1 Mengen – Abbildungen – Gruppen

1.1 Vorbemerkung.

Die Mathematik ist in gewissem Sinne die Wissenschaft von Mustern in abstrakten Strukturen. Aufgebaut werden diese abstrakten Strukturen durch präzise definierte Begriffe, und zwar indem diese miteinander verknüpft werden, so dass *Aussagen* entstehen. Eine typische solche Aussage ist der Satz "*Es gibt unendlich viele Primzahlen*"[1]. Die Begriffe "unendlich viele", "(Natürliche) Zahl" und "Primzahl" müssen vorher definiert worden sein; "es gibt" ist ein logischer Quantor, der sogenannte Existenzquantor. Aus diesen Begriffen und aus vorher als wahr erkannten Aussagen gewinnt man durch regelrechtes, also den Gesetzen der Aussagenlogik folgendes Schließen die zitierte neue Aussage. Durch die Korrektheit der involvierten logischen Schlüsse erweist sie sich als *wahr* und qualifiziert sich somit als *Satz*.

Neue Begriffe werden unter Zuhilfenahme der Logik gebildet aus bereits vorher definierten Begriffen. Sind die Begriffe "Natürliche Zahl" und "Teilbarkeit" erklärt, lässt sich mit ihrer Hilfe der Begriff "Primzahl" definieren. Weil aber jede neue Aussage nur unter Rekurs auf bereits als wahr erkannte Aussagen bewiesen werden kann, ist es notwendig, eine Anzahl von Begriffen zu versammeln, die als definiert, und Aussagen, die als wahr *festgelegt* werden und als Grundlage alles Kommenden dienen. Sie bilden die "*Axiome*". Axiome können selbst nicht bewiesen werden, weil es keine noch fundamentaleren Aussagen gibt, die man zu ihrem Beweis heranziehen könnte. Vielmehr stellen sie das Fundament dar, auf das nun - mit immer neuen Begriffen, die aus dem Begriffsvorrat der Axiome logisch aufbauend gebildet werden - Satz auf Satz gestellt wird, allein unter Verwendung korrekter logischer Schlüsse[2].

Formalistisch gesehen haben Intuition, Anschauung und der Blick auf die Anwendungen in diesem Spiel logischer Konstruktion nirgends einen Platz. Praktisch gesehen aber – und mit den Augen des Historikers betrachtet erst recht – spielen diese Komponenten jedoch eine zentrale Rolle im Aufbau der Mathematik. Naturwissenschaft, Technik, Ökonomie usw. fordern der

[1] Diese Aussage hat bereits EUKLID im 3. Jahrhundert vor Christus beweisen können.

[2] Es ist naheliegend, daraus ein Wissenschaftsprogramm abzuleiten, nämlich den Anspruch einzulösen, auf die beschriebene axiomatische Weise die gesamte Mathematik vollständig und widerspruchsfrei aufzubauen. "Wir müssen wissen und wir werden wissen!" hat David HILBERT diesen Anspruch selbstbewusst formuliert. Im 20. Jahrhundert jedoch hat dieses Selbstbewusstsein einige heftige Schläge einstecken müssen. Es führte aber aus dem Rahmen dieser Vorlesung leider weit hinaus, diese faszinierende Thematik weiterzuverfolgen. Sie ist mit den Namen der Mathematiker (respektive Logiker) Kurt GÖDEL und Alan TURING verknüpft.

Mathematik Begriffe ab, die sie für die präzise Erforschung ihres eigenen Phänomenbereichs brauchen. Das erklärt die enorme Bedeutung der Mathematik für letztlich alle komplexen Methoden, Verfahren und Technologien der modernen Zivilisation. Kaum ein Laie hat auch nur annähernd eine Vorstellung davon, wieviel tiefe und hochkomplizierte Mathematik dahintersteckt, wenn er mit seinem Smartphone eine verschlüsselte Textnachricht verschickt – von der Funktionalanalysis der Quantentheorie, die hinter der Computertechnik steht, bis hin zur Algebra von Polynomringen bei der Verschlüsselung ist alles an Bord, was gut und teuer ist. Umgekehrt hat gerade die Physik ganz wesentlich die Bildung großer Teile der Mathematik erschlossen[3].

Wir werden im Folgenden aber *nicht* den Weg wählen, aus formalen Axiomen nur durch regelrechtes logisches Schließen die Lineare Algebra aufzubauen. Das wäre entschieden zu umständlich (wiewohl sich einiges an zunächst aufwändig erscheinendem begrifflichem Instrumentarium später wiederum als sehr hilfreich und arbeitssparend erweisen würde), und außerdem wollen wir das Vorwissen, das jeder aus der Schule mitbringt, und die Anschaulichkeit gerade der Begriffe der Linearen Algebra nutzen, um zügig voranzukommen[4]. Wir werden also Argumente zulassen, die zum Beispiel aus der Anschauung des dreidimensionalen Raumes kommen, strenggenommen logisch unvollständig sind und irgendwie "*hand waving*". Wirklich *falsch* darf es natürlich nicht sein, wie wir argumentieren, aber mathematische Exaktheit streben wir gar nicht erst an. Argumentationen sind andererseits essenziell, um zu verstehen, wie die verschiedenen Begriffe untereinander zusammenhängen.

Denn Ziel ist es, ein belastbares Netz aus Begriffen zu schaffen, mit denen Sinn, Bedeutung und Anschauung verbunden sind. Wenn die Knoten dieses Netzes von Begriffen gebildet werden, dann sind Argumentationen, Beweise und gedanklich schlussfolgernde Überlegungen die Verbindungen zwischen den Knoten. Ohne diese Verbindungen würde alles auseinanderfallen. Es ist aber notwendig, ein starkes Netz zu knüpfen, damit die später – gerade auch in der beruflichen Praxis – hinzukommenden neuen Begriffe durch das Netz aufgefangen und darin eingebaut werden können. Ein Teil dieser schlussfolgernden Überlegungen realisiert sich durch das, was man landläufig "rechnen" nennt. Es soll aber an dieser Stelle betont werden, dass das Rechnenkönnen

[3]Das ist spürbar bis in die Namensgebung der mathematischen Begriffe hinein. Von der Logik des axiomatischen Aufbaus her könnte man mathematische Begriffe ja *irgendwie* benennen, mit selbstausgedachten Vokabeln – in der Praxis orientieren sich die Namen aber natürlich an den Anwendungen, aus denen heraus sie entstanden sind.

[4]Einer der ambitioniertesten Versuche, die ganze Mathematik aus einem Satz von Axiomen und Schlussregeln aufzubauen, sind die Principia Mathematica des Logikers und Philosophen Bertrand Russell. Sie sind nicht dafür bekannt, zügig voranzukommen. In der Tat wird häufig kolportiert, dass man die ersten etwa 1.000 Seiten dieses Werkes bewältigen müsse, um zu dem – dann natürlich ohne jede Anschauung auskommenden und logisch stringenten – Beweis zu kommen, dass $1 + 1 = 2$ ist.

weder notwendig noch hinreichend ist[5] für das Verständnis wie auch für das Anwendenkönnen der Linearen Algebra. Um es konkret zu machen: natürlich muss man *auch* die Determinante einer 3×3-Matrix ausrechnen können, wenn man verstehen möchte, was Lineare Abbildungen ausmacht. Aber es ist nicht ausreichend, so etwas zu können, um zu einem echten Verständnis zu gelangen, und es ist das Verständnis, um das es geht. Das Konzept der Determinante erschließt sich bei weitem nicht durch Ausrechnenkönnen. Und in der beruflichen Praxis wird es mit überwältigender Wahrscheinlichkeit niemals geschehen, dass man von den vorkommenden (und meistens eben auch sehr großen) Matrizen *von Hand* die Determinante ausrechnen muss. Hingegen muss man zum Verstehen, Anpassen, Erweitern eines Algorithmus gegebenenfalls durchaus eine sehr genaue Vorstellung vom begrifflichen Konzept der Determinante haben. Das Rechnen kann man dann im Zweifelsfall einem Computer Algebra System (CAS) überlassen.

Im folgenden Abschnitt versammeln wir einiges Grundlegendes über Logik, jedenfalls so weit wir es brauchen, um *hand waving* zielführend argumentieren zu können.

1.2 Aussagenlogik.

Sind A und B zwei mathematische Aussagen, so bedeute $A \Rightarrow B$ (lies "aus A folgt B"): wenn A richtig ist, dann trifft auch B zu. Das darf man nicht verwechseln mit $A \Leftarrow B$, was gleichbedeutend ist mit $B \Rightarrow A$ und heißt, dass A richtig ist, wenn B zutrifft.

