

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 man auch schreiben 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
- $\{x \in \mathbb{R} : x^2 \in \mathbb{Q} \text{ und } x \geq 0\}$ - 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, z.B. wenn 1 und $1'$ beide neutrale Element der Multiplikation sind, dann gilt ja

$$1' \stackrel{(MN)x=1'}{=} 1 \cdot 1' \stackrel{(MK)}{=} 1' \cdot 1 \stackrel{(MN)x=1}{=} 1,$$

also insgesamt $1' = 1$. Dh, alle möglichen neutralen Elemente der Multiplikation sind in der Tat dasselbe Element.

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 strukturelle 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 2.11. 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) $\forall x \in \mathbb{R} \text{ mit } x \neq 0 : (x^{-1})^{-1} = x$

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, dass 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.)

Bemerkung 2.12. *In den bisherigen Beweisen ließen sich die Schlussfolgerungen jeweils leicht aus den Axiomen herleiten. Wir brauchten noch keine feineren Methoden wie z.B. den indirekten Beweis (Widerspruchsbeweis). Dies wird sich im Folgenden ändern.*

Die bisher definierte Körperaxiome ermöglichen Rechnen mit Gleichungen, für das Rechnen mit Ungleichungen brauchen wir den Begriff der (An)Ordnung. (vergleiche Kapitel 3 in O.Forsters Buch) Primär muss man festlegen, welche Zahlen "positiv", d.h. größer als Null sind. Diese Zahlen müssen dann die im Folgenden angeführten Eigenschaften haben:

II. Anordnungsaxiome

Es gibt eine Menge \mathbb{P} von reellen Zahlen (d.h. $\mathbb{P} \subset \mathbb{R}$), so dass

(O.1) $\forall x \in \mathbb{R}$ gilt *genau* eine der Aussagen: $x \in \mathbb{P}, x = 0, -x \in \mathbb{P}$ "Trichotomie"

(O.2) Wenn $x \in \mathbb{P}$ & $y \in \mathbb{P}$ dann $x + y \in \mathbb{P}$ "Abgeschlossenheit bezüglich Addition"

(O.3) Wenn $x \in \mathbb{P}$ & $y \in \mathbb{P}$ dann $xy \in \mathbb{P}$ "Abgeschlossenheit bezüglich Multiplikation"

Definition 2.13. Wir sagen

$0 < x$ (d.h. x ist *positiv*) gdw. $x \in \mathbb{P}$; $0 > x$ (d.h. x ist *negativ*) gdw. $-x \in \mathbb{P}$
 $x < y$ (d.h. y größer x) gdw. $0 < y - x$; $x > y$ (d.h. y kleiner x) gdw. $0 > y - x$
 $x \leq y$ gdw. ($x < y$ oder $x = y$); $x \geq y$ gdw. ($x > y$ oder $x = y$)

Bemerkung 2.14. a) *jedes $x \in \mathbb{R}$ ist positiv, negativ oder null*

b) *nach Satz 1.5 gilt $x = y \Leftrightarrow 0 = y - x$, also $\forall x, y \in \mathbb{R} : x < y$ oder $x > y$ oder $x = y$*

c) *$x < y \Leftrightarrow -(x - y) = y - x \in \mathbb{P} \Leftrightarrow 0 > x - y \Leftrightarrow y > x$, also y grösser x genau dann wenn x kleiner y*

d) *$x \leq y \Leftrightarrow y - x \in \mathbb{P}_0 = \mathbb{P} \cup \{0\}$ nichtnegativ*

Satz 2.15. *Transitivität der Ordnung $\forall x, y, z \in \mathbb{R} : (x < y \text{ \& } y < z) \Rightarrow x < z$*

Beweis

Bemerkung 2.16. *Also $(x \leq y \text{ \& } y \leq z) \Rightarrow x \leq z$, mit $x < z$ falls zudem $x < y$ oder $y < z$.*

Lemma 2.17. *Translationsinvarianz $\forall x, y, z \in \mathbb{R} : x < y \Leftrightarrow x + z < y + z$*

Beweis

Lemma 2.18. *$\forall x, y, u, v \in \mathbb{R} : (x < y \text{ \& } u < v) \Rightarrow x + u < y + v$*

Beweis

Proposition 2.19. *Spiegelung* $\forall x, y \in \mathbb{R} : x < y \Leftrightarrow -y < -x$

Beweis

Lemma 2.20. $\forall x, y, z \in \mathbb{R}$ mit $x < y : (0 < z \Rightarrow zx < zy), (0 > z \Rightarrow zx > zy)$

Beweis

Korollar 2.21. $\forall x, y, u, v \in \mathbb{R} : (0 \leq x < y \ \& \ 0 \leq u < v) \Rightarrow xu < yv$

Beweis

Satz 2.22. $\forall x \in \mathbb{R} : x^2 \geq 0$, und $x^2 > 0 \Leftrightarrow x \neq 0$.

