

Elemente der Arithmetik und Algebra II

Sommersemester 2004

Vorlesungsmanuskript

zur Vorlesung von Maria Specovius

FB Mathematik/Informatik, Universität Kassel

Inhaltsverzeichnis

1 Vollständige Induktion

3

1 Vollständige Induktion

Wir beschäftigen uns noch einmal mit der Identität

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2} \quad \text{für } n \in \mathbb{N} \quad (1.1)$$

und geben für diese im folgenden einen alternativen Beweis.

Zunächst könnten wir (1.1) für einige n “durchprobieren” und würden dabei feststellen, daß beide Seiten gleiche Ergebnisse liefern. Das wäre natürlich kein Beweis dafür, daß (1.1) für alle $n \in \mathbb{N}$ richtig ist: Betrachten Sie (zur Warnung!) z.B. die Behauptung:

$$n^2 + n + 41 \text{ ist eine Primzahl.}$$

Dies ist für $n = 1, 2, \dots, 39$ wahr und erst für $n = 40$ (wegen $40^2 + 40 + 41 = 41 \cdot 41$) falsch.

Wir überlegen uns nun folgendes: Wir bezeichnen die Aussage (1.1) für ein bestimmtes $n \in \mathbb{N}$ als $A(n)$. Daß die Aussage $A(1)$ wahr ist, können wir einfach durch einsetzen verifizieren. Angenommen wir hätten, daß für (beliebiges) $n \in \mathbb{N}$ gilt

$$A(n) \text{ wahr} \implies A(n+1) \text{ wahr}, \quad (1.2)$$

so könnten wir folgern

$$A(1) \implies A(2) \implies A(3) \implies \dots \quad (1.3)$$

Bevor wir nun diese Aussagenkette weiter “interpretieren”, prüfen wir, ob in unserem Beispiel (1.2) gilt: Wir nehmen also an, daß

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$$

für (irgendein) $n \in \mathbb{N}$ wahr ist. Dann gilt für $n+1$

$$\begin{aligned} 1 + 2 + 3 + \dots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Damit haben wir für unser Beispielproblem (1.2) gezeigt, und können damit (1.3) folgern.

“Erwischen” wir aber in (1.3) alle $n \in \mathbb{N}$, bzw., haben wir damit tatsächlich bewiesen, daß $A(n)$ für alle $n \in \mathbb{N}$ wahr ist?

Angenommen, daß wäre nicht der Fall, d.h., angenommen, es gäbe ein $m \in \mathbb{N}$ für das $A(m)$ falsch ist. Dann gäbe es (und so haben wir schon öfter argumentiert!) ein kleinstes $m \in \mathbb{N}$ für das $A(m)$ falsch ist. Da $A(1)$ wahr ist, muß $m > 1$ sein, also $m-1 \geq 1$ gelten.

Nun ist aber (wegen der Minimalität von m) $A(m-1)$ wahr und daraus folgt wegen (1.2), daß auch $A(m)$ wahr sein muß. Widerspruch! Also: $A(m)$ ist für alle $m \in \mathbb{N}$ wahr.

Damit können wir aus unserer obigen Argumentation tatsächlich die Summenformel für alle $n \in \mathbb{N}$ folgern!!!

Zusammenfassend: Unter der Voraussetzung, daß **jede nichtleere Teilmenge der natürlichen Zahlen ein kleinstes Element besitzt** (Dies nennt man übrigens das *Wohlordnungsprinzip*. Wer wollte dies in Frage stellen?), haben wir für die Menge von Aussagen $A(n)$, $n \in \mathbb{N}$, gezeigt: Ist

- i) $A(1)$ wahr, und gilt
- ii) für $n \in \mathbb{N}$: $A(n)$ wahr $\implies A(n+1)$ wahr,

so ist

$$A(n) \text{ wahr für alle } n \in \mathbb{N}.$$

Schritt i) nennt man den *Induktionsanfang*, Schritt ii) den *Induktionsschritt* und darin “ $A(n)$ wahr” die *Induktionsvoraussetzung* und “ $A(n+1)$ wahr” die *Induktionsbehauptung*.

Hat man eine Menge von Aussagen $A(n)$ für $n \in \mathbb{N}$ mit $n \geq k \in \mathbb{N}$, $k \in \mathbb{N}$, gegeben, so ist natürlich der Induktionsanfang “ $A(1)$ wahr” durch “ $A(k)$ wahr” zu ersetzen und der Induktionsschritt für $n \in \mathbb{N}$ mit $n \geq k$ zu beweisen.

Unabhängig davon bezeichnet man dieses Vorgehen als *vollständige Induktion*. Daß durch dieses Vorgehen die Wahrheit von $A(n)$ für alle $n \in \mathbb{N}$ bewiesen ist, nennt man das *Prinzip der vollständigen Induktion*.

Bemerkung.

Wir haben schon im letzten Semester festgestellt, dass man in der Mathematik von einem System von nicht beweisbaren (- man könnte auch sagen: Gottgegebenen -) Aussagen startet, diese nennt man **Axiome**, sozusagen die Spielsteine der Mathematik. Mit den Gesetzen der Logik leitet man dann neue Aussagen aus den Axiomen her, und/oder konstruiert neue Dinge oder benennt spezielle Eigenschaften, für die dann weitere Begriffe eingeführt werden (**Definitionen**). Wir haben in Abschnitt 8 im letzten Semester die Axiome der Mengenlehre benutzt, um die uns bekannten Rechenregeln für die natürlichen Zahlen herzuleiten.

Bei der Herleitung des Induktionsprinzips haben wir als Axiom das Wohlordnungsprinzip benutzt. Äquivalent hätten wir dieses auch aus dem Dirichlet’schen Schubfachprinzip folgern können. Dieses besagt: Wenn ich $m \in \mathbb{N}$ Gegenstände auf $n \in \mathbb{N}$ Schubfächer mit $n < m$ verteile, dann liegt in wenigstens einem Schubfach mehr als ein Element. Dieses erscheint genauso evident wie das Wohlordnungsprinzip, wogegen gegen das Prinzip der vollständigen Induktion eher Vorbehalte formuliert werden könnten. Erwähnt sei (und das ist nicht schwierig zu beweisen, siehe z.B. F.Padberg, R.Danckwert, M.Stein, *Zahlbereiche*), daß diese drei Prinzipien tatsächlich äquivalent sind. Ausserdem: Will man die Menge \mathbb{N} der natürlichen Zahlen charakterisieren, führt letztlich um die Induktionseigenschaft kein Weg herum. Die für die Kardinalzahlen hergeleiteten Rechenregeln z.B. reichen

nicht aus. Andererseits ist es nicht notwendig, alle von uns für Kardinalzahlen hergeleiteten Rechenregeln in einer Charakterisierung zu berücksichtigen. Das bekannteste (die Induktionseigenschaft als ein Axiom enthaltende) Axiomensystem stammt von Peano. Vgl. dazu auch die Bemerkungen und Hinweise in dem oben erwähnten Buch von F. Padberg et al. oder auch in A. Kirsch, *Mathematik wirklich verstehen*.

Weitere Beispiele für die Anwendung der vollständigen Induktion.

a) Für $n \in \mathbb{N}$ gilt

$$\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}. \quad (1.4)$$

Beweis. Die Aussage $A(n)$ ist hier $\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}$.

Induktionsanfang: $A(1)$ ist richtig, es gilt nämlich: Für $n = 1$ ergibt die linke Seite von (1.4) 1 und die rechte Seite $\frac{1(1+1)(2 \cdot 1 + 1)}{6} = 1$.

Induktionsschritt: Für ein $n \in \mathbb{N}$ gelte (1.4), d.h. $A(n)$ sei wahr. Zu zeigen ist, daß daraus die Richtigkeit von $A(n+1)$ folgt. Es ergibt sich

$$\begin{aligned} \sum_{i=1}^{n+1} i^2 &= \sum_{i=1}^n i^2 + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= (n+1) \frac{n(2n+1) + 6(n+1)}{6} \\ &= \frac{n+1}{6} (2n^2 + 7n + 6). \end{aligned}$$

Andererseits ist

$$\begin{aligned} \frac{(n+1)(n+2)(2(n+1)+1)}{6} &= \frac{n+1}{6} (n+2)(2n+3) \\ &= \frac{n+1}{6} (2n^2 + 7n + 6). \end{aligned}$$

Also folgt aus der Richtigkeit von $A(n)$ stets die Richtigkeit von $A(n+1)$. Der Satz ist damit bewiesen. ■

b) Für $n \in \mathbb{N}$ gilt

$$n^2 + n \text{ ist eine gerade Zahl.} \quad (1.5)$$

Beweis.

Induktionsanfang: Für $n = 1$ ist $1^2 + 1 = 2$ eine gerade Zahl.

Induktionsschritt: Für $n \in \mathbb{N}$ sei $n^2 + n$ eine gerade Zahl. Dann gilt

$$(n+1)^2 + (n+1) = n^2 + n + 2(n+1).$$

$n^2 + n$ ist nach Induktionsvoraussetzung eine gerade Zahl und $2(n+1)$ ist offenbar auch eine gerade Zahl. Da eine Summe gerader Zahlen gerade ist, muß $(n+1)^2 + (n+1)$ ebenfalls gerade sein. ■

(Beweis ohne vollständige Induktion: Für $n \in \mathbb{N}$ ist $n^2 + n = n(n + 1)$. Da entweder n oder $n + 1$ eine gerade Zahl ist, muß $n^2 + n$ gerade sein.)

c) Für $x \in \mathbb{R}$ mit $x \geq -1$ und $n \in \mathbb{N}$ gilt

$$(1 + x)^n \geq 1 + nx. \quad (1.6)$$

Beweis.

Induktionsanfang: Für $n = 1$ gilt

$$(1 + x)^1 \geq 1 + 1 \cdot x$$

für $x \geq -1$.

Induktionsschritt: Für $n \in \mathbb{N}$ und $x \geq -1$ gelte (1.6). Dann gilt

$$\begin{aligned} (1 + x)^{n+1} &= (1 + x)^n(1 + x) \\ &\geq (1 + nx)(1 + x) \\ &= 1 + (n + 1)x + nx^2 \\ &\geq 1 + (n + 1)x, \end{aligned}$$

da $(1 + x) \geq 0$ für $x \geq -1$ und $nx^2 \geq 0$. ■

d) Für $n \in \mathbb{N}$ mit $n > 4$ gilt

$$2^n > n^2. \quad (1.7)$$

Beweis.

Induktionsanfang: Für $n = 5$ ist $2^5 = 32$ und $5^2 = 25$, also $2^5 > 5^2$.

Induktionsschritt: Für $n \in \mathbb{N}$ mit $n > 4$ gelte

$$2^n > n^2.$$

Dann ergibt sich

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &> 2 \cdot n^2 = n^2 + n \cdot n \\ &> n^2 + 4 \cdot n = n^2 + 2n + 2n \\ &> n^2 + 2n + 1 \\ &= (n + 1)^2. \end{aligned}$$
■

e) Für $n \in \mathbb{N}$ gilt

$$\sum_{i=1}^n \frac{1}{i(i+1)} = 1 - \frac{1}{n+1}. \quad (1.8)$$

Beweis.

Induktionsanfang: Für $n = 1$ ist $\frac{1}{1(1+1)} = 1/2$ und $1 - \frac{1}{1+1} = 1/2$.

Induktionsschritt: Für $n \in \mathbb{N}$ gelte

$$\sum_{i=1}^n \frac{1}{i(i+1)} = 1 - \frac{1}{n+1}.$$

Daraus folgt

$$\begin{aligned} \sum_{i=1}^{n+1} \frac{1}{i(i+1)} &= \sum_{i=1}^n \frac{1}{i(i+1)} + \frac{1}{(n+1)(n+2)} \\ &= 1 - \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} \\ &= 1 - \frac{n+2-1}{(n+1)(n+2)} \\ &= 1 - \frac{1}{n+2}. \end{aligned}$$

■

f) Ein Beispiel mit Bezug zum Kunstunterricht.

Wird ein Blatt Papier durch Geraden in Flächen unterteilt, so reichen immer zwei Farben zum Färben aus der Flächen aus, so dass zwei benachbarte Flächen verschiedene Farben haben.

Beweis durch Induktion nach Anzahl der Geraden

Induktionsanfang: Eine Gerade teilt ein Viereck in zwei Flächen, also kommt man mit zwei Farben aus, z.B. Schwarz und Weiss.

Induktionsschritt: Sei das Blatt durch n Geraden in Flächen unterteilt und mit 2 Farben eingefärbt. Wir zeichnen eine weitere Gerade ein. Diese Gerade teilt das Blatt wieder insgesamt in zwei Flächen A_1 und A_2 , wobei die Flächen entlang der Geraden jetzt die „falschen“ Farben haben, jede Fläche A_1 oder A_2 für sich genommen aber richtig eingefärbt ist. Wir gehen deshalb in A_1 in allen Flächen zur jeweils anderen Farbe über und erhalten damit wieder ein korrekt eingefärbtes Blatt.

Bemerkungen

a) Auf den Induktionsanfang kann nicht verzichtet werden, oder mit anderen Worten: Aus „ $A(n)$ wahr $\implies A(n+1)$ wahr“ für $n \in \mathbb{N}$ folgt noch lange nicht „ $A(n)$ wahr für $n \in \mathbb{N}$ “.

Behauptung: Für alle $n \in \mathbb{N}$ gilt $3 + 3^2 + 3^3 + \dots + 3^n = \frac{3}{2}3^n$.

Induktionsschritt: Für $n \in \mathbb{N}$ gelte $3 + 3^2 + 3^3 + \dots + 3^n = \frac{3}{2}3^n$. Daraus folgt für $n+1$

$$3 + 3^2 + 3^3 + \dots + 3^n + 3^{n+1} = \frac{3}{2}3^n + 3^{n+1} = \frac{3}{2}3^{n+1}.$$

Damit ist allerdings die Behauptung noch nicht für alle $n \in \mathbb{N}$ bewiesen. Tatsächlich ist diese sogar für alle $n \in \mathbb{N}$ offensichtlich falsch, da $3 + 3^2 + 3^3 + \dots + 3^n \in \mathbb{N}$ und $\frac{3}{2}3^n \notin \mathbb{N}$

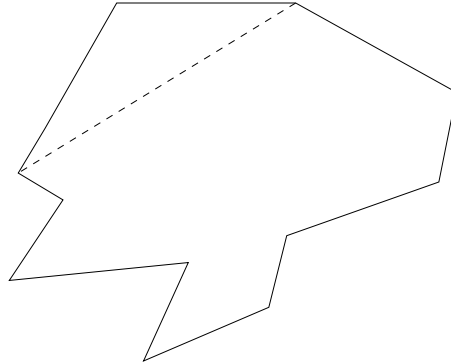
für alle $n \in \mathbb{N}$ gilt. $n = 1$ liefert z.B. $3 \neq \frac{9}{2}$.

b) Ein weiteres Beispiel für eine Induktion, die nicht bei $n = 1$ anfängt, liefert die

Behauptung: In jedem n -Eck ($n \geq 3$) beträgt die Summe der Innenwinkel $(n - 2) \cdot 180^\circ$.