Sind zwei Aussagen A und B durch $A \Rightarrow B$ verbunden, so sagt man, A sei *hinreichend* für B und umgekehrt, B sei *notwendig* für A. Die erstere Sprechweise ist naheliegend, die zweite ist aber ebenfall suggestiv, denn wenn B nicht gilt, kann A nimmermehr wahr sein – *wäre* A wahr, würde wegen $A \Rightarrow B$ ja auch B gelten. Ist A sowohl hinreichend als auch notwendig für B, gelten also $A \Rightarrow B$ wie auch $B \Rightarrow A$. Das kann man als $A \Leftrightarrow B$ abkürzen und sagt dann, die beiden Aussagen A und B seien *äquivalent.*

Eine Aussage A können wir *verneinen.* Zum Beispiel wird die Aussage "zu jedem $\varepsilon > 0$ gibt es ein δ mit $|f(x_0) - f(x)| < \varepsilon$ für alle x, wenn nur $|x_0 - x| < \delta$ ausfällt" verneint zu "nicht zu *jedem* $\varepsilon > 0$ gibt es ein δ mit $|f(x_0) - f(x)| < \varepsilon$ für alle x, wenn nur $|x_0 - x| < \delta$ ausfällt", oder anders formuliert "es gibt ein $\varepsilon > 0$, so dass $|f(x_0) - f(x)| \geqslant \varepsilon$ bleibt für jedes δ und $|x_0 - x| < \delta$".

[5] Im nächsten Abschnitt werden die Begriffe "notwendig" und "hinreichend" als Grundlagenbegriffe der Aussagenlogik näher erklärt.

Ferner können Aussagen mittels logischer Verknüpfungen verbunden werden. Die wichtigsten in dieser Vorlesung vorkommenden sind die logische *Konjunktion* und die logische *Disjunktion*, gemeinsprachlich und im Folgenden “Und-Verknüpfung” respektive “Oder-Verknüpfung” genannt. Eine Aussage, die aus zwei mit “und” verknüpften Teilsussagen zusammengesetzt ist, ist genau dann wahr, wenn beide Teilaussagen gleichzeitig wahr sind. Eine Aussage, die aus zwei mit “oder” verknüpften Teilaussagen zusammengesetzt ist, ist genau dann wahr, wenn wenigstens eine der beiden Teilaussagen wahr ist (es handelt sich demnach beim logischen “oder” um ein nichtausschließendes “oder”). In den Übungen gibt es einfache Beispiele dazu. Im übrigen sei die sogenannte BOOLE*sche Algebra* als axiomatische Formalisierung der Aussagenlogik erwähnt. Sie spielt als *Schaltalgebra* eine beduetende Rolle in der Informatik.

1.3 Mengen und Mengenverknüpfungen.

Die beiden zentralen Begriffe, mit denen wir es immer und immer wieder zu tun haben werden, sind die der *Menge* und der *Abbildung*. In diesem Abschnitt wenden wir uns ersterem zu und setzen *naiv*, also ohne axiomatisch-formale Basis für die in der Definition verwendeten Begriffe, das folgende fest

> **Definition.** Eine *Menge* ist eine (irgendwie) wohldefinierte Gesamtheit von wohlunterschiedenen Objekten des Denkens oder der Anschauung. Diese Objekte heißen dann *Elemente* der Menge.

Als Definition ist das, wie gesagt, eher eine philosophische denn eine mathematische, denn sie wimmelt von Begriffen, von denen eigentlich nicht in präziser Weise klar ist, was sie bedeuten sollen. Wir wollen uns daran aber nicht stören, denn bei den Mengen, mit denen wir es zu tun haben werden, wird sich das nicht als Problem erweisen. Auf zwei wichtige Konstituenten der Definition wollen wir aber hier (und in den Übungen) gleichwohl eingehen.

- Eine Menge kennt zunächst einmal keine *Ordnung*. Die Mengen $\{1, 2, 3\}$ und $\{3, 1, 2\}$ sind *identisch*. (Zur Schreibweise mit den sogenannten “Mengenklammern” siehe weiter unten.)
- Die Elemente einer Menge sind *wohlunterschieden*: so etwas wie $\{1, 2, 2, 5\}$ ist *identisch* mit $\{1, 2, 5\}$.

Wichtig, weil in dieser Vorlesung – und nicht nur dort – immer wieder verwendet, sind die folgenden **Schreibweisen** und Sprechweisen. Ist x ein Objekt der Menge M, so schreiben wir $x \in M$ und lesen "x ist Element von M" oder "x liegt in M". Ist dies andererseits jedoch nicht der Fall, drücken wir das durch $x \notin M$ aus und sagen, x sei nicht Element von M oder x liege nicht in M.

Es gibt mehrere Arten, Mengen explizit anzugeben. Mehr oder weniger allen gemeinsam ist die Verwendung der geschweiften sogenannten *Mengenklammern* "$\{$" und "$\}$", die zwischen sich die Beschreibung der Menge einschließen. Bei kleinen Mengen von nur ein paar Elementen kann man diese einfach einzeln hineinschreiben: so ist zum Beispiel $\{6, 3, 9\}$ die Menge der drei Zahlen 3, 6 und 9. Man kann mittels dreier "und so weiter"-Punkte auch eine Menge als $\{3, 6, 9, 12, ...\}$ schreiben. Das würde hier die Menge der ganzzahligen Vielfachen von 3 bezeichnen. Man sollte das aber nur dann tun, wenn durch die Schreibweise und aus dem Zusammenhang wirklich ganz klar ist, was die drei Pünktchen tatsächlich meinen. Geht alles das nicht mehr, können wir die Elemente einer Menge auch durch eine gemeinsame Eigenschaft charakterisieren: zum Beispiel $\{n \in \mathbb{N} \,|\, n \text{ ist gerade}\}$. Statt des senkrechten Striches, der die gemeinsame Bedingung in der Klammer abtrennt, findet sich übrigens häufig auch ein Doppelpunkt. Die Menge $\mathbb{N}$, die in diesem Beispiel auftaucht, ist eine der Standardbezeichnungen für Zahlenmengen, auf die wir weiter unten noch zu sprechen kommen werden.

Es sollte vielleicht eigens Erwähnung finden, dass Mengen nicht immer nur Zahlen enthalten müssen. Die Menge $\{(1, 2), (3, 4), 5\}$ zum Beispiel hat drei Elemente: die beiden 2-Tupel[6] $(1, 2)$ und $(3, 4)$ sowie die Zahl 5. Sie ist verschieden von etwa der Menge $\{(1, 2, 3, 4, 5)\}$, die nur ein einziges Element enthält, ein 5-Tupel. Die Mengen $\{1, 2, 3, 4, 5\}$, $\{(1, 2, 3, 4, 5)\}$ und $\{(5, 4, 3, 2, 1)\}$ sind alle untereinander verschieden, während $\{5, 4, 3, 2, 1\}$ der ersten gleich ist – man mache sich dies an Hand der Definition sorgfältig klar! Im Übrigen darf eine Menge durchaus auch selber wieder Mengen enthalten. Die Menge $\{\{1, 2, 3\}\}$ ist absolut wohldefiniert und enthält – *ein einziges* Element! (nämlich welches?) Darauf aufsetzend können wir dann auch die *Menge aller Teilmengen* einer vorgegebenen Menge M bilden. Man nennt sie *Potenzmenge* von M und kürzt sie mit $\mathcal{P}(M)$ ab. Es handelt sich wohlgemerkt also bei $\mathcal{P}(M)$ stets um eine Menge, die selber wieder Mengen enthält.

Für den praktischen Umgang mit Mengen hat es sich als genialen Schachzug erwiesen, auch

[6] Das sind *geordnete* Paare (x, y) von Elementen irgendwelcher Mengen. 3-Tupel, 4-Tupel usw. sind entsprechend definiert. Wir kommen darauf noch zurück.

eine Menge zuzulassen, die *überhaupt kein* einziges Element enthält. Man nennt diese Menge naheliegenderweise die **Leere Menge**. Man kann sie durch das Symbol $\{\}$ bezeichnen oder auch durch $\varnothing$, einer Art durchgestrichenen Kringels.

Die folgenden feststehenden Symbole für die Standard-Zahlenmengen werden auch wir immer wieder kommentarlos benutzen:

$\mathbb{N} = \{1, 2, 3, 4, 5, ...\}$ ist die Menge der *Natürlichen Zahlen.*

$\mathbb{N}_0 = \{0, 1, 2, 3, 4, 5, ...\}$ ist die Menge der *nichtnegativen Ganzen Zahlen.*

$\mathbb{Z} = \{..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...\}$ ist die Menge der *Ganzen Zahlen.*

$\mathbb{Q} = \{\frac{p}{q} \,|\, p, q \in \mathbb{Z}$ und $q \neq 0\}$ ist die Menge der *Rationalen Zahlen*, also der Bruchzahlen.

$\mathbb{R}$ ist die Menge der *Reellen Zahlen.*

$\mathbb{C}$ ist die Menge der *Komplexen Zahlen.*

Wie die einzelnen Zahlenmengen axiomatisch festgelegt werden, insbesondere wie man die Reellen Zahlen aus den Rationalen Zahlen gewinnt vermittels DEDEKINDscher Schnitte, soll uns hier nicht weiter interessieren. Einen Minimalabriss der Komplexen Zahlen, die uns in der Matrizenrechnung hie und da begegnen werden, gibt es als Anhang zu diesem Kapitel. Ansonsten gehen wir mit allen diesen Zahlen so um, wie wir es in der Schule gelernt haben.