Beweis: Idee - mit vollständiger Fallunterscheidung.

Korollar 2.23. $0 < 1$, da $1 = 1 \cdot 1 = 1^2$

Obwohl $1 > 0$ und auch die etwas allgemeinere Ungleichung $0 < x^2, x \neq 0$ sehr natürlich erscheinen, sind sie zentral für die weitere Entwicklung der Analysis! Weil in GF(3), siehe Beispiel 2.11, $1 + 1 + 1 = 0$ kann in diesem Körper keine geeignete Menge \mathbb{P} "positiver" Elemente gefunden werden.

Im nächsten Abschnitt werden wir zeigen, dass umgekehrt jede positive reelle Zahl auch das Quadrat einer reellen Zahl ist. Dies wird noch ein weiteres (letztes) Axiom brauchen. Zuerst vollenden(zeigen) wir die Rechenregeln für Ungleichungen aus der Schule.

Proposition 2.24. $\forall x, y \in \mathbb{R} :$

a) $x > 0 \Leftrightarrow x^{-1} > 0$

b) $0 < x < y \Rightarrow 0 < y^{-1} < x^{-1}$ ("Spiegelung an der 1")

Beweis

a) Wenn $x > 0$, dann $x \neq 0$ und $x^{-1} \neq 0$ (Lemma 1.9.b)). Somit $0 < x^{-1}x^{-1}$ wegen Satz 1.22. Wegen $x > 0$ zeigt Lemma 1.20, dass

$$0 = x \cdot 0 < x(x^{-1} \cdot x^{-1}) = (x \cdot x^{-1})x^{-1} = 1 \cdot x^{-1} = x^{-1}.$$

Umgekehrt, da $(x^{-1})^{-1} = x$ folgt aus dem gerade Gezeigten die Umkehrimplikation.

b) Da $0 < x, y$ gilt nach Teil a), dass $0 < x^{-1}, y^{-1}$ und also $0 < x^{-1}y^{-1}$. Nun nutzen wir wieder Lemma 1.20, um

$$0 = 0(x^{-1}y^{-1}) < y^{-1} = x(x^{-1}y^{-1}) < x^{-1} = y(x^{-1}y^{-1})$$

zu folgern.

Beispiel 2.25. Seien $x, y \in \mathbb{R}$ und $x > 0$ sowie $y > 0$. Dann gilt $x < y$ genau dann wenn $x^2 < y^2$.

Beweis

Beispiel 2.26. Wenn $x, y \in \mathbb{R}$, dann folgt aus $x^2 + y^2 = 0$, dass $x = y = 0$.

Beweis: Idee Widerspruch und Satz 2.22.

Beispiel 2.27. Sei $0 < x < y$ und möge \sqrt{xy} existieren (dh. positive Zahl, deren Quadrat xy ist). Dann gilt die AG-Ungleichung (zwischen arithmetischem und geometrischem Mittel)

$$y > \frac{x+y}{2} > \sqrt{xy} > x.$$

Beweis: Idee - für die mittlere Ungleichung quadrieren (nutze Bsp 2.25) und quadratische Ergänzung (dh nutze binomischen Formel für Quadrate).

Absolutbetrag, Maximum und Minimum

Definition 2.28. Sei $x \in \mathbb{R}$, wir definieren den Betrag von x als

$$|x| = \begin{cases} x & \text{wenn } x > 0 \\ 0 & \text{wenn } x = 0 \\ -x & \text{wenn } x < 0 \end{cases}$$

Bemerkung 2.29. i) wichtige geometrische Bedeutung: $|x - y|$ Abstand von x zu y

ii) aus der Definition (mit Fallunterscheidung $x >, =, < 0$) folgt leicht

$$x \leq |x| = |-x|, |x| \geq 0 \text{ mit "=" gdw. } x = 0$$

Lemma 2.30. Für alle $x, y \in \mathbb{R}$ gilt:

- a) $|x| \leq y \Leftrightarrow -y \leq x \leq y$ (und dann $y \geq 0$),
- b) Sei $\sigma \in \{-1, 1\}$ dann $\sigma x \leq |x|$, und falls $x \geq 0$ dann $|\sigma x| = |x| = x$.

Beweis: a) Wenn $-y \leq x \leq y$ dann $x \leq y$ und $-x \leq y$. Da $|x| \in \{x, -x\}$, folgt $|x| \leq y$. Umgekehrt, wenn $|x| \leq y$ dann sicher $y \geq 0$ und entweder $x \geq 0$ und somit $y \geq |x| = x \geq 0 \geq -y$ oder $x < 0$ und also $y \geq |x| = -x \geq 0 \geq -y$ impliziert nach Prop. 2.19 $-y \leq -(-x) = x \leq -(-y) = y$. b) nutze Bem 2.29.ii).

