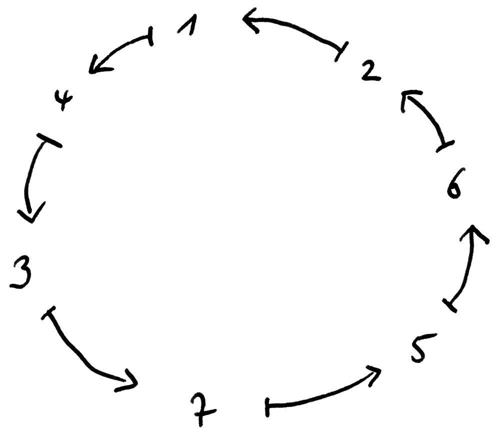
Hier ist zu verstehen, daß wir für alle $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$ mit $\alpha_1 + \ldots + \alpha_r = n$ den angegebenen Ausdruck nehmen und alle diese Ausdrücke aufsummieren.

Ergänzende Übung 1.5.22. Eine **zyklische Anordnung** einer endlichen Menge M ist eine Abbildung $z : M \to M$ derart, daß wir durch mehrmaliges Anwenden von z auf ein beliebiges Element $x \in M$ jedes Element $y \in M$ erhalten können. Man zeige, daß es auf einer n-elementigen Menge mit $n \geq 1$ genau $(n-1)!$ zyklische Anordnungen gibt. Die Terminologie „zyklische Anordnung“ ist etwas unglücklich, da unsere Struktur nun beim besten Willen keine Anordnung im Sinne von [AN1] 2.3 ist. Andererseits ist aber das Angeben einer Anordnung auf einer endlichen Menge M schon auch etwas Ähnliches.

Ergänzende Übung 1.5.23. Sei X eine Menge mit $n \geq 1$ Elementen und sei m eine natürliche Zahl. Man zeige, daß es genau $\binom{n+m-1}{n-1}$ Abbildungen $f : X \to \mathbb{N}$ gibt mit $\sum_{x \in X} f(x) = m$. Hinweis: Man denke sich $X = \{1, 2, \ldots, n\}$ und veranschauliche sich dann f als eine Folge auf $f(1)$ Punkten gefolgt von einem Strich gefolgt von $f(2)$ Punkten gefolgt von einem Strich und so weiter, insgesamt also eine Folge aus $n + m - 1$ Symbolen, davon m Punkten und $n - 1$ Strichen.

1.6 Ergänzungen zur Mengenlehre*

1.6.1 (**Kommutativität kartesischer Produkte**). Ich insistiere darauf, daß gegeben Mengen X, Y die kartesischen Produkte $X \times Y$ und $Y \times X$ für uns verschiedene Mengen sind. Es gibt zwischen diesen kartesischen Produkten zwar die ausgezeichneten Bijektionen $\tau_{X,Y} : X \times Y \xrightarrow{\sim} Y \times X$ mit $(x, y) \mapsto (y, x)$ und $\tau_{Y,X}$ ist stets die Umkehrabbildung zu $\tau_{X,Y}$, aber $\tau_{X,X}$ muß keineswegs die Identität auf X^2 sein, das gilt vielmehr nur für $|X| \leq 1$.



Versuch der graphischen Darstellung einer zyklischen Anordnung auf der Menge $\{1, 2, \ldots, 7\}$. Die Pfeile $\mapsto$ sollen jeweils den Effekt der Abbildung z veranschaulichen.

x	1	2	3	4	5	6
f(x)	2	0	0	4	4	0

11 4444 5555

• • | | | • • • • | • • • • |

Eine Abbildung $f : \{1, 2, \ldots, n\} \to \mathbb{N}$ im Fall $n = 6$ mit Wertesumme $m = 10$ und die Veranschaulichung nach der Vorschrift aus Übung 1.5.23 als Folge bestehend aus m Punkten und $n - 1$ Strichen.

Vorschau 1.6.2. In [AL] 5.3.6 zeigen wir den Satz von Schröder-Bernstein: Sind X und Y Mengen und gibt es sowohl eine Injektion $f : X \hookrightarrow Y$ als auch eine Injektion $g : Y \hookrightarrow X$, so gibt es sogar eine Bijektion $b : X \xrightarrow{\sim} Y$.

Definition 1.6.3. Die Menge aller Abbildungen von X nach Y bezeichne ich mit

$$\mathrm{Ens}(X, Y)$$

nach der französischen Übersetzung **ensemble** des deutschen Begriffs „Menge".

1.6.4 (**Diskussion der Terminologie**). Üblicher ist statt unserem $\mathrm{Ens}(X, Y)$ die Notation Y^X. Noch gebräuchlicher ist in der deutschen Literatur die Bezeichnung $\mathrm{Abb}(X, Y)$ für die Menge aller Abbildungen von X nach Y. Ich will jedoch in [LA2] 7.1.4 die „Kategorie aller Mengen" wie Gabriel [Gab62] mit Ens bezeichnen und für je zwei Objekte X, Y einer Kategorie $\mathcal{C}$ die Menge aller „Morphismen" von X nach Y mit $\mathcal{C}(X, Y)$. Das erklärt die hier gewählte Bezeichnung für Mengen von Abbildungen.

1.6.5 (**Exponentialgesetz**). Gegeben drei Mengen X, Y, Z erhalten wir eine Bijektion

$$\mathrm{Ens}(X \times Y, Z) \xrightarrow{\sim} \mathrm{Ens}(X, \mathrm{Ens}(Y, Z))$$

durch die Vorschrift $f \mapsto f(x, \ )$ mit der Notation $f(x, \ )$ für die Abbildung $y \mapsto f(x, y)$. Etwas vage formuliert ist also eine Abbildung $X \times Y \to Z$ von einem kartesischen Produkt $X \times Y$ in eine weitere Menge Z dasselbe wie eine Abbildung, die jedem $x \in X$ eine Abbildung $Y \to Z$ zuordnet, und umgekehrt natürlich auch dasselbe wie eine Abbildung, die jedem $y \in Y$ eine Abbildung $X \to Z$ zuordnet. In der exponentiellen Notation liest sich das besonders suggestiv als kanonische Bijektion $Z^{(X \times Y)} \xrightarrow{\sim} (Z^X)^Y$. Wegen dieser Notation zitiert man diese Aussage auch als das **Exponentialgesetz**. In wieder anderen Worten sind also die in der Schule derzeit so beliebten „Funktionen mit Parameter" nichts anderes als „Funktionen von zwei Variablen, bei denen eine der beiden Variablen als Parameter bezeichnet wird".

Vorschau 1.6.6. Später bezeichnen wir eine Abbildung $X \times Y \to Z$ auch als eine 2-**Multiabbildung** und notieren sie $X \curlyvee Y \to Z$ mit dem als reinem Trenner zu verstehenden Symbol $\curlyvee$ und erklären allgemeiner „r-Multiabbildungen" für beliebiges $r \in \mathbb{N}$ sowie deren „Multiverknüpfung", aber alles zu seiner Zeit.

Ergänzung 1.6.7 (**Unmögliche Surjektionen**). Eine Abbildung $f : X \to \mathcal{P}(X)$ von einer Menge in ihre Potenzmenge kann nie surjektiv sein. In der Tat, betrachten wir in X die Teilmenge $A = \{x \in X \mid x \notin f(x)\}$, so kann es kein $y \in X$ geben mit $f(y) = A$, denn für solch ein y hätten wir entweder $y \in A$ oder $y \notin A$, und aus $y \in A$ alias $y \in f(y)$ folgte $y \notin A$, wohingegen aus $y \notin A$ alias $y \notin f(y)$ folgte $y \in A$. Ordnen wir etwa jedem Menschen die Menge aller der Menschen zu, die er liebt, und betrachten die Menge aller Menschen, die sich nicht selbst lieben, so wird diese Menge für keinen Menschen genau aus all den Menschen bestehen, die er liebt.

Ergänzung 1.6.8. Gegeben eine Menge X mag man sich eine Abbildung $X \to \mathbb{N}$ veranschaulichen als eine „Menge von Elementen von X, in der jedes Element mit einer wohlbestimmten Vielfachheit vorkommt“. Aufgrund dieser Vorstellung nennen wir eine Abbildung $X \to \mathbb{N}$ auch eine **Multimenge** von Elementen von X. Unter der **Kardinalität einer Multimenge** verstehen wir die Summe über die Werte der entsprechenden Abbildung an allen Stellen $x \in X$, aufgefaßt als ein Element von $\mathbb{N} \sqcup \{\infty\}$. Ich notiere Multimengen durch Mengenklammern mit einem vorgestellten unteren Index μ. So wäre etwa ${}_{\mu}\{5, 5, 5, 7, 7, 1\}$ eine Multimenge von natürlichen Zahlen der Kardinalität 6. Diese Notation ist aber nicht gebräuchlich. Die Gesamtheit aller endlichen Multimengen von Elementen einer Menge X notiere ich auch $\mathbb{N}X$. Eine Multimenge der Kardinalität Zwei von Elementen einer Menge X nenne ich ein **ungeordnetes Paar** von Elementen von X.

1.6.9. Gegeben $S \supset T$ eine Menge mit einer Teilmenge und $f : S \to S$ eine Selbstabbildung von S sagen wir, T sei **stabil unter** f und f **stabilisiert** T, wenn gilt $f(T) \subset T$. Gilt sogar $f(T) = T$, so sagen wir, T **werde von** f **festgehalten**. Gilt noch stärker $f(t) = t \ \forall t \in T$, so sagen wir, T **werde von** f **punktweise festgehalten**.

Beispiel 1.6.10. Für jede Menge X mag man die **Mengenabbildung** $X \hookrightarrow \mathcal{P}(X)$, $x \mapsto \{x\}$ betrachten. Ihr Bild ist die Menge

$$\mathcal{P}_1(X) \subset \mathcal{P}(X)$$

aller einelementigen Teilmengen von X. Die Umkehrabbildung der so entstehenden Bijektion $X \xrightarrow{\sim} \mathcal{P}_1(X)$ notieren wir $\mathrm{elt} : \mathcal{P}_1(X) \to X$ und nennen sie die **Elementabbildung**. Sie ordnet jeder einelementigen Teilmenge von X ihr einziges Element zu.

Vorschau 1.6.11 (**Formalisierung des Begriffs der natürlichen Zahlen**). Wir werden in [LA1] 4.1 zeigen, daß es Paare (N, s) gibt bestehend aus einer Menge N und einer injektiven Abbildung $s : N \to N$ derart, daß $N \backslash s(N)$ aus genau einem Element o besteht und daß jede s-stabile Teilmenge von N, die o enthält, bereits ganz N sein muß. Weiter werden wir zeigen, daß solch ein Paar im Wesentlichen eindeutig bestimmt ist in dem Sinne, daß es für jedes weitere derartige Paar (N', s') genau eine Bijektion $\varphi : N \xrightarrow{\sim} N'$ gibt mit $s'\varphi = \varphi s$. Im Rahmen der ganz naiven Mengenlehre kann man solch ein Paar unmittelbar angeben als $(\mathbb{N}, s)$ mit $s : n \mapsto (n + 1)$. Bei einem etwas formaleren Aufbau der Mathematik aus der Mengenlehre mag man umgekehrt von derartigen Paaren ausgehen und so zu einer Definition von $\mathbb{N}$ und der Addition auf $\mathbb{N}$ gelangen, vergleiche [LA1] 4.1 folgende. Hier liegt auch der Schlüssel für eine formale Rechtfertigung des Prinzips der vollständigen Induktion.

Vorschau 1.6.12. Sie sehen bereits an dieser Stelle, wie problematisch der Begriff der Gleichheit im Grunde genommen ist und wie nah er an der Wurzel mathematischen Denkens liegt. Um ein besonders einfaches Beispiel zu bemühen, mag man sich fragen, ob je zwei einelementige Mengen gleich sind. Unsere Antwort hier muß lauten: Natürlich nicht, zwei einelementige Teilmengen einer gegebenen Menge etwa sind genau dann gleich, wenn sie dasselbe Element enthalten. Allerdings gibt es andererseits zwischen je zwei einelementigen Mengen genau eine Bijektion, eine einelementige Menge ist also „eindeutig bis auf eindeutige Bijektion".

Übungen

Ergänzende Übung 1.6.13. Gegeben eine fest gedachte Menge Y können wir für jede weitere Menge A eine Abbildung $\mathrm{ev}_A : A \to \mathrm{Ens}(\mathrm{Ens}(A, Y), Y)$, genannt die **Evaluations-** oder **Auswertungsabbildung**, erklären durch die Vorschrift $\mathrm{ev}_A : a \mapsto (f \mapsto f(a))$. Man zeige, daß für jede Menge X die Komposition

$$\mathrm{Ens}(X, Y) \to \mathrm{Ens}(\mathrm{Ens}(\mathrm{Ens}(X, Y), Y), Y) \to \mathrm{Ens}(X, Y)$$

von $\mathrm{ev}_{\mathrm{Ens}(X,Y)}$ mit dem Vorschalten $(\circ\, \mathrm{ev}_X)$ von ev_X die Identität auf $\mathrm{Ens}(X, Y)$ ist. Später werden Sie diese Aussage möglicherweise als die „Dreiecksidentität" im Kontext „adjungierter Funktoren" in [TF] 4.8.1 verstehen lernen.

1.7 Logische Symbole und Konventionen

1.7.1. In der mathematischen Fachsprache meint **oder** immer, daß auch beides erlaubt ist. Wir haben diese Konvention schon benutzt bei der Definition der Vereinigung in 1.3.1 durch die Vorschrift $X \cup Y = \{z \mid z \in X \text{ oder } z \in Y\}$. Zum Beispiel haben wir $\{1, 2\} \cup \{2, 3\} = \{1, 2, 3\}$. In diesem Zusammenhang muß ich die schöne Geschichte erzählen von dem Logiker, der seinem Freund erzählt, er habe ein Kind bekommen. Der Freund fragt: „Ist es ein Junge oder ein Mädchen?" worauf der Logiker antwortet: „Ja!"

Ergänzung 1.7.2 (**Herkunft des Vereinigungssymbols**). In den „Arithmetes principia" von Guiseppe Peano scheint das Symbol $\cup$ zum ersten Mal vorzukommen, allerdings als Symbol für „oder". Peano schreibt: „Signum $\cup$ legitur *vel*" und „vel" heißt „oder" auf lateinisch. Der Kontext legt nahe, daß $\cup$ an den Buchstaben v erinnern soll. Das Symbol $\vee$ hatte Peano schon als Symbol für „verum" verbraucht.

In der Bedeutung der Vereinigung zweier Mengen habe ich das Symbol zuerst bei Bourbaki gesehen.

1.7.3. Sagt man der mathematischen Fachsprache, es gebe ein Objekt mit diesen und jenen Eigenschaften, so ist stets gemeint, daß es *mindestens ein* derartiges Objekt geben soll. Hätten wir diese Sprachregelung rechtzeitig vereinbart, so hätten wir zum Beispiel das Wörtchen „mindestens" in Teil 2 von 1.5.4 bereits weglassen können. Sagt ihnen also ein Mathematiker, er habe einen Bruder, so kann es auch durchaus sein, daß er noch weitere Brüder hat! Will man in der mathematischen Fachsprache Existenz und Eindeutigkeit gleichzeitig ausdrücken, so sagt man, es gebe **genau ein** Objekt mit diesen und jenen Eigenschaften. Sagt ihnen also ein Mathematiker, er habe genau einen Bruder, so können sie sicher sein, daß er nicht noch weitere Brüder hat.

1.7.4. Die folgenden Abkürzungen erweisen sich als bequem und werden häufig verwendet:

$\forall$	für alle (ein umgedrehtes A wie „alle")
$\exists$	es gibt (ein umgedrehtes E wie „existiert")
$\exists!$	es gibt genau ein
$\ldots \Rightarrow \cdots$	aus ... folgt $\cdots$
$\ldots \Leftarrow \cdots$	... folgt aus $\cdots$
$\ldots \Leftrightarrow \cdots$	... ist gleichbedeutend zu $\cdots$

Ist zum Beispiel $f : X \to Y$ eine Abbildung, so können wir unsere Definitionen injektiv, surjektiv, und bijektiv etwas formaler so schreiben:

$$\begin{array}{lcl} f \text{ injektiv} & \Leftrightarrow & ((f(x) = f(z)) \Rightarrow (x = z)) \\ f \text{ surjektiv} & \Leftrightarrow & \forall y \in Y \exists x \in X \text{ mit } f(x) = y \\ f \text{ bijektiv} & \Leftrightarrow & \forall y \in Y \exists! x \in X \text{ mit } f(x) = y \end{array}$$

1.7.5. In den Zeiten des Bleisatzes war es nicht einfach, neue Symbole in Druck zu bringen. Irgendwelche Buchstaben verdreht zu setzen, war jedoch unproblematisch. So entstanden die Symbole $\forall$ und $\exists$. Sie heißen **Quantoren**.