Induktionsanfang: Für $n = 3$ ist die Aussage klar, da die Summe der Winkel in jedem Dreieck bekanntermaßen 180° beträgt.

Induktionsschritt: Die Summe der Innenwinkel in einem n -Eck betrage $(n - 2) \cdot 180^\circ$. Daraus folgt für ein $n + 1$ -Eck durch Ergänzen einer Verbindungslinie



für die Summe der Innenwinkel $(n - 2) \cdot 180^\circ + 180^\circ = ((n + 1) - 2) \cdot 180^\circ$.

2 Zahlbereichserweiterungen I

Obwohl wir in den vergangenen Kapiteln schon andere Zahlen als die natürlichen Zahlen benutzt haben, wollen wir auch auf diese noch einmal einen grundsätzlichen Blick werfen. Es sind dies die

- ganzen Zahlen \mathbb{Z} ,
- rationalen Zahlen \mathbb{Q} ,
- die reellen Zahlen \mathbb{R} ,
- die komplexen Zahlen \mathbb{C} .

Alle diese Zahlen wollen wir unter den folgenden Aspekten betrachten:

1. Warum braucht man sie?
2. Wie konstruiert man sie?
3. Gibt es gemeinsame Strukturen? Was sind die Unterschiede?

In diesem Abschnitt soll es zunächst um die beiden ersten Fragen gehen. Bei negativen Zahlen und Brüchen gibt es ganz anschauliche Gründe für deren Notwendigkeit. Wie rechnet man mit Schulden, wie teilt man Torten? Mathematisch betrachtet heißt das: Wie löse ich bei gegebenem $a, b \in \mathbb{N}$ die Gleichungen

$$a + x = b, \quad a \cdot x = b?$$

Wir wissen bereits: Sind $a, x, b \in \mathbb{N}$, so folgt $a + x \in \mathbb{N}$, $a \cdot x \in \mathbb{N}$, also gibt es gewisse Kombinationen von Elementen $a, b \in \mathbb{N}$, für die Lösungen der Gleichungen existieren. Wir haben auch schon gesehen: Ist x eine Lösung von $a + x = b$, so ist x eindeutig bestimmt (Streichungsregel der Addition: Satz 8.9), genauso folgt mit der Streichungsregel der Multiplikation (Satz 8.12) die Eindeutigkeit der Lösung von $a \cdot x = b$. Dass es nicht immer eine Lösung gibt, ist klar, wenn man z.B. die Gleichungen $9 + x = 3$ und $9 \cdot x = 3$ betrachtet. Auch wenn wir die negativen Zahlen aus unserem Kopf verbannen, können wir mit unseren schon bekannten Sätze bei der Gleichung $9 + x = 3$ wie folgt argumentieren: Aus den Gesetzen für die Kleinerbeziehung in Abschnitt 8 folgt: Für jedes $x \in \mathbb{N}$ ist $9 + x > 9$ (8.14 iii angewandt auf $m = 0$, $n = x$ und $p = 9$), aber wir wissen: $3 < 9$, daher kann es ein solches x nicht geben. Ähnlich verfährt man bei der Gleichung $a \cdot x = b$. Offensichtlich ist reichen die natürlichen Zahlen hierfür nicht aus, die Erweiterung der Zahlen in der Form, dass beide Gleichungen lösbar sind, führt auf die ganzen und die rationalen Zahlen.

Die Konstruktion wird in beiden Fällen genauso durchgeführt wie bei den natürlichen Zahlen: Mittels einer Äquivalenzrelation auf einer geeigneten Grundmenge, die Zahlen werden dann durch Äquivalenzklassen repräsentiert.

Wir erinnern uns: Bei natürlichen Zahlen war die Grundmenge die Menge aller endlichen Mengen, die Äquivalenzrelation war die Gleichmächtigkeit von Mengen. Schließlich

repräsentieren alle Mengen, die gleichmächtig sind zur Menge meiner Finger an der rechten Hand, die Zahl 5 etc., d.h. wir haben den Äquivalenzklassen eigene Namen gegeben.

Jetzt haben wir $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ schon zur Verfügung und können damit weiter arbeiten.

2.1 Die Konstruktion der negativen Zahlen

Wir erinnern uns an die Definition der Addition auf \mathbb{N} : Hierfür haben wir Vereinigungen von Mengen betrachtet. Damit folgt: Die Gleichung $a + x = b$ ist lösbar in \mathbb{N}_0 , wenn $a \leq b$ gilt. Man muss hierzu aus einer Menge, die b repräsentiert, nur a Elemente wegnehmen und erhält eine Menge mit x Elementen. Oder: Wenn man von einer Menge der Mächtigkeit 9 zu einer Menge der Mächtigkeit 3 kommen will, muss man ja nur 6 Elemente wieder wegnehmen, sozusagen die Subtraktion als eigenständige Aktion einführen. Diese anschauliche Vorstellung kommt aber auch schnell an ihre Grenzen – selbst im täglichen Leben – sie erklärt z.B. nicht, wie man 763 Euro ausgeben kann, obwohl man nur 200 auf dem Konto hat.

Hier hilft eine andere Anschauung eher weiter:

Die Darstellung auf dem Zahlenstrahl, (man mache sich klar, dass das einen anderen Aspekt von Zahlen wiedergibt als die Kardinalität endlicher Mengen!) $3 + 6 \leftrightarrow$ starte bei 3 und gehe auf dem Strahl 6 Einheiten nach rechts. Die Umkehrung dieser Operation: Gehe 6 Einheiten nach links. Wenn man eine Fortsetzung des Strahls nach links über die 0 zulässt, kann man beliebige Einheiten nach links gehen.

Weiter stellen wir fest: $6 \rightarrow 0$, $7 \rightarrow 1$, $10 \rightarrow 4 \dots$ bedeutet immer dieselbe Operation: 6 Einheiten nach links gehen. Sammeln wir alle Zahlenpaare, die durch diese Operation miteinander verbunden sind, so können wir das so beschreiben: $\{(x_1, x_2) | x_2 - x_1 = -6\}$.

Hiervon ausgehend können wir die negativen Zahlen als Äquivalenzklassen von Zahlenpaaren konstruieren.

Wir betrachten als Grundmenge $\mathbb{N}_0 \times \mathbb{N}_0 = \{(x_1, x_2) : x_1, x_2 \in \mathbb{N}\}$. Zwei Paare (x_1, x_2) , (y_1, y_2) sollen äquivalent sein, wenn auf dem Zahlenstrahl die gleiche Operation von x_1 zu x_2 und von y_1 zu y_2 führt, dh. wenn $x_2 - x_1 = y_2 - y_1$ gilt. Das Zeichen \sim und negative Zahlen verbannen wir aber jetzt.

Lemma 2.1 Auf $\mathbb{N}_0 \times \mathbb{N}_0$ sei folgende Relation gegeben:

$$(x_1, x_2) \sim (y_1, y_2) \text{ genau dann, wenn } x_2 + y_1 = x_1 + y_2. \quad (2.9)$$

Dies definiert eine Äquivalenzrelation auf $\mathbb{N}_0 \times \mathbb{N}_0$.

Beweis: Reflexivität: $(x_1, x_2) \sim (x_1, x_2)$, denn $x_1 + x_2 = x_1 + x_2$.

Symmetrie: Es gelte $(x_1, x_2) \sim (y_1, y_2) \implies x_2 + y_1 = x_1 + y_2$. \implies mit Satz 8.8 (i) (Kommutativgesetz der Addition) und Kommutativität des $=$ Zeichens: $y_2 + x_1 = y_1 + x_2$, d.h. $(y_1, y_2) \sim (x_1, x_2)$.

Transitivität: Es gelte $(x_1, x_2) \sim (y_1, y_2)$ und $(y_1, y_2) \sim (z_1, z_2) \implies$

$x_2 + y_1 = x_1 + y_2$ und $y_2 + z_1 = y_1 + z_2 \implies x_2 + y_1 + y_2 + z_1 = x_1 + y_2 + y_1 + z_2 \implies$
mit dem Kommutativgesetz der Addition und der Streichungsregel: $x_2 + z_1 = x_1 + z_2$,
somit gilt $(x_1, x_2) \sim (z_1, z_2)$. ■

Definition 2.2 Die Äquivalenzklassen bezüglich der in 2.1 eingeführten Äquivalenzrelation nennen wir **ganze Zahlen**. Bezeichnung für die Menge der ganzen Zahlen: \mathbb{Z} .

Wie definieren weiter eine Operation „+“ auf \mathbb{Z} durch

$$[(x_1, x_2)] + [(y_1, y_2)] = [(x_1 + y_1, x_2 + y_2)] \quad (2.10)$$

Bemerkung 2.3 Die Addition ist wohldefiniert, d.h. unabhängig von der Wahl der Repräsentanten. Ist nämlich $(x'_1, x'_2) \in [(x_1, x_2)]$ und $(y'_1, y'_2) \in [(y_1, y_2)]$, so folgt

$$x'_1 + x_2 = x'_2 + x_1, \quad y'_1 + y_2 = y'_2 + y_1 \quad \Rightarrow \quad [(x'_1 + y'_1, x'_2 + y'_2)] = [(x_1 + y_1, x_2 + y_2)].$$

Das ist jetzt eine mathematisch saubere, aber leider nicht sehr anschauliche Konstruktion. Wie finden wir aber jetzt die uns vertrauten Zahlen und die uns vertraute Addition wieder? Dazu zuerst einige Beispiele:

$[(0, 0)] = \{(m, m) | m \in \mathbb{N}_0\}$: denn $(x_1, x_2) \sim (0, 0) \Leftrightarrow x_1 + 0 = x_2 + 0 \Leftrightarrow x_1 = x_2$ (Streichungsregel).

$[(3, 9)]$: $(4, 10), (0, 6) \in [(3, 9)]$, denn $4 + 9 = 10 + 3$ und $0 + 9 = 6 + 3$.

Es folgt aber mit dem gleichen Argument: $(10, 4), (6, 0) \in [(9, 3)]$. ABER: $(9, 3) \notin [(3, 9)]$, die Paare $(9, 3)$ und $(3, 9)$ repräsentieren verschiedene ganze Zahlen.

Allgemein können wir uns folgendes überlegen:

Lemma 2.4 1. $(x_1, x_2) \sim (x_2, x_1) \Leftrightarrow (x_1, x_2) \in [(0, 0)]$.

2. Für alle $m \in \mathbb{N}_0$ gilt: $[(0, m)] = \{(x_1, x_1 + m) | x_1 \in \mathbb{N}_0\}$,
 $[(m, 0)] = \{(x_1, x_1 + m) | x_1 \in \mathbb{N}_0\}$

3. $[(x_1, x_2)] + [(x_2, x_1)] = [(0, 0)]$.

4. Die Addition ist assoziativ.

5. Die Addition ist kommutativ.

6. $\mathbb{N}_0 \times \mathbb{N}_0 = [(0, 0)] \cup [(0, 1)] \cup [(0, 2)] \cup \dots \cup [(1, 0)] \cup [(2, 0)] \cup \dots$

Beweis

1. Gilt $(x_1, x_2) \sim (x_2, x_1) \Rightarrow x_1 + x_1 = 2x_1 = x_2 + x_2 = 2x_2 \Rightarrow$ mit der Streichungsregel der Multiplikation: $x_1 = x_2$.

2. folgt unmittelbar aus der Definition.

3. Folgt aus der Definition von + und $[(0, 0)] = \{(m, m) | m \in \mathbb{N}_0\}$.

4. Folgt ebenfalls aus der Definition von + und der Assoziativität der Addition auf \mathbb{N}_0 .

5. Folgt ebenfalls aus der Definition von + und der Kommutativität der Addition auf \mathbb{N}_0 .

6. Hier ist eine Mengengleichheit zu zeigen, also zwei Inklusionen. „ \supset “ ist elementar. „ \subset “ Ist $(x_1, x_2) \in \mathbb{N}_0 \times \mathbb{N}_0$, so gilt mit dem Trichotomiegesetz:
 Entweder $x_1 = x_2 \implies (x_1, x_2) \in [(0, 0)]$
 oder $x_1 < x_2$, dann findet man wie oben ein $m \in \mathbb{N}$ mit $x_1 + m = x_2$, $\implies (x_1, x_2) \in [(0, m)]$ nach 2.,
 oder $x_2 < x_1$, dann findet man wie oben ein $m \in \mathbb{N}$ mit $x_2 + m = x_1$, $\implies (x_1, x_2) \in [(m, 0)]$ ebenfalls nach 2.

■

Bezeichnung: Wir können also $m \in \mathbb{N}_0$ mit der Äquivalenzklasse $[(0, m)]$ identifizieren: die Abbildung $h : \mathbb{N}_0 \rightarrow \mathbb{Z}, m \mapsto [(0, m)]$ ist injektiv, und es gilt:

$$h(m + n) = [(0, m + n)] = [(0, m)] + [(0, n)] = h(m) + h(n)$$

in diesem Sinne sagen wir: $\mathbb{N}_0 \subset \mathbb{Z}$.

Ist $[(x_1, x_2)] \in \mathbb{Z}$, so setzen wir $[(x_2, x_1)] =: -[(x_1, x_2)]$. D.h. identifizieren wir für $m \in \mathbb{N}_0$ $m = [(0, m)]$, so erhalten wir: $[(m, 0)] := -m$.

Dann finden wir in Lemma 2.4 die uns vertrauten Regeln wieder.

Folgerung 2.5 1. $m = -m \Leftrightarrow m = 0$,

2. **(A1)** $m + 0 = m$ für alle $m \in \mathbb{Z}$, (Existenz eines neutralen Elementes bez +)

3. **(A2)** $m + (-m) = 0$ für alle $m \in \mathbb{Z}$, (Existenz eines inversen Elementes bez +)

4. **(A3)** $(l + m) + n = l + (m + n)$ für alle $l, m, n \in \mathbb{Z}$. (Assoziativität der Addition)

5. **(A4)** $m + n = n + m$ für alle $m, n \in \mathbb{Z}$. (Kommutativität der Addition)

6. $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}$.