Definition 2.31. Sei $x \in \mathbb{R}$, wir definieren das Signum (entspricht Vorzeichen) von x als

$$\operatorname{sgn}(x) = \begin{cases} 1 & \text{wenn } x > 0 \\ -1 & \text{wenn } x < 0 \end{cases}$$

Bemerkung 2.32. $\operatorname{sgn}(0)$ wird im Allgemeinen und in dieser VL als 1 definiert, auch -1 ist möglich und ebenfalls $\operatorname{sgn}(0) = 0$ wird gelegentlich in der Literatur verwendet. In jedem Falle gilt, wie der zweite Punkt in 2.29 (oder direkte FU) zeigt

$$\forall x \in \mathbb{R} : |x| = \operatorname{sgn}(x) \cdot x \text{ und } x = \operatorname{sgn}(x) \cdot |x|.$$

Dies hilft oftmals, lästige FUn einzusparen.

Satz 2.33. Für alle $x, y \in \mathbb{R}$

- a) $|xy| = |x||y|$ Multiplikativität
- b) $|x + y| \leq |x| + |y|$ Dreiecks-Ungleichung!

Beweis: Ideen Nutze Lemma 2.30b), für a) mit $\operatorname{sgn}(x)$ und $\operatorname{sgn}(y)$, für b) mit $\operatorname{sgn}(x+y)$.

Definition 2.34. Seien $x, y \in \mathbb{R}$ gegeben, wir definieren dann

$$\min(x, y) = \begin{cases} x & \text{wenn } x \leq y \\ y & \text{wenn } x > y \end{cases}, \text{ und } \max(x, y) = \begin{cases} y & \text{wenn } x \leq y \\ x & \text{wenn } x > y \end{cases}.$$

Lemma 2.35. Für alle $x \in \mathbb{R}$

$$\max(x, y) = \frac{x+y}{2} + \frac{|x-y|}{2} \text{ und } \min(x, y) = \frac{x+y}{2} - \frac{|x-y|}{2}.$$

Beweis FU:

Die geometrische Bedeutung dieser Formel ist klar: gehe von der Mitte $\frac{x+y}{2}$ zwischen zwei Zahlen x, y den halben Abstand $\frac{|x-y|}{2}$ der beiden Zahlen in positive Richtung und gelange zur grösseren der beiden Zahlen. Analog für $\min(x, y)$.

Mittels $\max(x, y, z) = \max(x, \max(y, z))$ usw. ist Maximum und analog Minimum für beliebige “endliche” (noch zu definieren!) Mengen reeller Zahlen definiert. Diese größten und kleinsten Elemente einer Menge existieren nicht mehr, wenn wir, wie im Folgenden, allgemeine unendliche Mengen betrachten.

Beispiel 2.36. $M = \{x \in \mathbb{R} : x > 0\}$ hat kein Minimum, das heißt es gibt kein kleinstes Element in dieser Menge.

Beweis indirekt

Definition 2.37. Sei $M \subset \mathbb{R}$ beliebig

- a) $s \in \mathbb{R}$ ist $\max M$, das Maximum der Menge M , wenn $s \in M$ und $\forall x \in M : x \leq s$.
 $s \in \mathbb{R}$ ist $\min M$, das Minimum der Menge M , wenn $s \in M$ und $\forall x \in M : x \geq s$
- b) $s \in \mathbb{R}$ ist obere Schranke (**OS**) für M wenn $\forall x \in M : x \leq s$, $s \in \mathbb{R}$ ist untere Schranke (**US**) für M wenn $\forall x \in M : x \geq s$
- $s \in \mathbb{R}$ ist **Supremum** von M ($s = \sup M$) wenn s die kleinste aller oberen Schranken von M ist, d.h.

$$(\forall x \in M : x \leq s) \text{ \& } (\forall t \text{ OS von } M : t \geq s).$$

- $s \in \mathbb{R}$ ist **Infimum** von M ($s = \inf M$) wenn s die größte aller unteren Schranken von M ist, d.h.

$$(\forall x \in M : x \geq s) \text{ \& } (\forall t \text{ US von } M : t \leq s).$$

- M ist von oben (bzw. unten) beschränkt wenn es eine obere (bzw. untere Schranke) für M gibt. M beschränkt wenn von unten und oben beschränkt.

Beispiel 2.36. (Fortsetzung) $M = \{x \in \mathbb{R} : x > 0\}$ hat keine OS, s ist US gdw. $s \leq 0$, also $\inf M = 0$ aber $\sup M$ existiert nicht.

