

1. DAS FUNDAMENT DER MATHEMATIK: MENGEN UND ABBILDUNGEN

Der Begriff der Menge ist fundamental in der Mathematik, formal wenn auch nicht immer am schnellsten oder intuitivsten, lässt sich jedes mathematische Objekt als Menge auffassen. Hierauf beruht die universelle Gültigkeit und absolute Zuverlässigkeit mathematischer Resultate, wenn auch oftmals weniger formale, wie zB geometrisch - anschauliche, Auffassungen dem Verständnis und der Gewinnung neuer Erkenntnis besser dienen. Wir werden hier die mengentheoretische Sicht wohl mehr als in der Schulmathematik betonen, müssen aber auf eine vollständig formale Abhandlung verzichten.

Diese würde die Sprache der Mathematik (Logik) in einem Umfang benutzen, der noch nicht vorhanden ist. Ihr Aufbau würde unser Vorankommen unnötig verzögern, zumal diese Begriffe der Logik sowieso später im Studium der Informatik gründlicher behandelt werden.

1.1. Grundlegendes über Mengen.

Definition 1.1. Menge (*intuitive Definition von G. Cantor*) ist die Zusammenfassung von Objekten (Elementen), die eine bestimmte Eigenschaft (" $P(x)$ gilt") haben.

Wir schreiben $x \in M$ wenn x ein Element von M ist, d.h. zu M gehört, und $x \notin M$ andernfalls. Dies kann schreibt man als

$$M = \{x : P(x) \text{ ist wahr}\}, \text{ also } x \in M \text{ bedeutet genau, dass } P(x) \text{ gilt.}$$

Den Grundbegriff mathematische Aussage (der sich nur über eine strikte Einschränkung der Formeln, welche diese beschreiben, widerspruchsfrei halten lässt - siehe Fundamentalkrise der Mathematik) führen wir hier aus obigen Gründen nicht formal ein. Wir betreiben also **naïve** Mengenlehre, werden aber Situationen vermeiden, die mit den strikten Einschränkungen (Zermelo- Fraenkel oder Bernays-Gödel- von Neumann) kollidieren.

Zwei Mengen A und B sind gleich, wenn sie dieselben Elemente haben, d.h. jedes Element von A auch ein Element von B ist, und umgekehrt jedes Element von B auch in A ist. ("Extensionalitätsprinzip" der ML).

Typischerweise studieren wir $\{x \in X : P(x)\}$, d.h. die Menge aller x aus einer (grossen fixen "Universal-")Menge X , für die die (mathematische) Aussage $P(x)$ wahr ist. Z.B. kann X die Menge aller natürlichen, ganzen oder reellen Zahlen sein oder auch aller Punkte der Ebene (alle diese Begriffe werden noch definiert).

Beispiel 1.2.

- $\{n \in \mathbb{N} : n > 5\}$ alle natürlichen Zahlen größer als 5, dh 6 und alle nachfolgenden
- $\{n \in \mathbb{Z} : \text{es existiert ein } k \in \mathbb{Z} \text{ mit } n = 2k - 1\}$, die ungeraden ganzen Zahlen
- $\{x \in \mathbb{R} : x^2 \in \mathbb{Q} \text{ \& } x \geq 0\}$ - die "Wurzeln" der rationalen Zahlen

Definition 1.3. Wir sagen A ist Teilmenge von B (Notation $A \subset B$), wenn alle Elemente von A auch zu B gehören. (Statt A Teilmenge von B sagen wir oft A ist kleiner(oder auch kleiner gleich) B).

Analog zur Ordnungsrelation für reelle Zahlen ist $A \subset B$ gleichbedeutend mit $B \supset A$. wir schreiben $A \subsetneq B$ wenn $A \subset B$ und $A \neq B$ und sagen A ist *strikt* kleiner als B .

Unterschied: Nicht alle Mengen sind in diesem Sinne vergleichbar! Jedenfalls gilt

$$A = B \Leftrightarrow (A \subset B \text{ und } B \subset A),$$

Grundlage einer typischen Methode um die Gleichheit zweier Mengen zu zeigen.