Aus gegebenen Mengen können wir neue schaffen. Die folgenden *Mengenverknüpfungen* sind elementar wichtig:

Definition. Seien M und N zwei beliebige Mengen. Dann heißt

$M \cup N := \{x \,|\, x \in M$ oder $x \in N\}$ die *Vereinigungsmenge* von M und N;

$M \cap N := \{x \,|\, x \in M$ und $x \in N\}$ die *Schnittmenge* von M und N;

$M \backslash N := \{x \,|\, x \in M$ und $x \notin N\}$ das *Komplement* von N in M.

$M \cup N$ entsteht, anschaulich gesprochen, aus M und N, indem man deren Elemente zusammenkippt. $M \cap N$ entsteht, indem man alle diejenigen Elemente zusammentut, die sowohl in M als auch in N enthalten sind. Das Komplement $M \backslash N$ umfasst alle Elemente von M, die nicht auch in N sind. Wenn man die logischen Verknüpfungen "und" und "oder" durch die Symbole "$\wedge$" und "$\vee$" ersetzt, sieht man die Verwandtschaft der obigen Mengenverknüpfungen mit der Aussagenlogik: $x \in M \cap N \iff x \in M \wedge x \in N$. Nicht zufällig sind die logischen Verknüpfungszeichen so orientiert (Öffnung nach oben beziehungsweise unten) wie die Mengenverknüpfungszeichen, die sie erzeugen.– Für das Komplement einer Menge N in einer Menge M findet sich häufig eine alternative Notationsweise, nämlich für den Fall, dass M eine *Grundmenge* ist, auch *Universum* genannt, also sozusagen die maximal gegebene Menge, in der wir uns stets bewegen. Wenn wir beispielsweise Untersuchungen machen, die sich ausschließlich mit Teilmengen von Reellen Zahlen befassen, würden wir $\mathbb{R}$ als die Grundmenge ansprechen, in der wir uns aufhalten. Das Komplement $\mathbb{R} \backslash N$ einer Teilmenge N von $\mathbb{R}$ wird dann gerne als N^{c} bezeichnet – C für "*complement*" – oder auch nur als N'. Das sind dann ganz einfach alle Reellen Zahlen außerhalb von N.

Eine weitere Methode, aus vorgegebenen Mengen weitere zu erzeugen, ist die Bildung *cartesischer Produkte*[7]. Hier lautet die

Definition. Das *cartesische Produkt* der beiden Mengen M und N ist festgelegt als

$$M \times N := \{\, (x, y) \,|\, x \in M \text{ und } y \in N\} \ .$$

Es handelt sich also um alle *geordneten Paare*, die man bilden kann, wenn das erste Element des Paares aus M stammt und das zweite aus N. Es dürfte induktiv klar sein, wie Produkte der Form $M \times N \times O$ und so weiter zu verstehen sind. Abkürzend schreibt man $M \times M$ auch als M^2, $M \times M \times M$ als M^3 etc. In den Übungen schauen wir uns Beispiele dazu an. Für uns in der Linearen Algebra werden die Mengen $\mathbb{R}^n$ und $\mathbb{C}^n$ außerordentlich wichtig werden, also die geordneten n-Tupel $(x_1, x_2, \ldots, x_n)$ von reellen beziehungsweise komplexen Zahlen. Diese Tupel sind quasi die Archetypen endlichdimensionaler reeller respektive komplexer Vektoren.

Mengen können zueinander in Beziehungen stehen. Beispielsweise sehen wir, dass alle Elemente der Menge $\{2, 3\}$ auch in der Menge $\{1, 4, 3, 2\}$ vorkommen (wenn auch nicht umgekehrt). Wir schreiben $M \subseteq N$ und sagen, M sei eine **Teilmenge** von N, auch *Untermenge* genannt, wenn für alle x die Schlussfolgerung $x \in M \Rightarrow x \in N$ richtig ist. Gleichbedeutend kann man das übrigens auch als $N \supseteq M$ notieren, wenn es eben gerade praktischer ist. Das Zeichen "$\subset$" findet

[7]so bezeichnet nach dem französischen Philosophen und Mathematiker René DESCARTES, der sich – der Mode seiner Zeit folgend – in latinisierter Form auch "Cartesius" nannte.

Verwendung, wenn $M \subseteq N$ gilt, es aber ein $x \in N$ mit $x \notin M$ gibt: M ist dann eine "echte" Unter- oder Teilmenge von N, das heißt N entält noch einige Elemente mehr als M. Die Zeichen "$\subset$" und "$\subseteq$" beziehungsweise "$\supset$" und "$\supseteq$" haben untereinander also Beziehungen, die vergleichbar sind denen der Zeichen "$<$" und "$\leqslant$" beziehungsweise "$>$" und "$\geqslant$".

Zwei Mengen M und N heißen *gleich*, in Zeichen $M = N$, wenn gleichzeitig $M \subseteq N$ und $N \subseteq M$ gelten. Diese Festlegung erscheint so einleuchtend wie überflüssig, wenn man nur an Mengen wie $\{1, 2, 3\}$ denkt. In komplexeren Gefilden ist es aber manchmal wirklich schwierig, die Gleichheit zweier Mengen direkt einzusehen. Man geht den entsprechenden Beweis unter Umständen sinnvollerweise so an, dass man zunächst $M \subseteq N$ beweist und dann $N \subseteq M$.

Für die Leere Menge $\varnothing$ legen wir fest, dass $\varnothing \subseteq M$ gilt, die Leere Menge ist also Teilmenge *jeder* Menge[8].

Mit diesen ganzen Begrifflichkeiten und Verknüpfungen lassen sich schon durchaus komplexe Aussagen formulieren und beweisen. Für ein System[9] $\mathcal{S}$ von Mengen gilt beispielsweise $(\bigcup_{M\in\mathcal{S}})' = \bigcap_{M\in\mathcal{S}} M'$, wenn das Hochkomma die Komplementbildung bezeichnet. Das ist eine der MORGANschen Komplementierungsregeln: das Komplement der Vereinigung aller Mengen eines Systems ist gleich der Schnittmenge aller Komplemente dieser Mengen. Die MORGANschen Regeln haben eine äquivalente Formulierung in der Aussagenlogik, das heißt in der Schaltalgebra.

Viele derartiger Aussagen kann man sich recht einfach klarmachen, wenn man sie mit Hilfe von VENN-Diagrammen visualisiert. Eine geschlossene, irgendwie halbwegs runde oder rundovale Linie in der Ebene stellt dabei eine Menge M vor, das heißt: die Punkte innerhalb der Linie sollen die Elemente der Menge sein, die Punkte auf dem Zeichenblatt, die außerhalb liegen, gehören nicht zur Menge. Zeichnet man eine zweite Menge N dazu in der Weise, dass sich die Linien zweimal kreuzen, kann man das Gebiet schraffieren, das zu jeder der beiden Mengen gehört und damit die Schnittmenge der beiden Mengen $M \cap N$ zeichnerisch repräsentiert. Es ist dann nicht schwer, sich an Hand der Zeichnung zum Beispiel folgendes zu verdeutlichen: $(M\backslash N) \cup (N\backslash M) = (M \cup N)\backslash(M \cap N)$. Etwas schwieriger wird diese Art der "Beweisführung" nur, wenn unendliche Mengensysteme ins Spiel kommen. Das wird aber eher in Gebieten wie

[8]... was man nicht vergessen sollte, wenn man die Potenzmenge $\mathcal{P}(M)$ einer Menge M bildet. Die Leere Menge gehört da nämlich dieser Festlegung wegen mit hinein.

[9]Man konstruiert *Systeme* von Mengen statt *Mengen* von Mengen zur Vermeidung sogenannter Antinomien. Ein System von Mengen ist im wesentlichen eine Menge von Mengen, in der es nicht vorkommt, dass eben dieses System auch ein Element (seiner selbst) ist.

Topologie oder Maßtheorie der Fall sein und weniger in unserer Linearen Algebra.

Mit Mengen allein kann man nun wenig anfangen. Die einzelnen Elemente einer Menge, die "nur" Menge ist, lassen sich ja überhaupt nicht zueinander in Beziehung setzen. Man verdeutliche sich, dass mit der Schaffung der Natürlichen Zahlen $\mathbb{N}$ noch keineswegs definiert ist, was $2 + 2$ bedeuten soll oder ob $4 < 5$ ist oder nicht: weder eine *Verknüpfung* zwischen den Elementen von $\mathbb{N}$ ist vorderhand definiert noch eine Größer-Kleiner-Relation. Wie in der Vorbemerkung angedeutet, macht man deshalb den nächsten Schritt und stattet die betrchteten Mengen mit zusätzlichen *Strukturen* aus. Wenn eine Menge zusätzlich eine Struktur bekommt, redet man gerne von einem *Raum*. Mit bestimmten Verknüpfungen ausgestattet, kann eine Menge so zu einer Gruppe werden, zu einem Vektorraum, zu einem topologischen Raum, zu einer Riemannschen Mannigfaltigkeit und so weiter. Immer handelt es sich um Mengen, nur sind auf diesen in axiomatischer Weise Zusatzstrukturen erklärt. *Die* Struktur der Linearen Algebra schlechthin ist die des Linearen Raumes, auch Vektorraum genannt. Zu seiner Definition gelangen wir wie folgt: zunächst betrachten wir das Konzept der *Abbildung* zwischen zwei Mengen, um dann bestimmte Arten von Abbildungen für die Definition der *Gruppe* zu verwenden. Von da ist es dann nur noch ein kleiner Schritt zum Begriff des Vektorraums.