Beweis

Die Existenz von \inf und \sup wann immer es entsprechende Schranken gibt, gilt nicht nur für so einfache Mengen wie dieses M (Intervall), sondern im Allgemeinen. Das unterscheidet \mathbb{R} von anderen Körpern und ist formuliert im letzten noch benötigten

III. Vollständigkeitsaxiom

(VA) Für jede nichtleere und von oben beschränkte Menge $M \subset \mathbb{R}$ existiert das Supremum $\sup M$.

Lemma 2.38. Sei M eine Menge reeller Zahlen, dann $(\exists \max M \Leftrightarrow \sup M \in M)$

Beweis

Proposition 2.39. Sei $M \subset \mathbb{R}$ nichtleer und von oben beschränkt, $s \in \mathbb{R}$. Dann

- $s \geq \sup M \Leftrightarrow \forall m \in M : m \leq s$
- $s = \sup M \Leftrightarrow (\forall m \in M : m \leq s \ \& \ \forall \varepsilon > 0 \ \exists m \in M : s - \varepsilon < m)$

APPROXIMATIONSPRINZIP

Beweis

Lemma 2.40. *Seien $M, N \subset \mathbb{R}$ nichtleer und von oben beschränkt. Dann*

- a) $\inf(-M) = -\sup M$,
- b) $\sup(M + N) = \sup M + \sup N$,

wobei $-M = \{-m : m \in M\}$ ist die "Spiegelung" von M , und $M + N = \{m + n : m \in M \text{ \& } n \in N\}$ die Summe der beiden Mengen ist.

Beweis Teil a) siehe ÜZ4. Teil b) etwas schwerer - aber nicht wirklich schwer: nutzen Approximationseigenschaft und $\frac{\varepsilon}{2}$ -Trick.

Nun die erste überraschende und wichtige Konsequenz des Vollständigkeitsaxioms.

Satz 2.41. *Für alle positiven reellen x existiert ein eindeutiges $w > 0$, so dass $w^2 = x$.*

Wir schreiben für diese Zahl $w = \sqrt{x}$ und nennen sie Wurzel aus(von) x .

Beweis Eindeutigkeit schon gezeigt. Die Schlüsselidee für Existenz ist zu zeigen, dass $w^2 = x$ wobei $w = \sup\{y > 0 : y^2 < x\}$. Hierfür sowohl $w^2 > x$ als auch $w^2 < x$ durch "Linearisierung der Quadratfunktion" zu Widersprüchen führen.

Dass heißt, z_z die Ungleichungen $x^2 > 2$ und $x^2 < 2$ bleiben gültig wenn x nur "wenig" geändert wird. Hierzu explizite (und geeignete! - je nach Typ der Ungleichung) Vereinfachungen von $(x + \delta)^2 = x^2 + 2\delta x + \delta^2$ finden. Stabilität von Ungleichungen wie $f(x) > y$ hat mit "Stetigkeit" der Funktion f zu tun - diese erhalten wir später allgemeiner ohne explizites Rechnen ("softer") für den "Zwischenwertsatz". Deshalb diesen Beweis verstehen!!

Zahlbereiche

Nachdem wir alle grundlegenden Axiome für \mathbb{R} eingeführt und erste Anwendungen gesehen haben, benennen wir noch wichtige Teilmengen von \mathbb{R} – wie die natürlichen, die ganzen und die rationalen Zahlen.

Definition 2.42. $M \subset \mathbb{R}$ heißt induktiv wenn $1 \in M$ und $\forall n \in \mathbb{R} : n \in M \Rightarrow n + 1 \in M$.

zB $\mathbb{R} \supset (0, \infty) \supset [1, \infty) \supset \{1\} \cup [2, \infty)$ sind 4 verschiedene induktive Mengen.

Satz 2.43. *Es gibt eine kleinste induktiven Menge, dh. sie ist Teilmenge jeder induktiven Menge. Diese kleinste induktive Menge ist eindeutig, wird mit \mathbb{N} bezeichnet und ihre Elemente werden natürliche Zahlen genannt.*

Beweis- Idee: der Durchschnitt der Familie aller induktiven Mengen ist induktiv - das heißt, wir definieren

$$\mathbb{N} = \{n \in \mathbb{R} : \text{wenn } M \subset \mathbb{R} \text{ dann } n \in M \},$$

und zeigen dieses \mathbb{N} ist induktiv - trivialerweise die kleinste.

Korollar 2.44. (Schwach)es Induktionsprinzip: M induktiv $\Rightarrow \mathbb{N} \subset M$. Also wenn P eine mathematische Aussage ist, so dass: $P(1)$ wahr ist und für alle $n \in \mathbb{N}$ aus $P(n)$ wahr auch $P(n+1)$ wahr folgt, dann gilt $P(n)$ für alle $n \in \mathbb{N}$.