Definition 1.4. Die leere Menge ist diejenige Menge, welche keine Elemente hat und wird mit \emptyset bezeichnet.

Für jedes mathematische Objekt a bezeichnet $\{a\}$ diejenige Menge, die a und nur a als einziges Element enthält. Sie heißt Einermenge mit Element a . (dh $\{a\} = \{x : x=a\}$)

Bemerkung: Spätestens jetzt sieht man, wie schwer es allein wäre, den Begriff "gleich sein", z.B. im Sinne von oben, rigoros zu definieren.

DIY: Zeigen Sie als Übung, dass die Mengen \emptyset , $\{\emptyset\}$ und $\{\{\emptyset\}\}$ alle paarweise voneinander verschieden sind.

Definition 1.5. Aus gegebenen Mengen A, B konstruieren wir

- $A \cap B = \{x : x \in A \text{ \& } x \in B\}$ Schnittmenge, Durchschnitt von A und B
- $A \cup B = \{x : x \in A \text{ oder } x \in B\}$ Vereinigung von A und B
- $A \setminus B = \{x : x \in A \text{ \& } x \notin B\}$ Differenzmenge von A und B

Die Mengen A und B heißen *disjunkt*, falls $A \cap B = \emptyset$, d.h. sie keine gemeinsamen Elemente haben.

Es gilt also z.B.

$$\{a, b\} = \{a\} \cup \{b\} = \{a\} \cup \{a, b\} = \{b, a\}, \{1, 2, 3, 4, 5\} \setminus \{4, 2, 6\} = \{3, 1, 5\}.$$

Es gibt viele "Rechenregeln" für \cap und \cup , wir erwähnen die wichtigsten, die Assoziativität, Kommutativität und Distributivität ausdrücken (symmetrischer als für "+" und "·"!!)

Lemma 1.6. Für alle Mengen A, B und C gilt

- i) $(A \cup B) \cup C = A \cup (B \cup C)$
- ii) $(A \cap B) \cap C = A \cap (B \cap C)$
- iii) $A \cup B = B \cup A$
- iv) $A \cap B = B \cap A$
- v) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
- vi) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

Beweis:(Ihrer Wahl)

Als letzte grundlegende Mengenoperation führen wir die Produktmenge ein, mit der sich z.B. die Euklidische Ebene aus der Zahlengeraden konstruieren lässt. Hierzu brauchen wir den Begriff des geordneten Paares, den klarerweise haben x - und y -Koordinate eines Punktes in der Ebene ganz verschiedene Bedeutung! Also $(1, 0) \neq (0, 1)$, aber bei Mengen gilt ja $\{0, 1\} = \{1, 0\}$!?

Definition 1.7. Für die mathematischen Objekte a und b definieren wir das geordnete Paar $(a, b) = \{\{a\}, \{a, b\}\}$.

Dann erhalten wir wie gewünscht

Lemma 1.8. Für alle mathematischen Objekte a, b, c, d gilt

$$(a, b) = (c, d) \Leftrightarrow (a = c \text{ und } b = d).$$

Beweis: Idee: Rückrichtung trivial, bleibt z_z aus $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ folgt $a = c$ und $b = d$. Da a und c einzeln in Mengen auftreten, ist es wohl leichter zuerst $a = c$ z_z .

Dies beweisen wir **indirekt**, d.h. mit **Widerpruch**. **Sonst** wäre $a \neq c$ und also $c \notin \{a\}$. Dies zeigt $\{a\} \neq \{c\}$ und $\{a\} \neq \{c, d\}$ wegen des Existenzialitätsprinzips, also $\{a\} \notin \{\{c\}, \{c, d\}\}$ - ein Widerspruch zur Voraussetzung. Damit kann "sonst" nicht eintreten und es muss $a = c$ gelten.