1.4 Abbildungen.

Verkürzt formuliert, besteht die Mathematik aus dem Studium derjenigen Muster und Strukturen, die man mit den Begriffen von "Menge" und "Abbildung" fassen kann. Mit Mengen haben wir uns nun beschäftigt, jetzt kommen die Abbildungen dran.

Eine *Abbildung*, synonym auch *Funktion* genannt, besteht aus drei Stücken: der *Definitionsmenge*, der *Zielmenge* und der *Abbildungsvorschrift*. Es ist wichtig, sich dies zu verdeutlichen, zumal in der Schulmathematik sehr stark die Funktions- oder Abbildungs*vorschrift* betont wird und die beiden anderen Bestimmungsstücke "Definitionsmenge" und "Zielmenge" so mitlaufen. Die Angaben "$f(x) = x^2$" oder "$y = \sin(x)$" sind aber unvollständig. Was sind denn das für Elemente, die f da quadrieren soll? Zahlen? und wenn ja, welche? oder am Ende gar Matrizen oder Operatoren? Es ist auch nicht verzichtbar, die Zielmenge einer Funktion explizit anzugeben – wichtige Eigenschaften wie Invertierbarkeit hängen davon ab. Wir setzen jetzt zunächst einmal die

Definition. Eine **Abbildung** oder **Funktion** f ordnet *jedem* Element einer *Definitionsmenge* D *genau ein* Element einer *Zielmenge* Z zu. Wir schreiben $f : D \to Z; x \mapsto f(x)$.

Ein paar Bemerkungen dazu:

- Die Vorschrift f ordnet *jedem* Element von D genau ein Element in Z zu. Deshalb ist zum Beispiel $f : \mathbb{R} \to \mathbb{R}; x \mapsto \frac{1}{x}$ *keine* gültig definierte Abbildung (warum genau nicht?).
- Die Vorschrift f ordnet jedem Element von D *genau ein* Element in Z zu. Deshalb ist zum Beispiel $f : \mathbb{R} \to \mathbb{R}; x \mapsto \pm 2$ *keine* gültig definierte Abbildung.
- Hingegen ist es nicht erforderlich, dass zu *jedem* Element der Zielmenge ein Element der Definitionsmenge gehört, das vermittels f ihm zugewiesen wird.
- Auch darf es sein, dass es zwei oder mehrere Elemente in D gibt, denen f ein und dasselbe Element in Z zuweist.
- Zwei Abbildungen $f : D \to Z; x \mapsto f(x)$ und $g : E \to Y; x \mapsto g(x)$ heißen *gleich*, wenn $D = E$ und $Z = Y$ ist *und* die beiden Abbildungsvorschiften f und g übereinstimmen. Letzteres allein genügt also nicht!
- Wenn $y = f(x)$ ist für ein $x \in D$, nennt man y auch Bild(punkt) von x unter f.
- Alle diejenigen $x \in D$, die von f auf ein vorgelegtes $y \in Z$ abgebildet werden, formen die *Urbildmenge* von y unter f. Man notiert sie üblicherweise als $f^{-1}(y)$. Formal ist also $f^{-1}(y) := \{x \in D \,|\, f(x) = y\}$. Die Notation $f^{-1}(y)$ ist allerdings nicht ganz unproblematisch. Es handelt sich ja *nicht* um die Anwendung einer wie auch immer definierten Funktion $f^{-1} : Z \to D$ auf y (und diese Funktion kann es durchaus geben – siehe weiter unten –, muss es aber nicht notwendigerweise), sondern um die immer mögliche Definition einer *Menge* unter Verwendung des Punktes y und der Vorschrift f (die dafür keine "umgekehrte" Vorschrift f^{-1} zu kennen braucht). Übrigens braucht man sich durchaus nicht auf ein einzelnes $y \in Z$ zu beschränken für diese Urbild-Bildung. Wir können leicht auch $f^{-1}(Y)$ definieren als Urbildmenge für irgendeine nicht notwendig einpunktige Teilmenge $Y \subseteq Z$ via $f^{-1}(Y) := \{x \in D \,|\, f(x) \in Y\}$. So gesehen wäre es schön, wenn man sich für die Schreibung des Urbildes eines Punktes y auf $f^{-1}(\{y\})$ verständigen würde. Tut man aber leider nicht.

- Es ist üblich, verschiedenartige Pfeilsymbole in der Definition der Abbildung zu benutzen – so, wie oben zu sehen (eines der Symbole hat einen zusätzlichen senkrechten Strich am linken Ende).

Zum Verständnis der folgenden Elementarbegriffe hilft es, sich eine Funktion zeichnerisch darzustellen analog zu den im Abschnitt über Mengen angeregten VENN-Diagrammen: die Definitionsmenge D bekommt eine geschlossene Kreislinie, die Zielmenge Z kriegt auch eine, und die Elemente in beiden markiert man zusätzlich durch Kreuzchen oder besser dicke Punkte. Dann kann man sich die Funktionsvorschrift durch Pfeile visualisieren, die bei einem Punkt in D beginnen und je auf einen Punkt in Z weisen. Die Definition verlangt, dass von *jedem* Punkt in D ein Pfeil ausgeht. Nicht jeder Punkt in Z aber muss getroffen werden. Es darf andererseits aber sein, dass ein Punkt in Z von mehreren Pfeilen getroffen wird. Wenn man sich nun überlegt, unter welchen Bedingungen ein *Umkehren* der Pfeile wieder zu einer gültigen Abbildung führt, diesmal *von Z nach D*, dann sieht man schnell ein: das klappt nur, wenn a) *jeder* Punkt in Z von einem Pfeil getroffen wird (denn sonst wäre die "umgekehrte" Abbildung nicht auf *ganz* Z definiert) und b) niemals *mehrere* Pfeile ein und dasselbe Element in Z treffen (denn sonst wüssten wir beim Umkehren nicht, welches Element aus D diesem Element aus Z zugewiesen werden soll). Das Bild, das auf dem Papier entsteht, wenn man sich eine umkehrbare Abbildung basteln will, zeigt zwei geschlossene Kreislinien für D und für Z mit gleichvielen Elementen darin und Pfeilen, die diese immer paarweise verbinden; es ist dann sozusagen egal, ob wir die Pfeilspitzen nach links oder nch rechts weisen lassen.

Um diese anschauliche Vorstellung etwas mathematischer aufzuschreiben – gedanklich wird es nicht schwieriger –, formulieren wir die folgende naheliegende

> **Definition.** Sei $f : D \to Z; x \mapsto f(x)$ eine Abbildung der Definitionsmenge D in die Zielmenge Z. Die Teilmenge $B \subseteq Z$ von Z, die vermöge der Festlegung $B := \{y \in Z \mid \textit{es gibt mindestens ein } x \in D \textit{ mit } y = f(x)\}$ definiert ist, heißt **Bild** von D in Z unter f oder einfach $\mathrm{Bild}(f)$. Außerhalb des deutschen Sprachraums ist die Schreibweise $\mathrm{Im}(f)$ verbreitet.

Weiter oben haben wir bereits vom "Bild" eines Punktes $x \in D$ unter f gesprochen. Das war dann ein *Punkt* in Z. Das "Bild von f" ist hingegen eine Menge, nämlich einfach alle diejenigen Elemente der Zielmenge, die Bilder sind unter f von Elementen aus D. Man kann das auch einfach als $f(D)$ schreiben, wenn man sich vor Augen hält, was das bedeutet: sukzessive *alle* Punkte von D in f einsetzen und dann schauen, welche Teilmenge von Z man so generiert.

Eine der Bedingungen, die wir brauchen, um eine vorgegebene Abbildung umkehren zu können, war, dass jedes Element der Zielmenge von einem Pfeil getroffen wird. Mit der gerade vorgenommenen Begriffsbildung schreibt sich das einfach als $\mathrm{Bild}\, f = Z$. Es gibt eine eigene Bezeichnung für Funktionen mit dieser Eigenschaft:

> Eine Abbildung $f : D \to Z$ heißt **surjektiv**, wenn $\mathrm{Bild}\, f = Z$ ist.

Diese Wortschöpfung ist vermutlich nur für hartgesottene Lateiner anschaulich[10]. In der englischsprachigen Literatur heißen solche Abbildungen einfach "*onto*".

Die andere Bedingung für Umkehrbarkeit war, dass niemals zwei oder mehr x-Werte aus D auf ein und dasselbe $y \in Z$ geworfen, zwei beliebig herausgegriffenen verschiedenen x-Werten also immer auch zwei verschiedene y-Werte zugewiesen werden. Auch dafür gibt es, wen wird es wundern, wieder eine gelehrtsprachliche Bezeichnung:

> Eine Abbildung $f : D \to Z$ heißt **injektiv**, wenn für zwei beliebige $x_1, x_2 \in D$ mit $x_1 \neq x_2$ stets $f(x_1) \neq f(x_2)$ folgt.