Beweis- Idee: Nur überprüfen, dass die Menge M aller $n \in \mathbb{N}$, für die $P(n)$ gilt, induktiv ist. Aber das ist ja trivial!

Bemerkung Wenn $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, dann $(0 \in M \text{ und } (n \in M \Rightarrow n+1 \in M))$ impliziert $\mathbb{N}_0 \subset M$, da $0+1 \in M$ also M induktiv und somit $\mathbb{N} \subset M$, Also wenn P mathematische Aussage, so dass: $P(0)$ und $\forall n \in \mathbb{N}_0 : P(n) \Rightarrow P(n+1)$, dann gilt $P(n)$ für alle $n \in \mathbb{N}_0$.

Definition 2.45. Summen-und Produktsymbol Für $n, m, k \in \mathbb{N}_0$ setzen wir ("rekursive Definition")

$$\begin{aligned} \sum_{k=n}^{n-1} a_k &= 0 \text{ (leere Summe)}, \forall m \geq n-1 : \sum_{k=n}^{m+1} a_k = \left(\sum_{k=n}^m a_k \right) + a_{m+1} \\ \prod_{k=n}^{n-1} a_k &= 1 \text{ (leeres Produkt)}, \forall m \geq n-1 : \prod_{k=n}^{m+1} a_k = \left(\prod_{k=n}^m a_k \right) \cdot a_{m+1} \\ a^n &= \prod_{k=1}^n a, \text{ Potenz } (a^0 = 1 \text{ wenn } a \neq 0), n! = \prod_{k=1}^n k, \text{ Fakultät } (0! = 1) \end{aligned}$$

Mit Induktion kann man zeigen, diese Symbole sind für $a_k \in \mathbb{R}$ immer wohl definiert.

Satz 2.46. Bernoullische Ungleichung:

a) $\forall n \in \mathbb{N} \forall x \in \mathbb{R}$ mit $x \geq -1$: $(1+x)^n \geq 1+nx$.

b) Überdies gilt $\forall n \in \mathbb{N} \forall x \in \mathbb{R}$ wenn $n \geq 2 (=1+1)$ und $(x \geq -1 \text{ \& } x \neq 0)$ dann

$$(1+x)^n > 1+nx. \quad (*)$$

Beweis-Idee: Falls $n = 1$ oder $x = 0$ sind Behauptungen a) und b) trivial. Also oBdA $x \neq 0$ und $n \neq 1, \Rightarrow n \geq 2$ (wird noch gezeigt). Somit b) z_z , hierzu fixieren wir $x \in [-1, 0) \cup (0, \infty)$, betrachten die Aussage $P(n)(= P_x(n)) : (n = 1 \text{ oder } (*))$ gilt) und beweisen sie mit Induktion.

Proposition 2.47. Für $n \in \mathbb{N}$ sei $a_n = \left(1 + \frac{1}{n}\right)^n$. Dann $\forall n \in \mathbb{N} : a_n < a_{n+1}$.

Beweis Idee: zB $\frac{a_n}{a_{n-1}} > 1$ für $n \geq 2$ mit Bernoullischer Ungleichung beweisen (einfacher abzuschätzen, und dass jedes natürliche $n \neq 1$ einen Vorgänger hat zeigt Lemma 2.52.)

Definition 2.48. Für $n, k \in \mathbb{N}_0$ ist der Binominalkoeffizient definiert durch

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} \left(= \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots 1} \right) & \text{für } 0 \leq k \leq n \\ 0 & \text{wenn } k > n. \end{cases}$$

$$\text{z.B. } \binom{n}{0} = \binom{n}{n} = 1, \binom{n}{1} = n, n > 0, \binom{n}{k} = \binom{n}{n-k}, 0 \leq k \leq n.$$

Lemma 2.49. Vom Pascalschen Dreieck

$$\forall n \in \mathbb{N}_0 \forall k \in \mathbb{N} : \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Beweis Wenn $k > n$ Definition direkt nutzen, sonst Bruchrechnung.

Satz 2.50. Binominalsatz Mit der (Zusatz) Vereinbarung $0^0 = 1$ gilt

$$\forall x, y \in \mathbb{R} \forall n \in \mathbb{N}_0 : (x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$$

Beweis Idee: Induktion in n unter Benutzung von Lemma 2.49.

Obwohl wir \mathbb{N} über die Eigenschaft induktive Menge definiert haben, erlaubt es als Zahlenbereich, die Rechenoperationen, wie aus der Elementarmathematik gewohnt, auszuführen.

Lemma 2.51.

$$\forall n, m \in \mathbb{N} : n + m \in \mathbb{N} \ \& \ n \cdot m \in \mathbb{N}.$$

Beweis: Idee – mit Induktion, zuerst für beliebiges aber fixes $n \in \mathbb{N}$ Induktion in m machen für die Addition. Dies dann nutzen, um wieder für beliebiges aber fixes $n \in \mathbb{N}$ Induktion in m für die Multiplikation zu machen. $P_n^+(m) : n+m \in \mathbb{N}$, $P_n^-(m) : n \cdot m \in \mathbb{N}$.