Weiter gilt noch: $-(-m) = m$ für alle $m \in \mathbb{Z}$. (Nach Definition: Ist $m = [(x_1, x_2)]$, wobei $x_2 - x_1 = m$, so ist $-m = [(x_2, x_1)]$ und $-(-m) = [(x_1, x_2)]$.)

Satz 2.6 Die Gleichung $a + x = b$ ist für alle $a, b \in \mathbb{Z}$ eindeutig lösbar.

Beweis: Es gibt eine Lösung: $x = b + (-a)$, denn

$$a + x = a + (b + (-a)) \underset{(A4)}{=} a + ((-a) + b) \underset{(A3)}{=} (a + (-a)) + b \underset{(A2)}{=} 0 + b = b$$

Die Eindeutigkeit (wissen wir bisher nur in \mathbb{N} !):

Sind $x, y \in \mathbb{Z}$ mit $a + y = b \implies a + x = a + y \implies (-a) + (a + x) = (-a) + (a + y) \implies$ mit (A3), (A4), (A1) und (A2): $((-a) + a) + x = (a + (-a)) + x = 0 + x = x = ((-a) + a) + y = (a + (-a)) + y = 0 + y = y$, also $x = y$. ■

Wir setzen auch die Multiplikation von \mathbb{N}_0 auf \mathbb{Z} fort:

$$[(x_1, x_2)] \cdot [(y_1, y_2)] := [(x_1 y_2 + x_2 y_1, x_1 y_1 + x_2 y_2)], \quad (2.11)$$

(Das dies die richtige Formel ist, sieht man, wenn die Identifizierung $[(x_1, x_2)] = x_2 - x_1$, $[(y_1, y_2)] = y_2 - y_1$ benutzt). Auch hier zeigt eine elementare Rechnung, dass das Produkt unabhängig von den Repräsentaten der Äquivalenzklassen ist. Benutzen wir die „kanonischen“ aus Lemma 2.4 6., so sehen wir für $m, n \in \mathbb{N}$ mit $m = [(0, m)]$, $n = [(0, n)]$:

$$\begin{aligned} m \cdot n &= [(0, m)] \cdot [(0, n)] = [(0, m \cdot n)], \\ (-m) \cdot n &= [(m, 0)] \cdot [(0, n)] = [(m \cdot n, 0)], \\ -m \cdot (-n) &= [(m, 0)] \cdot [(n, 0)] = [(0, m \cdot n)] = m \cdot n, \\ 1 \cdot n &= [(0, 1)] \cdot [(0, n)] = [(0, n)] = n, \\ (-1) \cdot n &= [(1, 0)] \cdot [(0, n)] = [(n, 0)] = -n. \end{aligned}$$

Weiter gilt auch für $m, n \in \mathbb{Z}$, und

$$l \in \mathbb{Z} \setminus \{0\} := \mathbb{Z}^*$$

die Kürzungsregel:

$$m \cdot l = n \cdot l \Rightarrow m = n.$$

In der Tat: Ist $m = [(m_1, m_2)]$, $n = [(n_1, n_2)]$, und $l \in \mathbb{N}$, d.h. $l = [(0, l)]$, und gilt:

$$[(m_1 \cdot l, m_2 \cdot l)] = [(n_1 \cdot l, n_2 \cdot l)],$$

$\Rightarrow m_1 \cdot l = n_1 \cdot l + b$, $m_2 \cdot l = n_2 \cdot l + b \Rightarrow m_1 \cdot l + n_2 \cdot l + b = n_1 \cdot l + b + m_2 \cdot l$
 $\Rightarrow (m_1 + n_2) \cdot l = (n_1 + m_2) \cdot l$, und damit $(m_1, m_2) \sim (n_1, n_2)$, also $m = n$. Genauso argumentiert man, wenn $l = [(l, 0)] \in -\mathbb{N}$ ist.

Insbesondere folgt hieraus auch

$$m \cdot n = 0 \quad \Leftrightarrow \quad m = 0 \text{ oder/und } n = 0. \quad (2.12)$$

In der Tat: Eine Richtung ist schon ok, sei also $m \cdot n = 0$. Ist $m \neq 0$, so gilt: $0 = m \cdot n = m \cdot 0$, also folgt mit der Kürzungsregel $n = 0$. Analog: Ist $n \neq 0$, so ist $m = 0$.

Ebenso kann man Hilfe der Definitionen das Distributivgesetz nachrechnen:

$$l \cdot (m + n) = l \cdot n + l \cdot n \quad (D)$$

Im folgenden benutzen wir wieder abkürzend:

$$m + (-n) =: m - n.$$

Definition 2.7 Seien $m, n \in \mathbb{Z}$. Dann definieren wir:

1. Wir setzen $|m| := m$, falls $m \in \mathbb{N}_0$, und $|m| := -m$, falls $-m \in \mathbb{N}$.
2. Wir sagen: $m|n \Leftrightarrow \text{ex. } z \in \mathbb{Z} \text{ mit } z \cdot m = n$.
3. Für ganze Zahlen $m, n \in \mathbb{Z}^*$ definieren wir den $\text{ggT}(m, n)$ durch $\text{ggT}(m, n) = \text{ggT}(|m|, |n|)$.

2.2 Konstruktion der rationalen Zahlen

Wie wir in Satz 2.6 gesehen haben, kann man die Gleichung $a + x = b$ in \mathbb{Z} jetzt immer lösen, allerdings die Gleichung $a \cdot x = b$ im allgemeinen immer noch nicht. Wir konstruieren daher durch eine analoge Konstruktion wie bei \mathbb{Z} eine weitere Menge von Zahlen, die Bruchzahlen oder rationalen Zahlen. Dazu setzen wir $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ und wir definieren auf $\mathbb{Z} \times \mathbb{Z}^*$ eine passende Äquivalenzrelation.

Lemma 2.8 *Die Relation*

$$(x_1, x_2) \sim (y_1, y_2) \iff x_1 \cdot y_2 = y_1 \cdot x_2 \quad (2.13)$$

definiert auf $\mathbb{Z} \times \mathbb{Z}^*$ eine Äquivalenzrelation.

Beweis: Reflexivität: $(x_1, x_2) \sim (x_1, x_2)$, denn $x_1 \cdot x_2 = x_1 \cdot x_2$.

Symmetrie: Es gelte $(x_1, x_2) \sim (y_1, y_2) \implies x_1 \cdot y_2 = y_1 \cdot x_2 \implies y_1 \cdot x_2 = x_1 \cdot y_2$, d.h. $(y_1, y_2) \sim (x_1, x_2)$.

Transitivität: Es gelte $(x_1, x_2) \sim (y_1, y_2)$ und $(y_1, y_2) \sim (z_1, z_2) \implies$

$$x_1 \cdot y_2 = y_1 \cdot x_2 \text{ und } y_1 \cdot z_2 = z_1 \cdot y_2 \implies (x_1 \cdot y_2) \cdot (y_1 \cdot z_2) = (y_1 \cdot x_2) \cdot (z_1 \cdot y_2) \implies$$

falls $y_1 \neq 0$: mit dem Kommutativgesetz und Assoziativgesetz der Multiplikation in \mathbb{Z} und der Kürzungsregel: $x_1 \cdot z_2 = z_1 \cdot x_2$, somit gilt $(x_1, x_2) \sim (z_1, z_2)$.

Falls $y_1 = 0$, musste auch schon $x_1 = 0 = z_1$ gelten. ■

Wie sehen jetzt die Äquivalenzklassen aus?

Klar ist: Die 0 spielt eine Sonderrolle: $[(0, x_2)] = [(0, 1)]$ für alle $x_2 \in \mathbb{Z}$, $x_2 \neq 0$.

Auf $\mathbb{Z}^* \times \mathbb{Z}^*$ gilt mit $l \in \mathbb{Z}^*$: Ist $x'_1 = l \cdot x_1$, $x'_2 = l \cdot x_2$, dann gilt: $(x_1, x_2) \sim (x'_1, x'_2)$.

„Man darf mit Zahlen $\neq 0$ erweitern und erhält denselben Bruch.“

Andersherum gelesen heißt das aber auch:

„Man darf gemeinsame Teiler weglassen und erhält denselben Bruch“.

Für jedes Paar $(x_1, x_2) \in \mathbb{N} \times \mathbb{N}$ gilt also $(x_1, x_2) \in [(p, q)]$ mit $x_1 = p \cdot \text{ggT}(x_1, x_2)$, $x_2 = q \cdot \text{ggT}(x_1, x_2)$, (p und q sind dann teilerfremd!).

Weiter folgt aus dem Satz 12.5 über die eindeutige Primzahlzerlegung: Sind $(p, q) \in \mathbb{N} \times \mathbb{N}$ und $(p', q') \in \mathbb{N} \times \mathbb{N}$ jeweils teilerfremde Paare, so gilt

$$(p, q) \sim (p', q') \iff p = p' \text{ und } q = q'.$$

Definition 2.9 Die Äquivalenzklassen bezüglich der in 2.1 eingeführten Äquivalenzrelation nennen wir **rationale Zahlen**. Bez: \mathbb{Q} .

Wie definieren die **Addition** auf \mathbb{Q} durch

$$[(x_1, x_2)] + [(y_1, y_2)] = [(x_1 \cdot y_2 + y_1 \cdot x_2, x_2 \cdot y_2)]. \quad (2.14)$$

und die **Multiplikation** auf \mathbb{Q}_+ durch

$$[(x_1, x_2)] \cdot [(y_1, y_2)] = [(x_1 \cdot y_1, x_2 \cdot y_2)]. \quad (2.15)$$

Wie immer, müssen wir uns davon überzeugen, dass diese Definitionen mathematisch sinnvoll sind:

2.2 Konstruktion der rationalen Zahlen

Wie wir in Satz 2.6 gesehen haben, kann man die Gleichung $a + x = b$ in \mathbb{Z} jetzt immer lösen, allerdings die Gleichung $a \cdot x = b$ im allgemeinen immer noch nicht. Wir konstruieren daher durch eine analoge Konstruktion wie bei \mathbb{Z} eine weitere Menge von Zahlen, die Bruchzahlen oder rationalen Zahlen. Dazu setzen wir $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ und wir definieren auf $\mathbb{Z} \times \mathbb{Z}^*$ eine passende Äquivalenzrelation.

Lemma 2.8 *Die Relation*

$$(x_1, x_2) \sim (y_1, y_2) \iff x_1 \cdot y_2 = y_1 \cdot x_2 \quad (2.13)$$

definiert auf $\mathbb{Z} \times \mathbb{Z}^*$ eine Äquivalenzrelation.

Beweis: Reflexivität: $(x_1, x_2) \sim (x_1, x_2)$, denn $x_1 \cdot x_2 = x_1 \cdot x_2$.

Symmetrie: Es gelte $(x_1, x_2) \sim (y_1, y_2) \implies x_1 \cdot y_2 = y_1 \cdot x_2 \implies y_1 \cdot x_2 = x_1 \cdot y_2$, d.h. $(y_1, y_2) \sim (x_1, x_2)$.

Transitivität: Es gelte $(x_1, x_2) \sim (y_1, y_2)$ und $(y_1, y_2) \sim (z_1, z_2) \implies$

$$x_1 \cdot y_2 = y_1 \cdot x_2 \text{ und } y_1 \cdot z_2 = z_1 \cdot y_2 \implies (x_1 \cdot y_2) \cdot (y_1 \cdot z_2) = (y_1 \cdot x_2) \cdot (z_1 \cdot y_2) \implies$$

falls $y_1 \neq 0$: mit dem Kommutativgesetz und Assoziativgesetz der Multiplikation in \mathbb{Z} und der Kürzungsregel: $x_1 \cdot z_2 = z_1 \cdot x_2$, somit gilt $(x_1, x_2) \sim (z_1, z_2)$.

Falls $y_1 = 0$, musste auch schon $x_1 = 0 = z_1$ gelten. ■

Wie sehen jetzt die Äquivalenzklassen aus?

Klar ist: Die 0 spielt eine Sonderrolle: $[(0, x_2)] = [(0, 1)]$ für alle $x_2 \in \mathbb{Z}$, $x_2 \neq 0$.

Auf $\mathbb{Z}^* \times \mathbb{Z}^*$ gilt mit $l \in \mathbb{Z}^*$: Ist $x'_1 = l \cdot x_1$, $x'_2 = l \cdot x_2$, dann gilt: $(x_1, x_2) \sim (x'_1, x'_2)$.

„Man darf mit Zahlen $\neq 0$ erweitern und erhält denselben Bruch.“

Andersherum gelesen heißt das aber auch:

„Man darf gemeinsame Teiler weglassen und erhält denselben Bruch“.

Für jedes Paar $(x_1, x_2) \in \mathbb{N} \times \mathbb{N}$ gilt also $(x_1, x_2) \in [(p, q)]$ mit $x_1 = p \cdot \text{ggT}(x_1, x_2)$, $x_2 = q \cdot \text{ggT}(x_1, x_2)$, (p und q sind dann teilerfremd!).

Weiter folgt aus dem Satz 12.5 über die eindeutige Primzahlzerlegung: Sind $(p, q) \in \mathbb{N} \times \mathbb{N}$ und $(p', q') \in \mathbb{N} \times \mathbb{N}$ jeweils teilerfremde Paare, so gilt

$$(p, q) \sim (p', q') \iff p = p' \text{ und } q = q'.$$

Definition 2.9 Die Äquivalenzklassen bezüglich der in 2.1 eingeführten Äquivalenzrelation nennen wir **rationale Zahlen**. Bez: \mathbb{Q} .

Wie definieren die **Addition** auf \mathbb{Q} durch

$$[(x_1, x_2)] + [(y_1, y_2)] = [(x_1 \cdot y_2 + y_1 \cdot x_2, x_2 \cdot y_2)]. \quad (2.14)$$

und die **Multiplikation** auf \mathbb{Q}_+ durch

$$[(x_1, x_2)] \cdot [(y_1, y_2)] = [(x_1 \cdot y_1, x_2 \cdot y_2)]. \quad (2.15)$$

Wie immer, müssen wir uns davon überzeugen, dass diese Definitionen mathematisch sinnvoll sind:

Lemma 2.10 Die Operationen „+“ und „·“ sind wohldefiniert, d.h. unabhängig von der Wahl der Repräsentanten.