Englisch heißen sie "*one-to-one*". Und dann setzen wir noch einen drauf:

> Eine Abbildung $f : D \to Z$ heißt **bijektiv**, wenn sie surjektiv und injektiv ist. Man nennt bijektive Abbildungen auch *Bijektionen*.

Bijektivität heißt anschaulich gesprochen also folgendes: jedem x wird durch f genau ein y zugewiesen, und zu jedem y gehört genau ein x, so dass f diesem x das y zuweist. Das ist genau die oben beschriebene Situation mit den Kreisen, Punkten und Pfeilen, wo die Punkte in D und die Punkte in Z paarweise einander zugeordnet sind. Wir können in diesem Fall, und *nur* in diesem Fall, die Abbildung $f : D \to Z$ **umkehren** zu einer Abbildung $f^{-1} : Z \to D$. Die Pfeile

[10] *iacere* heißt "werfen". Das zielt vermutlich auf die Wirkung der Pfeile ab, die ein $x \in D$ in das zugehörige $f(x) \in Z$ "werfen".

ändern allesamt ihre Richtung, und Definitions- und Zielmenge ändern ihre Rollen: was für f Definitionsmenge war, ist Zielmenge für f^{-1}, und umgekehrt. Die so gebildete Funktion f^{-1} heißt **Umkehrfunktion** oder auch **Inverse** von f.

In den Übungen werden ein paar Beispiele gegeben für Funktionen, die injektiv, surjektiv oder beides sind oder nichts davon. Es ist wichtig, sich diese Elementarbegriffe an einfachen Beispielen zu verdeutlichen – wir werden sie in der Matrizenrechnung ständig verwenden. Man betrachte etwa die drei Funktionen $f : \mathbb{R} \to \mathbb{R}; x \mapsto x^2$, $g : \mathbb{R} \to \mathbb{R}_0^+; x \mapsto x^2$, $h : \mathbb{R}_0^+ \to \mathbb{R}; x \mapsto x^2$ und $k : \mathbb{R}_0^+ \to \mathbb{R}_0^+; x \mapsto x^2$. Obwohl die Funktionsvorschrift immer "x quadrieren" lautet, ist eine von ihnen surjektiv, aber nicht injektiv; eine ist injektiv, aber nicht surjektiv; eine ist weder injektiv noch surjektiv und eine ist sowohl injektiv als auch surjektiv (mithin bijektiv). Umkehrbar ist natürlich nur die letztere, und die Umkehrfunktion lautet...? Ja – und welche ist welche?

Wenn wir, ausgehend von einem $x \in D$, das bijektive f anwenden, in $f(x) \in Z$ landen und auf dieses $f(x)$ dann f^{-1} anwenden, landen wir offensichtlich wieder in D, und zwar konstruktionsgemäß gerade wieder in x. Das ist ja die Grundidee des Umkehrens: Ändern der Pfeilrichtung. Um dies mathematisch hinzuschreiben, bedürfen wir zunächst des Begriffs der Hintereinanderausführung von Abbildungen, der aber genau das meint, was wir uns anschaulich darunter vorstellen würden:

> Es seien $f : D_f \to Z_f$ und $g : D_g \to Z_g$ zwei Abbildungen und es gelte $D_g \supseteq \operatorname{Bild} f$. Dann heißt die Abbildung $g \circ f : D_f \to Z_g$ die **Zusammensetzung** der Abbildungen f und g, auch *iterierte* Abbildung oder *Komposition* genannt; sie ist definiert durch $(g \circ f)(x) := g(f(x)) \in Z_g$ für alle $x \in D_f$.

Man beachte, dass diese Definition zulässig, man sagt: *wohldefiniert* ist: zunächst bildet f das x aus seinem Definitionsbereich in ein $f(x)$ ab, das in Z_f liegt, das heißt genauer in $\operatorname{Bild} f$ als Teilmenge von Z_f. Nun ist dieses $\operatorname{Bild} f$ voraussetzungsgemäß eine Teilmenge von D_g. Auf ganz D_g, mit Sicherheit also auch auf dem darin enthaltenen $\operatorname{Bild} f$ ist aber g definiert und kann somit auf $f(x)$ angewandt werden, liefernd $g(f(x))$. Man mache sich eine Zeichnung dazu und beachte die Reihenfolge, in denen f und g anzuwenden sind und in $g \circ f$ sowie $g(f(x))$ auftreten. Beim Zeichnen erfasse man auch den allgemeinen Fall, dass nämlich die drei Mengen Z_f, $\operatorname{Bild} f$ und D_g untereinander alle verschieden sind!

Die Komposition von Funktionen ist nichts Exotisches. Die Analysis wimmelt von ihnen – $x \mapsto \sin^2(x)$, $x \mapsto \frac{1}{1+x}$, $x \mapsto \mathrm{e}^{x^2}$ und so weiter und so weiter; schon im Schulunterricht nimmt man durch, wie man solche Zusammensetzungen ableitet, mittels Substitution integriert et cetera. Die Zusammensetzung Linearer Abbildungen, die wir in einem eigenen Kapitel studieren werden, wird sich auf der Ebene der zugehörigen Matrizen als Matrixmultiplikation entpuppen, ein schlechterdings unentbehrliches Werkzeug. Hier interessiert uns zunächst einmal die Zusammensetzung einer bijektiven Funktion mit ihrer Umkehrung, von der wir weiter oben bereits in anschaulicher Weise gesehen haben, dass sie von einem anfänglichen x wieder zu diesem zurückführt. In der folgenden Definition der Umkehrfunktion verwenden wir den Begriff der **Identität** Id_M auf einer Menge M. Das ist eine Abbildung von einer Menge in sich selbst, die sozusagen gar nichts tut: $\mathrm{Id}_M : M \to M; x \mapsto x$. Wenn jetzt $f : D \to Z$ eine Bijektion ist, gibt es zu jedem $y \in Z$ genau ein $x \in D$ mit $f(x) = y$, denn die Existenz eines solchen x folgt ja aus der Surjektivität von f und die Eindeutigkeit aus seiner Injektivität.

Definition. Ist $f : D \to Z$ eine Bijektion, liefert die Festlegung $Z \ni y \mapsto x =: f^{-1}(y)$ mit $f(x) = y$ eine eindeutig bestimmte Abbildung $f^{-1} : Z \to D$, die **Umkehrabbildung** von f. Es gelten $f^{-1} \circ f = \mathrm{Id}_D$ und $f \circ f^{-1} = \mathrm{Id}_Z$.

Die Visualisierung von Funktionen, Zusammensetzungen, Umkehrfunktionen usw. mit Mengensymbolen, Punkten und Pfeilen ist sehr suggestiv und hilfreich, wenn man an strukturellen Aussagen interessiert ist, die man sich klarmachen möchte. Je nachdem, um welche Art von Abbildung es sich handelt, sind aber andere Möglichkeiten sinnvoll, sie sich vor Augen zu führen, also irgendwie zu zeichnen. Bei *reellen* Abbildungen $f : \mathbb{R} \to \mathbb{R}; x \mapsto f(x)$ hat sich eine Malmethode etabliert, die wirklich so hilfreich ist, dass man sie im praktischen Umgang mit solchen Abbildungen als für quasi zwingend erforderlich halten kann: der *Graph* der Funktion. Kurz gesagt, bildet man aus allen x der Definitionsmenge und den zugehörigen $f(x)$ in der Zielmenge die *Punktepaare* $(x, f(x)) \in \mathbb{R} \times \mathbb{R} \equiv \mathbb{R}^2$ und zeichnet diese in die Zeichenebene $\mathbb{R}^2$ ein. Die Funktion wird dann also als Linie dargestellt, die die Eigenschaft hat, über *jedem* x der Definitionsmenge *genau einmal* durchzugehen. Das ist so suggestiv, dass man von diesem Graphen zuweilen auch als "der Funktion" oder "der Kurve" spricht. Genaugenommen ist für eine Funktion $f : \mathbb{R} \ni D \to \mathbb{R}; x \mapsto f(x)$ ihr Graph aber eben $\mathrm{graph}(f) := \{(x, f(x)) \in \mathbb{R}^2 \mid x \in D\}$, das heißt eine Teilmenge der Zeichenebene $\mathbb{R}^2$. Manchmal wird man halt doch sorgfältiger unterscheiden müssen: wenn man von "der Fläche unter der Kurve" von hier bis dort spricht - meint man dann einfach die entsprechende Punktmenge als Teilmenge des $\mathbb{R}^2$, die ja immer von positivem Maß ist, oder kommen Vorzeichen ins Spiel? Wie auch immer – schon in der Schulmathematik ist uns diese Methode, Funktionen darzustellen, vertraut geworden, und sie ist in vielen Fällen ein sehr gute Hilfsmittel, um sich zu orientieren, Beweisideen zu bekommen und so weiter. Wenn man Mathematik so "*hand waving*" betreibt, wie wir das tun, mag die Anschauung durch den Graph einer Funktion sogar formale Beweise mehr als einmal ersetzen... Gerade deshalb sei man sich aber der Grenzen dieser Wahrheitsfindungsmethode bewusst!