Die Voraussetzung gibt nun also $\{\{a\}, \{a, b\}\} = \{\{a\}, \{a, d\}\}$, bleibt $b = d$ zu zeigen. Hierzu machen wir eine **vollständige Fallunterscheidung**. **Falls** $a = b$, dann folgt $\{\{a\}\} = \{\{a\}, \{a, d\}\}$ und also $\{a\} = \{a, d\}$. Dh $d \in \{a\}$ und also $a = b = c = d$. **Sonst** $b \notin \{a\}$, also $\{a, b\} = \{a, d\}$ und somit $b \in \{a, d\}$. Also $b = a$ oder $b = d$, aber $a = b$ war ja gerade mit "sonst" ausgeschlossen, also muss $b = d$ gelten. ☺

Nun können wir Triple $(a, b, c) := ((a, b), c)$, Quadruple $(a, b, c, d) = ((a, b, c), d)$ usw als geordnete Objekte mit analogen Gleichheitskriterien definieren.

Definition 1.9. Für zwei Mengen A und B ist ihr (kartesisches) Produkt definiert als die Menge

$$A \times B = \{(a, b) \mid a \in A \text{ und } b \in B\} := \{x \mid \text{es existieren } a \in A \text{ und } b \in B \text{ mit } x = (a, b)\}.$$

Die linke, kompaktere Schreibweise wird wegen der Schreibökonomie öfters genutzt.

1.2. Grundlegendes über Abbildungen. Wir beginnen mit einer recht abstrakt anmutenden Definitionen, diese ist das Resultat eines Verallgemeinerungsprozesses, der über sehr lange Zeit ging. Beispiele aus der Schulmathematik erläutern das Ganze aber sehr gut.

Definition 1.10. Eine Abbildung F bildet eine Menge X in eine Menge Y ab, wenn

$$F \subset X \times Y, \quad \forall x \in X \exists y \in Y : (x, y) \in F \text{ und } \forall (x, y), (x, y') \in F : y = y'.$$

Wir schreiben dann $F : X \rightarrow Y$, und wenn $(x, y) \in F$ dann schreiben wir $y = F(x)$. Wir identifizieren also die Abbildung $F = \{(x, F(x)) \mid x \in X\}$ direkt mit ihrem "Graphen".

Dann heißt X der Definitionsbereich, mit $\text{dmn}(F)$ bezeichnet, und das Bild der Funktion ist $\text{im}(F) = \{y \in Y : \text{existiert ein } x \in X \text{ mit } y = F(x)\}$. Der Wertebereich der Funktion ist (für uns) nicht eindeutig festgelegt: jede Menge, die $\text{im}(f)$ enthält, kann als solcher genutzt werden.

Wenn $Y = \mathbb{R}$, (eventuell \mathbb{C}, \mathbb{R}^n) nennen wir F oftmals Funktion und benutzen gerne kleine Buchstaben f, g, h, \dots

Nun ein paar Illustrationen für Funktionen, wir greifen dabei Resultaten aus dem nächsten Kapitel vor, was aber hier erlaubt sein sollte, da diese auch schon in der Schule diskutiert wurden.

Beispiel 1.11.