Beweis

Für die Addition: Seien $(x'_1, x'_2) \in [(x_1, x_2)]$, $(y'_1, y'_2) \in [(y_1, y_2)]$, dann gilt $x_1 \cdot x'_2 = x'_1 \cdot x_2$, $y_1 \cdot y'_2 = y'_1 \cdot y_2$ und es ist zu zeigen, dass hieraus folgt

$$\begin{aligned} (x_1 \cdot y_2 + y_1 \cdot x_2, x_2 \cdot y_2) &\sim (x'_1 \cdot y'_2 + y'_1 \cdot x'_2, x'_2 \cdot y'_2), \text{ also} \\ (x_1 \cdot y_2 + y_1 \cdot x_2) \cdot (x'_2 \cdot y'_2) &= (x'_1 \cdot y'_2 + y'_1 \cdot x'_2) \cdot (x_2 \cdot y_2). \end{aligned}$$

Die Rechenregeln für die Addition und die Multiplikation in \mathbb{Z} liefern:

$$\begin{aligned} (x_1 \cdot y_2 + y_1 \cdot x_2) \cdot (x'_2 \cdot y'_2) &= x_1 \cdot y_2 \cdot x'_2 \cdot y'_2 + y_1 \cdot x_2 \cdot x'_2 \cdot y'_2 = \\ x_1 \cdot x'_2 \cdot y_2 \cdot y'_2 + y_1 \cdot y'_2 \cdot x_2 \cdot x'_2 &= x'_1 \cdot x_2 \cdot y_2 \cdot y'_2 + y'_1 \cdot y_2 \cdot x_2 \cdot x'_2 = \\ x'_1 \cdot y'_2 \cdot x_2 \cdot y_2 + y'_1 \cdot x'_2 \cdot y_2 \cdot x_2 &= (x'_1 \cdot y'_2 + y'_1 \cdot x'_2) \cdot (x_2 \cdot y_2). \end{aligned}$$

Beweis für die Multiplikation: **Übungsaufgabe!** ■

Beispiel: $[(4, 3)] + [(9, 12)] = [(4 \cdot 12 + 3 \cdot 9, 3 \cdot 12)] = [(75, 36)]$
 $[(8, 6)] + [(3, 4)] = [(4 \cdot 8 + 6 \cdot 3, 6 \cdot 4)] = [(50, 24)]$, weiter: $(75, 36) \sim (50, 24)$, da $50 \cdot 36 = 1800 = 75 \cdot 24$. Benutzung der teilerfremden Darstellung: $[(4, 3)] + [(3, 4)] = [(4 \cdot 4 + 3 \cdot 3, 3 \cdot 4)] = [(25, 12)]$, und man sieht auch leicht: $(75, 36) \sim (25, 12) \sim (50, 24)$.

An diesem Beispiel erkennt man noch etwas: Die Äquivalenzrelation aus Lemma 2.10 ist die „Richtige“!

Man würde nicht mit der Vorstellung auskommen: Zwei „Brüche“ sollen äquivalent sein, wenn sie durch „Erweitern oder Kürzen“ mit ganzen Zahlen ineinander umrechnen kann.

Lemma 2.11 Es gelten folgende Rechengesetze für die Addition und die Multiplikation auf \mathbb{Q} :

1. „Es gibt eine 0“:

$$[(x_1, x_2)] + [(0, 1)] = [(x_1, x_2)] \tag{A1}$$

2. „Zu jeder Zahl a gibt es -a“:

$$[(x_1, x_2)] + [(-x_1, x_2)] = [(0, 1)] \tag{A2}$$

3. Es gibt eine „1“:

$$[(x_1, x_2)] \cdot [(m, m)] = [(x_1, x_2)] \cdot [(1, 1)] = [(x_1, x_2)] \tag{M1}$$

4. „Zu jeder Zahl a ≠ 0 gibt es 1/a“: Ist $x_1 \neq 0$

$$[(x_1, x_2)] \cdot [(x_2, x_1)] = [(m, m)] = [(1, 1)] \tag{M2}$$

5. Für beide Operationen gilt das Assoziativgesetz. (A3), (M3)

6. Addition und Multiplikation sind kommutativ. (A4), (M4)

7. Es gilt das Distributivgesetz:

$$[(x_1, x_2)] \cdot ([(y_1, y_2)] + [(z_1, z_2)]) = [(x_1, x_2)] \cdot [(y_1, y_2)] + [(x_1, x_2)] \cdot [(z_1, z_2)] \tag{D}$$

$$8. [(x_1, x_2)] \cdot [(y_1, y_2)] = [(0, 1)] \Leftrightarrow x_1 = 0 \text{ und/oder } y_1 = 0.$$

Beweis Beim Beweis ist immer zu beachten: Behauptet werden Gleichheiten zwischen Äquivalenzklassen, also zwischen Mengen. Da wir aber nachgewiesen haben, dass die Operationen unabhängig von der Auswahl der Repräsentanten sind, können wir uns auf das Rechnen mit Repräsentanten beschränken. Der wesentliche Punkt ist hierbei, wie beim Nachrechnen der Rechengesetze in \mathbb{Z} : Durch die Definition wird das Rechnen in \mathbb{Q} auf das Rechnen in \mathbb{N} bzw. \mathbb{Z} zurückgeführt. Dort „kennen“ wir aber schon alle Rechengesetze, weil wir sie unter der Annahme, dass die Axiome der Mengenlehre gültig sind, auf \mathbb{N} schon bewiesen und dann auch auf \mathbb{Z} erweitert haben.

Exemplarisch wollen wir hier das Distributivgesetz nachrechnen. **Die anderen: Übungsaufgaben!** Beweis von (D):

$$\begin{aligned} [(x_1, x_2)] \cdot (([y_1, y_2]) + [(z_1, z_2)]) &= \quad (\text{Definition von } +) \\ [(x_1, x_2)] \cdot [(y_1 \cdot z_2 + z_1 \cdot y_2, y_2 \cdot z_2)] &= \quad (\text{Definition von } \cdot) \\ [(x_1 \cdot (y_1 \cdot z_2 + z_1 \cdot y_2), x_2 \cdot y_2 \cdot z_2)] &= \quad (\text{Distributivgesetz in } \mathbb{Z}) \\ [(x_1 \cdot y_1 \cdot z_2 + x_1 \cdot z_1 \cdot y_2, x_2 \cdot y_2 \cdot z_2)] &= \quad (\text{Erweitern mit } x_2) \\ [((x_1 \cdot y_1 \cdot z_2 + x_1 \cdot z_1 \cdot y_2) \cdot x_2, x_2 \cdot y_2 \cdot z_2 \cdot x_2)] &= \quad (\text{Distr. in } \mathbb{Z}) \\ [(x_1 \cdot y_1 \cdot z_2 \cdot x_2 + x_1 \cdot z_1 \cdot y_2 \cdot x_2, x_2 \cdot y_2 \cdot z_2 \cdot x_2)] &= \quad (\text{Definition von } +) \\ [(x_1 \cdot y_1, x_2 \cdot y_2)] + [(x_1 \cdot z_1, x_2 \cdot z_2)] &= \\ [(x_1, x_2)] \cdot [(y_1, y_2)] + [(x_1, x_2)] \cdot [(z_1, z_2)]. & \end{aligned}$$

Zu 6.: „ \Leftarrow “ Aus $x_1 = 0$ oder $y_1 = 0$ folgt $[(x_1, x_2)] \cdot [(y_1, y_2)] = [(0, x_2 \cdot y_2)] = [(0, 1)]$. „ \Rightarrow “ Ist $[(x_1, x_2)] \cdot [(y_1, y_2)] = [(0, 1)]$, dann folgt insbesondere: $x_1 \cdot y_1 = 0$, und die Behauptung folgt aus (2.12).

Auch hier möchten wir die uns vertrauten ganzen Zahlen wiederfinden. „Wiederfinden“ heißt mathematisch: Wir suchen eine Abbildung $k : \mathbb{Z} \rightarrow \mathbb{Q}$ mit den Eigenschaften: k ist injektiv und

$$k(m + n) = k(m) + k(n), \quad k(m \cdot n) = k(m) \cdot k(n) \quad (2.16)$$

Die Abbildung $k(n) = [(n, 1)]$ leistet das Gewünschte:

$$k(n + m) = [(n + m, 1)] = [(m, 1)] + [(n, 1)] = k(m) + k(n), \quad k(m \cdot n) = [(m \cdot n, 1)] = [(m, 1)] \cdot [(n, 1)] = k(m) \cdot k(n). \text{ Ist } n \neq m, \text{ dann gilt auch } (n, 1) \approx (m, 1), \text{ also sind } [n, 1] \text{ und } [(m, 1)] \text{ verschiedene Äquivalenzklassen und damit } k(m) \neq k(n), \text{ somit ist } k \text{ injektiv.}$$

Wir schreiben im folgenden die rationalen Zahlen $r = [(x_1, x_2)] \in \mathbb{Q}$ wieder wie gewohnt. Wir wählen einen passenden Repräsentanten $(z, n) \in [(x_1, x_2)]$ von r und schreiben die Zahl in der Form $\frac{z}{n}$. z heißt **Zähler** von r , n heißt **Nenner** von r . Das Inverse gemäß 2.11. 4 bezeichnen wir mit r^{-1} . Ist $n = 1$, also $r \in \mathbb{Z}$, so lassen wir den Nenner beim Schreiben meist weg. Somit gilt für alle $r \in \mathbb{Q}$: $1 \cdot r = r \cdot 1 = r$, und für $r \neq 0$: $r \cdot r^{-1} = r^{-1} = 1$. Die Formel in Lemma 2.11. 4 gibt auch an, wie man r^{-1} erhält:

$$r = \frac{z}{n} \quad \Rightarrow \quad r^{-1} = \frac{n}{z}.$$

Insbesondere gilt für $m = \frac{m}{1} \in \mathbb{Z}$:

$$m^{-1} = \frac{1}{m}.$$

Obwohl das „klar“ ist, sei das an dieser Stelle besonders betont. Diese beiden Schreibweisen betonen nämlich zwei verschiedene Vorstellungen: m^{-1} drückt aus: ich betrachte das multiplikative Inverse, also die Zahl m^{-1} mit $m \cdot m^{-1} = 1$, wohingegen $\frac{1}{m}$ ursprünglich heißt: ich betrachte den m -ten Teil eines Ganzen.

Man mache sich an dieser Stelle klar, dass wir hier nur mathematisch sauber das formuliert haben, was wir beim Rechnen mit Brüchen unbewusst tun: Ab Klasse 7 „weiss“ jeder (hoffentlich!), dass $\frac{2}{4}$ dieselbe Zahl wie $\frac{4}{8}$ oder $\frac{1}{2}$ darstellt – obwohl das eigentlich nicht selbstverständlich ist, warum sollte es auch? Aber bis dahin müssen auch die Schüler einen ähnlichen Prozess wie oben nachvollzogen und verinnerlicht haben.

Satz 2.12 Sei $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$. Für jedes $a, b \in \mathbb{Q}^*$ hat die Gleichung $a \cdot x = b$ die eindeutig bestimmte Lösung $x = a^{-1} \cdot b \in \mathbb{Q}^*$. Gilt $a \cdot b = 0$, so folgt: Entweder ist $a = 0$ oder/und $b = 0$.

Beweis: Setze $x = a^{-1} \cdot b$, so gilt $a \cdot x = a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = 1 \cdot b = b$. Ist x' eine weitere Zahl aus \mathbb{Q} mit $a \cdot x' = b$, so gilt: $a^{-1} \cdot (a \cdot x') = a^{-1} \cdot b$, aber $a^{-1} \cdot (a \cdot x') = (a^{-1} \cdot a) \cdot x' = 1 \cdot x' = x'$. ■

Man beachte, dass wir das Kommutativgesetz hier nicht gebraucht haben!

Bemerkung 2.13 Warum man durch 0 nicht teilen darf!

Bei der Konstruktion fällt sofort eine gewisse Unsymmetrie bei den beteiligten Paaren auf: $x_1 \in \mathbb{Z}$, aber $x_2 \neq 0$. Durch 0 teilen bedeutet in der Konstruktion auch Paare $(x_1, 0)$ zuzulassen. Was würde passieren, wenn wir $x_2 = 0$ zulassen? Der ganze Aufbau startet mit Lemma 2.8, und zwar mit der Tatsache, dass die Relation eine Äquivalenzrelation definiert. Es macht sicher keine Schwierigkeiten, die Relation $(x_1, x_2) \sim (y_1, y_2) \Leftrightarrow x_1 \cdot y_2 = y_1 \cdot x_2$ auf $\mathbb{Z} \times \mathbb{Z}$ zu definieren. Reflexivität und Symmetrie sind dann immer noch vorhanden, aber an der Transitivität scheitert es dann: $(1, 0) \sim (0, 0)$, $(0, 0) \sim (0, 1)$ aber $(1, 0) \not\sim (0, 1)$! Hat man aber keine Äquivalenzrelation, lassen sich die Rechenoperationen nicht richtig definieren.

Bemerkung 2.14 Zusammenfassend stellen wir fest: Wir haben eine Menge \mathbb{Q} konstruiert, auf der es zwei Verknüpfungen $+$ und \cdot gibt mit den folgenden Eigenschaften.

Gesetze der Addition

- (A1) Es gibt ein neutrales Element bez $+$, d.h. es gibt ein Element 0 mit $a+0 = 0+a = a$ für alle $a \in \mathbb{Q}$.
- (A2) Es gibt immer ein inverses Element bez. $+$, d.h. für alle $a \in \mathbb{Q}$ existiert $a' \in \mathbb{Q}$ mit $a + a' = a' + a = 0$. (Dieses Element nennen wir üblicherweise $-a$.)
- (A3) Es gilt das Assoziativgesetz: $(a + b) + c = a + (b + c)$ für alle $a, b, c \in \mathbb{Q}$.

(A4) Es gilt das Kommutativgesetz: $a + b = b + a$ für alle $a, b \in \mathbb{Q}$.

Gesetze der Multiplikation

(M1) Es gibt ein neutrales Element bez. \cdot , d.h. es gibt ein Element 1 mit $a \cdot 1 = 1 \cdot a = a$ für alle $a \in \mathbb{Q}$.

(M2) In \mathbb{Q}^* gibt immer ein inverses Element bez. \cdot , d.h. für alle $a \in \mathbb{Q}^*$ existiert $a^* \in \mathbb{Q}^*$ mit $a \cdot a^* = a^* \cdot a = 1$. (Dieses Element nennen wir üblicherweise a^{-1} .)

(M3) Es gilt das Assoziativgesetz: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle $a, b, c \in \mathbb{Q}$.

(M4) Es gilt das Kommutativgesetz: $a \cdot b = b \cdot a$ für alle $a, b \in \mathbb{Q}$.