Bevor wir, wie versprochen, zum Begriff der Gruppe kommen, spezialisieren wir den ja immer noch recht allgemeinen Abbildungsbegriff auf eine bestimmte Klasse von Abbildungen, den sogenannten *Verknüpfungen.* Erst mal die Definition, und dann schauen wir uns an, was sie bedeutet:

> Sei M eine nichtleere Menge. Eine Abbildung $\varphi : M \times M \to M$ heißt (algebraische) **Verknüpfung** auf M .

Mit anderen Worten: einem 2-Tupel, einem geordneten *Paar* von Elementen aus M wird ein *einzelnes* Element aus M zugeordnet: $(a, b) \mapsto \varphi((a, b)) \in M$. Ist das etwas Kompliziertes oder etwas Besonderes? Im Gegenteil! Diese Art von Abbildung ist die erste, die der Mensch lernt, und zwar bereits im Kleinkindalter: man nimmt zwei Zahlen und addiert sie. Für die meisten Verknüpfungen wählt man dieser Einfachheit halber denn auch eine andere Schreibweise: statt $\varphi((a, b))$[11] notiert man das "Ergebnis" der Verknüpfung von a und b als $a \circ b$, wobei das "$\circ$" steht für ein "$+$" bei der Addition, ein "$\cdot$" bei der Multiplikation und so weiter. Wir könnten also $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}; (m, n) \mapsto \varphi(m, n) := m + n$ für die Addition Natürlicher Zahlen hinschreiben.

Zwei Bemerkungen noch hierzu:

- Bei Addition und Multiplikation von Zahlen ist die Reihenfolge egal, aber im Allgemeinen legt die Definition der Verknüpfung *nicht* fest, dass $\varphi(a, b) = \varphi(b, a)$ ist (oder anders notiert $a \circ b = b \circ a$). Wären a und b Matrizen und stünde "$\circ$" für die Matrixmultiplikation, wäre diese Vertauschbarkeit definitiv nicht gegeben! Verknüpfungen, die *doch* vertauschbar sind, erhalten einen besonderen Namen, weil sie besonders wichtig sind. Dazu mehr im gleich folgenden Abschnitt über Gruppen.

[11] Wobei dies, wenn es denn geschrieben wird, üblicherweise weniger pedantisch als $\varphi(a, b)$ erscheint.

- Die Definition $\varphi : M \times M \to M$ fordert gewissermaßen implizit, dass das Ergebnis der Verknüpfung zweier Elemente aus M wiederum in M liegen muss (*Abgeschlossenheit*). Es liefert deshalb zum Beispiel *keine* wohldefinierte Verknüpfung, $\mathbb{N} \times \mathbb{N} \ni (m, n) \mapsto \psi(m, n) := \frac{m}{n}$ festzulegen, denn wenn auch $\psi(6, 2) = 3$ wäre, so würde doch $\psi(1, 2)$ aus $\mathbb{N}$ herausführen – das ist nicht zulässig bei einer Verknüpfung.

1.5 Gruppen.

Jetzt haben wir alle Begrifflichkeiten beisammen, um zu definieren, was eine *Gruppe* ist: im Prinzip nicht viel mehr als eine Menge M, ausgestattet mit einer Verknüpfung $M \times M \to M; (m, n) \mapsto m \circ n$, wobei letztere allerdings noch gewissen Einschränkungen unterliegen soll. Diese sind modelliert nach einem sehr abstrakten Begriff von Symmetrie; in der Tat finden sich Anwendungen für Gruppen überall dort, wo in der Natur, oder auch in Kunst oder Wissenschaft, Symmetrien zu finden sind: Spiegelungs- und Drehsymmetrien bei geometrischen Figuren, aber auch bei Lebewesen – etwa die Rotationssymmetrien vieler Blüten –; Raumtransformationssymmetrien bei Kristallgittern usw. Letztendlich sind Symmetrien in der modernen Physik die Grundprinzipien der fundamentalen Wechselwirkungen, und dementsprechend spielt die Theorie insbesondere sogenannter kontinuierlicher Gruppen, auch Lie-Gruppen genannt, dort eine absolut zentrale Rolle. Für uns ist an dieser Stelle von Relevanz aber nur die elementare

Definition. Das Paar $(G, \circ)$ aus einer nichtleeren Menge G und einer Verknüpfung $G \times G \to G; (a, b) \mapsto a \circ b$ heißt **Gruppe**, wenn die folgenden Bedingungen erfüllt sind:

- Die Verknüpfung ist assoziativ, das heißt es gilt für alle $a, b, c \in G$, dass stets $(a \circ b) \circ c = a \circ (b \circ c)$ ist.
- Es gibt in G ein eindeutiges sogenanntes *Neutrales Element* n, für das $a \circ n = n \circ a = a$ ist für jedes $a \in G$.
- Zu jedem $a \in G$ gibt es ein eindeutig bestimmtes Element $a' \in G$ mit $a \circ a' = a' \circ a = n$, wo $n \in G$ das Neutrale Element von G ist. Dieses jedem a eindeutig zugeordnete a' heißt *Inverses Element* von a.

Die einfachsten Beispiele für Gruppen sind uns längst vertraut: $(\mathbb{Z}, +)$, die Ganzen Zahlen mit der Addition, oder auch $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$. Hingegen ist $\mathbb{N}$ mit der Addition *keine*

Gruppe! warum nicht? Bei der Addition ist das Neutrale Element jeweils die 0 und das Inverse zu a wird als $-a$ bezeichnet. Ferner sind $(\mathbb{Q}\backslash\{0\},\cdot)$ und $(\mathbb{R}\backslash\{0\},\cdot)$ Gruppen mit der Multiplikation als Verknüpfung. Hier ist jeweils die 1 das Neutrale Element und $a^{-1} \equiv \frac{1}{a}$ das Inverse zu a; weil man durch 0 nicht dividieren darf, muss sie aus den Mengen $\mathbb{Q}$ und $\mathbb{R}$ herausgenommen werden, damit diese zu einer Gruppe gemacht werden können; anders formuliert: 0 hat kein multiplikativ Inverses. $\mathbb{Z}$ ist mit der Multiplikation keine Gruppe, weil die multiplikativ Inversen Ganzer Zahlen keine Ganzen Zahlen sind. Schreibweisentechnisch ist es übrigens verbreitet, das Verknüpfungssymbol $\circ$ bei Gruppen mit "Additionscharakter" (was immer das genau ist) als "$+$" zu schreiben und bei Gruppen mit multiplikativem Charakter als "$\cdot$", entsprechend die Inversen zu a als $-a$ beziehungsweise a^{-1}. Bei multiplikativen Gruppen, aber auch, wenn man mit allgemeinen Gruppen abstrakt umgeht, lässt man das Verknüpfungszeichen gerne auch einfach mal ganz weg und schreibt ab statt $a \cdot b$ oder $a \circ b$.

Hier noch ein paar erläuternde Bemerkungen zu obiger Definition. Zunächst: in einer Gruppe $(G,\circ)$ gibt es *ein einziges* Neutrales Element, zu jedem Element aber *ein eigenes* Inverses Element. Ein Element und sein Inverses Element sind in gewissem Sinne *zueinander* invers, das heißt, das Inverse des Inversen eines Elements ist dieses Element selbst. Der Nachweis dazu findet sich in den Übungen als Beispiel dafür, wie man – in notwendigerweise sehr formaler Weise – so einen gruppentheoretischen Beweis führt. Im Falle der gerade genannten Beispiele haben wir uns an diesen Umstand gewöhnt: $-(-4) = 4$ und $\frac{1}{\frac{1}{3}} = 3$...

Ebenso vertraut ist uns das Assoziativgesetz der Addition wie das der Multiplikation, so vertraut, dass wir darüber leicht seinen Charakter eines Postulats[12] vergessen könnten. Es ist eben *nicht* jede Verknüpfung assoziativ! Ein Beispiel findet sich in den Übungen. Außerdem könnten wir verleitet sein, zu glauben, es sei stets $a \circ b = b \circ a$, es gelte also das schon in der Schulmathematik so genannte Kommutativgesetz. Das ist alles andere als der Fall! Für ein sehr einfaches Gegenbeispiel sei wieder auf die Übungen verwiesen. In der Linearen Algebra werden wir aber ständig Matrizen miteinander multiplizieren müssen, und es sei hier schon betont, dass die Matrixmultiplikation eben *nicht* kommutativ ist: wenn L und M zwei quadratische Matrizen sind, können wir sowohl $L \cdot M$ wie auch $M \cdot L$ bilden – die resultierenden Produktmatrizen werden im Allgemeinen aber *verschieden* sein! – Natürlich ist es angenehm, mit einer Verknüpfung zu arbeiten, bei der man auf die Reihenfolge nicht zu achten braucht, weil das Kommutativgesetz gilt. Das hat zu einer eigenen Namensgebung geführt: eine Gruppe $(G,\circ)$, bei der die Verknüpfung

[12] Für die in unserem Skript immer mal wieder eigens angesprochenen Lateiner zur Erinnerung: *postulare* heißt "fordern".

kommutativ ist, stets also $a \circ b = b \circ a$ für alle $a, b \in G$ gilt, heißt *kommutative* oder **Abel**sche Gruppe.