- (1) $f : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ definiert durch $f(a) = 4 - a$ für $a \in \{1, 2, 3\}$
- (2) $f : \mathbb{N} \rightarrow \mathbb{N}$ definiert als $f(n) = 1$ für alle $(\forall)n \in \mathbb{N}$, eine konstante Funktion
- (3) $f : \mathbb{N} \rightarrow \mathbb{Q}$ definiert als $f(n) = \frac{1}{n}$ wenn $n \in \mathbb{N}$
- (4) $f : \mathbb{R} \rightarrow \mathbb{R}$ definiert durch $\forall x \in \mathbb{R} \quad f(x) = x$, die Identität (auf \mathbb{R})
- (5) $f : \mathbb{R} \rightarrow \mathbb{R}$ definiert durch $\forall x \in \mathbb{R} \quad f(x) = x^2$, die Standardparabel
- (6) $f : \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+$ definiert durch $\forall x \in \mathbb{R} \quad f(x) = x^2$, hierbei $\mathbb{R}_0^+ = \{x \in \mathbb{R} : x \geq 0\}$. Diese Funktion f_6 ist verschieden von der Funktion f_5 aus (5), obwohl sie die gleiche Formel nutzt, hat sie ganz andere Eigenschaften, siehe unten. (Def 1.13)
- (7) $f : \mathbb{R} \rightarrow \mathbb{R}$ definiert durch $f(x) = x$ wenn $x \geq 0$ und $f(x) = x^3$ sonst (dh $x < 0$), eine der vielen Funktionen/Abbildungen die nicht durch eine (einzige) geschlossene Formel dargestellt werden. (DIY*: kann als Grenzwert einer geschlossenen Formel dargestellt werden)

Definition 1.12. Bild und Urbild

Sei $F : X \rightarrow Y$ eine Abbildung und seien $X' \subset X$ und $Y' \subset Y$ gegeben. Dann definieren wir

$$F(X') = \{F(x) : x \in X'\} \subset Y \text{ als } F\text{-Bild von } X', \text{ und}$$

$$F^{-1}(Y') = \{x \in X, F(x) \in Y'\}, \text{ das } F\text{-Urbild von } Y'.$$

Bemerkung/Warnung Das F -Urbild existiert immer, auch wenn die "inverse Funktion F^{-1} ", siehe unten, nicht definiert ist. $F(X) = \text{im}(F)$ gilt auch immer.

Lemma 1.13. Sei $F : X \rightarrow Y$ und beliebige $X_1, X_2 \subset X$ sowie $Y_1, Y_2 \subset Y$ gegeben. Dann gilt

- a) $F(X_1 \cup X_2) = F(X_1) \cup F(X_2)$,
- b) $F(X_1 \cap X_2) \subset F(X_1) \cap F(X_2)$,
- c) $F^{-1}(Y_1 \cup Y_2) = F^{-1}(Y_1) \cup F^{-1}(Y_2)$ und
- d) $F^{-1}(Y_1 \cap Y_2) = F^{-1}(Y_1) \cap F^{-1}(Y_2)$.

Beweis:

Nun wollen wir Begriffe einführen, die beschreiben, inwieweit F eine umkehrbare Abbildung ist.

Definition 1.14. Eine Abbildung $F : X \rightarrow Y$ heißt

- *injektiv* (auch 1 – 1 genannt) wenn $F(x) = F(x') \Rightarrow x = x'$,
- *surjektiv* (bildet auf Y ab, engl "onto") wenn $\forall y \in Y \exists x \in X : F(x) = y$,
- *bijektiv* wenn F injektiv und surjektiv ist.

Bemerkung Man sieht sofort: F ist injektiv genau dann wenn das F Urbild jeder Einermenge von Y leer oder eine Einermenge ist. Und F ist surjektiv genau dann wenn $F(X) = Y$ genau dann wenn das Urbild jeder nichtleeren Teilmenge von Y nichtleer ist. Die Beispiele aus 1.11 zeigen, dass eine Abbildung F surjektiv werden kann, ohne F zu ändern, wohl aber das Y , siehe $\hat{f}_2 : \mathbb{N} \rightarrow \{1\}, \forall n \in \mathbb{N} : \hat{f}_2(n) = 1$, aber dies geht immer ($Y = F(X)$). Wenn eine Funktion F nicht injektiv ist, muss man einige Paare aus F entfernen um Injektivität zu erreichen (5) versus (6).

Definition 1.15. Inverse- oder Umkehrfunktion Sei $F : X \rightarrow Y$ bijektiv. Dann definieren wir die Umkehrfunktion als

$F^{-1} : Y \rightarrow X$ so: wenn $y \in Y$ dann ist $F^{-1}(y)$ dasjenige $x \in X$ welches $F(x) = y$ erfüllt.