1.7.6. Bei den „für alle" und „es gibt" kommt es in der mathematischen Fachsprache, anders als in der weniger präzisen Umgangssprache, entscheidend auf die Reihenfolge an. Man betrachte zum Beispiel die beiden folgenden Aussagen:

„Für alle $n \in \mathbb{N}$ gibt es $m \in \mathbb{N}$ so daß gilt $m \geq n$"

„Es gibt $m \in \mathbb{N}$ so daß für alle $n \in \mathbb{N}$ gilt $m \geq n$"

Offensichtlich ist die Erste richtig, die Zweite aber falsch. Weiter mache man sich klar, daß die „für alle" und „es gibt" bei Verneinung vertauscht werden. Äquivalent sind zum Beispiel die beiden folgenden Aussagen

„Es gibt kein $n \in \mathbb{N}$ mit $n^2 = 2$“

„Für alle $n \in \mathbb{N}$ gilt nicht $n^2 = 2$“

1.7.7. Wollen wir zeigen, daß aus einer Aussage A eine weitere Aussage B folgt, so können wir ebensogut zeigen: Gilt B nicht, so gilt auch A nicht. In formelhafter Schreibweise haben wir also

$$(A \Rightarrow B) \Leftrightarrow ((\text{nicht } B) \Rightarrow (\text{nicht } A))$$

Wollen wir zum Beispiel zeigen $(g \circ f \text{ surjektiv}) \Rightarrow (g \text{ surjektiv})$, so reicht es, wenn wir uns überlegen: Ist g nicht surjektiv, so ist $g \circ f$ erst recht nicht surjektiv. Oder ein Beispiel aus dem täglichen Leben: Die Aussage (Wenn ein Mensch ein Kind gebiert, ist er eine Frau) ist gleichbedeutend zur Aussage (Wenn ein Mensch keine Frau ist, gebiert er auch keine Kinder). Nicht folgern kann man dahingegen die Aussage (Wenn ein Mensch kein Kind gebiert, ist er keine Frau).

1.7.8. In der Literatur findet man oft die Abkürzung **oBdA** für „ohne Beschränkung der Allgemeinheit“.

2 Algebraische Grundbegriffe

Auf der Schule versteht man unter einer „reellen Zahl“ meist einen unendlichen Dezimalbruch, wobei man noch aufpassen muß, daß verschiedene unendliche Dezimalbrüche durchaus dieselbe reelle Zahl darstellen können, zum Beispiel gilt in den reellen Zahlen ja

$$0{,}99999\ldots = 1{,}00000\ldots$$

Diese reellen Zahlen werden dann addiert, subtrahiert, multipliziert und dividiert ohne tiefes Nachdenken darüber, wie man denn zum Beispiel mit den eventuell unendlich vielen Überträgen bei der Addition und Subtraktion umgehen soll, und warum dann Formeln wie $(a+b)-c = a+(b-c)$ wirklich gelten, zum Beispiel für $a = b = c = 0{,}999\ldots$. Dieses tiefe Nachdenken wollen wir im Folgenden vom Rest der Vorlesung abkoppeln und müssen dazu sehr präzise formulieren, welche Eigenschaften für die Addition, Multiplikation und Anordnung in „unseren“ reellen Zahlen gelten sollen. In der Terminologie, die in den folgenden Abschnitten eingeführt wird, werden wir die reellen Zahlen charakterisieren als einen angeordneten Körper, in dem jede nichtleere Teilmenge mit einer unteren Schranke sogar eine größte untere Schranke besitzt. Von dieser Charakterisierung ausgehend erklären wir dann, welche reelle Zahl ein gegebener unendlicher Dezimalbruch darstellt, und errichten das Gebäude der Analysis. In demselben Begriffsgebäude modellieren wir auch den Anschauungsraum, vergleiche [LA1] 3.1.9 und [LA2] 1.6.4. Um diese Charakterisierungen und Modellierungen verständlich zu machen, führen wir zunächst einige grundlegende algebraische Konzepte ein, die Ihnen im weiteren Studium der Mathematik noch oft begegnen werden.

2.1 Mengen mit Verknüpfung

Definition 2.1.1. Eine **Verknüpfung** $\top$ **auf einer Menge** X ist eine Abbildung

$$\begin{array}{ccc} X \times X & \to & X \\ (x, y) & \mapsto & x \top y \end{array}$$

Jedem angeordneten Paar (x, y) mit $x, y \in X$ wird also ein Element $(x \top y) \in X$ zugeordnet.

2.1.2. Das unverfängliche Symbol $\top$ benutze ich, um mich an dieser Stelle noch nicht implizit auf einen der Standardfälle Addition oder Multiplikation festlegen zu müssen. Das Wort „Verknüpfung“ erhält damit eine gegenüber 1.5.1 erweiterte Bedeutung: Statt der Verknüpfung von zwei Abbildungen kann damit auch allgemeiner eine abstrakte Verknüpfung auf einer beliebigen Menge gemeint sein. Was im Einzelfall gemeint ist, gilt es aus dem Kontext zu erschließen.

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	1	1	1
2	0	1	2	2	2
3	0	1	2	3	3
4	0	1	2	3	4

Man kann Verknüpfungen auf endlichen Mengen darstellen durch ihre **Verknüpfungstafel**. Hier habe ich etwa die Verknüpfungstafel der Verknüpfung $\min$ auf der Menge $\{0, 1, 2, 3, 4\}$ angegeben. Eigentlich muß man sich dazu einigen, ob im Kästchen aus der Spalte m und der Zeile n nun $m \top n$ oder vielmehr $n \top m$ stehen soll, aber bei einer kommutativen Verknüpfung wie $\min$ kommt es darauf zum Glück nicht an.

und	Wahr	Falsch
Wahr	Wahr	Falsch
Falsch	Falsch	Falsch

oder	Wahr	Falsch
Wahr	Wahr	Wahr
Falsch	Wahr	Falsch

Die Wahrheitstafeln für „und“ und „oder“. Gemeint ist hier wie stets in der Mathematik das „nichtausschließende oder“. Sagen wir, es gelte A oder B, so ist insbesondere auch erlaubt, daß beides gilt. Bei der Wahrheitstafel für das „ausschließende oder“ müßte oben links als Verknüpfung von „Wahr“ mit „Wahr“ ein „Falsch“ stehen.

Beispiele 2.1.3. 1. Die Addition von ganzen Zahlen ist eine Verknüpfung

$$\begin{array}{rcl} \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ (m, n) & \mapsto & m + n \end{array}$$

2. Die Multiplikation von ganzen Zahlen ist eine Verknüpfung

$$\begin{array}{rcl} \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ (m, n) & \mapsto & m \cdot n \end{array}$$

3. Die Zuordnung $\min$, die jedem Paar von natürlichen Zahlen die kleinere zuordnet, wenn sie verschieden sind, und eben diese Zahl $\min(n, n) = n$, wenn sie gleich sind, ist eine Verknüpfung

$$\begin{array}{rrcl} \min: & \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \\ & (m, n) & \mapsto & \min(m, n) \end{array}$$

4. Eine Abbildung $Z \to Z$ von einer Menge Z in sich selbst nennen wir eine **Selbstabbildung von** Z. Wir kürzen die Menge aller Selbstabbildungen einer Menge Z Z mit $\operatorname{Ens}(Z) := \operatorname{Ens}(Z, Z)$ ab. Die Verknüpfung von Abbildungen liefert eine Verknüpfung auf der Menge $\operatorname{Ens}(Z)$ aller Selbstabbildungen von Z, in Formeln

$$\begin{array}{rcl} \operatorname{Ens}(Z) \times \operatorname{Ens}(Z) & \to & \operatorname{Ens}(Z) \\ (f, g) & \mapsto & f \circ g \end{array}$$

5. Die Subtraktion von ganzen Zahlen ist eine Verknüpfung

$$\begin{array}{rcl} \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ (m, n) & \mapsto & m - n \end{array}$$

6. Jede Verknüpfung $\top$ auf einer Menge induziert eine Verknüpfung auf ihrer Potenzmenge vermittels der Vorschrift

$$U \top V := \{u \top v \mid u \in U,\ v \in V\}$$

7. Gegeben Mengen mit Verknüpfung $(X, \top)$ und $(Y, \perp)$ erklären wir die **komponentenweise Verknüpfung** auf ihrem Produkt $X \times Y$ durch die Vorschrift $((x, y), (x', y')) \mapsto ((x \top x'), (y \perp y'))$.

8. Logische Operationen wie „und“, „oder“, „impliziert“ können als Verknüpfungen auf der zweielementigen Menge $\{\mathrm{Wahr}, \mathrm{Falsch}\}$ aufgefaßt werden. Die zugehörigen Verknüpfungstabellen heißen **Wahrheitstafeln**. Bei einem formalen Zugang werden diese Tafeln, wie sie für „und“ und „oder“ auf der vorhergehenden Seite zu finden sind, zur Definition der jeweiligen Begriffe.

2.1.4. Sei $(X, \top)$ eine Menge mit Verknüpfung.

1. Gegeben Elemente $a, b \in X$ sagen wir, a ist ein **Linksteiler** von b, wenn es $d \in X$ gibt mit $a \top d = b$. Analog erklären wir **Rechtsteiler**;

2. Ein Element $a \in X$ heißt **linkskürzbar**, wenn die Verknüpfung mit a eine Injektion $(a\cdot) : X \hookrightarrow X$ liefert. Analog erklären wir die Eigenschaft **rechtskürzbar**. Ein Element, das linkskürzbar und rechtskürzbar ist, nennen wir **kürzbar**. Ein nicht kürzbares Element nennen wir **nichtkürzbar**.

Beispiel 2.1.5. Die kürzbaren Elemente von $(\mathbb{Z}, \cdot)$ sind alle von Null verschiedenen Elemente. In $(\mathbb{Z}, +)$ sind alle Elemente kürzbar. Die linkskürzbaren Elemente von $\mathrm{Ens}(Z)$ sind die Surjektionen. Die rechtskürzbaren Elemente von $\mathrm{Ens}(Z)$ sind die Injektionen.

2.1.6. Sei $(X, \top)$ eine Menge mit Verknüpfung. Eine Teilmenge $U \subset X$ heißt **abgeschlossen unter der Verknüpfung**, wenn aus $x, y \in U$ folgt $x \top y \in U$. Natürlich ist in diesem Fall auch $(U, \top)$ eine Menge mit Verknüpfung. Man spricht dann von der **auf U induzierten Verknüpfung**. Zum Beispiel ist $\mathbb{N} \subset \mathbb{Z}$ abgeschlossen unter der Addition, aber $\mathbb{Z}\backslash\{0\} \subset \mathbb{Q}\backslash\{0\}$ ist nicht abgeschlossen unter der durch die Division gegebenen Verknüpfung $(m, n) \mapsto m/n$.

Definition 2.1.7. Eine Verknüpfung $\top$ auf einer Menge X heißt **assoziativ**, wenn gilt $x \top (y \top z) = (x \top y) \top z \ \forall x, y, z \in X$. Sie heißt **kommutativ** oder **abelsch**, wenn gilt $x \top y = y \top x \ \forall x, y \in X$. Gilt für zwei vorgegebene Elemente die Identität $x \top y = y \top x$, so sagen wir, daß diese beiden Elemente **kommutieren**.

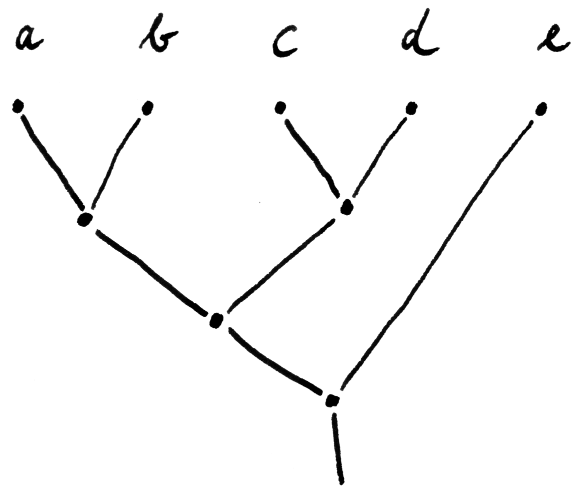
2.1.8 (**Diskussion der Terminologie**). Die Bezeichnung „abelsch" ehrt den norwegischen Mathematiker Nils Henrik Abel.

Beispiele 2.1.9. Von unseren Beispielen sind die ersten Drei assoziativ und kommutativ, das Vierte ist assoziativ aber nicht kommutativ falls Z mehr als ein Element hat, das Fünfte ist weder assoziativ noch kommutativ.

2.1.10. Ist eine Verknüpfung $\top$ auf einer Menge A assoziativ, so liefern auch ungeklammerte Ausdrücke der Form $a_1 \top a_2 \top \ldots \top a_n$ wohlbestimmte Elemente von A, und zwar ist genauer das Resultat unabhängig davon, wie wir die Klammern setzen. Um diese Erkenntnis zu formalisieren, vereinbaren wir für einen ungeklammerten Ausdruck die „von hinten hochgeklammerte" Interpretation

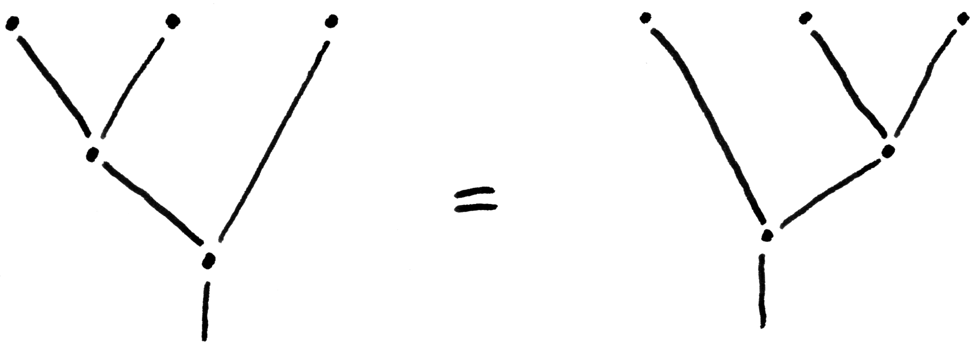
$$a_1 \top a_2 \top \ldots \top a_n := a_1 \top (a_2 \top (\ldots (a_{n-1} \top a_n) \ldots))$$

und zeigen dann das folgende Lemma.



$$((a \top b) \top (c \top d)) \top e$$

Mögliche „Klammerungen“ mag man sich graphisch wie oben angedeutet veranschaulichen. Die Assoziativität bedeutet dann graphisch so etwas wie



Das Gleichheitszeichen meint nur, daß beide Klammerungen stets dasselbe liefern, wenn wir oben drei Elemente unserer Menge mit Verknüpfung einfüllen.

Lemma 2.1.11 (Assoziativität macht Klammern überflüssig). *Gegeben eine Menge mit einer assoziativen Verknüpfung* $(A, \top)$ *und* $a_1, \ldots, a_n, b_1, \ldots, b_m \in A$ *gilt mit der von hinten hochgeklammerten Interpretation für ungeklammerte Ausdrücke*

$$(a_1 \top \ldots \top a_n) \top (b_1 \top \ldots \top b_m) = a_1 \top \ldots \top a_n \top b_1 \top \ldots \top b_m$$

Beweis. Wir folgern mit den Definitionen für die erste Gleichheit und dem Assoziativgesetz für die zweite Gleichheit die Identität

$$\begin{array}{rcl} (a_1 \top \ldots \top a_n) \top (b_1 \top \ldots \top b_m) & = & (a_1 \top (a_2 \top \ldots \top a_n)) \top (b_1 \top \ldots \top b_m) \\ & = & a_1 \top ((a_2 \top \ldots \top a_n) \top (b_1 \top \ldots \top b_m)) \end{array}$$

und sind fertig mit vollständiger Induktion über n. □

2.1.12. Das Wort „Lemma“, im Plural „Lemmata“, kommt vom griechischen Wort $\lambda\alpha\mu\beta\alpha\nu\epsilon\iota\nu$ für „nehmen“ und bezeichnet in der Mathematik kleinere Resultate oder auch Zwischenschritte von größeren Beweisen, denen der Autor außerhalb ihres engeren Kontexts keine größere Bedeutung zumißt.

Vorschau 2.1.13. Die Zahl der Möglichkeiten, einen Ausdruck in $n+1$ Faktoren so zu klammern, daß in jedem Schritt nur die Verknüpfung von je zwei Elementen zu berechnen ist, heißt die **n-te Catalan-Zahl** und wird C_n notiert. Die ersten Catalan-Zahlen sind $C_0 = C_1 = 1$, $C_2 = 2$ und $C_3 = 5$: Die fünf möglichen Klammerungen von 4 Elementen sind etwa $(ab)(cd)$, $a(b(cd))$, $a((bc)d)$, $((ab)c)d$ und $(a(bc))d$. Im allgemeinen zeigen wir in [AN1] 6.3.8, daß sich die Catalan-Zahlen durch die Binomial-Koeffizienten [EIN] 1.1.17 ausdrücken lassen vermittels der amüsanten Formel

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$

2.1.14. Gegeben eine Menge mit assoziativer und kommutativer Verknüpfung $(A, \top)$ kommt es beim Verknüpfen noch nicht einmal auf die Reihenfolge an. Sind genauer $a_1, \ldots, a_n$ mit $n \geq 1$ gegeben und ist $\sigma : \{1, \ldots, n\} \xrightarrow{\sim} \{1, \ldots, n\}$ eine bijektive Abbildung, so gilt

$$a_1 \top \ldots \top a_n = a_{\sigma(1)} \top \ldots \top a_{\sigma(n)}$$

Wir betrachten das als offensichtlich und schreiben keinen Beweis aus.