Mit Mengen, Abbildungen, Verknüpfungen und Gruppen haben wir jetzt alle Begriffe erläutert, die es braucht, um den Zentralbegriff der Linearen Algebra einzuführen, den *Vektorraum*, auch *Linearen Raum* genannt. Das wird im nächsten Kapitel geschehen. Zum Schluss dieses Kapitels gibt's noch den versprochenen Primer zum Thema "Komplexe Zahlen".

1.6 Reelle und Komplexe Zahlen.

Man könnte versucht sein, zu denken, mit den Reellen Zahlen $\mathbb{R}$ habe man alles, was man braucht: man kann sie addieren und multiplizieren, es gibt zu jeder reellen Zahl x ein additiv Inverses $-x$, so dass man auch subtrahieren kann ($x - y := x + (-y)$), und es gibt zu jeder reellen Zahl x außer der Null ein multiplikativ Inverses $\frac{1}{x}$, so dass auch die Division erklärt werden kann ($\frac{x}{y} := x \cdot \frac{1}{y}$). Assoziativgesetz und Kommutativgesetz für Addition und Multiplikation sowie das Distributivgesetz für die Verbindung zwischen beiden sorgen für Einfachheit und Übersichtlichkeit beim Rechnen. Die Reellen Zahlen bilden damit, wie der Algebraiker weiß, einen sogenannten "Körper". Außerdem ist $\mathbb{R}$ *vollständig* in dem Sinne, dass eine Folge reeller Zahlen, deren Elemente sich immer näher kommen, auch in $\mathbb{R}$ konvergiert, es gibt also einen entsprechenden Grenzwert in $\mathbb{R}$; die Reellen Zahlen sind nicht irgendwie "löchrig"[13]. Damit kann man dann Analysis treiben und all das, was Physiker und andere Naturwissenschaftler für die Formulierung und Anwendung ihrer Naturgesetzte brauchen.

Warum also sollte man den Körper der Rellen Zahlen noch einmal erweitern wollen? Es gibt tatsächlich vielerlei Gründe für die Schaffung einer Körpererweiterung namens "Komplexe Zahlen", bezeichnet mit $\mathbb{C}$. Teils sind sie mathematischer Natur, teils sind sie aus den Anforderungen der Anwendungen heraus entstanden oder eine Mischung aus beidem. Auch aus historischer Sicht wäre es interessant, die Entstehung des Konzepts "imaginärer" Zahlen zu verfolgen; schon die Namensgebung für diesen Betandteil der Komplexen Zahlen verrät, dass sich die Mathematiker und Anwender damals nicht so ganz darüber im Klaren waren, was es mit diesen Zahlen wohl auf sich hat. Wir können auf die Mannigfaltigkeit dieser Aspekte hier (leider) nicht eingehen. Es möge genügen, darauf hinzuweisen, dass die Komplexen Zahlen – anders als die Rellen Zahlen –

[13] Wir verzichten hier auf eine genauere Definition des Begriffs der Vollständigkeit. Er hat sowieso eher in der Analysis seinen Platz als hier in der Linearen Algebra.

algebraisch abgeschlossen sind, was bedeutet, dass im Komplexen jede Polynomgleichung eine Lösung besitzt. Konkret hat zum Beispiel die Gleichung $x^2 = -1$ im Reellen *keine* Lösung, denn das Quadrat einer rellen Zahl ist ja nie negativ. Im Komplexen hingegen ist $x^2 = -1$ sehr wohl lösbar, wie wir weiter unten sehen werden! Es gibt endlos Beispiele dafür, wie die Betrachtung eines Problems “im Komplexen” Klarheit und Übersichtlichkeit schafft gegenüber der ein reellen Sichtweise oder sogar begriffliche Verknüpfungen aufzeigt, die man im Rellen gar nicht sehen kann. Die trigonometrischen Funktionen Sinus und Cosinus etwa sind, im Komplexen aufgefasst, quasi Bestandteile der komplexen Exponentialfunktion – was im Reellen vollkommen unsichtbar ist. Auch haben die naturwissenschaftlichen und technischen Anwender Bedarf an den zusätzlichen Möglichkeiten, die die Komplexen Zahlen bereitstellen. Der Elektroingenieur beispielsweise schätzt die elegante Art und Weise, mittels komplexer Größen für Wechselströme, Wechselspannungen und Widerständen Ordnung und Übersicht in Wechselstromschaltungen zu bringen; natürlich könnte er sich zumindest im Prinzip auf reelle Größen beschränken, der Umgang mit diesen wäre dann allerdings nur etwas für starke Nerven. Die Physiker wieder haben die modernen Theorien der Mikrophysik – Quantenmechanik, Quantenfeldtheorien usw. – von vornherein mit komplexen Größen errichtet. Letztlich könnte man formulieren, dass sich die *rein rechnerische* Stärke der Komplexen Zahlen immer dann ausspielt, wenn es im weitesten Sinne um Schwingungen oder Wellen geht. Von den Möglichkeiten, die auf struktureller Ebene entstehen, wenn die Komplexen Zahlen ins Spiel genommen werden, ist damit noch gar nichts gesagt. Es sei nur kurz hingewiesen auf das in der Algorithmik unverzichtbare Konzept der *fast Fourier transformation* (FFT) und auf das sogenannte *Residuenkalkül*.

Dass die Komplexen Zahlen eine *Erweiterung* der Reellen Zahlen sind, sieht man sofort – es handelt sich bei komplexen Zahlen nämlich um Zahlen*paare* (x, y), wobei beide Einträge ihrerseits reell sind. *Addieren* kann man zwei komplexe Zahlen tatsächlich auch so, wie wenn es sich einfach um Elemente aus $\mathbb{R}^2$ handelte: es ist $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$. Wenn wir nun aber einfach eine komponentenweise Multiplikation hinzufügten, käme in der Tat nichts anderes dabei heraus als zwei Kopien von $\mathbb{R}$, die nebeneinander gestellt sind. Das liefe auf eine Art “*parallel computing*” hinaus, gäbe uns aber keine wirklich neue Struktur an die Hand. Die Multiplikation zweier komplexer Zahlen verknüpft die beiden Kopien von $\mathbb{R}$ vielmehr in charakteristischer Weise, “vermischt” sie sozusagen, jedoch derart, dass die entstehende Struktur einen Körper darstellt. Und zwar gilt $(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2)$. Direkt eingängig scheint diese Festlegung vielleicht nicht zu sein. Aber wir werden gleich sehen, dass sie doch naheliegend ist und, entgegen dem Anschein, leicht zu merken.

Wir identifizieren nämlich zunächst eine Art "Basis" der Komplexen Zahlen durch die beiden "Einheitsvektoren" $(1,0)$ und $(0,1)$. Wenn wir vermöge der gerade vorgenommenen Definition der Produktbildung dann $(1,0)\cdot(x,y)$ betrachten, sehen wir, dass $(1,0)\cdot(x,y) = (1\cdot x - 0\cdot y\,,\ 1\cdot y + 0\cdot x) = (x,y)$ ist, die $(1,0)$ also quasi die Rolle einer multiplikativen "1" spielt. Wir können daher die Menge aller $(x,0) \in \mathbb{C}$ mit $\mathbb{R}$ identifizieren und statt $(k,0)\cdot(x,y) = (kx,y)$ auch einfach $k \cdot (x,y)$ schreiben. Ferner – und das ist jetzt wirklich interessant – haben wir $(0,1)\cdot(x,y) = (-y,x)$ (hier sieht man das "Twisting", das durch die Multiplikation erzeugt wird) und insbesondere $(0,1)\cdot(0,1) = (-1,0)$. Die $(0,y) \in \mathbb{C}$ heißen "imaginäre Zahlen". Wenn wir wie üblich den "Einheitsvektor" $(0,1)$ in der imaginären Richtung durch i abkürzen und diese Identifikation verwenden, haben wir soeben $\mathrm{i}^2 = \mathrm{i}\cdot\mathrm{i} = -1$ gezeigt. Hier liegt der Kern des Umstands, dass Gleichungen wie $x^2 = -1$ in $\mathbb{C}$ tatsächlich Lösungen haben: nämlich i und $-$i.