Bemerkung Die Existenz eines solchen x folgt aus der Surjektivität von F , seine Eindeutigkeit da F injektiv ist. **Dann** gilt auch $\forall Y' \subset Y : F^{-1}(Y') = (F^{-1})(Y')$, was die etwas verwirrende aber praktische Notation für F -Urbilder erklärt.

Beispiel 1.16. Die Funktion f_6 aus Beispiel 11(6) ist injektiv (siehe Übungszettel) und surjektiv (wie der Zwischenwertsatz für stetige Funktionen aus zeigen wird). Ihre Umkehrfunktion ist die

$$(\text{Quadrat})\text{Wurzelfunktion} \quad (f_6)^{-1} : \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+ \text{ mit } (f_6)^{-1}(x) = \sqrt{x}.$$

Der letzte wichtig(st)e Begriff betrifft eine Operation speziell für Abbildungen, die es erlaubt weitere zu konstruieren

Definition 1.17. Zusammensetzung

Seien Mengen X, Y, Z und Abbildungen $F : X \rightarrow Y, G : Y \rightarrow Z$ gegeben, dann definieren wir die Verkettung von G und F als

$$G \circ F : X \rightarrow Z \text{ durch } (G \circ F)(x) = G(F(x)) \text{ wenn } x \in X.$$

Es gibt viele sehr allgemeine aber etwas abstrakte Resultate über Verkettung, hier nur 2 ganz einfache, bevor wie die Beispiele aus 1.11 konkret nutzen.

Lemma 1.18. Seien Mengen X, Y, Z und Abbildungen $F : X \rightarrow Y, G : Y \rightarrow Z$ gegeben.

Dann ist F injektiv falls $G \circ F$ injektiv ist, und G surjektiv wenn $G \circ F$ so ist. Beide Schlussfolgerungen lassen sich nicht umkehren!

Beweis:

Beispiel 1.19. (1) $f_5 \circ f_3 : \mathbb{N} \rightarrow \mathbb{Q}$, $f_5 \circ f_3(n) = \frac{1}{n^2}$
(2) Sei $f : \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+$ definiert als $d(x) = \sqrt{x}$. Wenn g das quadratische Polynom $y \mapsto y^2 - 3y + 1$ für alle reellen y . Dann ist $g \circ f : \mathbb{R}_0^+ \rightarrow \mathbb{R}$ gegeben durch

$$g \circ f(x) = (\sqrt{x})^2 - 3\sqrt{x} + 1 = x + 1 - 3\sqrt{x} \text{ für alle } x \geq 0.$$

2. REELLE ZAHLEN

Diese sind das Brot des Analytikers. Für die Konstruktion der reellen Zahlen siehe W.Rudins Buch “Analysis”, wir setzen hier die Existenz gleich voraus. Dann sind die reellen Zahlen eine Menge \mathbb{R} mit

- zwei Rechenoperationen die jedem Paar $(x, y) \in \mathbb{R} \times \mathbb{R}$ zweier reeller Zahlen ein Element $x + y \in \mathbb{R}$ bzw. $x \cdot y \in \mathbb{R}$ zuordnen, und
- einer Ordnungs- (oder Vergleichsrelation) $<$

so dass die im Folgenden allmählich diskutierten 13 Axiome gelten.

I. Körperaxiome

Davon gibt es 9, und sie betreffen nur die Rechenoperationen (siehe auch Kapitel 2 im Buch Otto Forster, Analysis 1, Differential- und Integralrechnung einer Veränderlichen, elektronische CampusLizenz an der Uni Leipzig)