Beide Operationen sind miteinander verbunden durch das *Distributivgesetz*

(D) $a \cdot (b + c) = a \cdot b + a \cdot c$, und $(a + b) \cdot c = a \cdot c + b \cdot c$ für alle $a, b, c \in \mathbb{Q}$.

Diese Regeln heißen auch *Körperaxiome*. Eine Menge mit zwei Verknüpfungen $+$, \cdot (- wie auch immer $+$ und \cdot im konkreten Fall ausgerechnet werden), für die diese Regeln gelten, heißt ein *Körper*.

Noch einige Überlegungen, die in jedem Körper gelten:

Zu gegebenem a gibt es genau ein a' mit $a + a' = 0$. Ist nämlich auch $a + a'' = 0$, so haben wir $a' = a' + 0 = a' + (a + a'') = (a' + a) + a'' = 0 + a'' = a''$.

Analog: Zu gegebenem $a \neq 0$ gibt es genau ein a^* mit $a \cdot a^* = 1$.

Offensichtlich spielen 0 und 1 spezielle Rollen. Für die Zahl -1 , also die Zahl mit $1 + (-1) = 0$ gilt:

$$-a = (-1) \cdot a, \text{ da } a + (-1) \cdot a = (1 + (-1)) \cdot a = 0 \cdot a = 0, \quad (2.17)$$

und die Zahl $-a$ eindeutig ist: Wir kürzen auch hier wieder ab:

$$a - b := a + (-b).$$

Weiterhin gilt:

$$(-1) \cdot (-1) = 1, \text{ also: } (-1)^{-1} = \frac{1}{-1} = -1, \quad (2.18)$$

in \mathbb{Q}^* sind 1, (-1) die beiden einzigen Zahlen, die mit ihrem multiplikativen Inversen übereinstimmen. Sonst hat man immer $a \neq \frac{1}{a}$. Aus (2.17) und (2.18) folgt auch für alle $r = \frac{z}{n}$:

$$-\frac{z}{n} = (-1) \cdot \frac{z}{n} = \frac{-z}{n} = \frac{z}{-n}$$

Bemerkung 2.15 Warum $1 + 1 = 2$ ist und warum das überhaupt nicht selbstverständlich ist!

$1 + 1 = 2$, das gilt als Prototyp einer Aussage, die völlig klar ist, und die doch jedes Kind kennt. Diese Aussage ist wahr – in \mathbb{N} , und weil wir die Addition als Äquivalenzklasse von Vereinigungsmengen eingeführt haben: Daumen \cup Zeigefinger = neue Menge, und wir haben dann **definiert**: dies entspricht der Zahl 2.

Das ist überhaupt nicht selbstverständlich!

In vielen Büchern wird nicht von den Mengen und ihren Axiomen ausgegangen, sondern von Zahlen, der vollständigen Induktion und Körperaxiomen.

Beginnt man z.B. so: Es gibt eine Menge K mit mitsamt den Rechenregeln wie oben, dann muss $1 + 1 = 2$ nicht gelten. Zunächst kann man sich klar machen, was in so einer Menge K enthalten sein muss: Es muss eine 0 und eine 1 geben, diese entsprechen jetzt nicht mehr der leeren Menge und der Menge mit einem Element, sondern spielen Rollen: neutrales Element bezüglich $+$ und \cdot , aus diesen speziellen Rollen folgt, dass $0 \neq 1$ gelten muss, sonst verwickelt man sich in Widersprüche. Weiterhin muss es Inverse geben, und man muss immer wissen, was $a + b$ bzw $a \cdot b$ sein soll. Da können wir uns überlegen, dass man mit folgenden Tafeln schon auskommt:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Wie man es dreht und wendet, alle Rechengesetze sind erfüllt, aber $1 + 1 = 0 \dots$

Damit ist aber auch klar, dass die Körperaxiome allein nicht ausreichen, um das festzulegen, was wir uns unter rationalen Zahlen vorstellen.

2.3 Ordnung auf \mathbb{Q} , das Archimedische Axiom

Wir können die Relation $<$ ebenfalls auf \mathbb{Q} erweitern. Hierzu legen wir zuerst eine Ordnung auf \mathbb{Z} fest **Man mache sich klar, dass das dieselbe Definition ist wie auf Blatt 2, Aufgabe 3!)**

Definition 2.16 Für $l, m \in \mathbb{Z}$ sagen wir:

$$\begin{aligned} m > 0 &\Leftrightarrow m \in \mathbb{N}, & m > l &\Leftrightarrow m - l \in \mathbb{N} \\ m \geq 0 &\Leftrightarrow m \in \mathbb{N}_0, & m \geq l &\Leftrightarrow m - l \in \mathbb{N}_0 \end{aligned}$$

Diese Definition stimmt auf $\mathbb{N}(\subset \mathbb{Z})$ mit der Definition von $m > l$ aus Teil I, die ja über Teilmengenbeziehungen erklärt war, überein. Statt $m > l$, $m \geq l$ können wir auch schreiben: $l < m$, $l \leq m$ (Merkregel: Die Spitze zeigt immer zur kleineren Zahl.)

Wegen der Charakterisierung in Folgerung 2.5 6. haben wir

$$0 > m \Leftrightarrow -m > 0 \quad (\text{oder } 0 < -m). \tag{2.19}$$

Lemma 2.17 1. Sind $l, m \in \mathbb{Z}$ mit $l > m$ und $k \in \mathbb{Z}^*$, dann

$k > 0 \Leftrightarrow l \cdot k > m \cdot k$ „Bei Multiplikation mit positiven Zahlen bleibt die Ungleichung erhalten“

$k < 0 \Leftrightarrow l \cdot k < m \cdot k$ „Bei Multiplikation mit negativen Zahlen dreht sich die Ungleichung um“

Gilt $l \geq m$ und $k \in \mathbb{Z}$, dann

$$\begin{aligned} k \geq 0 &\Rightarrow l \cdot k \geq m \cdot k \\ k \leq 0 &\Rightarrow l \cdot k \leq m \cdot k \end{aligned}$$

2.

$$\begin{aligned} l \cdot k > 0 &\Leftrightarrow l, k \in \mathbb{N} \quad \text{oder} \quad -l, -k \in \mathbb{N}. \\ l \cdot k < 0 &\Leftrightarrow l, -k \in \mathbb{N} \quad \text{oder} \quad -l, k \in \mathbb{N}. \end{aligned}$$

Beweis: Zu 1. Zuerst „ \Rightarrow “ in beiden Fällen.

Zu 1. $l > m, k > 0$ heißt: $l - m \in \mathbb{N}, k \in \mathbb{N} \Rightarrow k \cdot (l - m) = k \cdot (l + (-m)) = k \cdot l + k \cdot (-m) \in \mathbb{N}$,
 $\Rightarrow k \cdot l > k \cdot m$.

$l > m, k < 0$ heißt: $l - m \in \mathbb{N}, -k \in \mathbb{N} \Rightarrow (-k) \cdot (l - m) \in \mathbb{N}$, wegen $(-k) \cdot (l - m) = -k \cdot l + (-k) \cdot (-m) = -k \cdot l + k \cdot m = k \cdot m - k \cdot l$ heißt das $k \cdot m > k \cdot l$.

Jetzt „ \Leftarrow “

Hat man die beiden Ungleichungen $l > m$ und $l \cdot k > m \cdot k$, dann muss $k > 0$ sein, denn andernfalls würde nach dem schon Bewiesenen $l \cdot k < m \cdot k$ gelten.

Der zweite Fall: Genauso!

2. folgt aus 1. mit $m = 0$.

In \mathbb{Q} funktioniert das im Prinzip genauso. Wir legen zunächst fest, was positive rationale Zahlen sind. Betrachten wir zunächst nur solche Klassen $[(z, n)]$ mit $z, n \in \mathbb{N}$, diese Menge nennen wir \mathbb{Q}_+ , die Menge der positiven rationalen Zahlen. In der vertrauteren Schreibweise heisst das: Eine rationale Zahl $r = \frac{z}{n}$ heisst positiv, wenn nach „Aus kürzen“ Zähler und Nenner positiv sind:

$$\mathbb{Q}_+ = \left\{ \frac{z}{n} \mid \text{es gibt } p, q \in \mathbb{N}, \text{ mit } \frac{z}{n} \sim \frac{p}{q} \text{ d.h. } z \cdot q = p \cdot n \right\} \quad (2.20)$$

Statt $r = \frac{z}{n} \in \mathbb{Q}_+$ schreiben wir auch: $r > 0$. Wegen $m = \frac{m}{1}$ für $m \in \mathbb{N}$, haben wir: $\mathbb{N} \subset \mathbb{Q}_+$.

Da für eine ganze Zahl $m \neq 0$ immer gilt: $m > 0$, oder $m < 0$, folgt weiter für eine beliebige Darstellung $r = \frac{p}{q}$:

$$r = \frac{p}{q} > 0 \Leftrightarrow \text{entweder: } p > 0, q > 0, \text{ oder: } p < 0, q < 0.$$

Man kann das auch noch einfacher ausdrücken

$$r = \frac{p}{q} > 0 \quad \Leftrightarrow \quad p \cdot q > 0.$$

Hieraus folgt sofort:

$$r > 0 \Leftrightarrow r^{-1} > 0.$$

Da $p \cdot q \in \mathbb{Z}$, sind die beiden anderen Möglichkeiten für das Produkt von Zähler und Nenner:

$$\begin{aligned} p \cdot q = 0 &\Leftrightarrow p = 0 \text{ (} q = 0 \text{ ist ja verboten!)} \\ p \cdot q < 0 &\Leftrightarrow p < 0, q > 0 \text{ oder } q < 0, p > 0. \end{aligned}$$

Im letzten Fall erhalten wir: Ist $p \cdot q < 0$, so gilt $(-1)p \cdot q > 0$ nach Lemma 2.17, und dann ist $\frac{(-1)p}{q} = \frac{-p}{q} = -\frac{p}{q} \in \mathbb{Q}_+$.

Aus der Definition von \mathbb{Q}_+ sowie den Definitionen von $+$ und \cdot erhalten wir außerdem sofort: Summen und Produkte von positiven rationalen Zahlen sind wieder positiv.

$$r, s \in \mathbb{Q}_+ \Rightarrow r + s \in \mathbb{Q}_+, r \cdot s \in \mathbb{Q}_+.$$

Die letzten drei Regeln stellen wir extra zusammen:

Satz 2.18 *Die Ordnung auf \mathbb{Q}*

(O1) *Für eine rationale Zahl $r = \frac{z}{n}$ gilt genau eine der drei Möglichkeiten:*

$$r > 0, \quad r = 0, \quad -r > 0. \quad \text{Trichotomiegesetz}$$

$$(O2) \quad r > 0, s > 0 \quad \Rightarrow r + s > 0.$$

$$(O3) \quad r > 0, s > 0 \quad \Rightarrow r \cdot s > 0.$$

Bemerkung Die drei Regeln (O1), (O2) und (O3) heißen *Ordnungsaxiome*. Zusammen mit den Körperaxiomen machen sie \mathbb{Q} zu einem *angeordneten Körper*. Wir sind hier von der Ordnung auf \mathbb{N} , die durch die natürliche Ordnung von Mengen definiert wird, ausgegangen, und haben diese dann auf \mathbb{Z} und \mathbb{Q} erweitert. Man kann auch \mathbb{Q} mitsamt den Körperaxiomen und den Ordnungsaxiomen als gegeben annehmen (deshalb „Axiome“ und nicht Ordnungssätze!). Die Ordnungsaxiome reichen aus, um das Rechnen mit Ungleichungen auf \mathbb{Q} vollständig zu regeln, alle anderen Rechenregeln für Ungleichungen kann man allein mit diesen und den Körperaxiomen beweisen.

Wir benutzen allerdings die spezielleren Informationen, die wir in \mathbb{Q} schon haben. Wir definieren jetzt wie in 2.3

$$\begin{aligned} r > s &\Leftrightarrow r - s > 0, & r \geq s &\Leftrightarrow r - s \geq 0. \\ r < s &\Leftrightarrow r - s < 0, & r \leq s &\Leftrightarrow r - s \leq 0. \end{aligned}$$

Damit folgt für zwei Zahlen $r, s \in \mathbb{Q}$ aus (O1) sofort: Entweder $r > s$, $r = s$ oder $r < s$.

Folgerung 2.19 *Seien $r, s, t \in \mathbb{Q}$*

$$1. r > s, t > 0 \Rightarrow r \cdot t > s \cdot t.$$

$$2. r \geq s, t \geq 0 \Rightarrow r \cdot t \geq s \cdot t.$$

$$3. r > s, t < 0 \Rightarrow r \cdot t < s \cdot t.$$

$$4. r \geq s, t \leq 0 \Rightarrow r \cdot t \leq s \cdot t.$$

5. Sind $r, s > 0$ oder $r, s < 0$, dann gilt

$$r > s \Leftrightarrow r^{-1} < s^{-1}, \quad r \geq s > 0 \Leftrightarrow r^{-1} \leq s^{-1},$$

(„Beim Bilden der Kehrwerte drehen sich die Ungleichungen um“) *Warum stimmt das nicht auf ganz \mathbb{Q} ?*

6. $r^2 =: r \cdot r \geq 0$, und für $r \neq 0$ gilt immer $r^2 > 0$.

zum Beweis: 1., 2., **zur Übung**

3. $r > s \Rightarrow r - s > 0, t < 0 \Rightarrow -t > 0 \Rightarrow$ mit (O3): $(-t) \cdot (r - s) > 0$, d.h. nach (D) $(-t) \cdot r + (-t) \cdot (-s) = (-t) \cdot r + t \cdot s > 0 \Rightarrow$ Beh. 4. aus (O1)

5. Ist $r = \frac{z}{n}, s = \frac{p}{q}$, dann ist $r - s = \frac{z \cdot q - p \cdot n}{n \cdot q} > 0$. Da $r, s > 0$, dürfen wir $z, n, p, q > 0$ voraussetzen. Somit muss auch $z \cdot q - p \cdot n > 0$ gelten. Damit folgt:

$$\frac{1}{r} - \frac{1}{s} = \frac{n}{z} - \frac{q}{p} = \frac{n \cdot p - q \cdot z}{z \cdot p} < 0.$$

6. schon klar.