Definition 2.1.15 (Iterierte Verknüpfungen). Sei $(X, \top)$ eine Menge mit Verknüpfung. Ist $n \in \{1, 2, \ldots\}$ eine von Null verschiedene natürliche Zahl und $x \in X$, so schreiben wir

$$\underbrace{x \top x \top \ldots \top x}_{n\text{-mal}} =: n^{\top} x$$

Ich erinnere daran, daß wir in 2.1.10 für derartige Ausdrücke im Zweifelsfall die Interpretation als „von hinten hochgeklammerte Verknüpfung“ vereinbart hatten.

2.1.16. Wird unsere Verknüpfung $+$ notiert, so schreibt man statt n^+x meist kurz nx. Wird unsere Verknüpfung mit einem runden Symbol wie etwa $*$ notiert, so schreibt man statt n^*x meist kurz x^n oder etwas ausführlicher x^{*n} oder $x^{(*n)}$.

2.1.17 (**Iterationsregeln**). Sei $(A, \top)$ eine Menge mit assoziativer Verknüpfung. Sind m, n zwei von Null verschiedene natürliche Zahlen, so erhalten wir mithilfe unseres Lemmas 2.1.11 zur Überflüssigkeit von Klammern bei assoziativen Verknüpfungen die Regeln $(n + m)^\top a = (n^\top a)\top(m^\top a)$ und $(nm)^\top a = n^\top(m^\top a)$. Ist unsere Verknüpfung außerdem auch noch kommutativ, so gilt zusätzlich die Regel $n^\top(a\top b) = (n^\top a)\top(n^\top b)$. Wenn man es ganz genau nimmt, muß man für einen formalen Beweis die formale Einführung der natürlichen Zahlen [LA1] 4.1.5 abwarten, wo Sie das dann als Übung [LA1] 4.1.39 behandeln dürfen.

Definition 2.1.18. Gegeben eine Menge mit Verknüpfung $(X, \top)$ heißt ein Element $e \in X$ ein **neutrales Element** von $(X, \top)$, wenn gilt

$$e\top x = x\top e = x \quad \forall x \in X$$

2.1.19 (**Eindeutigkeit neutraler Elemente**). In einer Menge mit Verknüpfung $(X, \top)$ kann es höchstens ein neutrales Element e geben, denn für jedes weitere Element e' mit $e'\top x = x\top e' = x \quad \forall x \in X$ haben wir $e' = e'\top e = e$. Wir dürfen also den bestimmten Artikel verwenden und in einer Menge mit Verknüpfung von *dem* neutralen Element reden und es mit e_X bezeichnen.

Definition 2.1.20. Ein **Monoid** ist eine Menge mit einer assoziativen Verknüpfung, in der es ein neutrales Element gibt.

2.1.21. Das Wort „Monoid“ ist wohl von griechisch „$\mu o\nu o\varsigma$“ für „allein“ abgeleitet: Ein Monoid besitzt nur eine einzige Verknüpfung. Für ein kommutatives Monoid schlage ich die abkürzende Bezeichnung **Abmonoid** vor, mit der Vorsilbe „Ab“ für „abelsch“.

2.1.22 (**Additiv und multiplikativ notierte Monoide**). Notiert man in einem Monoid M die Verknüpfung mit dem Symbol $+$, so notiert man das neutrale Element meist 0_M oder abkürzend 0 und nennt es das **Null-Element** oder abkürzend die **Null** und spricht von einem **additiv notierten Monoid**. Nur kommutative Monoide werden additiv notiert. Notiert man in einem Monoid M die Verknüpfung mit einem eher runden Symbol wie $\cdot$ oder $\circ$ oder $*$ oder auch einfach durch Hintereinanderschreiben, so notiert man das neutrale Element oft 1_M oder abkürzend 1 und nennt es das **Eins-Element** oder abkürzend die **Eins** und spricht von einem **multiplikativ notierten Monoid**.

Beispiele 2.1.23. Die natürlichen Zahlen bilden mit der Addition ein Monoid $(\mathbb{N}, +)$ mit neutralem Element 0. Sie bilden auch mit der Multiplikation ein Monoid $(\mathbb{N}, \cdot)$ mit neutralem Element 1. Für jede Menge Z ist die Menge $\operatorname{Ens}(Z)$ der Selbstabbildungen von Z mit der Verknüpfung $\circ$ von Abbildungen als Verknüpfung ein Monoid mit neutralem Element id_Z. Die leere Menge ist *kein* Monoid, ihr fehlt das neutrale Element. Jede einelementige Menge ist mit der einzig möglichen Verknüpfung ein Monoid.

2.1.24 (**Nullfach iterierte Verknüpfung in Monoiden**). Ist $(M, \top)$ ein Monoid, so erweitern wir unsere Notation $n^{\top}a$ aus 2.1.15 auf alle natürlichen Zahlen $n \in \mathbb{N}$, indem wir

$$0^{\top}a := e_M$$

als das neutrale Element e_M von M verstehen, für alle $a \in M$. Damit gelten unsere Iterationsregeln 2.1.17 dann sogar für alle $n, m \in \mathbb{N}$, vergleiche [LA1] 4.1.29.

2.1.25 (**Notationen für nullfach iterierte Verknüpfung**). Sei ein Monoid M gegeben. Wird seine Verknüpfung $+$ notiert, so schreibt man auch für $n = 0$ statt $n^{+}x$ meist kurz nx und meint also mit $0x$ das neutrale Element von M, in Formeln

$$0x := 0_M$$

Wird seine Verknüpfung mit einem runden Symbol wie etwa $*$ notiert, so schreibt man auch für $n = 0$ statt $n^{*}x$ meist kurz x^n oder etwas ausführlicher x^{*n} oder $x^{(*n)}$ und meint insbesondere mit x^0 das neutrale Element von M, in Formeln

$$x^0 := 1_M$$

2.1.26 (**Summen- und Produktzeichen**). Gegeben eine Abbildung $I \to M$, $i \mapsto a_i$ von einer endlichen Menge in ein additiv beziehungsweise multiplikativ notiertes Abmonoid M vereinbaren wir die Notationen

$$\sum_{i \in I} a_i \qquad \text{beziehungsweise} \qquad \prod_{i \in I} a_i$$

für die „Verknüpfung aller a_i mit $i \in I$“. Ist I die leere Menge, so vereinbaren wir, daß dieser Ausdruck das neutrale Element von M bedeuten möge, also 0 beziehungsweise 1. Für die konstante Abbildung $I \to \mathbb{N}$, $i \mapsto 1$ haben wir zum Beispiel

$$\sum_{i \in I} 1 = |I|$$

Unsere Konvention [EIN] 1.1.14 für mit einem Laufindex notierte Summen beziehungsweise Produkte verwenden wir bei kommutativen Monoiden analog.

Ergänzung 2.1.27. Gegeben eine Menge mit Verknüpfung $(M, \top)$ kann man die Assoziativität und die Existenz eines neutralen Elements dahingehend zusammenfassen, daß wir für jedes $r \geq 0$ ausgezeichnete „Multiverknüpfungen“ $M^{\times r} \to M$ zur Verfügung haben, die eine gewisse „Multiassoziativität“ erfüllen, die ich hier nicht genauer ausschreiben will. Das neutrale Element ist dabei die „Multiverknüpfung des Nulltupels“. In diesem Licht betrachtet gehören bei einer Verknüpfung die Forderungen der Assoziativität und der Existenz eines neutralen Elements zusammen. Ich schlage vor, eine Verknüpfung mit diesen beiden Eigenschaften **unitärassoziativ** zu nennen. Ein Monoid ist damit eine Menge mit einer unitärassoziativen Verknüpfung.

Übungen

Übung 2.1.28. Sei Z eine Menge. Das Schneiden von Teilmengen ist eine Verknüpfung

$$\begin{array}{rccc} \cap : & \mathcal{P}(Z) \times \mathcal{P}(Z) & \to & \mathcal{P}(Z) \\ & (A, B) & \mapsto & A \cap B \end{array}$$

auf der Potenzmenge. Dasselbe gilt für die Vereinigung und das Bilden der Differenzmenge. Welche dieser Verknüpfungen sind kommutativ oder assoziativ? Welche besitzen neutrale Elemente?

Ergänzende Übung 2.1.29. Man gebe die Wahrheitstafeln für $\Rightarrow$ und $\Leftrightarrow$ an. Bezeichne weiter $\neg : \{\mathrm{Wahr}, \mathrm{Falsch}\} \to \{\mathrm{Wahr}, \mathrm{Falsch}\}$ die „Verneinung“. Man zeige, daß die Formel

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

beim Einsetzen beliebiger Wahrheitswerte aus $\{\mathrm{Wahr}, \mathrm{Falsch}\}$ für A und B stets den Wert Wahr ausgibt, in Übereinstimmung mit unseren eher intuitiven Überlegungen in 1.7.7.

2.2 Gruppen

2.2.1. Ich empfehle, bei der Lektüre dieses Abschnitts die Tabelle nach 2.2.13 gleich mitzulesen, die die Bedeutungen der nun folgenden Formalitäten in den zwei gebräuchlichsten Notationssystemen angibt. In diesen Notationssystemen sollten alle Formeln aus der Schulzeit vertraut sein. Ich erinnere daran, daß wir ein Monoid definiert hatten als eine Menge mit einer assoziativen Verknüpfung, für die es in unserer Menge ein neutrales Element gibt.

Definition 2.2.2. 1. Ist $(M, \top)$ ein Monoid und $a \in M$ ein Element, so nennen wir ein weiteres Element $\bar{a} \in M$ **invers zu** a, wenn gilt $a \top \bar{a} = e =$

$\bar{a}\top a$ für $e \in M$ das neutrale Element unseres Monoids. Ein Element eines Monoids, das ein Inverses besitzt, heißt **invertierbar**;

2. Eine **Gruppe** ist ein Monoid, in dem jedes Element ein Inverses besitzt;

3. Eine **kommutative Gruppe** oder **abelsche Gruppe** ist eine Gruppe, deren Verknüpfung kommutativ ist.

Beispiele 2.2.3. Von unseren Beispielen 2.1.3 für Mengen mit Verknüpfung oben ist nur $(\mathbb{Z}, +)$ eine Gruppe, und diese Gruppe ist kommutativ. Ein anderes Beispiel für eine kommutative Gruppe ist die Menge $\mathbb{Q}$ der rationalen Zahlen mit der Addition als Verknüpfung, ein weiteres die Menge $\mathbb{Q}\backslash\{0\}$ der von Null verschiedenen rationalen Zahlen mit der Multiplikation als Verknüpfung. Auch jedes einelementige Monoid ist eine Gruppe.

2.2.4. Der Begriff einer „Gruppe“ wurde von Évariste Galois (1811-1832) in die Mathematik eingeführt. Er verwendet den Begriff „Gruppe von Transformationen“ sowohl in der Bedeutung einer „Menge von bijektiven Selbstabbildungen einer gegebenen Menge“ als auch in der Bedeutung einer „Menge von bijektiven Selbstabbildungen einer gegebenen Menge, die abgeschlossen ist unter Verknüpfung und Inversenbildung“, und die damit in der Tat ein Beispiel für eine Gruppe im Sinne der obigen Definition bildet. Unsere obige Definition 2.2.2 geht auf eine Arbeit von Arthur Cayley aus dem Jahre 1854 mit dem Titel „On the theory of groups as depending on the symbolic equation $\theta^n = 1$“ zurück und wurde damit formuliert, bevor Cantor die Sprache der Mengenlehre entwickelte. Die Terminologie „abelsche Gruppe“ wurde zu Ehren des norwegischen Mathematikers Niels Hendrik Abel eingeführt.

Lemma 2.2.5. *Jedes Element eines Monoids besitzt höchstens ein Inverses.*

Beweis. Aus $a\top\bar{a} = e$ und $b\top a = e$ folgt durch Anwenden von $b\top$ auf die erste Gleichung mit dem Assoziativgesetz sofort $\bar{a} = b$. □

2.2.6. Wir dürfen also den bestimmten Artikel benutzen und von nun an von *dem* Inversen eines Elements eines Monoids und insbesondere auch einer Gruppe reden. Gegeben ein invertierbares Element ist offensichtlich auch sein Inverses invertierbar und das Inverse des Inversen ist wieder das ursprüngliche Element, in Formeln $\bar{\bar{a}} = a$.

2.2.7. Beim Beweis von Lemma 2.2.5 haben wir stärker gezeigt: Besitzt ein Element eines Monoids ein „Rechtsinverses“ und ein „Linksinverses“, so stimmen diese überein.

Lemma 2.2.8. *Sind a und b invertierbare Elemente eines Monoids, so ist auch $a\top b$ invertierbar mit Inversem $\overline{(a\top b)} = \bar{b}\top\bar{a}$.*

	123	213	312	321	132	231
123	123	213	312	321	132	231
213	213	123	321	312	231	132
312	312	132	231	213	321	123
321	321	231	132	123	312	213
132	132	312	213	231	123	321
231	231	321	123	132	213	312

Die Verknüpfungstafel der Gruppe aller Permutationen der Menge $\{1, 2, 3\}$. Eine solche Permutation σ habe ich dargestellt durch das geordnete Zahlentripel $\sigma(1)\sigma(2)\sigma(3)$, und im Kästchen aus der Zeile τ und der Spalte σ steht $\tau \circ \sigma$.

Beweis. In der Tat rechnen wir schnell $(a\top b)\top(\bar{b}\top\bar{a}) = e = (\bar{b}\top\bar{a})\top(a\top b)$. Diese Formel ist auch aus dem täglichen Leben vertraut: Wenn man sich morgends zuerst die Strümpfe anzieht und dann die Schuhe, so muß man abends zuerst die Schuhe ausziehen und dann die Strümpfe. □

2.2.9 (**Gruppe der invertierbaren Elemente eines Monoids**). Die invertierbaren Elemente eines Monoids bilden insbesondere stets eine unter der Verknüpfung abgeschlossene Teilmenge. Diese Teilmenge enthält offensichtlich das neutrale Element und ist folglich mit der induzierten Verknüpfung eine Gruppe. Für die Gruppe der invertierbaren Elemente eines multiplikativ notierten Monoids M verwenden wir die Notation $M^\times$. Zum Beispiel haben wir $\mathbb{Z}^\times = \{1, -1\}$. Dieses Kreuz soll nicht als x gelesen werden, es ist vielmehr ein mißbrauchtes Multiplikationssymbol.

Beispiel 2.2.10. Für jede Menge Z ist die Menge aller Bijektionen von Z auf sich selbst eine Gruppe, mit der Komposition von Abbildungen als Verknüpfung. Wir notieren diese Gruppe $\mathrm{Ens}^\times(Z)$ in Übereinstimmung mit unserer Konvention 2.2.9, schließlich handelt es sich um die Gruppe der invertierbaren Elemente des Monoids $\mathrm{Ens}(Z)$. Ihre Elemente heißen die **Permutationen von** Z. Die Gruppe der Permutationen einer Menge Z ist für $|Z| > 2$ nicht kommutativ. Das Inverse einer Bijektion ist ihre Umkehrabbildung.

Definition 2.2.11 (Negativ iterierte Verknüpfung invertierbarer Elemente). Ist $(M, \top)$ ein Monoid und $a \in M$ invertierbar, so erweitern wir unsere Notation $n^\top a$ aus 2.1.24 weiter auf alle ganzen Zahlen $n \in \mathbb{Z}$, indem wir für n negativ setzen $n^\top a := (-n)^\top \bar{a}$.

2.2.12 (**Iterationsregeln**). Gegeben ein invertierbares Element a eines Monoids gelten offensichtlich sogar für alle ganzen Zahlen $n \in \mathbb{Z}$ die Regeln $(n+m)^\top a = (n^\top a)\top(m^\top a)$ und $(nm)^\top a = n^\top(m^\top a)$. Sind a, b invertierbare Elemente eines Monoids mit $ab = ba$, so gilt zusätzlich $n^\top(a\top b) = (n^\top a)\top(n^\top b)$ für alle $n \in \mathbb{Z}$. Wenn man es ganz genau nehmen will, muß man hierfür die formale Einführung der ganzen Zahlen [LA1] 4.2.12 abwarten.