Addition		Multiplikation	
(AA)	$(x + y) + z = x + (y + z)$	(MA)	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$ $\forall x, y, z \in \mathbb{R}$ Assoziativgesetz
(AK)	$x + y = y + x$	(MK)	$x \cdot y = y \cdot x$ $\forall x, y \in \mathbb{R}$ Kommutativgesetz
(AN)	$\exists 0 \in \mathbb{R} \forall x \in \mathbb{R} : 0 + x = x$	(MN)	$\exists 1 \in \mathbb{R} : (1 \neq 0 \ \& \ \forall x \in \mathbb{R} : 1 \cdot x = x)$ neutrales Element
(AI)	$\forall x \in \mathbb{R} \exists y \in \mathbb{R} : x + y = 0$	(MI)	$\forall x \in \mathbb{R} \text{ mit } x \neq 0 \exists y \in \mathbb{R} : x \cdot y = 1$ inverses Element
(DG)	$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$		$\forall x, y, z \in \mathbb{R}$ Distributivgesetz

Bemerkung 2.1. Neutrale Elemente in (AN),(MN) sind eindeutig, dies macht die rechten Seiten in (AI),(MI) wohldefiniert. Denn

Das neutrale Element der Addition wird als Null bezeichnet, das neutrale Element der Multiplikation als Eins.

Bemerkung 2.2. Wir sehen, ohne das Distributivgesetz wären die Addition und die Multiplikation fast gleichwertige(”isomorphe”) Operationen, man beachte allerdings den

Ausschluss der Null in (MI). Erst dieses neunte Axiom bricht die weitgehende Symmetrie zwischen diese beiden.

Bemerkung 2.3. Inverse Elemente in (AI),(MI) sind eindeutig für gegebenes x , siehe Satz 2.5 für eine allgemeinere Behauptung. Wir schreiben $-x$ bzw. x^{-1} für additives bzw. multiplikatives Inverses.

Bemerkung 2.4. Die 9 Körperaxiome charakterisieren \mathbb{R} noch nicht, es gibt andere (noch zu diskutierende) Körper, welche diese ebenfalls erfüllen. Siehe, zB. Beispiel 2.10. Ein ganz trivialer Körper ist $\{0\}$ mit den Operationen $0 + 0 = 0 = 0 \cdot 0$. Um dieses Beispiel auszuschliessen, fordern wir im Folgenden **immer** $0 \neq 1$.

Satz 2.5. *Eindeutige Lösbarkeit von Gleichungen*

- a) $\forall x, y \in \mathbb{R} \exists z \in \mathbb{R} : x + z = y$. Dieses z ist eindeutig und durch $z = y + (-x)$ gegeben.
- b) $\forall x, y \in \mathbb{R}$ mit $x \neq 0 \exists z \in \mathbb{R} : xz = y$ Dieses z ist eindeutig und durch $z = y(x^{-1})$ gegeben.

Wir schreiben $z = y - x$ für die Lösung in a) und $z = y/x$ für die Lösung in b).

Beweis:

NuN die b). Analog zu a), aber um multiplikatives Inverses zu nutzen, brauchen wir gemäß (MI) dass $x \neq 0$, wie vorausgesetzt.

Sonst wie zuvor: wenn es ein z mit $x \cdot z = y$, dann erhalten wir durch Multiplikation beider Seiten der Gleichung mit (x^{-1}) von links wieder eine Gleichheit, nämlich

$$(x^{-1})(xz) = (x^{-1})y.$$

Wir vertauschen die beiden Seiten und formen/vereinfachen die neue rechte Seite:

$$x^{-1} \cdot y = (x^{-1})(xz) \stackrel{MA}{=} ((x^{-1}x)z) \stackrel{MI}{=} 1 \cdot z \stackrel{MN}{=} z.$$

Somit ist $x^{-1}y = yx^{-1}$ der einzige Kandidat für z . Durch Einsetzen lässt sich leicht überprüfen, dass es eine(dh die einzige Lösung ist). Oder wir bemerken eben, dass sich der Übergang von der ersten zur zweiten Gleichung umkehren lässt indem wir letztere mit x von links multiplizieren. Das bedeutet, unsere **Umformungen** waren **äquivalent**. \square

Satz 2.6. $\forall x \in \mathbb{R} : 0 \cdot x = 0$.

Korollar 2.7. $\forall x \in \mathbb{R} : (-1) \cdot x = -x$.