Zum Vergleichen von Brüchen ist allerdings folgende Beobachtung **Übungsaufgabe!** viel praktischer als die Definition. Aus unseren bisherigen Betrachtungen sehen wir: Für jedes $r \in \mathbb{Q}$ existiert eine Darstellung, bei der der Nenner > 0 ist. Wenn wir nur solche Darstellungen betrachten, dann gilt:

$$\begin{aligned} \text{falls } n, q > 0: \quad \frac{z}{n} < \frac{p}{q} &\Leftrightarrow z \cdot q < p \cdot n, \\ \frac{z}{n} \leq \frac{p}{q} &\Leftrightarrow z \cdot q \leq p \cdot n. \end{aligned}$$

Eine weitere Beobachtung in den rationalen Zahlen: Auch Brüche können beliebig groß werden, z.B. kann man ja einen festen Bruch beliebig oft zu sich selbst addieren, und da die natürliche Zahlen „groß“ werden, gilt – das sei als Motto für die Beschäftigung mit Mathematik fett gedruckt:

Auch mit kleinen Schritten konstanter Länge kommt man beliebig weit, solange man nur konsequent einen Schritt nach dem anderen tut!

Für rationale Zahlen heißt das:

(AA) Zu $r, s \in \mathbb{Q}_+$ gibt es immer ein $m \in \mathbb{N}$ mit $m \cdot r > s$.

In der Tat: Ist $r < s$ (nur der Fall ist spannend ...), $r = \frac{z}{n}, s = \frac{p}{q}$. Wähle m mit $m \cdot z \cdot q > p \cdot n$.

Die Eigenschaft (AA) wird als das *Archimedische Axiom* bezeichnet. Damit ist die Charakterisierung von \mathbb{Q} abgeschlossen. Man sieht zum Beispiel sofort: $1 + 1 = 0$ kann jetzt nicht mehr passieren, denn der merkwürdige Körper aus Bemerkung 2.15 kann den Ordnungsaxiomen nicht genügen. Da dort offensichtlich $1 = -1$ gilt, kann man nicht entscheiden, ob $1 > 0$ oder $-1 > 0$ gelten soll. Damit wäre aber das Trichotomiegesetz schon verletzt.

3 Strukturen aus der Algebra: Gruppe, Ringe, Körper

3.1 Gruppen

Vergleicht man die Gesetze (A1)–(A4) und (M1)–(M4), so stellt man eine grosse Ähnlichkeit in den Strukturen fest. Man kann das zugrundeliegende Konzept für sich betrachten. Zunächst einmal präzisieren wir das Wort **Verknüpfung auf einer Menge** A . Ist A eine Menge, so nennen wir eine Abbildung $v : A \times A \rightarrow A$ eine Verknüpfung. Meist schreibt man hier statt $v(a, b) : a v b$ und nimmt auch keinen Buchstaben, sondern irgendein anderes Symbol.

Beispiele 3.1

1. $+$: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}; (a, b) \mapsto a + b$
2. \cdot : $\mathbb{Q}_+ \times \mathbb{Q}_+ \rightarrow \mathbb{Q}_+; (a, b) \mapsto a \cdot b$.
3. \otimes : $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}; (a, b) \mapsto a \otimes b := \max(a, b)$
4. $A = S_n :=$ Menge aller bijektiven Abbildungen von $\{1, 2, \dots, n\}$ in $\{1, 2, \dots, n\}$.
Verknüpfung: $\circ : A \times A \rightarrow A; (f, g) \mapsto f \circ g$ (Hintereinanderausführung von Abbildungen)

Definition 3.2 Eine **Gruppe** ist Menge G mit einer Verknüpfung $* : G \times G \rightarrow G$, für die folgendes gilt:

- (G1) Es gibt ein neutrales Element bez $*$, d.h. es gibt ein $e \in G$ mit $g * e = e * g = g$ für alle $g \in G$.
- (G2) Für alle $g \in G$ existiert ein g' mit $g * g' = g' * g = e$ (Existenz von inversen Elementen)
- (G3) Es gilt das Assoziativgesetz: $(f * g) * h = f * (g * h)$ für alle $f, g, h \in G$.

Gilt außerdem noch das Kommutativgesetz

- (G4) $g * h = h * g$ für alle $g, h \in G$,

dann heißt die Gruppe kommutativ oder **Abel'sche Gruppe**.

Menge und Verknüpfung gehören also bei einer Verknüpfung zusammen, das drückt man oft auch so aus: Eine Gruppe ist ein Paar $(G, *)$ mit den Eigenschaften (G1)-(G3).

Beispiele 3.3

1. Aus Bemerkung 2.14 sehen wir sofort: $(\mathbb{Q}, +)$ und (\mathbb{Q}^*, \cdot) sind Abelsche Gruppen.
2. $(\mathbb{Z}, +)$ ist eine Abelsche Gruppe, hingegen ist (\mathbb{Z}, \cdot) keine Gruppe: (G2) ist nicht erfüllt ((G1),(G3),(G4) allerdings schon).

3. Die Verknüpfung \otimes aus Beispiel 3.1 3. ist assoziativ und kommutativ, es gibt auch ein neutrales Element: $\max(n, 1) = \max(1, n) = n$ für alle $n \in \mathbb{N}$, aber (G2) ist nicht erfüllt.

Um das 4. Beispiel aus 3.1 näher beleuchten zu können, benötigen wir folgende Aussage:

Lemma 3.4 *Seien B eine Menge, f, g, h Abbildungen von B nach B , dann gilt*

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

für alle $x \in B$.

Beweis: Ist $x \in B$, $h(x) = y$, $g(y) = z$ und $f(z) = b$, so gilt: $(f \circ g) \circ h(x) = (f \circ g)(y) = f(g(y)) = f(z) = b$. Andersherum ist $g \circ h(x) = g(h(x)) = g(y) = z$, und $f(z) = f \circ (g \circ h)(x) = b$. ■

Bezeichnen wir mit $id_B : B \rightarrow B$ die Abbildung mit $id_B(x) = x$ für alle $x \in B$, so gilt sicher: $(f \circ id_B)(x) = f(x) = (id_B \circ f)(x)$ für alle $x \in B$. Ist $f : B \rightarrow B$ bijektiv, so existiert die Umkehrabbildung $f^{-1} : B \rightarrow B$, und nach Definition der Umkehrabbildung gilt:

$$f \circ f^{-1} = f^{-1} \circ f = id_B.$$

Fazit: Für jede Menge B bildet die Menge aller bijektiven Abbildungen von B in sich, versehen mit der Verknüpfung \circ , eine Gruppe. Bevor wir uns dieser Art von Gruppen etwas genauer zuwenden, noch einige allgemeine Feststellungen.

Satz 3.5 *Sei $(G, *)$ eine Gruppe. Dann gilt:*

1. *Es gibt genau ein neutrales Element e .*
2. *Zu jedem $g \in G$ existiert genau ein Element g' mit $g * g' = g' * g = e$, **Bez:** $g' := g^{-1}$.
*Achtung: Es wird nicht behauptet: $g \neq g^{-1}$!**
3. *Für jedes a, b besitzt die Gleichung $a * x = b$ genau eine Lösung $x = a^{-1} * b$, analog die Gleichung $y * a = b$ die eindeutige Lösung $y = b * a^{-1}$. **Warum muss man hier einen Unterschied machen?***

Beweis: Zu 1. Sind e, \tilde{e} zwei neutrale Elemente, so haben wir $e = e * \tilde{e} = \tilde{e}$. **Warum?**
2. und 3. können nach genauem Studium der bisherigen Vorlesung selbst durchgeführt werden: zu 2. vergl p.19, zu 3. etwa den Beweis von Satz 2.12.

Definition 3.6 und einige Bezeichnungen

1. Eine Teilmenge einer Gruppe $(G, *)$, die selbst wieder eine Gruppe bildet, heißt *Untergruppe*.

2. Ist $g \in G$, $m \in \mathbb{N}_0$, so definieren wir g^m durch Induktion nach m , nämlich: $g^0 := e$, $g^{m+1} := g * g^m$, also

$$g^m = \underbrace{g * g * \dots * g}_{m\text{-mal}}$$

3. g , m wie oben, so ist $g^{-m} := (g^m)^{-1}$. Ist das dasselbe wie $(g^{-1})^m$ und warum?

Beispiele: $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Q}, +)$, hingegen ist (\mathbb{N}, \cdot) keine Untergruppe von (\mathbb{Q}_+, \cdot) !

Eine triviale Untergruppe hat jede Gruppe: $\{e\}$, und für jede Untergruppe \tilde{G} gilt $e \in \tilde{G}$.

Wenn G mehr als ein Element hat, kann man auch immer eine Untergruppe finden, die kommutativ ist und spannender als $\{e\}$: Generell stellt man fest: Ist $(G, *)$ eine Gruppe, und $g \in G$, so bildet die Menge $\{g^l : l \in \mathbb{Z}\}$ immer eine kommutative (!) Gruppe, die von g erzeugte *zyklische Untergruppe*. **Bez:** $\langle g \rangle$.

Z.B. wird $(\mathbb{Z}, +)$ von der Zahl 1 erzeugt. Man kann aber auch die von 2 erzeugte Untergruppe betrachten, hier schreibt man natürlich nicht 2^m , sondern $2 + 2 + \dots + 2 = m \cdot 2$, entsprechend: $(-m) \cdot 2$. Fazit: Die geraden Zahlen bilden bez. der Addition eine Gruppe. Allgemein: Für beliebiges $m \in \mathbb{N}$ bilden die durch m teilbaren ganzen Zahlen eine zyklische Gruppe in $(\mathbb{Z}, +)$, diese wird erzeugt von der Zahl m .

Frage: Welche Untergruppe erzeugt -1 in (\mathbb{Q}^*, \cdot) ?

Offensichtlich kann man zwei Fälle unterscheiden: Entweder ist $x^m = e$ für irgendein m , wie oben, oder $x^m \neq e$ für alle $m \in \mathbb{Z}$. Im ersten Fall sagt man: Die zyklische Gruppe hat die Ordnung m (wobei m minimal gewählt ist), sonst ist die Ordnung ∞ . Also: die von -1 erzeugte Untergruppe in (\mathbb{Q}^*, \cdot) hat die Ordnung 2, die vom neutralen Element e erzeugte triviale Untergruppe hat immer die Ordnung 1, und die von $m \neq 0$ in $(\mathbb{Z}, +)$ erzeugten Untergruppen haben die Ordnung ∞ .

3.2 Beispiel: Permutationsgruppen

Zurück zu Beispiel 3.1.4. Die Menge aller bijektiven Abbildungen von n Zahlen auf sich, versehen mit der Hintereinanderausführung, bilden eine Gruppe. In diesem speziellen Fall heißen die Abbildungen *Permutationen*, die Gruppe entsprechend *Permutationsgruppe*. Betrachten wir den Fall $n = 4$ mit

$$f : \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 3, \\ 3 \mapsto 4 \\ 4 \mapsto 1 \end{array} \Rightarrow f^{-1} \begin{array}{l} 1 \mapsto 4 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \\ 4 \mapsto 3. \end{array}$$

$$g : \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \\ 4 \mapsto 4 \end{array} \Rightarrow f \circ g : \begin{array}{l} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 4 \\ 4 \mapsto 1 \end{array}, \text{ aber } g \circ f : \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 4 \\ 4 \mapsto 2 \end{array}$$

Hieran sieht man, dass diese Gruppe nicht kommutativ ist: Verkettungen von Abbildungen ist i.a. nicht kommutativ. Insbesondere sind Permutationsgruppen keine kommutativen Gruppen, im Gegensatz zu $(\mathbb{Z}, +)$ oder (\mathbb{Q}_+, \cdot) . Betrachten wir die von f erzeugte Untergruppe:

$$f^2 = f \circ f : \begin{array}{l} 1 \mapsto 3 \\ 2 \mapsto 4 \\ 3 \mapsto 1 \\ 4 \mapsto 2 \end{array} \quad f^3 = f \circ f^2 : \begin{array}{l} 1 \mapsto 4 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \\ 4 \mapsto 3 \end{array} , \Rightarrow f^4 = f \circ f^3 : \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 2 \\ 3 \mapsto 3 \\ 4 \mapsto 4 \end{array}$$

Also haben wir $f^4 = id$, f erzeugt also eine Untergruppe der Ordnung 4, und wir wissen daher außerdem

$$f^3 = f^{-1}, \quad f^2 = f^{-2}, \quad f = f^{-3}, \quad f^5 = f, \quad \text{allgemein } f^m = f^{m \bmod 4}.$$

Permutationsgruppen haben immer nur endlich viele Elemente, sie sind Beispiele für *endliche Gruppen*.

Definition 3.7 Eine Gruppe $(G, *)$ heißt endlich, wenn sie nur endlich viele Elemente besitzt. Die Anzahl der Elemente heißt *Ordnung* der Gruppe. **Bez.** $ord G$. Insbesondere ist bei einer zyklischen Gruppe $\langle g \rangle$: $ord \langle g \rangle = m$, wobei m die kleinste Zahl mit $g^m = e$ ist. Deshalb sagt man auch: das Element hat die Ordnung m , mit der gleichen Abkürzung: $ord g$.

Bei einer Permutationsgruppe kann die Ordnung ausrechnen.

Bei einem Element gibt es nur eine Möglichkeit einer Abbildung: $1 \rightarrow 1$. Jetzt betrachten wir $n \geq 2$, und wir wollen ein $f \in S_n$ wählen. Wieviele Möglichkeiten gibt es? Hierzu muss man beachten, dass zwei Abbildungen als verschieden angesehen werden, wenn sie sich in nur einer Auswertung unterscheiden. Betrachten wir noch einmal als Beispiel die S_4 :

$$f : \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 3, \\ 3 \mapsto 4, \\ 4 \mapsto 1 \end{array} , \quad g : \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 3, \\ 3 \mapsto 1 \\ 4 \mapsto 4 \end{array}$$

f und g sind zwei verschiedene Elemente der S_4 , obwohl sie die Zahlen 1, 2 jeweils auf dasselbe Bild abbilden. Das kann man sich auch klarmachen, wenn man z.B. Sitzordnungen betrachtet. In einer Klasse mit 30 Kindern unterscheiden sich Sitzordnungen schon, wenn man nur zwei Kinder vertauscht – und den Rest sitzen lässt. (Das kann auch einen hör- und spürbaren Unterschied machen, wenn es gerade die zwei Hauptstörenfriede betrifft!) Die Menge der Sitzordnungen in einer Klasse mit 30 Kids kann man dann wohl auch als so etwas wie eine Realisierung der S_{30} auffassen. Dann kann man alle Sitzordnungen durchprobieren. Wenn man dann **nach wieviel Versuchen?** immer noch keine Ruhe hat, hat man ein ernstes Problem. Wieviele Sitzordnungen gibt es also?