2.2.13. Bei additiv geschriebenen Monoiden bezeichnet man das Inverse von a, sofern es existiert, meist als das **Negative** von a und notiert es $-a$. Bei multiplikativ notierten kommutativen Monoiden verwendet man die Bruchnotation $1/a$ und b/a aus nebenstehender Tabelle, falls a invertierbar ist. Bei nichtkommutativen multiplikativ notierten Monoiden benutzt man für das Inverse von a die von der im folgenden erklärten allgemeinen Notation a^n abgeleitete Notation a^{-1}. Die nebenstehende Tabelle faßt die üblichen Notationen für unsere abstrakten Begriffsbildungen in diesem Kontext zusammen und gibt unsere allgemeinen Resultate und Konventionen in diesen Notationen wieder.

abstrakt	additiv	multiplikativ
$a\top b$	$a+b$	$a\cdot b$, $a\circ b$, ab
e	$\hat{0}$	$\hat{1}$
$\bar{b}$	$-b$	$\hat{1}/b, b^{-1}$
$a\top\bar{b}$	$a-b$	$a/b, ab^{-1}$
$n^\top a$	na	a^n
$e\top a = a\top e = a$	$\hat{0}+a = a+\hat{0} = a$	$\hat{1}\cdot a = a\cdot\hat{1} = a$
$a\top\bar{a} = e$	$a-a=\hat{0}$	$a/a=\hat{1}$
$\bar{\bar{a}} = a$	$-(-a)=a$	$\hat{1}/(\hat{1}/a)=a$
$(-1)^\top a = \bar{a}$	$(-1)a=-a$	$a^{-1}=\hat{1}/a$
$\overline{(a\top b)} = \bar{b}\top\bar{a}$	$-(a+b)=(-b)+(-a)$	$(ab)^{-1}=b^{-1}a^{-1}$, $\hat{1}/ab=(\hat{1}/b)(\hat{1}/a)$
$\overline{(a\top\bar{b})} = b\top\bar{a}$	$-(a-b)=b-a$	$\hat{1}/(a/b)=b/a$
$n^\top(m^\top a) = (nm)^\top a$	$n(ma)=(nm)a$	$(a^m)^n=a^{nm}$
$(m+n)^\top a = (m^\top a)\top(n^\top a)$	$(m+n)a=(ma)+(na)$	$a^{(m+n)}=(a^m)(a^n)$
$\overline{n^\top a} = (-n)^\top a$	$-(na)=(-n)a$	$(a^n)^{-1}=a^{-n}$
$0^\top a = e$	$0a=\hat{0}$	$a^0=\hat{1}$
$n^\top(a\top b) = (n^\top a)\top(n^\top b)$	$n(a+b)=(na)+(nb)$	$(ab)^n=(a^n)(b^n)$

Konventionen und Formeln in verschiedenen Notationssystemen. Bereits diese Tabelle muß mit einigen Hintergedanken gelesen werden, weil die Symbole $+, -$ darin in zweierlei Bedeutung vorkommen: Manchmal meinen sie konkrete Operationen in $\mathbb{Z}$, manchmal stehen sie aber auch für Verknüpfung, Inversenbildung und neutrale Elemente in abstrakten Monoiden. Ich habe den Symbolen $0, 1$ einen Hut aufgesetzt und $\hat{0}, \hat{1}$ geschrieben, wenn sie neutrale Elemente in abstrakten Monoiden bedeuten. Das werde ich aber nicht durchhalten.

2.2.14 (**Notationen für negativ iterierte Verknüpfung**). Sei ein Monoid M gegeben und sei $x \in M$ invertierbar. Wird unser Monoid additiv notiert, so schreibt man auch für negatives $n \in \mathbb{Z}$ statt n^+x meist kurz nx und meint also mit nx das Negative von $(-n)x$. Wird unser Monoid multiplikativ notiert, also mit einem runden Symbol wie etwa $*$, so schreibt man auch für negatives $n \in \mathbb{Z}$ statt n^*x meist kurz x^n oder etwas ausführlicher x^{*n} oder $x^{(*n)}$ und meint also mit x^n das Inverse von x^{-n}.

Beispiel 2.2.15. Im Fall einer bijektiven Abbildung $f : Z \xrightarrow{\sim} Z$ ist die Umkehrabbildung $f^{-1} : Z \xrightarrow{\sim} Z$ das Inverse f^{-1} des invertierbaren Elements f des Monoids $\operatorname{Ens}(Z)$. Ebenso ist im Fall einer von Null verschiedenen rationalen Zahl $a \in \mathbb{Q}$ ihr Inverses im multiplikativen Monoid $\mathbb{Q}$ der Kehrbruch $1/a = a^{-1}$. Unsere Konvention verträgt sich also recht gut mit verschiedenen anderen Konventionen, die Sie bereits kennen mögen.

Übungen

Übung 2.2.16. Ein Element a eines Monoids M ist invertierbar genau dann, wenn es $b, c \in M$ gibt mit $b\top a = e = a\top c$ für e das neutrale Element.

Übung 2.2.17 (**Kürzen**). Sind a, b, c Elemente einer Gruppe, so folgt aus $a\top b = a\top c$ bereits $b = c$. Ebenso folgt aus $b\top a = c\top a$ bereits $b = c$. Dasselbe gilt allgemeiner in einem beliebigen Monoid, wenn wir a invertierbar annehmen.

Ergänzende Übung 2.2.18. Seien M ein Monoid und e sein neutrales Element. Man zeige: Unser Monoid ist genau dann eine Gruppe, wenn es für jedes $a \in M$ ein $\bar{a} \in M$ gibt mit $\bar{a}\top a = e$, und dies Element $\bar{a}$ ist dann notwendig das Inverse von a in M. Noch Mutigere zeigen: Ist A eine Menge mit assoziativer Verknüpfung und existiert ein $e \in M$ mit $e\top a = a \ \forall a \in M$ sowie für jedes $a \in M$ ein $\bar{a} \in M$ mit $\bar{a}\top a = e$, so ist M eine Gruppe. Hinweis: Man zeige, daß $\bar{a}\top$ bijektiv ist.

Ergänzende Übung 2.2.19. Gegeben eine Menge Z ist ihre Potenzmenge $\mathcal{P}(Z)$ mit der Verknüpfung $A + B := (A \cup B)\backslash(A \cap B)$ eine abelsche Gruppe.

Ergänzende Übung 2.2.20. Gegeben Gruppen G, H können wir das kartesische Produkt $G \times H$ zu einer Gruppe machen, indem wir darauf die komponentenweise Verknüpfung $(g, h)(g', h') := (gg', hh')$ betrachten.

Übung 2.2.21. Ein endliches Monoid $(M, \top)$, in dem für jedes Element $a \in M$ die Multiplikationsabbildung eine Injektion $(a\top) : M \hookrightarrow M$ ist, muß bereits eine Gruppe sein.

2.3 Homomorphismen

Didaktische Anmerkung 2.3.1. Ich habe diesen Abschnitt einmal erst später im Zusammenhang mit der Diskussion von linearen Abbildungen besprochen und habe es bereut.

Definition 2.3.2. Eine Menge mit einer völlig beliebigen, nicht notwendig assoziativen Verknüpfung heißt ein **Magma**. Gegeben Magmas $(X, \top)$ und $(Y, \perp)$ verstehen wir unter einem **Homomorphismus von Mengen mit Verknüpfung** oder auch **Homomorphismus von Magmas** eine Abbildung $\varphi : X \to Y$ derart, daß gilt $\varphi(a \top b) = \varphi(a) \perp \varphi(b)$ für alle $a, b \in X$. Die Menge aller solchen Homomorphismen von Magmas bezeichnen wir mit

$$\operatorname{Mag}(X, Y)$$

Beispiel 2.3.3. Sei Z eine Menge und $\mathcal{P}(Z)$ ihre Potenzmenge. Wir betrachten auf $\mathcal{P}(Z)$ die Verknüpfung $(A, B) \mapsto A \backslash B$. Ist $Z \hookrightarrow W$ eine Injektion, so ist die auf den Potenzmengen induzierte Abbildung ein Homomorphismus von Magmas

$$(\mathcal{P}(Z), \backslash) \to (\mathcal{P}(W), \backslash)$$

2.3.4. Sind unsere beiden Mengen mit Verknüpfung Monoide, so verstehen wir unter einem **Monoidhomomorphismus** einen Homomorphismus von Mengen mit Verknüpfung, der das neutrale Element auf das neutrale Element abbildet. Gegeben Monoide M und N bezeichnen wir die Menge aller Monoidhomomorphismen von M nach N mit

$$\operatorname{Mon}(M, N) := \{\varphi \in \operatorname{Mag}(M, N) \mid \varphi(e_M) = e_N\}$$

Ergänzung 2.3.5. Die beiden Bedingungen an einen Monoidhomomorphismus $\varphi : M \to N$ können in der in 2.1.27 eingeführten Terminologie dahingehend zusammengefaßt werden, daß die beiden Abbildungen $M^{\times r} \to M \to N$ und $M^{\times r} \to N^{\times r} \to N$, die durch φ und unsere Multiverknüpfungen gegeben werden, für alle $r \geq 0$ übereinstimmen sollen.

Beispiel 2.3.6. Gegeben Monoide M, N kann $\operatorname{Mon}(M, N) \subset \operatorname{Mag}(M, N)$ eine echte Teilmenge sein. Zum Beispiel ist die Abbildung $(\mathbb{Z}, +) \to (\mathbb{Z}, \cdot)$, die jede ganze Zahl auf die Null wirft, ein Homomorphismus von Mengen mit Verknüpfung, aber kein Monoidhomomorphismus.

2.3.7. Gegeben ein Monoid M und eine Gruppe G gilt stets

$$\operatorname{Mag}(M, G) = \operatorname{Mon}(M, G)$$

Jeder Homomorphismus φ von Mengen mit Verknüpfung von einem Monoid in eine Gruppe bildet also das neutrale Element auf das neutrale Element ab. In der

Tat folgt das aus $\varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e)$ durch Kürzen. Einen Homomorphismus zwischen zwei Gruppen, in Formeln eine Abbildung $\varphi : H \to G$ mit $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in H$, nennen wir einen **Gruppenhomomorphismus**. Gegeben Gruppen H und G bezeichnen wir die Menge aller Gruppenhomomorphismen von H nach G mit

$$\mathrm{Grp}(H, G)$$

Die neue Notation hat gegenüber den beiden bereits eingeführten alternativen Notationen $\mathrm{Mag}(H, G)$ und $\mathrm{Mon}(H, G)$ den Vorteil, uns daran zu erinnern, daß wir es mit Gruppen zu tun haben.

Definition 2.3.8. Ein **Isomorphismus** ist ein Homomorphismus ϕ mit der Eigenschaft, daß es einen Homomorphismus ψ in die Gegenrichtung gibt derart, daß beide Kompositionen $\psi \circ \phi$ und $\phi \circ \psi$ die Identität sind. Zwei Gruppen oder Monoide oder Magmas heißen **isomorph**, wenn es zwischen ihnen einen Isomorphismus gibt.

2.3.9. Die Terminologie kommt von griechisch „$\mu o \rho \varphi \eta$“ für „Gestalt, Struktur“ und griechisch „$o \mu o \iota \varsigma$“ für „gleich, ähnlich“. Auf deutsch könnte man statt Homomorphismus auch „strukturerhaltende Abbildung“ sagen. Das Wort „Isomorphismus“ wird analog gebildet mit griechisch „$\iota \sigma o \varsigma$“ für „gleich“.

2.3.10. In den Fällen der obigen Definition ist offensichtlich jeder bijektive Homomorphismus bereits ein Isomorphismus. Im weiteren Verlauf dieser Vorlesungen werden ihnen aber auch Arten von Homomorphismen begegnen, für die das nicht mehr richtig oder nicht einmal eine sinnvolle Aussage ist. Der erste derartige Fall wird Ihnen in diesen Vorlesungen in [LA1] 1.4.8 begegnen: Im Kontext teilgeordneter Mengen muß eine bijektive monoton wachsende Abbildung keineswegs ein „Isomorphismus von teilgeordneten Mengen“ sein alias eine monoton wachsende Umkehrabbildung besitzen.

Ergänzung 2.3.11. Den Begriff eines Homomorphismus verwendet man auch im Fall von Mengen ohne Verknüpfung: Unter einem **Homomorphismus von Mengen** versteht man schlicht eine Abbildung, unter einem **Isomorphismus von Mengen** eine Bijektion.

Beispiel 2.3.12 (**Gruppen mit höchstens zwei Elementen**). Je zwei Gruppen mit genau einem Element sind isomorph und es gibt zwischen ihnen genau einen Isomorphismus. Je zwei Gruppen mit genau zwei Elementen sind isomorph und es gibt zwischen ihnen genau einen Isomorphismus, der eben das neutrale Element auf das neutrale Element wirft und das nichtneutrale Element auf das nichtneutrale Element.

Beispiel 2.3.13 (**Dreielementige Gruppen**). Je zwei Gruppen mit genau drei Elementen sind isomorph und es gibt zwischen ihnen genau zwei Isomorphismen. Um das zu sehen, beschreiben wir eine endliche Menge mit Verknüpfung durch ihre Verknüpfungstabelle, die im Fall einer Gruppe auch **Gruppentafel** heißt. Zum Beispiel bilden diejenigen Permutationen der Menge $\{1, 2, 3\}$, die nicht genau eines unserer drei Elemente festhalten, unter der Hintereinanderausführung eine Gruppe mit der Gruppentafel

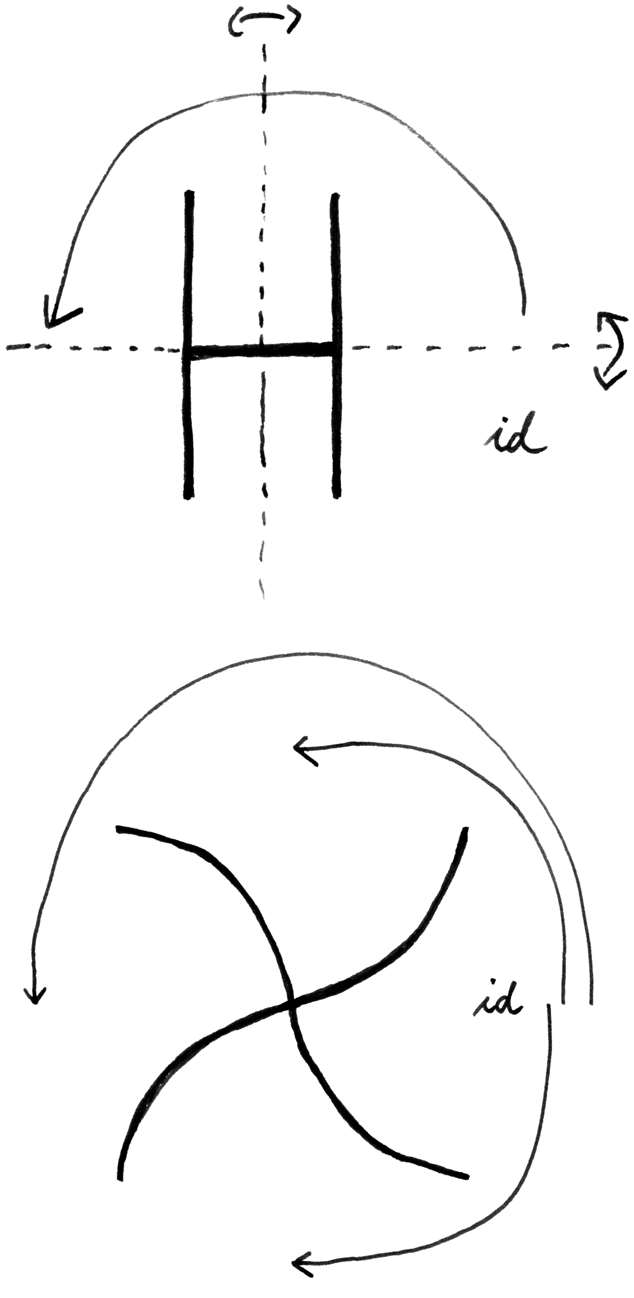
	1	ζ	η
1	1	ζ	η
ζ	ζ	η	1
η	η	1	ζ

Bei einer Gruppentafel muß nach der Kürzungsregel 2.2.17 in jeder Spalte und in jeder Zeile jedes Element genau einmal vorkommen. Man sieht so recht leicht, daß jede weitere Gruppe G mit genau drei Elementen zu der durch die obige Verknüpfungstafel gegebenen Gruppe isomorph sein muß. Anschaulich denke ich mir diese Gruppe meist als die Gruppe aller Drehungen der Ebene, die ein gleichseitiges Dreieck in sich selbst überführen. Der Nachweis, daß es zwischen je zwei dreielementigen Gruppen genau zwei Isomorphismen gibt, sei dem Leser zur Übung überlassen.

Beispiel 2.3.14 (**Vierelementige Gruppen**). Man sieht durch die Untersuchung von Verknüpfungstafeln recht leicht, daß es bis auf Isomorphismus höchstens zwei vierelementige Magmas mit neutralem Element gibt, in denen die Kürzungsregeln gelten in dem Sinne, daß in jeder Zeile und Spalte der Verknüpfungstafel jedes Element genau einmal vorkommt. Durch Betrachtung der nebenstehenden Bilder oder Interpretation als spezielle Permutationen einer geeigneten endlichen Menge überzeugt man sich auch leicht, daß diese Magmas sogar Gruppen sind, die sich dadurch unterscheiden, ob jedes Element sein eigenes Inverses ist oder nicht. Sie heißen im ersten Fall die **Klein'sche Vierergruppe** und im zweiten Fall die **vierelementige zyklische Gruppe**. Man mag zur Übung zeigen, daß es zwischen je zwei Klein'schen Vierergruppen genau sechs Isomorphismen gibt und zwischen zwei vierelementigen zyklischen Gruppen genau zwei Isomorphismen.

Definition 2.3.15. Eine Teilmenge eines Monoids heißt ein **Untermonoid**, wenn sie abgeschlossen ist unter der Verknüpfung und wenn sie zusätzlich das neutrale Element enthält.