Beweis:

$$x + (-1) \cdot x = x \cdot 1 + x \cdot (-1) = x \cdot (1 + (-1)) = x \cdot 0 = 0 \cdot x = 0 = x + (-x).$$

Also $x + (-1) \cdot x = x + (-x)$ Daraus folgt mit Addition von $-x$ von links, oder aus Satz 2.5 (dessen Beweis genau dies tut), die Behauptung.

Satz 2.8. $\forall x, y \in \mathbb{R} : xy = 0 \Leftrightarrow (x = 0 \text{ oder } y = 0)$.

Algebraiker formulieren das als: Keine "Nullteiler" in \mathbb{R} bzw einem Körper/ Integritätsbereich.

Beweis:

Lemma 2.9.

- a) $\forall x \in \mathbb{R} : -(-x) = x$
- b) $\forall x \in \mathbb{R} \text{ mit } x \neq 0 : (x^{-1} \neq 0 \text{ \& } (x^{-1})^{-1} = x)$

Beispiel 2.10. $z^2 = 1 \Leftrightarrow (z = 1 \text{ oder } z = -1)$.

Beispiel 2.11. Ein endlicher Körper

$GF(3) = \{0, 1, 2\}$ mit folgenden Rechenregeln ("Restklassen modulo 3" - für Experten).

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

also $2^{-1} = 2$ und $2 = -1$ hier.

Die Überprüfung der neun Körperaxiome von hand ist möglich aber mühsam. (Einfacher gestaltet sich dies z.B. für $GF(2) = \{0, 1\}$ mit entsprechenden Rechenregeln, von denen nur $1 + 1 = 0$ nicht unmittelbar aus (AN), (MN) oder Satz 1.5 folgt). Es zeigt sich, das für jede Primzahl p ein Körper $GF(p)$ mit p Elementen existiert, und die Gültigkeit der Körperaxiome (AA), (MA), (AK), (MK), (AN), (MN) und (DG) folgt leicht aus ähnlichen Aussagen für die natürlichen Zahlen ohne lästiges Probieren aller Einzelfälle.)

APPENDIX A. NOTATIONEN

Wir werden die hier zusammengetragenen Begriffe und Symbole in der Vorlesung jeweils bei Bedarf einführen, dieses Kapitel dient also zur nochmaligen Übersicht.

Definition A.1. Menge (*intuitive Definition von G. Cantor*) ist die Zusammenfassung von Objekten (Elementen), die eine bestimmte Eigenschaft (“die mathematische Aussage $P(x)$ gilt”) haben.

Wir schreiben $x \in M$ wenn x ein Element von M ist, d.h. zu M gehört, und $x \notin M$ andernfalls.

Typischerweise studieren wir $\{x \in X : P(x)\}$, d.h. die Menge aller x aus einer (grossen fixen “Universal-”)Menge X , für die die (mathematische) Aussage $P(x)$ wahr ist.

Wir sagen M ist Teilmenge von N (Notation $M \subset N$), wenn alle Elemente von M auch zu N gehören, zwei Mengen sind gleich wenn sie genau die gleichen Elemente haben. (Statt M Teilmenge von N sagen wir oft M ist kleiner (oder auch kleiner gleich) N). Analog zur Ordnungsrelation für reelle Zahlen ist $M \subset N$ gleichbedeutend mit $N \supset M$. wir schreiben $M \subsetneq N$ wenn $M \subset N$ und $M \neq N$ und sagen M ist *strikt* kleiner als N .