Statt (x,y) schreiben wir mittels dieser Basis und dieser Identifikation also einfacher $(x,y) = x\cdot(1,0) + y\cdot(0,1) = x + \mathrm{i}y$. Und wenn wir dann $\mathrm{i}^2 = -1$ im Kopf behalten, löst sich die obige Definition der Multiplikation komplexer Zahlen sehr eingängig auf: $(x_1 + \mathrm{i}y_1)\cdot(x_2 + \mathrm{i}y_2) = x_1x_2 + \mathrm{i}x_1y_2 + \mathrm{i}y_1x_2 + \mathrm{i}\cdot\mathrm{i}\cdot y_1y_2 = (x_1x_2 - y_1y_2) + \mathrm{i}\cdot(x_1y_2 + y_1x_2)$, ganz einfach wie im Reellen nach dem Distributivgesetz ausmultipliziert und anschließend geordnet nach "reellen" und "imaginären" Bestandteilen. Zusammenfassend: wir können also mit komplexen Zahlen so rechnen wie mit reellen Zahlen, nur müssen wir die imaginäre Einheit i mitschleppen und beachten, dass wegen $\mathrm{i}^2 = -1$ das Produkt zweier imaginärer Zahlen wieder mit einer reellen Zahl identifiziert wird. Im Sinne dieser Identifikation $\mathbb{C} \cong \mathbb{R} + \mathrm{i}\mathbb{R}$ zerlegen wir irgendeine gegebene komplexe Zahl z in ihren sogenannten "*Realteil*" $\mathfrak{Re}(z)$ und ihren "*Imaginärteil*" $\mathfrak{Im}(z)$ und schreiben $z = \mathfrak{Re}(z) + \mathrm{i}\mathfrak{Im}(z)$ [14].

Mit dieser Zerlegung in Real- und Imaginärteil einer komplexen Zahl können wir auch die Operation der *komplexen Konjugation* durchführen, die aus einer komplexen Zahl z wieder eine komplexe Zahl $\overline{z}$ macht, eben die "komplex Konjugierte" zu z: wir setzen für $z \equiv \mathfrak{Re}\, z + \mathrm{i}\mathfrak{Im}\, z$ einfach $\overline{z} := \mathfrak{Re}\, z - \mathrm{i}\mathfrak{Im}\, z$. Wie das im Einzelfall aussieht und wozu es gut ist, zeigt uns eine Übung an ein paar Beispielen.

Für das Folgende stellen wir uns die *komplexe Ebene* $\mathbb{C} \cong \mathbb{R} + \mathrm{i}\mathbb{R}$ konkret vor, also eine von links nach rechts zu höheren Werten sortierte x-Achse beziehungsweise $\mathfrak{Re}\, z$-Achse und senkrecht dazu eine von unten nach oben zu höheren Werten sortierte y-Achse beziehungsweise $\mathfrak{Im}\, z$-Achse;

[14] Man beachte also: der Imaginärteil von zum Beispiel $3 - 5\mathrm{i}$ ist -5 und nicht etwa $-5\mathrm{i}$. Real- und Imaginärteil komplexer Zahlen sind selbst *reelle* Zahlen.

im Mittelpunkt die $0 \in \mathbb{C}$ repräsentiert als $(0,0)$. Jede komplexen Zahl $z \in \mathbb{C}$ wird in dieser komplexen Ebene in genau einen Punkt verortet. Nun erinnere man sich an die aus der Schule bekannte Verwendung von *Polarkoordinaten*: statt x- und y-Wert beziehungsweise $\mathfrak{Re}\, z$- und $\mathfrak{Im}\, z$-Wert einer komplexen Zahl anzugeben, um zu beschrieben, wo in der Ebene sie liegt, benutzen wir den *Abstand* r des Punktes vom Ursprung sowie den *Winkel* φ, den der Zeigerstrahl vom Ursprung zum Punkt mit der x-Achse einschließt. Der Konvention gemäß ist dieser Winkel "mathematisch positiv" zu zählen, will heißen, wir beginnen mit dem Winkel 0 für Punkte auf der positiven x-Achse und zählen dann *gegen* den Uhrzeigersinn – haben also einen Winkel von $\frac{\pi}{2}$ für Punkte, die auf der positiven imaginären Achse liegen, und $-\pi$ für Punkte auf der negativen reellen Achse und so weiter. Man mache sich unbedingt hierzu die eine oder andere Zeichnung!

Wenn man sich die beiden Darstellungen eines z, einmal *cartesisch* durch $\mathfrak{Re}(z)$ und $\mathfrak{Im}(z)$ und einmal *polar* durch $r(z)$ und $\varphi(z)$, nebeneinander stellt, erhebt sich sofort die Frage, wie diese beiden Dartellungen jeweils ineinander zu überführen sind. Das ist natürlich nicht schwierig, aber man muss auf die in diesem Zusammenhang verbauten Konventionen achten.

Zunächst sei z gegeben in der Form $(\mathfrak{Re}(z), \mathfrak{Im}(z))$. Aus den Übungen wissen wir, dass $z\overline{z} = \mathfrak{Re}^2(z) + \mathfrak{Im}^2(z)$ ist, so dass wir nach dem Satz des PYTHAGORAS schließen können, dass $r(z) = \sqrt{z\overline{z}}$. Es wird daher $r(z)$ auch $|z|$ genannt (*Betrag* von z). Für die Berechnung von $\varphi(z)$ brauchen wir die weiter oben angeregten Zeichnungen zusammen mit etwas Trigonometrie. Man muss sich aber zunächst verdeutlichen, dass $\varphi(z)$ ohne weitere Einschränkungen gar nicht eindeutig ist, denn zu gegebenem $\varphi(z)$ könnten wir ja 2π oder ein Vielfaches davon addieren oder subtrahieren und würden wieder beim selben Punkt landen. Wir müssen das *Argument* $\arg(z)$ aus allen möglichen Winkeln $\varphi(z) \pm k \cdot 2\pi$ also irgendwie auswählen. Beispielsweise ist es üblich, zu fordern, dass $\arg(z) \in [-\pi, \pi)$ liegen soll; es gibt aber je nach Anlass und Anwendung auch andere Konventionen wie etwa $\arg(z) \in (0, 2\pi]$. Wenn es sich bei z nicht um die Zahl 0 handelt (wo der Winkel φ beliebig gesetzt werden kann), liest man aus der Zeichnung nun ab, dass $\mathfrak{Re}(z) = r \cos\varphi$ ist und $\mathfrak{Im}(z) = r \sin\varphi$. Eine Möglichkeit, φ zu berechnen, besteht also darin, eine trigonometrische Umkehrfunktion zu verwenden, und zwar so, dass die gewählte Konvention für das zulässige Winkelintervall eingehalten wird. Beispielsweise könnten wir wegen (Zeichnung!) $\mathfrak{Im}\, z \geqslant 0 \Rightarrow \varphi \in [0, \pi)$ wählen $\arg(z) = \arccos\left(\frac{\mathfrak{Re}\, z}{|z|}\right)$ und im Fall $\mathfrak{Im}\, z \leqslant 0 \Rightarrow \varphi \in [-\pi, 0)$ dann entsprechend $\arg(z) = -\arccos\left(\frac{\mathfrak{Re}\, z}{|z|}\right)$. Letztlich rechnet man in der Praxis durch Umkehrung des Sinus, Cosinus oder Tangens irgendeinen der φ aus und addiert oder subtrahiert 2π von Hand so, dass der resultierende Winkel die gewählte Konvention einhält und damit als $\arg z$ taugt.

Sind umgekehrt r und φ als Polarkoordinaten von z gegeben, wie bekommen wir dann daraus $\mathfrak{Re}\, z$ und $\mathfrak{Im}\, z$? Das ist einfach, und wir hatten es eigentlich gerade schon gesehen: $\mathfrak{Re}(z) = r(z)\, \cos\arg(z)$ und $\mathfrak{Im}(z) = r(z)\, \sin\arg(z)$.

Die Darstellung $z = \mathfrak{Re}\, z + \mathrm{i}\, \mathfrak{Im}\, z$ können wir daher auch in der Form $z = r(z) \cos\varphi + \mathrm{i}\, r(z) \sin\varphi$ schreiben, wenn φ das Argument $\arg z$ abkürzt, oder auch $z = |z|(\cos\varphi + \mathrm{i}\, \sin\varphi)$. Wir wollen dies als $z = |z|\mathrm{e}^{\mathrm{i}\varphi}$ schreiben; man möge das "e hoch i phi" gegebenenfalls lediglich als Kurzschreibweise auffassen: $\mathrm{e}^{\mathrm{i}\varphi} \equiv \cos\varphi + \mathrm{i}\, \sin\varphi$. Eine der Übungsaufgaben zeigt, dass diese e-Funktion tatsächlich die Funktionalgleichung der bekannten Exponentialfunktion erfüllt, und es soll hier kein Geheimnis daraus gemacht werden: $\mathrm{e}^{\mathrm{i}\varphi}$ *ist* tatsächlich nichts anderes als die aus der Analysis vertraute Exponentialfunktion angewandt auf die komplexe Zahl $\mathrm{i}\varphi$. Wie wendet man exp auf eine komplexe Zahl an? Nun, man erweitert die Potenzreihenentwicklungen für $\mathrm{e}^x := \sum \frac{1}{n!} x^n$ (und entsprechend die für die trigonometrischen Funktionen) auf komplexe Argumente. Konvergenzthemen werden in den Komplexen Zahlen genau so behandelt wie in den Reellen Zahlen. Allerdings führt uns diese Diskussion aus dem Rahmen der Linearen Algebra hinaus und mitten in die Analysis hinein... Wie man zwei in Polardarstellung gegebene komplexe Zahlen miteinander multipliziert und wie man in der Polardarstellung das komplex Konjugierte bildet, dazu findet sich etwas in den Übungen.