Definition 2.3.16. Eine Teilmenge einer Gruppe heißt eine **Untergruppe**, wenn sie abgeschlossen ist unter der Verknüpfung und der Inversenbildung und wenn sie zusätzlich das neutrale Element enthält. Ist G eine multiplikativ geschriebene



Die vier Symmetrien des Buchstabens H und des Sonnenrads, das wohl nicht zuletzt auch wegen seiner Symmetriegruppe so unvermittelt an furchtbare Zeiten der deutschen Geschichte erinnert.

Gruppe, so ist eine Teilmenge $U \subset G$ also eine Untergruppe genau dann, wenn in Formeln gilt: $a, b \in U \Rightarrow ab \in U$, $a \in U \Rightarrow a^{-1} \in U$ sowie $1 \in U$.

Ergänzung 2.3.17 (**Unter-was-auch-immer**). Die Begriffsbildungen eines Untermonoids und einer Untergruppe können als Spezialfälle eines allgemeineren Begriffsschemas verstanden werden. Danach wäre ein Untermonoid zu definieren als eine Teilmenge eines Monoids, die so mit einer Monoidstruktur versehen werden kann, daß die Einbettung ein Monoidhomomorphismus ist. Ebenso wäre eine Untergruppe zu definieren als eine Teilmenge eine Gruppe, die so mit einer Gruppenstruktur versehen werden kann, daß die Einbettung ein Gruppenhomomorphismus ist. Da diese Definitionen jedoch für Anwendungen erst aufgeschlüsselt werden müssen, haben ich die aufgeschlüsselten Fassungen als Definition genommen und überlasse den Nachweis der Äquivalenz zu den eben gegebenen Definitionen dem Leser zur Übung. Mehr dazu wird in [LA2] 7.3.12 erklärt.

Beispiele 2.3.18. In jeder Gruppe ist die einelementige Teilmenge, die nur aus dem neutralen Element besteht, eine Untergruppe. Wir nennen sie die **triviale Untergruppe**. Ebenso ist natürlich die ganze Gruppe stets eine Untergruppe von sich selber. Unsere kleinen Gruppen von eben lassen sich formal gut beschreiben als Untergruppen von Permutationsgruppen. Stellt man eine Permutation σ der Menge $\{1, 2, \ldots, n\}$ dar, indem man $\sigma(1)\sigma(2)\ldots\sigma(n)$ hintereinanderschreibt – bei $n \leq 9$ mag das angehen – so ist unsere dreielementige Gruppe die Untergruppe $\{123, 231, 312\}$ der entsprechenden Permutationsgruppe, oder ganz pedantisch isomorph dazu, unsere Klein'sche Vieregruppe die Untergruppe $\{1234, 2143, 4321, 3412\}$ der entsprechenden Permutationsgruppe und unsere vierelementige zyklische Gruppe die Untergruppe $\{1234, 4123, 3412, 2341\}$.

Ergänzung 2.3.19. Eine Menge mit einer assoziativen Verknüpfung heißt auch **Halbgruppe**. Gegeben Halbgruppen A und B schreiben wir $\mathrm{Halb}(A, B)$ statt $\mathrm{Mag}(A, B)$ für die Menge aller mit der Verknüpfung verträglichen Abbildungen von A nach B, als da heißt, aller **Halbgruppenhomomorphismen**. Wieder hat diese Notation den Vorteil, uns daran zu erinnern, daß wir es mit Halbgruppen zu tun haben. Für jede Halbgruppe A liefert die Vorschrift $\varphi \mapsto \varphi(1)$ eine Bijektion

$$\mathrm{Halb}(\mathbb{N}_{\geq 1}, A) \xrightarrow{\sim} A$$

Hierbei fassen wir $\mathbb{N}_{\geq 1}$ vermittels der Addition als Halbgruppe auf. Ein formaler Beweis muß auf eine formale Definition der natürlichen Zahlen warten und ist in [LA1] 4.1.5 enthalten.

Ergänzung 2.3.20. Betrachten wir die Menge $\mathbb{M}$ „aller möglichen Klammerungen von einem oder mehr Symbolen“ im Sinne von 2.1.13 und darauf die durch „Hintereinanderschreiben“ erklärte Verknüpfung sowie das Element $* \in \mathbb{M}$, das die einzig mögliche Verklammerung von einem einzigen Symbol meint, so liefert für jedes Magma X die Vorschrift $\varphi \mapsto \varphi(*)$ eine Bijektion

$$\mathrm{Mag}(\mathbb{M}, X) \xrightarrow{\sim} X$$

Übungen

Übung 2.3.21 (**Injektivität und Kern**). Gegeben ein Gruppenhomomorphismus oder allgemeiner ein Monoidhomomorphismus $\varphi : G \to H$ erklärt man den **Kern von** φ als das Urbild des neutralen Elements, in Formeln

$$\ker \varphi := \{g \in G \mid \varphi(g) = e\}$$

Man zeige, daß $\ker \varphi$ stets eine Untergruppe beziehungsweise ein Untermonoid von G ist. Man zeige weiter, daß im Gruppenfall φ genau dann injektiv ist, wenn sein Kern nur aus dem neutralen Element besteht.

Übung 2.3.22. Das Bild eines Monoids unter einem Monoidhomomorphismus ist stets ein Untermonoid. Das Urbild eines Untermonoids unter einem Monoidhomomorphismus ist stets ein Untermonoid.

Übung 2.3.23. Jeder Monoidhomomorphismus $M \to N$ bildet invertierbare Elemente auf invertierbare Elemente ab und induziert so einen Gruppenhomomorphismus $M^\times \to N^\times$.

Übung 2.3.24. Das Bild einer Untergruppe unter einem Gruppenhomomorphismus ist stets eine Untergruppe. Das Urbild einer Untergruppe unter einem Gruppenhomomorphismus ist stets eine Untergruppe.

Übung 2.3.25. Gegeben eine Menge Z ist das Bilden des Komplements ein Monoidhomomorphismus $(\mathcal{P}(Z), \cap) \to (\mathcal{P}(Z), \cup)$.

Übung 2.3.26. Die Multiplikation mit 5 ist ein Gruppenhomomorphismus von additiven Gruppen $(5\cdot) : \mathbb{Z} \to \mathbb{Z}$.

Übung 2.3.27 (**Induzierte Verknüpfung**). Sei $(X, \top)$ eine Menge mit Verknüpfung. Gegeben eine Injektion $U \hookrightarrow X$ gibt es höchstens eine Verknüpfung auf U derart, daß unsere Injektion ein Homomorphismus ist. Wenn es solch eine Verknüpfung gibt, heißt unsere Injektion **an die Verknüpfung angepaßt** und die fragliche Verknüpfung auf U die **auf** U **induzierte Verknüpfung**. Die Einbettung einer Teilmenge ist genau dann angepaßt, wenn unsere Teilmenge abgeschlossen ist unter der Verknüpfung im Sinne von 2.1.6. Die Eigenschaften der Assoziativität und Kommutativität übertragen sich auf die induzierte Verknüpfung.

Übung 2.3.28 (**Koinduzierte Verknüpfung**). Sei $(X, \top)$ eine Menge mit Verknüpfung. Gegeben eine Surjektion $X \twoheadrightarrow Q$ gibt es höchstens eine Verknüpfung auf Q derart, daß unsere Surjektion ein Homomorphismus ist. Wenn es solch eine Verknüpfung gibt, heißt unsere Surjektion **an die Verknüpfung angepaßt** und die fragliche Verknüpfung auf Q die **auf Q koinduzierte Verknüpfung**. Zum Beispiel ist die Surjektion $\mathbb{N} \twoheadrightarrow \{0, 1, \ldots, 9\}$, die jeder Zahl die letzte Ziffer ihrer Dezimaldarstellung zuordnet, angepaßt sowohl an die Addition als auch an die Multiplikation. Mehr dazu in [LA1] 5.2.4.

Übung 2.3.29 (**Eigenschaften einer koinduzierten Verknüpfung**). Die Eigenschaften der Assoziativität und Kommutativität übertragen sich auf die koinduzierte Verknüpfung. Das Bild des Einselements ist ein Einselement für die koinduzierte Verknüpfung, das Bild des Inversen ein Inverses. Jede koinduzierte Verknüpfung zu einer angepaßten Surjektion von einer Gruppe auf eine Menge macht besagte Menge zu einer Gruppe.

Ergänzende Übung 2.3.30 (**Universelle Eigenschaft der natürlichen Zahlen**). Man zeige, daß für jedes Monoid M die Vorschrift $\varphi \mapsto \varphi(1)$ eine Bijektion

$$\mathrm{Mon}(\mathbb{N}, M) \xrightarrow{\sim} M$$

liefert. Ein Monoidhomomorphismus vom additiven Monoid der natürlichen Zahlen in ein beliebiges weiteres Monoid ist also in Worten festgelegt und festlegbar durch das Bild des Elements $1 \in \mathbb{N}$. Hinweis: Man erinnere 2.1.24. Wenn man es ganz genau nimmt, muß man für diese Übung die formale Einführung der natürlichen Zahlen [LA1] 4.1.5 abwarten.

Übung 2.3.31 (**Universelle Eigenschaft der ganzen Zahlen**). Man zeige, daß für jede Gruppe G die Vorschrift $\varphi \mapsto \varphi(1)$ eine Bijektion

$$\mathrm{Grp}(\mathbb{Z}, G) \xrightarrow{\sim} G$$

liefert. Ein Gruppenhomomorphismus von der additiven Gruppe der ganzen Zahlen in irgendeine weitere Gruppe ist also in Worten festgelegt und festlegbar durch das Bild des Elements $1 \in \mathbb{Z}$. Hinweis: Man erinnere 2.2.12. Man beachte, daß die 1 nicht das neutrale Element der Gruppe $\mathbb{Z}$ meint, die hier vielmehr als additive Gruppe zu verstehen ist. Man gebe explizit den Gruppenhomomorphismus $\mathbb{Z} \to \mathbb{Z}$ mit $1 \mapsto 5$ an. Man gebe explizit den Gruppenhomomorphismus $\mathbb{Z} \to \mathbb{Q}\backslash\{0\}$ mit $1 \mapsto 5$ an. Wenn man es ganz genau nehmen will, muß man für diese Übung die formale Einführung der ganzen Zahlen [LA1] 4.2.12 abwarten.

Übung 2.3.32. Jeder Gruppenhomomorphismus $\varphi : G \to H$ vertauscht mit Inversenbildung, in Formeln $\varphi(a^{-1}) = (\varphi(a))^{-1}\ \forall a \in G$.

Ergänzende Übung 2.3.33. Gegeben eine Verknüpfung $X \times X \to X$, $(x, y) \mapsto xy$ auf einer Menge X erklärt man die **opponierte Verknüpfung** durch die Vorschrift $(x, y) \mapsto yx$. Oft schreibt man auch X^{opp} für die Menge X, versehen mit der opponierten Verknüpfung, und x° für das Element $x \in X$, aufgefaßt als Element von X^{opp}. Das hat den Vorteil, daß man sich das Verknüpfungssymbol sparen kann, die Definition der opponierten Verknüpfung läßt sich schreiben als $y^\circ x^\circ := (xy)^\circ$. Man zeige: Gegeben eine Gruppe G liefert das Bilden des Inversen stets einen Gruppenisomorphismus $G^{\mathrm{opp}} \xrightarrow{\sim} G$, $g^\circ \mapsto g^{-1}$ zwischen der **opponierten Gruppe** und der ursprünglichen Gruppe.

Ergänzende Übung 2.3.34. Jede Halbgruppe A kann man zu einem Monoid $\tilde{A}$ erweitern, indem man noch ein Element hinzunimmt und ihm die Rolle des neutralen Elements zuweist. Für jedes weitere Monoid M liefert dann das Vorschalten der Einbettung $A \hookrightarrow \tilde{A}$ eine Bijektion

$$\mathrm{Mon}(\tilde{A}, M) \xrightarrow{\sim} \mathrm{Halb}(A, M)$$

Übung 2.3.35. Eine Abbildung $\varphi : G \to H$ von Gruppen ist genau dann ein Gruppenhomomorphismus, wenn ihr Graph $\Gamma(\varphi) \subset G \times H$ eine Untergruppe des Produkts ist.

Übung 2.3.36. Jede Verknüpfung von Homomorphismen von Magmas ist wieder ein Homomorphismus von Magmas. Sind also in Formeln $g : U \to V$ und $f : V \to W$ Homomorphismen, so ist auch $f \circ g : U \to W$ ein Homomorphismus.

Übung 2.3.37. Gegeben ein surjektiver Homomorphismus $g : U \twoheadrightarrow V$ von Magmas und eine Abbildung $f : V \to W$ in ein weiteres Magma ist f genau dann ein Homomorphismus, wenn die Verknüpfung $f \circ g : U \to W$ ein Homomorphismus ist. Gegeben ein injektiver Homomorphismus von Magmas $f : V \hookrightarrow W$ und eine Abbildung $g : U \twoheadrightarrow V$ von einem weiteren Magma nach V ist g genau dann ein Homomorphismus, wenn die Verknüpfung $f \circ g : U \to W$ ein Homomorphismus ist.

2.4 Körper im Sinne der Algebra

2.4.1. Die algebraische Struktur eines Körpers wird den Hauptbestandteil unseres Axiomensystems für die reellen Zahlen in [AN1] 2.4 bilden. Gleichzeitig bildet sie die Grundlage für die Modellierung des Raums unserer Anschauung in der linearen Algebra.

Definition 2.4.2. Ein **Körper** $(K, +, \cdot)$ (englisch **field**, französisch **corps**) ist eine Menge K mit zwei kommutativen assoziativen Verknüpfungen, genannt die **Addition** $+$ und die **Multiplikation** $\cdot$ des Körpers, derart daß die folgenden drei Bedingungen erfüllt sind:

1. $(K, +)$ ist eine Gruppe, die **additive Gruppe** des Körpers;

2. Die vom neutralen Element der Addition $0_K \in K$ verschiedenen Elemente von K bilden eine unter der Multiplikation abgeschlossene Teilmenge, und diese Teilmenge $K \backslash \{0_K\}$ ist unter der Multiplikation ihrerseits eine Gruppe, die **multiplikative Gruppe** des Körpers;

3. Es gilt das **Distributivgesetz**

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \forall a, b, c \in K$$

Beispiele 2.4.3. Ein erstes Beispiel ist der Körper der rationalen Zahlen $(\mathbb{Q}, +, \cdot)$. Ein anderes Beispiel ist der zweielementige Körper mit den durch die Axiome erzwungenen Rechenregeln, der fundamental ist in der Informatik. Die ganzen Zahlen $(\mathbb{Z}, +, \cdot)$ bilden keinen Körper, da $(\mathbb{Z} \backslash \{0\}, \cdot)$ keine Gruppe ist, da es nämlich in $\mathbb{Z} \backslash \{0\}$ nur für 1 und -1 ein multiplikatives Inverses gibt. Es gibt keinen einelementigen Körper, da das Komplement seines Nullelements die leere Menge sein müßte: Dies Komplement kann dann aber unter der Multiplikation keine Gruppe sein, da es kein neutrales Element haben könnte.

Ergänzung 2.4.4 (**Ursprung der Terminologie**). Der Begriff „Körper" ist in diesem Zusammenhang wohl zu verstehen als „besonders gut unter den verschiedensten Rechenoperationen abgeschlossener Zahlbereich", in Analogie zu geometrischen Körpern wie Kugeln oder Zylindern, die man entsprechend als „besonders gut in sich geschlossene Bereiche des Raums" ansehen könnte. Die Bezeichnung als „Distributivgesetz" rührt daher, daß uns dieses Gesetz erlaubt, beim Multiplizieren eines Elements mit einer Summe den „Faktor auf die Summanden zu verteilen". Das Wort „distribution" für Verteilung von Nahrungsmitteln und dergleichen auf Französisch und Englisch kommt von demselben lateinischen Wortstamm, auf die auch unsere Bezeichnung „Distributivgesetz" zurückgeht.

2.4.5 (**Weglassen von Multiplikationssymbolen**). Beim Rechnen mit Buchstaben werden wir meist $ab := a \cdot b$ abkürzen. Das wäre beim Rechnen mit durch Ziffernfolgen dargestellten Zahlen wenig sinnvoll, da man dann nicht wissen könnte, ob 72 nun als „Zweiundsiebzig" oder vielmehr als „Sieben mal Zwei" zu verstehen sein soll. Beim Einsetzen von Zahlen für die Buchstaben müssen also wieder Multiplikationssymbole eingefügt werden.

Ergänzung 2.4.6 (**Weglassen von Additionssymbolen**). In der Schule und außerhalb der Mathematik ist es üblich, $1 + \frac{1}{2}$ mit $1\frac{1}{2}$ abzukürzen und „Anderthalb Stunden" zu sagen oder „Dreieinviertel Pfund". In diesem Fall wird also ein Additionssymbol weggelassen. Das ist jedoch in der höheren Mathematik nicht üblich. In der gesprochenen Sprache ist es ja noch viel merkwürdiger: Neunzehnhundertvierundachzig versteht jeder, in Symbolen geschrieben sieht $9\ 10\ 100\ 4 + 80$ dahingegen ziemlich sinnlos aus, und statt der üblichen Interpretation

$((9{+}10)100){+}4{+}80$ wären durchaus auch andere Interpretationen denkbar. In der gesprochenen Sprache scheint eher eine Konvention befolgt zu werden, nach der die Operationen der Reihe nach auszuführen sind wie bei einem Taschenrechner, wobei eine Multiplikation gemeint ist, wenn die zuerst genannte Zahl die Kleinere ist, und eine Addition, wenn sie die Größere ist. Nur die Zahlen von 13 bis 19 scheinen dieser Regel nicht zu gehorchen. Kein Wunder, daß es Erstklässlern schwer fällt, sich den Zahlenraum zu erschließen, wenn sie zuvor dieses Dickicht von Konventionen durchdringen müssen.