Allgemein: Es gibt n Möglichkeiten, $f(n)$ zu wählen. Da die Abbildung bijektiv sein soll, muss $f(n) \neq f(n-1)$ gelten. Also bleiben für $f(n-1)$ nur noch $(n-1)$ Möglichkeiten.

Jetzt sind schon 2 Zahlen vergeben, also bleiben für $f(n-2)$ noch $n-2$ Möglichkeiten. Fährt man so fort, so landet man bei nur noch einer Möglichkeit für $f(1)$. Also gibt es $n(n-1)\cdots 2\cdot 1 = n!$ verschiedene Permutationen der Zahlen $\{1, \dots, n\}$, oder $|S_n| = n!$. Für S_{30} heißt das also: $|S_{30}| = 30! = 265252859812191058636308480000000$. Daher können von Permutationen erzeugte zyklische Gruppen nur von endlicher Ordnung sein, spätestens bei $n!$ Wiederholungen (tatsächlich i.a. bei weniger...) *muss* man wieder bei der Identität sein.

3.3 Beispiel: Die Bewegungsgruppe der Ebene

Eine Kongruenzabbildung der Ebene $\Gamma = \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ auf sich ist eine Abbildung, die Abstände erhält, eine solche Abbildung ist bijektiv. Die Menge aller dieser Abbildungen bezeichnen wir mit \mathcal{K} . Ist $f \in \mathcal{K}$, so sieht man die Injektivität leicht: $P_1 \neq P_2$ in E genau dann, wenn der Abstand $\neq 0$ ist. Die Surjektivität erfordert mehr Arbeit im allgemeinen Fall.

Hintereinanderausführungen von Kongruenzabbildungen sind wieder Kongruenzabbildungen, und offensichtlich ist die identische Abbildung auch eine, daher bilden Kongruenzabbildungen eine Gruppe: die Bewegungsgruppe der Ebene. Hierbei kann man zunächst einmal zwischen orientierungserhaltenden und orientierungsumkehrenden Bewegungen unterscheiden.

Bildchen in der Vorlesung

Welche bilden nun eine Untergruppe von \mathcal{K} ?

Orientierungserhaltende Kongruenzabbildungen:

- Translationen oder Verschiebungen $V_{S,T}$
- Drehungen um einen Punkt M um einen Winkel α $D_{M,\alpha}$, wir lassen hier $\alpha \in (-\infty, \infty)$ zu: $\alpha > 0$ bedeutet Drehung im mathematisch positiven Sinn.

Orientierungsumkehrende Kongruenzabbildungen:

- Spiegelung an einer Geraden S_g
- Schubspiegelung oder Gleitspiegelung $G_{S,T,g}$

Jede Kongruenzabbildung kann als Hintereinanderausführung von den oben genannten darstellen (siehe hierzu auch die Vorlesung Elementargeometrie). Für jede dieser Abbildungsklassen kann man einzeln zeigen, dass sie surjektiv ist, indem man die Bewegung wieder rückgängig macht und so ein Urbild angibt. Beispielsweise bei einer Drehung: Ist $P' = (y_1, y_2) \in \Gamma$, so gilt für $P = D_{M,-\alpha}P'$:

$$D_{M,\alpha}(P) = D_{M,\alpha}D_{M,-\alpha}P' = P'.$$

Hier kann man sich unter anderem fragen:

- Was sind die von die einzelnen Elementen erzeugten zyklischen Untergruppen?
- Was sind die endlichen Untergruppen?
- Was sind endliche, zyklische Untergruppen?
- (Ist das eventuell dasselbe...?)

Translationen bilden eine Untergruppe von \mathcal{K} . (vergl. Bild in der Vorlesung) Analytische Darstellung einer Verschiebung $V_{S,T}$ am Beispiel $S = (1, 1)$, $T = (3, 5)$. Parallelverschiebung von $\mathbf{x} = (x_1, x_2)$ um \overline{ST} bedeutet $x_1 \rightarrow x_1 + 2, x_2 \rightarrow x_2 + 4$, ist der verschobene Punkt $\mathbf{y} = (y_1, y_2)$, so gilt:

$$\begin{aligned} y_1 &= x_1 + 2 \\ y_2 &= x_2 + 4 \end{aligned}, \text{ d.h. } V_{S,T} : \mathbb{R}^2 \rightarrow \mathbb{R}^2, (x_1, x_2) \mapsto (x_1 + 2, x_2 + 4).$$

Offensichtlich ist das dasselbe, wenn ich $S = (0, 0)$ und $T = (2, 4)$, durch geeignetes Verschieben von S , und T können wir immer erreichen, dass der „Anfangspunkt“ $S = (0, 0)$ ist. Wenn wir in \mathbb{R}^2 eine Verknüpfung „+“ definieren

$$(x_1, x_2) + (\tilde{x}_1, \tilde{x}_2) = (x_1 + \tilde{x}_1, x_2 + \tilde{x}_2),$$

so wird $(\mathbb{R}^2, +)$ eine kommutative Gruppe:

(G1) ist erfüllt: Neutrales Element $(0, 0)$, da $(x_1, x_2) + (0, 0) = (x_1, x_2) = (x_1, x_2) + (0, 0)$.

(G2) ist erfüllt: Inverses zu (x_1, x_2) : $(-x_1, -x_2)$.

(G3) ist erfüllt: (siehe Vorlesung).

Verschiebungen können wir dann auch beschreiben: Ist $\mathbf{a} = (a_1, a_2)$, so ist die Verschiebung $V_{\mathbf{a}} : \mathbb{R}^2 \rightarrow \mathbb{R}^2, \mathbf{x} \mapsto \mathbf{x} + \mathbf{a}$. Im Beispiel oben ist $\mathbf{a} = (2, 4)$.

Ist jetzt $\mathbf{b} = (-1, 7)$, so ist $\mathbf{a} + \mathbf{b} = (2, 4) + (-1, 7) = (1, 13)$.

$V_{\mathbf{b}}((x_1, x_2)) = (x_1 - 1, x_2 + 7)$.

$V_{\mathbf{b}} \circ V_{\mathbf{a}}((x_1, x_2)) = V_{\mathbf{b}}((x_1 + 2, x_2 + 4)) = (x_1 + 2 - 1, x_2 + 4 + 7) = V_{\mathbf{a}+\mathbf{b}}\mathbf{x}$.

Dies kann man auch allgemein nachrechnen:

$$V_{\mathbf{b}} \circ V_{\mathbf{a}}(\mathbf{x}) = V_{\mathbf{b}}((x_1 + a_1, x_2 + a_2)) = (x_1 + a_1 + b_1, x_2 + a_2 + b_2) = V_{\mathbf{a}+\mathbf{b}}(\mathbf{x}),$$

$$V_{(0,0)} = id_{\mathbb{R}^2}, \quad V_{\mathbf{a}}^{-1} = V_{-\mathbf{a}}.$$

Fazit: Die Gruppe der Translationen hat die Ordnung ∞ , jede zyklische Untergruppe (mit Aufnahme der vom Nullpunkt erzeugten) hat ebenfalls die Ordnung ∞ .

Drehungen um einen festen Punkt bilden ebenfalls eine Untergruppe, hier betrachten wir erst mal nur die Drehungen D_{α} um den Nullpunkt, α wird hier im Winkelmaß angegeben. Dreht man erst um den Winkel α , dann um den Winkel β , so erhält man die Drehung um den Winkel $\alpha + \beta$. Neutrales Element: Drehung um den Winkel $(0, 0)$, Inverses: Drehung um $-\alpha$. Weiter stellen wir fest: Drehung um 360° bewirkt dasselbe wie Drehung um 0° . Allgemein: $D_{\alpha} = D_{\alpha \pm 360^\circ}$. Weiter: Drehen wir z.B. um 60° , dann sind wir nach 6 Drehungen wieder am Ausgangspunkt angekommen, m.A. Worten: $(\langle D_{60^\circ} \rangle, \circ)$ ist eine

zyklische Gruppe der Ordnung 6. Genauso sieht man: Ist α ein Teiler von 360, d.h. ist $\alpha \cdot k = 360$, so gilt: $\text{ord } D_\alpha = k$.

Ist $\alpha = 0^\circ$, oder $\alpha = 360^\circ$, so ist $D_\alpha = id$, das gilt auch für jedes $\alpha = k \cdot 360^\circ$, mit $k \in \mathbb{Z}$. Ist z.B. $\alpha = 29^\circ$, so ist man erst nach 360 Drehungen wieder bei einem Vielfachen von 360° angekommen. Das liegt an dem Satz über die eindeutige Primzahlzerlegung: Wir suchen das kleinste $m \in \mathbb{N}$, für das es ein k gibt mit $k \cdot 360 = m \cdot 29$. Links und rechts müssen die gleichen Primteiler auftauchen, damit folgt: $29|k$ und $360|m$. Das kleinste m ist damit 360, und daraus erhalten wir $k = 29$. Diese Überlegung gilt allgemein, wenn 360 und $\alpha \in \mathbb{N}$ zwischen 0 und 360° liegt.

Betrachten wir $\alpha = 35^\circ$, so gilt offensichtlich schon $35 \cdot 60 = 7 \cdot 360$, und dieses ist das kleinste m , denn das Problem:

Finde das kleinste m mit $m \cdot \alpha = k \cdot 360^\circ$, (EO)

ist dasselbe wie: Finde m mit $m \cdot \alpha = \text{kgV}(\alpha, 360)$, falls $\alpha \in \mathbb{N}$, $0 < \alpha < 360$. Damit ist klar: In diesem Fall ist $\text{ord } D_\alpha = \text{kgV}(\alpha, 360)/\alpha$.

Betrachten wir allgemeiner den Fall $\alpha \in \mathbb{Q}$, also $\alpha = p/q$, $0 < \alpha < 360$. Dann gilt

(EO) \Leftrightarrow finde m mit $m \cdot p = k \cdot 360 \cdot q = \text{kgV}(360 \cdot q, p)$, also

$$0 < \alpha = \frac{p}{q} < 360 \quad \Rightarrow \quad \text{ord } D_\alpha = \frac{\text{kgV}(360 \cdot q, p)}{p}.$$

Sind eigentlich alle Drehungen von endlicher Ordnung?

Experiment in der Vorlesung

Analytische Darstellung einer Drehung D_γ um den Nullpunkt 0 :

Ist $\mathbf{x} = (x_1, x_2) \in \mathbb{R}^2$, α der von der positiven x_1 -Achse und $\overline{0\mathbf{x}}$ eingeschlossene Winkel, $|\mathbf{x}|$ die Länge der Verbindungslinie $\overline{0\mathbf{x}}$, dann gilt:

$$|\mathbf{x}| = \sqrt{x_1^2 + x_2^2}, \quad x_1 = |\mathbf{x}| \cos \alpha, \quad x_2 = |\mathbf{x}| \sin \alpha.$$

Ist $\mathbf{y}_1 = D_\gamma \mathbf{x}$, so muss gelten $|\mathbf{y}| = |\mathbf{x}|$, und für den zu \mathbf{y} gehörigen Winkel $\alpha' = \alpha + \gamma$. Da wir auch hier haben:

$$|\mathbf{y}| = \sqrt{y_1^2 + y_2^2}, \quad y_1 = |\mathbf{y}| \cos \alpha', \quad y_2 = |\mathbf{y}| \sin \alpha',$$

erhalten wir

$$y_1 = |\mathbf{x}| \cos(\alpha + \gamma), \quad y_2 = |\mathbf{x}| \sin(\alpha + \gamma).$$

Jetzt benutzen wir die sogenannten Additionstheoreme für \cos , und \sin :

$$\cos(\alpha + \gamma) = \cos \alpha \cos \gamma - \sin \alpha \sin \gamma, \quad \sin(\alpha + \gamma) = \sin \alpha \cos \gamma + \cos \alpha \sin \gamma.$$

Somit erhalten wir \mathbf{y} in der Form:

$$y_1 = \cos \gamma x_1 - \sin \gamma x_2, \quad y_2 = \sin \gamma x_1 + \cos \gamma x_2. \tag{3.1}$$

Beispiel: Nach einer Drehung um 30° hat der Punkt (x_1, x_2) die neuen Koordinaten:

$$y_1 = \frac{\sqrt{3}}{2}x_1 - \frac{1}{2}x_2, \quad y_2 = \frac{1}{2}x_1 + \frac{\sqrt{3}}{2}x_2.$$

Spiegelungen bilden keine Untergruppe, denn zwei Spiegelungen hintereinanderausgeführt lassen sich nicht wieder als Spiegelung darstellen, sondern erzeugen eine Drehung um **welchen Punkt und welchen Winkel? siehe Geometrie-Vorlesung!** Allerdings erzeugen Spiegelungen immer zyklische Untergruppen der Ordnung 2.

Endliche Bewegungsgruppen, Beispiel: Diedergruppen

Bildchen in der Vorlesung

Die Kongruenzabbildungen, die ein regelmäßiges n -Eck wieder auf sich selbst abbilden, bilden selbst eine Gruppe, man kann sie auf zwei Arten als Untergruppen auffassen – als eine Untergruppe bijektiven Abbildungen des n -Ecks auf sich, und als Untergruppe von \mathcal{K} . Diese Gruppen heißen *Diedergruppen* D_n , sie sind immer endlich, denn es gilt: $\text{ord } D_n = 2n$, die Kongruenzabbildungen sind Drehungen um $360 \cdot \frac{j}{n}$, $j = 1, \dots, n$, und Spiegelungen an den n Symmetrieachsen. Wieso sind das alle und was ist eine Spiegelung verkettet mit einer Drehung? (**Übungsaufgabe!**)

Diedergruppen kann man aber auch als Untergruppen von S_n auffassen, nummeriert man die Ecken z.B. entgegen dem Uhrzeigersinn, dann definiert eine Kongruenzabbildung eine Permutation der Ecken. Umgekehrt kann ist das nicht immer der Fall! Betrachten wir D_4 und S_4 . Die Drehungen wurden beschrieben durch f^k ,

$$f : \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 4 \\ 4 \mapsto 1 \end{array}$$

Die Spiegelungen sind

$$\begin{array}{cccc} 1 \mapsto 2 & 1 \mapsto 1 & 1 \mapsto 3 & 1 \mapsto 4 \\ 2 \mapsto 1 & 2 \mapsto 4 & 2 \mapsto 2 & 2 \mapsto 3 \\ 3 \mapsto 4 & 3 \mapsto 3 & 3 \mapsto 1 & 3 \mapsto 2 \\ 4 \mapsto 3 & 4 \mapsto 2 & 4 \mapsto 4 & 4 \mapsto 4 \end{array}$$

Die Permutation g aus den Beispielen oben kann man nicht als Element der D_4 auffassen.