Lemma 2.52.

$$\forall n \in \mathbb{N} : n = 1 \text{ oder } (n > 1 \ \& \ n - 1 \in \mathbb{N}).$$

Insbesondere ist $1 = \min \mathbb{N}$.

Beweis- Idee: $M = \mathbb{N} \setminus \{n\}$ echte Teilmenge von \mathbb{N} also keine induktive Menge. (oder Induktion in n , Standard)

Satz 2.53.

$$\forall n, m \in \mathbb{N} : n \leq m \text{ oder } n - m \in \mathbb{N}. \quad (: P_n(m))$$

Beweis-Idee: für fixes n Induktion in m , hierbei Lemma 2.52 für $m = 1$ und $k = n - m$ nutzen.

Wir haben also gezeigt: $m < n$ in $\mathbb{N} \Rightarrow m \leq n - 1$, denn $n - m \in \mathbb{N}$ also $n - m \geq 1$.

Definition 2.54. $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$ sind die ganzen Zahlen.

Proposition 2.55. a) $\mathbb{Z} = \mathbb{N} - \mathbb{N} = \{n - m : n, m \in \mathbb{N}\}$. b) (Deshalb) $\forall x, y \in \mathbb{Z} : x + y, x - y, x \cdot y \in \mathbb{Z}$.

Beweis: Idee - In a) nur $\mathbb{Z} \supset \mathbb{N} - \mathbb{N}$ nichttrivial, nutzen Lemma 2.53. Für b): nutze a) und Lemma 2.51 (mit oder ohne FU).

Definition 2.56. $\mathbb{Q} = \{\frac{p}{q} : p \in \mathbb{Z} \text{ \& } q \in \mathbb{N}\}$ sind die rationalen Zahlen. Also $q \neq 0$!

Klarerweise $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Bemerkung 2.57. $(\mathbb{Q}, +_{\mathbb{R}}, \cdot_{\mathbb{R}})$ mit $\mathbb{P}_{\mathbb{Q}} = \mathbb{P} \cap \mathbb{Q}$ erfüllt die 9 Körperaxiome und die 3 Anordnungsaxiome, dies lässt sich einfach überprüfen — da $\frac{p}{q} \frac{m}{n} = \frac{pm}{qn}$ und $\frac{p}{q} + \frac{m}{n} = \frac{pn+qm}{qn}$, führen die Operation $+, \cdot$ von $\mathbb{Q} \times \mathbb{Q}$ nach \mathbb{Q} zurück, $-\frac{p}{q} = \frac{-p}{q}$ und $(\frac{p}{q})^{-1} = \frac{q}{p}$ für $p > 0$, $(\frac{p}{q})^{-1} = \frac{-q}{-p}$ für $p < 0$ zeigt die Existenz der Inversen in \mathbb{Q} .

Starke Induktion

mal etwas Neues

Satz 2.58. WOHLORDNUNG DER NATÜRLICHEN ZAHLEN Sei $M \subset \mathbb{N}$ nichtleer, dann existiert $\min M$.

Beweis Idee – Für beliebiges aber fixes solches M mit Induktion (Korollar 2.44) in n zeigen:

$$\forall n \in \mathbb{N} : \exists m \in M : m \leq n \Rightarrow \exists \min M.$$

Korollar 2.59. STARKES INDUKTIONSPRINZIP Sei P eine mathematische Aussage, so dass $P(1)$ und $\forall n \in \mathbb{N} : (\forall k \in \mathbb{N} : k \leq n \Rightarrow P(k)) \Rightarrow P(n+1)$. Dann gilt $P(n)$ für jedes $n \in \mathbb{N}$.

Beweis Idee: Betrachte $M = \{n \in \mathbb{N} : P(n) \text{ falsch}\}$, falls $M \neq \emptyset$ gibt es einen Widerspruch für $n = \min M$.

Bemerkungen

- auch als Prinzip der "least criminals" bekannt, eine gute Übersetzung wäre: die kleinsten/ersten "Bösewichte" im Sinne von minimalen Gegenbeispielen. Es ist oftmals einfacher, die Existenz solcher als die Existenz allgemeiner Gegenbeispiele auszuschliessen.
- warum *starkes* Induktionsprinzip genannt: Um das entscheidende $P(n+1)$ zu beweisen, können wir nunmehr $P(1), P(2), \dots, P(n)$ voraussetzen. Bisher konnten wir nur $P(n)$ annehmen und also haben wir nun eine "stärkere" Beweismethode, die es erlaubt, mehr und "stärkere" Aussagen zu beweisen.
- eine einfacherere (meine Lieblings-)Formulierung, die allerdings von der bekannten Formulierung " $\Rightarrow P(n+1)$ " abweicht ist folgende.