2.4.7 (**Punkt vor Strich**). Wir vereinbaren zur Vermeidung von Klammern die Regel „Punkt vor Strich", so daß also zum Beispiel unter zusätzlicher Beachtung unserer Konvention des Weglassens von Multiplikationssymbolen, in diesem Fall das Weglassen des Punktes, das Distributivgesetz kürzer in der Form $a(b+c) = ab+ac$ geschrieben werden kann.

2.4.8 (**Multiplikation mit Null**). In jedem Körper K gilt $a0_K = 0_K \quad \forall a \in K$. Man folgert das aus $a0_K + a0_K = a(0_K + 0_K) = a0_K$ durch Hinzuaddieren von $-(a0_K)$ auf beiden Seiten. Für das neutrale Element der multiplikativen Gruppe des Körpers vereinbaren wir die Bezeichnung 1_K. Nach dem Vorhergehenden gilt $1_K b = b$ auch für $b = 0_K$, mithin für alle $b \in K$. Folglich ist $(K, \cdot)$ ein Monoid mit neutralem Element 1_K und der Menge aller von Null verschiedenen Elemente als Gruppe der invertierbaren Elemente, in Formeln $K\backslash\{0_K\} = K^\times$.

2.4.9 (**Binomische Formel**). Für alle a, b in einem Körper K und alle $n \geq 0$ gilt die binomische Formel

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

Um das einzusehen prüft man, daß wir bei der Herleitung nach [EIN] 1.1.23 nur Körperaxiome verwandt haben. Man beachte hierbei unsere Konvention $0_K^0 = 1_K$ aus 2.1.25, angewandt auf das Monoid $(K, \cdot)$. Die Multiplikation mit den Binomialkoeffizienten in dieser Formel ist zu verstehen als wiederholte Addition im Sinne der Bezeichnungskonvention na aus 2.1.16, angewandt auf den Spezialfall der additiven Gruppe unseres Körpers.

Lemma 2.4.10 (Folgerungen aus den Körperaxiomen). *In jedem Körper K gelten die folgenden Aussagen und Formeln:*

1. $ab = 0_K \quad \Rightarrow \quad (a = 0_K$ *oder* $b = 0_K)$;
2. $-a = (-1_K)a \quad \forall a \in K$;
3. $(-1_K)(-1_K) = 1_K$;
4. $(-a)(-b) = ab \quad \forall a, b \in K$;
5. $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$ *für alle* $a, c \in K$ *und* $b, d \in K^\times$;
6. $\frac{ac}{bc} = \frac{a}{b}$ *für alle* $a \in K$ *und* $b, c \in K^\times$;
7. $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ *für alle* $a, c \in K$ *und* $b, d \in K^\times$;
8. $m(ab) = (ma)b$ *für alle* $m \in \mathbb{Z}$ *und* $a, b \in K$.

Beweis.

1. In der Tat folgt aus $(a \neq 0_K$ und $b \neq 0_K)$ schon $(ab \neq 0_K)$ nach den Körperaxiomen.
2. In der Tat gilt $a+(-1_K)a = 1_K a+(-1_K)a = (1_K+(-1_K))a = 0_K a = 0_K$, und $-a$ ist ja gerade definiert als das eindeutig bestimmte Element von K mit der Eigenschaft $a + (-a) = 0_K$.
3. In der Tat gilt nach dem Vorhergehenden $(-1_K)(-1_K) = -(-1_K) = 1_K$.
4. Um das nachzuweisen ersetzen wir einfach $(-a) = (-1_K)a$ und $(-b) = (-1_K)b$ und verwenden $(-1_K)(-1_K) = 1_K$.
5. Das ist klar.
6. Das ist klar.
7. Das wird bewiesen, indem man die Brüche auf einen Hauptnenner bringt und das Distributivgesetz anwendet.
8. Das folgt durch wiederholtes Anwenden des Distributivgesetzes.

□

2.4.11 (**Minus mal Minus gibt Plus**). Die Frage, wie das Produkt zweier negativer Zahlen zu bilden sei, war lange umstritten. Mir scheint der vorhergehende Beweis das überzeugendste Argument für „Minus mal Minus gibt Plus“ : Es sagt salopp gesprochen, daß man diese Regel vereinbaren muß, wenn man beim Rechnen das Ausklammern ohne alle Einschränkungen erlauben will.

2.4.12 (**Ganze Zahlen und allgemeine Körper**). Für jeden Körper K und $n \in \mathbb{Z}$ setzen wir $n_K := n^+ 1_K = n 1_K$ in unserer Notation 2.2.11 beziehungsweise ihrer für additiv notierte Monoide vereinbarten Abkürzung. Für $n \in \mathbb{N}$ bedeutet das explizit $n_K := 1_k + \ldots + 1_K$ mit n Summanden. Nach der ersten Iterationsregel in 2.2.12 gilt stets $(n+m)_K = n_K + m_K$ und aus dem Distributivgesetz folgt leicht $n_K \cdot a = n^+ a$ oder abgekürzt $n_K a = na$ für alle $n \in \mathbb{Z}$ und $a \in K$. Mit der zweiten Iterationsregel in 2.2.12 folgt weiter für alle $m, n \in \mathbb{Z}$ die Identität $n_K m_K = (nm)_K$ über die Gleichungskette

$$n_K \cdot m_K = n^+ m_K = n^+(m^+ 1_K) = (nm)^+ 1_K = (nm)_K$$

Oft schreibt man deshalb kurz n, wenn eigentlich n_K gemeint ist, und insbesondere kürzt man eigentlich immer 0_K ab durch 0 und 1_K durch 1. Man beachte jedoch, daß für verschiedene ganze Zahlen $n \neq m$ durchaus $n_K = m_K$ gelten kann: Ist etwa K ein Körper mit zwei Elementen, so gilt $n_K = 0_K$ für gerades n und $n_K = 1_K$ für ungerades n. Vom höheren Standpunkt wird das alles nocheinmal in [LA1] 5.1.11 ausführlicher diskutiert werden.

Ergänzung 2.4.13. Den Begriff eines Homomorphismus verwendet man bei Mengen mit mehr als einer Verknüpfung analog. Zum Beispiel ist ein **Körperhomomorphismus** φ von einem Körper K in einen Körper L definiert als eine Abbildung $\varphi : K \to L$ derart, daß gilt $\varphi(a+b) = \varphi(a) + \varphi(b)$ und $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in K$ sowie $\varphi(1) = 1$. Die Bedingung $\varphi(1) = 1$ ist nur nötig, um den Fall der Nullabbildung auszuschließen. In anderen Worten mag man einen Körperhomomorphismus auch definieren als eine Abbildung, die sowohl für die Addition als auch für die Multiplikation ein Monoidhomomorphismus ist. Unter einem **Körperisomorphismus** verstehen wir wieder einen Körperhomomorphismus ϕ mit der Eigenschaft, daß es einen Körperhomomorphismus ψ in die Gegenrichtung gibt mit $\phi \circ \psi = \mathrm{id}$ und $\psi \circ \phi = \mathrm{id}$. Wieder ist jeder bijektive Körperhomomorphismus bereits ein Körperisomorphismus.

Übungen

Übung 2.4.14. Ist K ein Körper derart, daß es kein $x \in K$ gibt mit $x^2 = -1$, so kann man die Menge $K \times K = K^2$ zu einem Körper machen, indem man die Addition und Multiplikation definiert durch

$$\begin{array}{rcc} (a,b) + (c,d) & := & (a+c, b+d) \\ (a,b) \cdot (c,d) & := & (ac - bd, ad + bc) \end{array}$$

Die Abbildung $K \to K^2$, $a \mapsto (a, 0)$ ist dann ein Körperhomomorphismus. Kürzen wir $(a, 0)$ mit a ab und setzen $(0, 1) = \mathrm{i}$, so gilt $\mathrm{i}^2 = -1$ und $(a, b) = a + b\,\mathrm{i}$ und die Abbildung $a + b\,\mathrm{i} \mapsto a - b\,\mathrm{i}$ ist ein Körperisomorphismus $K^2 \xrightarrow{\sim} K^2$.

2.4.15. Auf die in der vorhergehenden Übung 2.4.14 erklärte Weise können wir etwa aus dem Körper $K = \mathbb{R}$ der „reellen Zahlen“, sobald wir ihn kennengelernt haben, direkt den Körper $\mathbb{C}$ der **komplexen Zahlen** konstruieren. Unser Körperisomorphismus gegeben durch die Vorschrift $a + b\,\mathrm{i} \mapsto a - b\,\mathrm{i}$ heißt in diesem Fall die **komplexe Konjugation** und wird auch $z \mapsto \bar{z}$ notiert. Man beachte, wie mühelos das alles in der Sprache der Mengenlehre zu machen ist. Als die komplexen Zahlen erfunden wurden, gab es noch keine Mengenlehre und beim Rechnen beschränkte man sich auf das Rechnen mit „reellen“ Zahlen, ja selbst das Multiplizieren zweier negativer Zahlen wurde als eine fragwürdige Operation angesehen, und das Ziehen einer Quadratwurzel aus einer negativen Zahl als eine rein imaginäre Operation. In gewisser Weise ist es das ja auch geblieben, aber die Mengenlehre liefert eben unserer Imagination eine wunderbar präzise Sprache, in der wir uns auch über imaginierte Dinge unmißverständlich austauschen können. Man kann dieselbe Konstruktion auch allgemeiner durchführen, wenn man statt -1 irgendein anderes Element eines Körpers K betrachtet, das kein Quadrat ist. Noch allgemeinere Konstruktionen zur „Adjunktion höherer Wurzeln“ oder sogar der „Adjunktion von Nullstellen polynomialer Gleichungen“ können Sie in der Algebra kennenlernen, vergleiche etwa [AL] 3.7.6. In [LA1] 2.7 diskutieren wir die komplexen Zahlen ausführlicher.

Ergänzende Übung 2.4.16. Ein Körperhomomorphismus ist stets injektiv.

2.5 Aufbau des Zahlensystems*

2.5.1. Der Aufbau des Zahlensystems

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

erscheint in diesem Text nur in einer Abfolge von Nebenbemerkungen und soll an dieser Stelle zusammenfassend dargestellt werden.

1. Die Konstruktion der natürlichen Zahlen $\mathbb{N}$ aus Grundbegriffen der Mengenlehre diskutiere ich in [LA1] 4.1.5. Kurz wurde das auch schon in 1.6.11 angerissen. Eine vollständig überzeugende Diskussion dieser Struktur ist meines Erachtens nur im Rahmen der Logik möglich.

2. Die Konstruktion der ganzen Zahlen $\mathbb{Z}$ aus den natürlichen Zahlen $\mathbb{N}$, ja der einhüllenden Gruppe eines beliebigen kommutativen Monoids wird in [LA1] 4.2.12 erklärt. Nach [AN1] 2.4.6 gibt es dann genau eine Multiplikation auf $\mathbb{Z}$, die unsere Multiplikation auf $\mathbb{N}$ fortsetzt und $\mathbb{Z}$ zu einem Ring macht.

3. Die Konstruktion des Körpers der rationalen Zahlen $\mathbb{Q}$ aus dem Integritätsbereich der ganzen Zahlen $\mathbb{Z}$, ja des Quotientenkörpers eines beliebigen kommutativen Integritätsbereichs wird in [LA1] 5.5.2 ausgeführt. Die Anordnung auf $\mathbb{Q}$ dürfen Sie selbst in [LA1] 5.5.19 konstruieren.

4. Die Konstruktion des angeordneten Körpers der reellen Zahlen $\mathbb{R}$ aus dem angeordneten Körper der rationalen Zahlen $\mathbb{Q}$ wird zur Beginn der Analysis in [AN1] 2.4.3 erklärt.

5. Die Konstruktion des Körpers der komplexen Zahlen $\mathbb{C}$ aus dem Körper der reellen Zahlen $\mathbb{R}$ wurde in 2.4.14 angerissen und wird in [LA1] 2.7 ausführlicher behandelt.

2.5.2 (**Gewinne und Verluste beim Aufbau des Zahlensystems**). Oft wird der Aufbau des Zahlensystems als eine Geschichte immer neuer Gewinne erzählt: Beim Übergang von $\mathbb{N}$ zu $\mathbb{Z}$ gewinnt man die Lösbarkeit aller Gleichungen des Typs $a + x = b$, beim Übergang von $\mathbb{Z}$ zu $\mathbb{Q}$ die Lösbarkeit aller Gleichungen des Typs $ax = b$ für $a \neq 0$, beim Übergang von $\mathbb{Q}$ zu $\mathbb{R}$ die Lösbarkeit aller Gleichungen des Typs $x^a = b$ für $a, b > 0$, und nach Übergang von $\mathbb{R}$ zu $\mathbb{C}$ besitzen sogar alle nichtkonstanten Polynome Nullstellen. Hier ist nur anzumerken, daß man die Lösbarkeit aller Gleichungen des Typs $x^a = b$ für $a, b > 0$ auch schon in einem abzählbaren Unterkörper von $\mathbb{R}$ erreichen könnte und daß der eigentliche Grund für den Übergang zu $\mathbb{R}$ analytischer Natur ist: Man gewinnt so den Zwischenwertsatz [AN1] 3.3.8. Man kann den Aufbau des Zahlensystems aber auch als eine Geschichte immer neuer Verluste erzählen: Beim Übergang von $\mathbb{N}$ zu $\mathbb{Z}$ verliert man die Existenz eines kleinsten Elements, beim Übergang von $\mathbb{Z}$ zu $\mathbb{Q}$ die Existenz unmittelbarer Nachfolger, beim Übergang von $\mathbb{Q}$ zu $\mathbb{R}$ die Abzählbarkeit, und beim Übergang von $\mathbb{R}$ zu $\mathbb{C}$ die Anordnung. Man kann noch weiter gehen zum Schiefkörper der sogenannten Quaternionen $\mathbb{H} \supset \mathbb{C}$ aus [LA1] 5.6.3, dabei verliert man die Kommutativität der Multiplikation, oder sogar zu den sogenannten Oktaven $\mathbb{O} \supset \mathbb{H}$ aus [AL] 3.12.4, bei denen die Multiplikation nicht einmal mehr assoziativ ist.

2.6 Verbände und Boole'sche Algebren*

Definition 2.6.1. Eine **Boole'sche Algebra** ist ein Tripel $(B, \wedge, \vee)$ bestehend aus einer Menge mit zwei assoziativen kommutativen Verknüpfungen derart, daß gilt:

1. Mit jeder unserer Verknüpfungen wird B ein Monoid. Man notiert 1 das neutrale Element zu $\wedge$ und 0 das neutrale Element zu $\vee$;

2. Jede unserer beiden Verknüpfungen ist „distributiv über der anderen“, in Formeln $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ und $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$;

3. Zu jedem $a \in B$ existiert $c \in B$ mit $a \wedge c = 0$ und $a \vee c = 1$. Man zeigt mühelos, daß dies Element c durch a eindeutig bestimmt ist, und notiert es $c = \neg a$ oder $c = \bar{a}$.

Ein **Homomorphismus von Boole'schen Algebren** ist eine Abbildung, die für beide Monoidstrukturen ein Homomorphismus von Monoiden ist. Gegeben Boole'sche Algebren B, C notieren wir $\mathrm{Boole}(B, C)$ die Menge aller Homomorphismen von B nach C.

2.6.2. Ein typisches Beispiel einer Boole'schen Algebra erhält man, indem man für eine beliebige Menge X das Tripel $(\mathrm{Pot}(X), \cap, \cup)$ bestehend aus ihrer Potenzmenge mit den Operationen Schnitt und Vereinigung betrachtet. In dieser Situation haben wir $1 = X$ sowie $0 = \emptyset$ und $\neg A = X \backslash A$ ist die Komplementmenge.

Definition 2.6.3. Ein **Verband** ist ein Tripel $(B, \wedge, \vee)$ bestehend aus einer Menge mit zwei assoziativen kommutativen Verknüpfungen derart, daß die **Absorptionsgesetze** $a \wedge (a \vee b) = a$ und $a \vee (a \wedge b) = a$ gelten für alle $a, b \in B$.

Beispiel 2.6.4. Als Übung 2.6.7 dürfen Sie zeigen, daß jede Boole'sche Algebra ein Verband ist.

Vorschau 2.6.5. Wir werden in [AN1] 2.3.9 sehen, daß eine teilgeordnete Menge, in der jede zweielementige Teilmenge ein Supremum und ein Infimum hat, zu einem Verband wird, wenn wir $a \vee b := \sup\{a, b\}$ und $a \wedge b := \inf\{a, b\}$ setzen, und daß wir so genau alle Verbände erhalten.