Aus gegebenen Mengen M, N konstruieren wir

- $M \cap N = \{x : x \in M \ \& \ x \in N\}$ Schnittmenge, Durchschnitt von M und N
- $M \cup N = \{x : x \in M \text{ oder } x \in N\}$ Vereinigung
- $M \setminus N = \{x : x \in M \ \& \ x \notin N\}$ Differenzmenge
- $M \times N = \{(x, y) : x \in M \ \& \ y \in N\}$ Produktmenge, wobei $(x, y) = (x', y')$ genau dann wenn $x = x'$ und $y = y'$ - geordnete Paare. Man kann diese auch als Mengen darstellen, zB. $(x, y) = \{\{x\}, \{x, y\}\}$.
- $\mathfrak{P}(M) = \{N : N \subset M\}$ die Potenzmenge von M

Spezielle Notation ist reserviert für

- \emptyset leere Menge, enthält *kein* Element
- $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$ natürliche Zahlen
- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ ganze Zahlen
- $\mathbb{Q} = \{\frac{m}{n} : m \in \mathbb{Z} \ \& \ n \in \mathbb{N}\}$ rationale Zahlen
- \mathbb{R} reellen Zahlen
- \mathbb{C} die komplexen Zahlen

Warnung: $\{\emptyset\} \neq \emptyset$!

Ausserdem bezeichnen wir Intervalle von ganzen oder reellen Zahlen durch die üblichen Notationen (die später flexibler gehandhabt werden):


- $\{k, \dots, m\} = \{l \in \mathbb{Z} : k \leq l \leq m\}$ wenn $k, m \in \mathbb{Z}$, das ist eine Teilmenge von \mathbb{N}_0 bzw. \mathbb{N} wenn $k \in \mathbb{N}_0$ bzw. $k \in \mathbb{N}$,
- $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$ abgeschlossenes Intervall für $a, b \in \mathbb{R}$,
- $(a, b) = \{x \in \mathbb{R} : a < x < b\}$ offenes Intervall für $a \in \{-\infty\} \cup \mathbb{R}$ und $b \in \mathbb{R} \cup \{\infty\}$, wobei wir $\pm\infty$ nicht als Teil des (algebraischen) Körpers \mathbb{R} betrachten können, aber annehmen, dass $\forall x \in \mathbb{R} : -\infty < x < \infty$.
- $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$ rechts offenes (halboffenes) Intervall für $a \in \mathbb{R}$ und $b \in \mathbb{R} \cup \{\infty\}$

- $(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$ links offenes (halboffenes) Intervall für $a \in \{-\infty\} \cup \mathbb{R}$ und $b \in \mathbb{R}$.

Definition A.2. Quantoren Wir benutzen die Abkürzungen

- $\forall x \dots$ bedeutet “für alle x gilt \dots ”
- $\exists x \dots$ bedeutet “es gibt ein x so dass \dots ”

Weitere (logische (Junktoren) und andere) Symbole:

- $\&$ für “und”
- \Rightarrow für “impliziert” und auch \curvearrowright im sehr ähnlichen Sinne von “also”
- \Leftrightarrow für “genau dann wenn”
- \nmid für “Widerspruch” (erzielt)
- $\#$ für Kardinalität, dh. Anzahl der Elemente einer Menge
- \odot, \square für q.e.d, d.h. Beweis beendet
-  für Warnung

Eine Abbildung F bildet eine Menge X in eine Menge Y ab, wenn

$$F \subset M \times N, \quad \forall x \in X \exists y \in Y : (x, y) \in F \text{ und } \forall (x, y), (x, y') \in F : y = y'.$$

Wenn $(x, y) \in F$ dann schreiben wir $y = F(x)$. Wir identifizieren also die Abbildung $F = \{(x, F(x)) : x \in X\}$ mit ihrem ”Graphen”. Wenn $Y = \mathbb{R}, \mathbb{C}$ (oder \mathbb{R}^n) nennen wir F oftmals Funktion und benutzen gerne kleine Buchstaben f, g, h, \dots

Eine Abbildung $F : X \rightarrow Y$ heißt

- injektiv (auch 1 – 1 genannt) wenn $F(x) = F(x') \Rightarrow x = x'$,
- surjektiv (bildet *auf* Y ab, engl ”onto”) wenn $\forall y \in Y \exists x \in X : F(x) = y$,
- bijektiv wenn F injektiv und surjektiv ist.