Sei P eine mathematische Aussage, so dass für jedes $n \in \mathbb{N}$ $P(n)$ gilt, falls
 $\forall k \in \mathbb{N} : k < n \Rightarrow P(k)$. Dann gilt $P(n)$ für alle $n \in \mathbb{N}$.

(DIY: zB $P(1)$ gilt dann)

Definition 2.60. Wir sagen p ist Primzahl, wenn $p \in \mathbb{N}$, $p > 1$ und
 $(p = n \cdot m, \text{ mit } n, m \in \mathbb{N}) \Rightarrow (n = 1 \text{ oder } m = 1)$.

Behauptung: Jedes $n \in \mathbb{N}$ mit $n > 1$ ist Produkt (eventuell einfaktorielles) endlich vieler Primzahlen. (Die Eindeutigkeit der Produktdarstellung ist viel tiefliegender!)

Beweis: Mit starker Induktion einfachst, mit Kor. 2.44 (schwache Induktion) unklar!

Lemma 2.61. $\forall n \in \mathbb{N} : (\exists k \in \mathbb{N} : n = 2k \text{ oder } \exists l \in \mathbb{N} : n = 2l - 1)$, und nur einer der Fälle tritt ein. (nennen n dann gerade bzw ungerade).

Beweis: Induktion, Widerspruch zu $1 = \min \mathbb{N}$ für Eindeutigkeit des Falles.

Satz 2.62. (Der Klassiker) $\sqrt{2} \notin \mathbb{Q}$, d.h. die Diagonale im Einheitsquadrat ist irrational.

Beweis: Idee- Mit ζ , betrachte eine Bruchdarstellung mit kleinstem Nenner. Zeige Zähler & Nenner gerade, wir können also kürzen! $M = \{q \in \mathbb{N} : \exists p \in \mathbb{N} : p^2/q^2 = 2\} \neq \emptyset$.

Rational versus Reell

Weil nicht alle reellen Zahlen rational sind, müssen wir das Verhältnis von \mathbb{Q} und \mathbb{R} studieren. Wir beginnen mit der folgenden Aussage, die auf Archimedes zurückgeführt wird, obwohl er Eudoxos von Knidos als Urheber erwähnt. Die Bezeichnung "Axiom" ist zwar in der Literatur aus historischen Gründen üblich, in der Theorie der reellen Zahlen jedoch unbegründet, da es sich hier um eine Konsequenz aus unseren 13 Axiomen handelt.

Satz 2.63. (Archimedisches "Axiom") *Die Menge \mathbb{N} der natürlichen Zahlen ist in \mathbb{R} nicht von oben beschränkt.*

Beweis: Idee: Mit ζ , betrachte dazu $\sup \mathbb{N}$ und Approximationsprinzip.

Korollar 2.64. (Eudoxos) $\forall x \in \mathbb{R} : x > 0 \Rightarrow \exists n \in \mathbb{N} : \frac{1}{n} < x$

Beweis: Idee: folgt direkt aus dem Archimedischen Axiom.

Nunmehr können wir zeigen, dass obwohl nicht alle Zahlen rational sind, die rationalen Zahlen zumindest alle Zahlen gut annähern können.

Satz 2.65. (Rationale Zahlen sind dicht) *Für alle $x < y$ reell existiert $z \in \mathbb{Q}$, die $x < z < y$ erfüllt.*

Beweis: Idee: Erst nach \mathbb{R}_+ verschieben. Nun führen kleine Schritte zum Ziel!

Die komplexen Zahlen

Als letzten Körper führen wir die komplexen Zahlen ein, in diesem Körper ist die in \mathbb{R} unlösbare Gleichung $x^2 + 1 = 0$ leicht lösbar.

Definition 2.66. Wir betrachten $\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(a, b) : a, b \in \mathbb{R}\}$ mit den Operationen

$$(a, b) + (c, d) = (a + c, b + d), (a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Dann ist \mathbb{C} ein Körper mit Nullelement $(0, 0)$ (neutral für "+") und Einselement $(1, 0)$ (neutral für "·").

Bemerkung 2.67.