Übungen

Übung 2.6.6. Man zeige für jedes Element a einer Boole'schen Algebra die Identitäten $a \wedge 0 = 0$ und $a \vee 1 = 1$. Hinweis: Man gehe von $1 = a \vee (\bar{a} \wedge 1)$ aus und verwende Distributivität.

Übung 2.6.7. Man zeige, daß jede Boole'sche Algebra ein Verband ist. Hinweis: Man gehe von $(b \wedge 0) \vee a = a$ nach 2.6.6 aus und verwende die Distributivität.

Übung 2.6.8. Man zeige für jedes Element a eines Verbandes $a \wedge a = a$ und $a \vee a = a$. Hinweis: Absorptionsgesetze mit $b = a \wedge a$ oder $b = a \vee a$.

3 Zur Darstellung von Mathematik*

3.1 Herkunft einiger Symbole

3.1.1. Ich habe versucht, etwas über die Herkunft einiger mathematischer Symbole in Erfahrung zu bringen, die schon aus der Schule selbstverständlich sind.

3.1.2. Das Pluszeichen $+$ ist wohl ein Auschnitt aus dem Symbol &, das hinwiederum enstanden ist durch Zusammenziehen der beiden Buchstaben im Wörtchen „et", lateinisch für „und".

3.1.3. Die Dezimaldarstellung der natürlichen Zahlen kam Mitte des vorigen Jahrtausends aus Indien über die Araber nach Italien. Bis dahin rechnete man in Europa in römischer Notation. Sie müssen nur versuchen, in dieser Notation zwei größere Zahlen zu multiplizieren, um zu ermessen, welchen wissenschaftlichen und auch wirtschaftlichen Fortschritt der Übergang zur Dezimaldarstellung bedeutete. Das Beispiel der Dezimaldarstellung zeigt in meinen Augen auch, wie entscheidend das sorgfältige Einbeziehen trivialer Spezialfälle, manchmal als „Theorie der leeren Menge" verspottet, für die Eleganz der Darstellung mathematischer Sachverhalte sein kann: Sie wurde ja eben dadurch erst ermöglicht, daß man ein eigenes Symbol für „gar nichts" erfand! Ich denke, daß der Aufbau eines effizienten Notationssystems, obwohl er natürlich nicht denselben Stellenwert einnehmen kann wie die Entwicklung mathematischer Inhalte, dennoch in der Lehre ein wichtiges Ziel sein muß. In diesem Text habe ich mir die größte Mühe gegeben, unter den gebräuchlichen Notationen diejenigen auszuwählen, die mir am sinnvollsten schienen, und sie soweit wie möglich aufzuschlüsseln. Wo es mir sinnvoll schien, habe ich auch nicht gezögert, neue Notationen einzuführen.

3.1.4. Das Wort von der „Theorie der leeren Menge" scheint auf Carl Ludwig Siegel zurückzugehen, der einmal gesagt haben soll: „Ich habe Angst, dass die Mathematik vor dem Ende des Jahrhunderts zugrunde geht, wenn dem Trend nach sinnloser Abstraktion – die Theorie der leeren Menge, wie ich es nenne – nicht Einhalt geboten wird".

3.1.5. Die Herkunft der logischen Symbole $\exists$ und $\forall$ als umgedrehte E und A haben wir bereits in 1.7.4 erwähnt. Sie wurden von Cantor in seiner Mengenlehre zuerst verwendet. Die Symbole $\mathbb{R}, \mathbb{Q}, \mathbb{N}, \mathbb{Z}$ wurden früher als fette Buchstaben gedruckt und zunächst nur beim Tafelanschrieb in der hier gegebenen Gestalt wiedergegeben, da man fetten Druck an der Tafel nicht gut darstellen kann.

3.2 Grundsätzliches zur Formulierung

3.2.1 (**Redundanz**). Es scheint mir wichtig, sich beim Schreiben über Mathematik immer vor Augen zu halten, daß die mathematische Terminologie und Formelsprache sehr wenig Redundanz aufweisen. Auch kleinste Fehler oder Ungenauigkeiten können dadurch schon zu den größten Mißverständnissen führen. Ich plädiere deshalb dafür, die Redundanz künstlich zu erhöhen und nach Möglichkeit alles dreimal zu sagen: Einmal in mathematischer Terminologie, einmal in Formeln, und dann noch einmal in weniger formellen Worten und mit Bildern.

3.2.2 (**Versprachlichung**). Ich halte es für ebenso wichtig wie delikat, den mathematischen Inhalten griffige Bezeichnungen zu geben. Wir wollen uns ja auch mit anderen Mathematikern unterhalten können, die nicht dasselbe Buch gelesen haben. Sogar dann, wenn ich nur mit mir selbst und einem einzigen Buch beschäftigt bin und bei einem Beweis, den ich gerade verstehen will, ganz präzise „Theorem 4.2" zitiert wird, stört es mich: Ich muß blättern, bin abgelenkt und mein Verstehen wird gebremst. Darüber hinaus kann ich mir Dinge viel besser merken, die griffige Bezeichnungen haben. Diese Bezeichnungen wirken wie Garderobenhaken im Kopf, an denen man Inhalte aufhängen und wiederfinden kann. Delikat ist, daß die Wahl einer Bezeichnung oft auch eine politische und historische Dimension hat. Delikat ist weiter, daß bei vielen üblichen Bezeichnungen verschiedene Varianten für ihre genaue Bedeutung im Umlauf sind. Ich versuche beides nach bestem Wissen und Gewissen offenzulegen.

3.2.3 (**Generalvoraussetzungen**). Ich selber lese keineswegs immer alles von vorne bis hinten durch und merke mir das bereits Gelesene. Vielmehr suche oft, um nicht zu sagen meist, nur gezielt spezielle Resultate, und lese dazu eher diagonal. Ich habe es deshalbnach Kräften vermieden, Generalvoraussetzungen einzustreuen, von der Art „von nun an bis zum Ende des Abschnitts sind alle unsere topologischen Räume Hausdorff" und dergleichen. Wenn das einmal bei speziellen Themen zu umständlich werden sollte, will ich strikt die Regel befolgen, daß Generalvoraussetzungen für eine Gliederungsstufe entweder direkt nach der Überschrift besagter Gliederungsstufe stehen müssen, oder aber direkt vor dem Beginn des ersten Abschnitts der nächsttieferen Gliederungsstufe, im Anschluß an die Vorrede, und dann als eigener Abschnitt „Generalvoraussetzungen".

3.2.4 (**Definition-Satz-Beweis**). Das Schema Definition-Satz-Beweis scheint mir für die Darstellung von Mathematik sehr gut geeignet und auch zum Lesen und Lernen äußerst effektiv, wenn es richtig angewendet wird: Wenn nämlich die Sätze so formuliert werden, daß ihre Aussagen auch für sich genommen schon sinnvoll und verständlich sind, sofern man die entsprechenden Definitionen parat hat. Dann kann man dieses Schema verstehen als eine Anleitung zum diagonalen Lesen. Demselben Ziel dient die Abstufung der Sätze durch die Bezeichnung als Satz, Korollar, Proposition, Lemma und dergleichen: Sie soll dem Leser zu erlauben, etwa durch Konzentration auf die Sätze eine schnelle Orientierung über die wesentlichen Aussagen und Resultate zu gewinnen. Diese Form ersetzt zu einem gewissen Maße, was man im Deutschunterricht lernt. Ich empfehle, mathematische Texte und Vorträge nicht mit einer Gliederung zu beginnen und auch nicht mit einem Schlußwort zu beenden, da das in Anbetracht der in der Mathematik eh üblichen Strukturierung durch das Schema „Definition-Satz-Beweis“ leicht dazu führt, daß die strukturellen Elemente im Vergleich zum eigentlichen Inhalt unverhältnismäßig viel Raum einnehmen.

3.2.5 (**Andere nummerierte Passagen**). In diesem Text gibt es auch viele Passagen, die einfach nur nummeriert sind. Hier handelt es sich meist um kleinere Aussagen mit Beweis, die mir für die „große Form“ Definition-Satz-Beweis zu unbedeutend oder zu offensichtlich schienen. Andere Textpassagen sind als *Ergänzung* oder *Ergänzende Übung* ausgewiesen: Damit ist gemeint, daß sie im unmittelbaren Zusammenhang ohne Schaden übersprungen werden können, daß sie jedoch aus dem vorhergehenden heraus verständlich sein sollten. Wieder andere Textpassagen sind als *Vorschau* oder *Weiterführende Übung* ausgewiesen: Damit ist gemeint, daß sie im unmittelbaren Zusammenhang ohne Schaden übersprungen werden können und daß ihr Verständnis Kenntnisse voraussetzt, bei denen nicht davon ausgehe, daß sie dem Leser an der entsprechenden Stelle bereits zur Verfügung stehen.

3.2.6 (**Satzzeichen in mathematischen Texten**). Satzzeichen wie Punkt und Komma stören aus meiner Sicht die Ästhetik von aus dem Text herausgestellten Formeln. Ich will deshalb die Regel aufstellen und befolgen, daß eine aus dem Text herausgestellte Formel stets mit einem nicht gedruckten Punkt dahinter zu denken ist, wenn der Text mit ihr aufhört oder wenn es darunter mit einem Großbuchstaben weitergeht. Ich werde den Fall vermeiden, daß hinter eine aus dem Text herausgestellte Formel nach den Regeln der Grammatik ein Komma gehören müßte.

3.2.7 (**Eigennamen in mathematischen Texten**). Ich übernehme aus dem Englischen den Apostroph bei Eigennamen und schreibe also zum Beispiel Zorn’sches Lemma. In der deutschen Literatur sind stattdessen Kapitälchen üblich, wie etwa ZORNsches Lemma, aber diese Hervorhebung im Schriftbild scheint mir ungebührlich viel Aufmerksamkeit zu binden.

3.3 Sprache und Mathematik

3.3.1. In diesem Abschnitt habe ich gesammelt, was mir beim Erklären von Mathematik und Schreiben über Mathematik besonders schwer fällt.

3.3.2 (**Umgangssprache versus mathematische Fachsprache**). Die mathematische Terminologie widmet freimütig Worte der Umgangssprache um und gibt ihnen präzise mathematische Bedeutungen, die mal mehr und mal weniger zur Ursprungsbedeutung verwandt sind. Man denke zum Beispiel an die Worte Menge, Abbildung, Gruppe, Ring, Körper. Mit dem Adjektiv **schmutzig** betone ich, daß ein Wort umgangssprachlich zu verstehen ist und nicht als ein Begriff der allein auf der Mengenlehre basierenden aseptisch steril perfekten Ideenwelt der reinen Mathematik.

3.3.3. Im Gegensatz zu dem, was in der Schule im Deutschunterricht gelernt wird, ist Wortwiederholung beim mathematischen Schreiben und Reden richtig und wichtig.

3.3.4 (**Erweiterung oder Zuspitzung durch Ergänzungen**). Bereits erklärte Begriffe werden in der mathematischen Fachsprache durch Ergänzungen mal spezifiziert, mal abgeschwächt, und manchmal sogar beides zugleich. Der noch wenig informierte Leser kann nur schwer erraten, was im Einzelfall zutrifft. So ist ein Primkörper etwas Spezielleres als ein Körper, ein Schiefkörper etwas Allgemeineres, und ein Erweiterungskörper „etwas mit zusätzlichen Daten“. Ein lokal kompakter Raum ist etwas allgemeineres als ein kompakter Raum. Eine universelle Überlagerung ist etwas Spezielleres als eine Überlagerung und eine verzweigte Überlagerung etwas Allgemeineres, das aber nur im Spezialfall von Flächen überhaupt sinnvoll definiert ist. Ein Borelmaß ist etwas Spezielleres als ein Maß und ein signiertes Maß etwas Allgemeineres. Eine Mannigfaltigkeit mit Rand ist etwas Allgemeineres als eine Mannigfaltigkeit, eine glatte Mannigfaltigkeit dahingegen eine spezielle Art von Mannigfaltigkeit, und ich könnte noch lange so fortfahren. Das führt leicht zu Verwirrung, aber ich habe auch keine Lösung.

3.3.5 (**Bestimmte und unbestimmte Artikel**). Problematisch scheint mir in mathematischen Texten die Verwendung bestimmter und unbestimmter Artikel, und ich bin fast neidisch auf die russische Sprache, die diese Unterscheidung nicht kennt. Sind mathematische Strukturen „eindeutig bis auf eindeutigen Isomorphismus“, wie Gruppen mit zwei Elementen oder Mengen mit einem Element, so fällt mir die Verwendung des bestimmten Artikels leicht. Häufig sind mathematische Strukturen jedoch nur „eindeutig bis auf nicht-eindeutigen Isomorphismus“: Etwa Mengen mit fünf Elementen, Gruppen mit drei Elementen oder Vektorräume gegebener Dimension über einem vorgegebenen Köper. Soll man dann den bestimmten oder den unbestimmten Artikel verwenden? Hier ist die Terminologie uneinheitlich: Man sagt üblicherweise „ein fünfdimensionaler reeller Vektorraum, eine abzählbar unendliche Menge“ aber „die euklidische Ebene, der Zerfällungskörper, der algebraische Abschluß, die universelle Überlagerung“, ohne daß ich dafür triftige Gründe ausmachen könnte. Vielleicht wäre es eine gute Idee, für nur bis auf nichteindeutigen Isomorphismus eindeutig bestimmte mathematische Objekte die bestimmten Artikel mit einer „abschwächenden Schlange“ in der Form „dẽr, dĩe, dãs“ zu verwenden.

3.3.6 (**Existenz in Definitionen**). Ich plädiere dafür, in mathematischen Texten die Formulierungen „Es existiert“ und „Es gibt“ ausschließlich in ihrer Bedeutung als Quantoren zu verwenden, da es sonst leicht zu Mißverständnissen kommen kann. Insbesondere plädiere ich sehr dafür, diese Formulierungen zu vermeiden, wenn es in Definitionen um die Vorstellung der „Ausgangsdaten“ geht. Die folgenden Beispiele mögen das illustrieren.

Mißverständlich: Eine Gruppe ist eine Menge, auf der es eine assoziative Verknüpfung gibt derart, daß es ein neutrales Element gibt und zu jedem Element ein Inverses.

Klarer: Eine Gruppe ist eine Menge mit einer assoziativen Verknüpfung derart, daß es ein neutrales Element gibt und zu jedem Element ein Inverses.

Pedantisch: Eine Gruppe ist ein Paar bestehend aus einer Menge und einer assoziativen Verknüpfung auf dieser Menge derart, daß es ein neutrales Element gibt und zu jedem Element ein Inverses.

In der Tat gibt es ja auf jeder nichtleeren Menge eine assoziative Verknüpfung, die sie zu einer Gruppe macht. Eine Gruppe ist aber keineswegs eine Menge mit gewissen Eigenschaften, sondern eine Menge mit Verknüpfung mit gewissen Eigenschaften. Das Ausgangsdatum bei dieser Definition ist in anderen Worten und ganz pedantisch formuliert ein Paar bestehend aus einer Menge zusammen mit mit einer Verknüpfung auf dieser Menge. Ich gebe zu, daß man auch die „klare“ Definition falsch verstehen könnte, aber an dieser Stelle würde ich dieser Formulierung wegen ihrer Kürze doch der Vorzug gegenüber der „pedantischen“ Formulierung einräumen.

Mißverständlich: Ein Körper heißt angeordnet, wenn es auf ihm eine Anordnung gibt derart, daß…

Klarer: Ein angeordneter Körper ist ein Körper mit einer Anordnung derart, daß…

Pedantisch: Ein angeordneter Körper ist ein Paar bestehend aus einem Körper mit einer Anordnung auf der ihm zugrundeliegenden Menge derart, daß…

Zur Verdeutlichung zum Abschluß noch ein Beispiel, in dem die mißverständliche Formulierung die korrekte Formulierung einer anderen Eigenschaft ist:

Mißverständlich: Eine Mannigfaltigkeit heißt orientiert, wenn es auf ihr eine Orientierung gibt.

Klarer: Eine orientierte Mannigfaltigkeit ist eine Mannigfaltigkeit mit einer Orientierung.

Pedantisch: Eine orientierte Mannigfaltigkeit ist ein Paar bestehend aus einer Mannigfaltigkeit mit einer Orientierung auf unserer Mannigfaltigkeit.

Hier ist die erste Formulierung in der Tat bei der üblichen Interpretation von „es gibt“ als Quantor die Definition einer orientierbaren, nicht die einer orientierten Mannigfaltigkeit.

3.3.7 (**Kampf dem Index**). Beim Schreiben von Mathematik in Formeln hat man oft mit der Schwierigkeit zu kämpfen, daß die wesentliche Information sich in Indizes verstecken will und die besonders wesentliche Information in Subindizes. Dem gilt es bewußt entgegenzuarbeiten.