- nur die Axiome (MA), (MK) und (DG) erfordern etwas Arbeit
- für $(a, b) \neq (0, 0)$ ist $(a/(a^2 + b^2), -b/(a^2 + b^2))$ das multiplikative Inverse !!
- $\mathbb{R} \equiv \mathbb{R} \times \{0\} \subset \mathbb{C}$, d.h. $x \rightarrow (x, 0)$ gibt \mathbb{R} als Unterkörper von \mathbb{C} - wir haben $x + y \rightarrow (x, 0) + (y, 0)$ und $x \cdot y \rightarrow (x, 0) \cdot (y, 0)$
- $(0, 1)^2 = (-1, 0)$!! Wir schreiben i für $(0, 1)$ und $a + bi$ für (a, b) Somit $i^2 = -1$ und \mathbb{C} kann nicht angeordnet werden, d.h. es gibt kein $\mathbb{P} \subset \mathbb{C}$, das (O.1), (O.2) und (O.3) erfüllt.
- Definition von "·" lässt sich "motivieren" aus Körperaxiomen und $(0, 1)^2 = (-1, 0)$.

Definition 2.68. Für $z = a + bi = (a, b) \in \mathbb{C}$ definieren wir

$$\operatorname{Re}(z) = a, \operatorname{Im}(z) = b, |z| = \sqrt{a^2 + b^2} \text{ Realteil, Imaginärteil und Betrag von } z$$

sowie

$$\bar{z} = a - bi \text{ die zu } z \text{ komplex konjugierte Zahl.}$$

Wie in \mathbb{R} ist $|z|$ der Abstand von z zum Ursprung (\mathbb{C} wird mit der Euklidischen Ebene \mathbb{R}^2 identifiziert).

Lemma 2.69. $\forall z, w \in \mathbb{C}$

- a) $\overline{z + w} = \bar{z} + \bar{w}, \overline{z \cdot w} = \bar{z} \cdot \bar{w} !$
- b) $\bar{\bar{z}} = z, |z| = \sqrt{z \cdot \bar{z}} = |\bar{z}|, \operatorname{Re}(z) = (z + \bar{z})/2, \operatorname{Im}(z) = (z - \bar{z})/2i.$

Beweis: Zweite Teilbehauptung von a) in der Tat entscheidend, zB Satz 2.70.c) & d).

Satz 2.70. Für alle $z, w \in \mathbb{C}$

- a) $|Re(z)| \leq |z|, |Im(z)| \leq |z|$ und $|Re(z)| = |z| \Leftrightarrow Im(z) = 0 \Leftrightarrow z \in \mathbb{R}$
- b) $|z| \geq 0, |z| = 0 \Leftrightarrow z = 0$ (wie in \mathbb{R})
- c) $|z \cdot w| = |z| \cdot |w|$ Multiplikativität (wie in \mathbb{R})
- d) $|z + w| \leq |z| + |w|$ Δ -Ungleichung (wie in \mathbb{R})

Beweis:

Proposition 2.71. Komplexe Quadratwurzeln Für gegebenes $c \in \mathbb{C}$ suchen wir alle (da kein "Positives" ausgezeichnet ist) $w \in \mathbb{C}$ mit $w^2 = c$.

Hierbei $w^2 = 0 \Leftrightarrow w = 0$, und wenn $c \neq 0$ dann ist

$$w_1 = \sqrt{\frac{|c| + Re(c)}{2}} + \sigma \sqrt{\frac{|c| - Re(c)}{2}}i \text{ wo } \sigma = \begin{cases} 1 & \text{für } Im(c) \geq 0 \\ -1 & \text{für } Im(c) < 0 \end{cases}$$

eine Lösung, die einzige andere Lösung ist $w_2 = -w_1$.

Jede quadratische Gleichung

$$0 = z^2 + az + b = (z + \frac{a}{2})^2 - (\frac{a^2}{4} - b) = (z + \frac{a}{2} + w)(z + \frac{a}{2} - w)$$

wobei $w^2 = \frac{a^2}{4} - b$ kann somit in \mathbb{C} gelöst werden.

Beweis:

IM ZUSAMMENHANG MIT DER EXPONENTIALFUNKTION UND DER EULERSCHEN FORMEL WERDEN WIR BALD EINEN GEOMETRISCHEREN ZUGANG ZU DEN KOMPLEXEN ZAHLEN \mathbb{C} FINDEN, DER DIESE ALS EBENE UND DIE RECHENOPERATIONEN ALS GEOMETRISCHE VERSCHIEBUNGEN UND DREHSTRECKUNGEN INTERPRETIERT.

Zum Beispiel, wenn $(0, z, w) \in \mathbb{C}$ ein Dreieck Δ in der komplexen Ebene darstellt und $u \in \mathbb{C}$, dann hat das Dreieck $(0+u = u, z+u, w+u)$ wieder Seiten der Länge $|z|, |w|, |z-w|$ (also kongruent und parallel zu Δ) und das Dreieck $0 \cdot u = 0, z \cdot u, w \cdot u$ Seiten der Länge $|z| \cdot |u|, |w| \cdot |u|, |z-w| \cdot |u|$, ist also ähnlich zu Δ und hat somit gleiche Winkel.

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.