3.4 Terminologisches zur leeren Menge*

Vorschau 3.4.1. Ich finde es oft schwierig, die leere Menge terminologisch korrekt einzubinden. Das ist aber ebenso wichtig wie der Beckenrand beim Schwimmbad, den man ja auch nicht wegläßt, obwohl man nachher nur im Wasser schwimmen will. Ich finde auch, daß das Bourbaki, den ich an sich sehr schätze, oft mißlungen ist. Meine Konventionen sind wie folgt:

1. Die leere Menge ist nach [AN1] 3.2.1 ein Intervall. So sind beliebige Schnitte von Intervallen wieder Intervalle;

2. Die leere Menge ist nach [LA1] 3.5.2 konvex. So sind beliebige Schnitte konvexer Mengen wieder konvex;

3. Die leere Menge ist *nicht* zusammenhängend. Die Zusammenhangskomponenten eines topologischen Raums sind seine maximalen zusammenhängenden Teilmengen und die leere Menge hat gar keine Zusammenhangskomponente. So hat für einen topologischen Raum mit nur endlich vielen Zusammenhangskomponenten der Vektorraum der stetigen Abbildungen in den Körper mit zwei Elementen als Dimension gerade die Zahl der Zusammenhangskomponenten. Die zusammenhängenden Teilmengen von $\mathbb{R}$ sind damit genau die *nichtleeren* Intervalle und nur jede *nichtleere* konvexe Teilmenge eines endlichdimensionalen reellen affinen Raums ist zusammenhängend;

4. Die Wirkung einer Gruppe G auf der leeren Menge ist nach [LA2] 5.1.7 *nicht* transitiv. Damit läßt sich jede G-Menge bis auf Reihenfolge und Isomorphismus eindeutig als eine disjunkte Vereinigung von transitiven G-Mengen darstellen;

5. Die leere Menge ist nach [LA1] 3.1.1 *kein* affiner Raum. Sie läßt ja nach der vorhergehenden Konvention auch keine transitive Operation eines Vektorraums zu. Daß damit der Schnitt zweier affiner Teilräume nicht notwendig wieder ein affiner Teilraum ist, nehme ich als kleineres Übel in Kauf;

6. Eine Abbildung von der leeren Menge in eine beliebige weitere Menge ist konstant, aber nicht einwertig, vergleiche 1.4.10;

4 Philosophisches und Didaktisches

In diesen Abschnitten habe ich einige Gedanken zur Mathematik und zum Unterrichten von Mathematik gesammelt, die nicht zum logisch kohärenten Aufbau des Stoffes selber beitragen und teilweise auch stark persönlich gefärbt sind.

4.1 Was ist Mathematik?

4.1.1. Das Wort „Mathematik“ kommt vom griechischen „$\mu\alpha\vartheta\eta\mu\alpha\tau\iota\kappa o\varsigma$“, das sich hinwiederum ableitet von „$\mu\alpha\vartheta\eta\mu\alpha$“ für „der Lerngegenstand, die Wissenschaft“ nach dem Verb „$\mu\alpha\nu\vartheta\alpha\nu\omega$“ für „lernen, verstehen“. Das Anhängen der Endung „-$\iota\kappa o\varsigma$“ oder im Anschluß an einen Vokal „-$\tau\iota\kappa o\varsigma$“ hat eine ähnliche Bedeutung wie im Deutschen das Anhängen von „-ig“ oder „-lich“ beziehungsweise „-tlich“, etwa wie in Mut $\mapsto$ mutig, Haar $\mapsto$ haarig, wohnen $\mapsto$ wohnlich oder eigen $\mapsto$ eigentlich. In diesem Sinne wäre die wörtliche Übersetzung von „$\mu\alpha\vartheta\eta\mu\alpha\tau\iota\kappa o\varsigma$“ also „das Lernige“ oder „das Verständliche“. Platon verwendet den Begriff „$\tau o\ \mu\alpha\vartheta\eta\mu\alpha\tau\iota\kappa o\nu$“ im Sinne von „der Forschungsgegenstand“ in Sophista 219c:2 und Timaeus 88c:1. In der hellenistischen Zeit verengte sich die Bedeutung ein erstes Mal und bezeichnete etwas, was wir heute eher als „Mathematik und Naturwissenschaften“ bezeichnen würden. Erst in neuerer Zeit verengte sich die Bedeutung weiter auf das, was wir heute unter Mathematik verstehen

4.1.2. Ich würde die heutige Mathematik in einem ersten Ansatz beschreiben als die „Wissenschaft von den einfachsten Begriffen“: Wieviel einfacher sind doch Zahlen und ihre Rechenregeln, Geraden und Ebenen, selbst Abbildungen zwischen Mengen im Vergleich zu Pflanzen und Menschen, Hass und Liebe, ja selbst Luft und Wasser! Diese einfachsten Begriffe müssen nun jedoch mit der größten Vorsicht und Präzision gehandhabt werden, damit uns unsere an den Umgang mit Pflanzen und Menschen, Hass und Liebe, Luft und Wasser gewöhnte Intelligenz nicht in die Irre führt. Die eigentliche Mathematik besteht dann darin, diese einfachsten Begriffe zu größeren Theorien zu kombinieren, und die eigentlichen Einsichten entstehen auch erst in dieser Gesamtschau. Ich sehe darin eine Affinität zur Musik, in der man ja auch von einfachsten Geräuschen, in der Klassik etwa von den Tönen der Tonleiter, ausgeht und diese einfachsten Grundbausteine zu Kompositionen kombiniert, deren Sinnhaftigkeit sich erst in der Gesamtschau erschließt. Auf einen Gegensatz zur Musik will ich im nächsten Absatz noch ausführlicher zu sprechen kommen: Während auch die schönste Musik meines Erachtens vom Komponisten nicht entdeckt sondern vielmehr erschaffen wird, scheint es sich mir bei der Mathematik gerade umgekehrt zu verhalten. Sicher gibt es sozusagen „komponierte“ mathematische Artikel, aber die mathematischen Inhalte selbst lassen sich von Menschenhand nicht formen und wollen entdeckt werden.

4.1.3. In diesem Zusammenhang will ich auf eine gerne diskutierte Frage eingehen: Wird Mathematik eigentlich entdeckt oder entwickelt? Aus meiner eigenen Erfahrung mit dieser widerspenstigen Materie und auch der Erfahrung beim Erklären von Beweisen scheint es mir offensichtlich, daß mathematische Inhalte „objektiv da sind“, also unabhängig vom menschlichen Subjekt existieren und entdeckt werden. Was jedoch entwickelt werden muß ist eine Sprache, die es uns ermöglicht, uns über diese Inhalte zu verständigen und sie zu nutzen. Hier kam und kommt es durchaus zu parallelen Entwicklungen, man denke etwa an die beiden Notationen $\dot{x}$ und $\frac{\mathrm{d}x}{\mathrm{d}t}$ für die Ableitung, an den Erwartungswert $\mathrm{E}(X)$ einer Zufallsvariable X in der Wahrscheinlichkeitstheorie, der ja nichts anderes ist als das Integral $\int f$ einer Funktion f in der Analysis, und nicht zuletzt an die verschiedenen Notationen für die natürlichen Zahlen durch römische Buchstaben oder arabische Ziffern.

4.1.4. Bildlich gesprochen scheint mir die Mathematik wie eine weitverzweigte Höhle, voller Wunder und wertvoller Mineralien, die wir Mathematiker einerseits erkunden und andererseits erschließen. Die Höhle selbst ist objektiv vorhanden und es gilt, immer weiter in sie vorzudringen und Neues zu entdecken und Neues wie Bekanntes nutzbar zu machen. Wo und wie dann jedoch Treppen und Wege und Lampen angebracht werden und eventuell sogar eine kleine Eisenbahn zum Transport der Mineralien, darin haben wir große Freiheit und in diesem Sinne wird Mathematik auch entwickelt. Natürlich sind diese beiden Aufgaben eng miteinander verwoben und wie weit wir selbst vordringen können hängt ganz wesentlich davon ab, wie weit unsere Vorläufer gekommen sind und wie weit sie die Höhle bereits zugänglich gemacht haben.

4.1.5. Die im vorhergehenden dargelegte Auffassung vom Sinn und Wesen der Mathematik bezeichnet man wegen ihrer engen Verwandtschaft mit Plato's Ideenlehre auch als „platonisch“. Barry Mazur fordert in seinem Aufsatz [Maz08] die Platoniker auf, zu erklären, warum Beweise denn uns als Mathematikern so wichtig sein sollten, wenn es nur um das Erkennen einer unabhängig von uns existierenden Wirklichkeit geht. Dieser Aufforderung will ich gerne nachkommen. Ich fasse Beweise auf als Beiträge zum großen Projekt, die Welt der mathematischen Inhalte dem menschlichen Verstand zugänglich zu machen. Mir scheint es in diesem Sinne eine wichtige Aufgabe, auch für bereits bewiesene Erkenntnisse möglichst glatte und für menschliche Gehirne transparente Beweise zu finden, aufzuschreiben und öffentlich zugänglich zu machen. Was das Beweisen angeht, gibt es auch durchaus verschiedene Ansätze: Anschauliche Beweise aus der Schulgeometrie, etwa für den Satz des Pythagoras oder andere elementargeometrische Sätze, wären um im Bild zu bleiben eher ein Art Wegesystem für Fußgänger, wohingegen sich professionelle Mathematiker seit etwa 1900 meist auf einem aus Mengenlehre aufgebauten Schienennetz bewegen, das zwar große anfängliche Investitionen erfordert, danach aber dem Verstand ein sehr schnelles, sicheres und tiefes Eindringen ermöglicht. Allerdings fällt es unseren durch die Bequemlichkeit dieses Zugangs verwöhnten Studenten meist bitter schwer, dann an interessanten und noch nicht erschlossenen Stellen wieder auszusteigen und sich zu Fuß weiter fortzubewegen oder gar selbst Schienen zu legen. Rechnergestützte Beweise sind für mich wie eine Erkundung mit Robotern nicht in derselben Weise befriedigend wie der persönliche Augenschein, aber wenn man an interessante Stellen partout nicht selbst hingelangen kann, sind doch schöne von Robotern geschossene Bilder allemal besser als gar nichts.

4.1.6. Die Mathematik wird insbesondere von Außenstehenden oft als eine tote Wissenschaft erlebt, in der „alles schon seit dreihundert Jahren bekannt sei“. Dieser Eindruck mag damit zusammenhängen, daß Mathematik durchaus „verholzt“ in dem Sinne, daß sie einen festen Stamm an Wissen und kodifizierter Sprache ausbildet. Das aber ermöglicht es unserer Wissenschaft auch gerade wieder, hoch hinaus zu wachsen, und damit das gelingen kann, müssen wir uns alle Mühe geben, in der mathematischen Terminologie keine Sprachverwirrung einreißen zu lassen.

4.1.7. Beim Erlernen dieser Wissenschaft soll man, so denke ich, nach Kräften versuchen, sich aller seiner gedanklichen Fähigkeiten zu bedienen. Geeignet für das Durchdringen mathematischer Sachverhalte scheinen mir insbesondere die räumliche oder noch besser die räumlich-zeitliche Anschauung, das abstrakte logische Denken und das formale Umformen von Zeichenketten auf Papier. Hilfreich kann auch unsere sprachliche Intelligenz sein: Bereits kleine Kinder lernen ja das Zählen, indem sie zunächst „Eins-Zwei-Drei-Vier-Fünf“ memorieren wie „Abrakadabra Simsalabim“, und ältere lernen ähnlich den Satz des Pythagoras oder die binomischen Formeln.

4.1.8. Die Mathematik schöpft große Kraft aus abstrakten Theorien, und nur allzuoft wollen diese ihre Herkunft verbergen und verkleiden sich als zufällig zusammengewürfelte Haufen aus Daten und Axiomen. Man darf sich davon nicht in die Irre führen lassen. Meist sind das vielmehr sehr sorgfältig konstruierte und in immer neuen Versionen an zahlreichen Beispielen erprobte Maschinen, die es einem erlauben, wie in einem Flugzeug mit großer Bequemlichkeit große Wegstrecken zurückzulegen und dabei die meisten konkreten Schwierigkeiten am Boden zu ignorieren. Das alles ist jedoch nur sinnvoll, wenn auch das Starten und das Landen gelingt, und das Herrichten von Start- und Landebahnen kann auch leicht so viel Arbeit bedeuten, daß das ganze Fliegen dadurch uninteressant wird. Bei mancher Theorie habe ich sogar den Eindruck, daß man nur startet aber nie mehr landet, oder noch schlimmer, daß man weder starten noch landen kann, sondern einfach nur sinnlos herumfliegt, aber das mag auch an meiner mangelnden Kenntnis der jeweiligen Theorie liegen – ich nenne besser keine Beispiele.

4.2 Didaktische Gedanken

4.2.1 (**Warum Vorlesungen?**). Warum hören und halten wir in der Mathematik eigentlich Vorlesungen? In der Zeit, in der das Drucken von Büchern noch nicht möglich oder zumindest schwierig und teuer war, mag es sinnvoll gewesen sein, einfach ein Buch vorzulesen, das dann in mehreren Kopien mitgeschrieben werden konnte: In Klöstern wurden etwa die Schriften der Antike und des Christentums lange Zeit auf diese Weise vor dem Vergessen und dem Zerfall gerettet. In der Zeit von Internet und Kopiergeräten kann es jedoch nicht mehr das Ziel einer Vorlesung sein, daß die beteiligten Studenten Mitschriften anfertigen, aus denen sie dann den Stoff lernen: Zu viel wird in solchen Vorlesungen falsch verstanden und falsch abgeschrieben, als daß ich nicht eher das Lernen aus Büchern empfehlen würde. Für den andauernden Erfolg der Vorlesung als Unterrichtsform fallen mir verschiedene Gründe ein.

1. Der Mensch ist nicht gern allein. Es lernt sich besser gemeinsam, man kann sich in der Pause und nach der Vorlesung untereinander über das Gelernte und das nicht Verstandene unterhalten und auch einfach so mal treffen. Die Pause dient insbesondere nicht allein zum Pinkeln oder zum Aufrechterhalten der Konzentration, und es ist doppelt schade, wenn sie ausfällt.

2. Die Vorlesung gibt einen gewissen Rhytmus vor, in dem gelernt und nicht Gelerntes ignoriert und auf später verschoben wird. Anfänger lernen aus Büchern leicht so, wie ganz kleine Kinder spaziergehen: Jeder Kieselstein ist interessant und eine Pause zur ausführlichen Betrachtung wert. Ganz zu Anfang ist das ja auch richtig so, aber dann muß doch die Vorlesung etwas schieben, damit es auch vorangeht.

3. Die Studenten müssen, insbesondere in der Mathematik, regelmäßig davon überzeugt werden, daß prinzipiell durchaus verständlich ist, was sie da lernen sollen, daß es sich nicht um eine Art Zauberformeln handelt, die von Generation zu Generation nur abgeschrieben werden. Sie von der Verständlichkeit des Stoffes zu überzeugen gelingt besonders gut durch das Entwickeln aus dem Kopf an der Tafel. Ein Beamer oder das Auflegen vorbereiteter Folien oder das Ablesen eines vorbereiteten Manuskripts wirken im Vergleich wesentlich weniger überzeugend.

4.2.2 (**Welche Übungen?**). Ich denke, daß man die Mathematik nicht erlernen kann, ohne Übungsaufgaben zu lösen. Allerdings sollten diese zu großen Teilen viel elementarer sein als die in diesem und den folgenden Texten vorgeschlagenen Übungen. Diese dienen eher dazu, ergänzenden Stoff in knapper Form zu präsentieren und sollen auf den Übungsblättern nur einen Teil der Übungen ausmachen.

Insbesondere in den Grundvorlesungen müssen ihnen auch nicht wenig mehr algorithmische Übungen zur Seite gestellt werden, von der Art: Löse dieses lineare Gleichungssystem, invertiere jene Matrix, zerlege dieses Polynom in irreduzible Faktoren und dergleichen mehr.

5 Danksagung

Für Korrekturen und Verbesserungen danke ich Markus Junker, Dominic Maier, Dimitri Guefack, Pascal Soergel.

Literatur

[AL] Skriptum Algebra und Zahlentheorie. Wolfgang Soergel.

[AN1] Skriptum Analysis 1. Wolfgang Soergel.

[EIN] Skriptum Einstimmung. Wolfgang Soergel.

[Gab62] Peter Gabriel. Des catégories abéliennes. *Bull. Soc. Math. France*, 90:323–448, 1962.

[LA1] Skriptum Lineare Algebra 1. Wolfgang Soergel.

[LA2] Skriptum Lineare Algebra 2. Wolfgang Soergel.

[Maz08] Barry Mazur. Mathematical platonism and its opposites. *Newsletter of the EMS*, 68:19–21, 2008.

[TF] Skriptum Fundamentalgruppe und Überlagerungstheorie. Wolfgang Soergel.

Indexvorwort

Hier werden die Konventionen zum Index erläutert. Kursive Einträge bedeuten, daß ich die fragliche Terminologie oder Notation in der Literatur gefunden habe, sie aber selbst nicht verwende. Bei den Symbolen habe ich versucht, sie am Anfang des Index mehr oder weniger sinnvoll gruppiert aufzulisten. Wenn sie von ihrer Gestalt her einem Buchstaben ähneln, wie etwa das $\cup$ dem Buchstaben u oder das $\subset$ dem c, so liste ich sie zusätzlich auch noch unter diesem Buchstaben auf. Griechische Buchstaben führe ich unter den ihnen am ehesten entsprechenden deutschen Buchstaben auf, etwa ζ unter z und ω unter o.

Index