3.4 Lineare Transformationen der Ebene, Matrixgruppen

Lineare Transformationen in der Ebene sind Abbildungen der Form $L : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $\mathbf{x} \mapsto L(\mathbf{x})$, wobei für $(y_1, y_2) = L(\mathbf{x})$ gilt

$$y_1 = ax_1 + bx_2, \quad y_2 = cx_1 + dx_2, \tag{3.2}$$

mit geeigneten festen Zahlen a, b, c, d . Wann ist eine solche Abbildung bijektiv? Betrachten wir z.B.

$$y_1 = 3x_1 + x_2, \quad y_2 = -4x_1 + x_2, \quad (3.3)$$

Testen wir zuerst die Surjektivität, da müssen wir für jedes $\mathbf{y} = (y_1, y_2) \in \mathbb{R}^2$ ein $\mathbf{x} = (x_1, x_2)$ finden, so dass die beiden Gleichungen erfüllt sind. Surjektivität ist also gezeigt, wenn für jedes gegebene Paar (y_1, y_2) das lineare Gleichungssystem (3.3) lösbar ist. Injektivität haben wir, falls für jedes gegebene Paar (y_1, y_2) nicht mehr als eine Lösung existiert. In dem Beispiel oben erhalten wir: $x = 1/7(y_1 - y_2)$, $x_2 = 4/7y_1 + 3/7y_2$. Da wir diese Lösung durch Äquivalenzumformung aus (3.3) erhalten, ist das auch die einzige Lösung.

Betrachten wir eine andere Transformation

$$y_1 = 3x_1 - x_2, \quad y_2 = -12x_1 + 4x_2, \quad (3.4)$$

so erhalten wir schon für $y_1 = y_2 = 0$ unendlich viele Lösungen, nämlich alle $\mathbf{x} = (\lambda, 3\lambda)$ und λ darf eine beliebige Zahl sein. Andererseits erhalten wir gar keine Lösung, wenn nicht $y_2 = -4 \cdot y_1$ gilt – das sieht man, wenn man die erste Gleichung mit 4 multipliziert und zur zweiten addiert.

Das Gleichungssystem (3.2) ist eindeutig nach x_1, x_2 auflösbar, wenn $ac - bc \neq 0$ gilt. Dann erhält man durch Äquivalenzumformung

$$x_1 = \frac{d}{ad - bc}y_1 - \frac{b}{ad - bc}y_2, \quad x_2 = -\frac{c}{ad - bc}y_1 + \frac{a}{ad - bc}y_2. \quad (3.5)$$

Hintereinanderausführungen von linearen Transformationen sind wieder lineare Transformationen: Betrachten wir zu (3.2) eine weitere lineare Transformation L' mit

$$y_1 = a'x_1 + b'x_2, \quad y_2 = c'x_1 + d'x_2, \quad (3.6)$$

so gilt mit $L'(L(\mathbf{x})) = \mathbf{y} = (y_1, y_2)$

$$\begin{aligned} y_1 &= (aa' + b'c)x_1 + (a'b + b'd)x_2 \\ y_2 &= (c'a + d'c)x_1 + (c'b + d'd)x_2 \end{aligned}$$

d.h. die Hintereinanderausführung ist wieder eine lineare Transformation, und die inverse Abbildung ist ebenfalls eine lineare Transformation – siehe (3.5).

Die linearen Transformationen sind durch ihre 2×2 -Koeffizientenmatrizen eindeutig festgelegt.

$$L \leftrightarrow \underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_A, \quad L' \leftrightarrow \underbrace{\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}}_B, \quad L' \circ L \leftrightarrow \underbrace{\begin{pmatrix} a'a + b'c & a'b + b'd \\ c'a + d'c & c'b + d'd \end{pmatrix}}_{B \cdot A}$$

Die Matrix $B \cdot A$ heißt das Matrixprodukt von B und A . Genau wie die Hintereinanderausführung von linearen Transformation ist auch das Matrixprodukt nicht kommutativ. Ist die lineare Transformation invertierbar, so erhalten wir aus (3.5) die Koeffizientenmatrix von L^{-1} ,

$$\begin{pmatrix} \frac{d}{ad-bc} & -\frac{b}{ad-bc} \\ -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} =: A^{-1}$$

Weiterhin stellen wir fest: genau wie die invertierbaren linearen Transformationen bilden auch die 2×2 -Matrizen von der Form A mit $ad - bc \neq 0$ eine Gruppe, die Gruppe GL_2 der invertierbaren 2×2 -Matrizen. Das neutrale Element ist die Koeffizientenmatrix der Identität, d.h. die Matrix

$$E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \text{„Einheitsmatrix“}$$

Der Ausdruck $ad - bc := \det A$ heißt *Determinante* von A . Bei den Beispielen von oben:

$$A := \begin{pmatrix} 3 & 1 \\ -4 & 1 \end{pmatrix}, \det A = 7, \quad A^{-1} = \begin{pmatrix} 1/7 & -1/7 \\ 4/7 & 3/7 \end{pmatrix},$$

$$B = \begin{pmatrix} 3 & -1 \\ -12 & 4 \end{pmatrix}, \det B = 12 - 12 = 0$$

Betrachten wir noch einmal das Beispiel der Drehungen um den Nullpunkt. Nach (3.1) lassen sich diese Drehungen durch lineare Transformationen von der Form ($a := \cos \gamma$, $b := \sin \gamma$)

$$y_1 = ax - by, \quad y_2 = bx + ay \quad \text{mit } a^2 + b^2 = 1, \text{ da } \sin^2 \gamma + \cos^2 \gamma = 1.$$

beschreiben. Somit erzeugen Drehungen Matrizen der Form

$$D := \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \text{ wobei } \det D = 1.$$

Drehungen um den Nullpunkt entsprechen also auch einer Untergruppe von GL_2 .

3.5 Ringe und Körper

Gehen wir noch mal zu den ganzen Zahlen zurück. Wir wissen: $(\mathbb{Z}, +)$ ist eine Gruppe, es gibt aber als Verknüpfung noch die Multiplikation, es gibt ein neutrales Element bezüglich \cdot , es gilt das Assoziativgesetz und das Kommutativgesetz bez. \cdot sowie das Distributivgesetz.

Diese Eigenschaften kann man nun auch „abstrakt“ betrachten, man kann sich andere Objekte anschauen mit analogen Strukturen.

Definition 3.11 Eine Menge R , versehen mit zwei Verknüpfungen $+$, \cdot , heißt **Ring**, wenn folgendes gilt:

1. $(R, +)$ ist eine kommutative Gruppe.
2. Es gilt das Assoziativgesetz bezüglich \cdot .
3. Es gilt das Distributivgesetz.

Existiert zusätzlich ein neutrales Element e bez. \cdot , so hat man einen **Ring mit Eins**. Gilt das Kommutativgesetz bezüglich \cdot , so spricht man von einem **kommutativen Ring**. Ein kommutativer Ring mit Eins, bei dem auch (R, \cdot) eine Gruppe ist, heißt **Körper**. Um deutlich zu machen, dass zu einem Ring sowohl die Menge R als auch die beiden Verknüpfungen gehören, schreiben wir $(R, +, \cdot)$. Hierbei müssen $+$, \cdot nicht unbedingt Addition und Multiplikation auf Zahlen bedeuten. Deshalb wollen wir im folgenden das neutrale Element bez $+$ im allgemeinen Fall n nennen.

Im Sinne von 3.5 gilt also $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins. Analog zum Begriff Untergruppe gibt es den Begriff **Unterring** oder **Teilring**.

Definition 3.12 Sei $(R, +, \cdot)$ ein Ring. Eine Teilmenge $U \subset R$ heißt **Unterring** oder **Teilring**, falls $(U, +, \cdot)$ selbst wieder ein Ring ist.

Beispiele

1. $U =$: Menge der geraden Zahlen, betrachtet als Teilmenge von $(\mathbb{Z}, +, \cdot)$. Wir wissen: Summe und Produkte von geraden Zahlen sind wieder gerade Zahlen, und ist a gerade, dann auch $-a$. Das können wir auch so ausdrücken: Die geraden Zahlen bilden einen Unterring von $(\mathbb{Z}, +, \cdot)$. Allgemein können wir sagen: Für eine feste Zahl $m \in \mathbb{N}$ bildet die Menge der durch m teilbaren Zahlen einen Unterring von $(\mathbb{Z}, +, \cdot)$.
2. $(\mathbb{Z}, +, \cdot)$ ein kommutativer Unterring mit Eins von $(\mathbb{Q}, +, \cdot)$.
3. $(\mathbb{Q}, +, \cdot)$ ist ein Körper, daher auch ein kommutativer Ring mit Eins.
4. $(\mathbb{N}_0, +, \cdot)$ ist *kein* Unterring von $(\mathbb{Z}, +, \cdot)$ (auch nicht von $(\mathbb{Q}, +, \cdot)$), weil $(\mathbb{N}_0, +)$ keine Gruppe ist.

In Abschnitt 2.2 haben wir gesehen: Durch eine geeignete Konstruktion kann man aus \mathbb{Z} einen Körper machen.

Frage Funktioniert diese Konstruktion immer, oder wenigstens immer, wenn man einen kommutativen Ring mit Eins hat?

Der entscheidende Punkt dabei war Lemma 2.8, und hierzu hatten wir die Kürzungsregel in \mathbb{Z} verwendet:

$$\text{Sind } a, b, c \in \mathbb{Z}, c \neq 0 \text{ mit } ac = bc \quad \Rightarrow \quad a = b. \quad (\text{KR})$$

Gilt diese Regel in jedem Ring? Hierzu betrachten wir ein weiteres Beispiel.

3.6 Eine Beispielklasse: Restklassenringe

Wir erinnern an die Schreibweise: $a \equiv b \pmod{m} \Leftrightarrow m|(a-b)$, für $m \in \mathbb{N}$, $m > 1$. Mit $m = 4$ haben wir $1 \equiv 5 \pmod{4}$, $17 \equiv 129 \pmod{5} \equiv 1 \pmod{4} \dots$ Wir erinnern uns: Die Relation $aRb \Leftrightarrow 4|(b-a)$, was dasselbe ist wie: $a \equiv b \pmod{4}$ definiert auf \mathbb{Z} eine Äquivalenzrelation, und es gibt vier disjunkte Äquivalenzklassen.

$$\begin{aligned} [0] &= \{0, 4, -4, 8, -8, \dots\} \\ [1] &= \{1, 5, -3, 9, -7, 13, -11, \dots\} \\ [2] &= \{2, 6, -2, 10, -6, \dots\} \\ [3] &= \{3, 7, -1, 11, -5, 15, -9, \dots\} \end{aligned}$$

Bei allgemeinem m haben wir m Äquivalenzklassen, die durch die möglichen „Reste“ nach Teilen durch m festgelegt werden. Sei $R_m = \{[0], [1], \dots, [m-1]\}$, d.h. wir beschreiben die Restklassen immer durch ihren kleinsten nichtnegativen Vertreter. Auf R_m definieren wir Verknüpfungen $+$ und \cdot durch:

$$[a] + [b] = [a + b], \text{ d.h. } c \in [a + b] \quad \Leftrightarrow \quad c \equiv (a + b) \pmod{m},$$

genauso

$$[a] \cdot [b] = [a \cdot b] \text{ d.h. } c \in [a \cdot b] \quad \Leftrightarrow \quad c \equiv (a \cdot b) \pmod{m}.$$

Die Assoziativgesetze sowie das Distributivgesetz „vererben“ sich von \mathbb{Z} auf die oben definierten Verknüpfungen. Betrachten wir den Fall $m = 4$. Dann ist $R_4 = \{[0], [1], [2], [3]\}$. Da wir hier nur 4 Äquivalenzklassen haben, können wir Verknüpfungstabellen aufstellen:

$$\begin{array}{c|c|c|c|c} + & [0] & [1] & [2] & [3] \\ \hline [0] & [0] & [1] & [2] & [3] \\ [1] & [1] & [2] & [3] & [0] \\ [2] & [2] & [3] & [0] & [1] \\ [3] & [3] & [0] & [1] & [2] \end{array} \quad \begin{array}{c|c|c|c|c} \cdot & [0] & [1] & [2] & [3] \\ \hline [0] & [0] & [0] & [0] & [0] \\ [1] & [0] & [1] & [2] & [3] \\ [2] & [0] & [2] & [0] & [2] \\ [3] & [0] & [3] & [2] & [1] \end{array}$$

Wir erhalten einen kommutativen Ring mit Eins, aber die Kürzungsregel gilt nicht mehr: $[2] \cdot [2] = [0] = [0] \cdot [2]$, aber $[2] \neq [0]$!

Betrachten wir als weiteres Beispiel $m = 5$, auch hier können wir genauso verfahren, wenn statt mod 4 modulo 5 rechnen. Die Verknüpfungstabeln ergeben jetzt – hier sind jetzt die eckigen Klammern weggelassen, gemeint sind aber die Klassen:

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

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

Hier sieht man jetzt: Streicht man in der Multiplikationstafel die Nullzeile und -Spalte, so ist auch $(\{[1], [2], [3], [4]\}, \cdot)$ eine Gruppe: Es gibt ein neutrales Element, $[1]$, und jedes Element hat ein Inverses bez. \cdot : $[2]^{-1} = [3]$, $[3]^{-1} = [2]$ ($= ([2]^{-1})^{-1}$), $[4]^{-1} = [4]$. In R_4 gilt dies nicht: $[2]$ besitzt dort kein Inverses bez. \cdot , statt dessen ist $[2] \cdot [2] = [0]$. Andererseits gilt: $[3]$ hat ein multiplikatives Inverses.

Offensichtlich kann dies immer passieren, wenn m keine Primzahl ist, denn ist $m = a \cdot b$, so gilt $[a] \cdot [b] = [0]$ in R_m . Tatsächlich haben wir

Satz 3.13 1. Sei Ist $\text{ggT}(m, a) = 1$, dann hat die Kongruenz

$$a \cdot x \equiv 1 \pmod{m}$$

bez. die Restklassengleichung

$$[a] \cdot [x] = [1]$$

genau eine Lösung.

2. Ist $a \cdot b = m$, wobei $1 < a, b < m$ echte Teiler von m sind, ($\neq 1, 2$), dann hat die Gleichung $[a] \cdot [x] = [1]$ keine Lösung.

Beweis Zu 1. Seien a, b Zahlen aus $\{1, 2, \dots, m\}$ mit $\text{ggT}(a, m) = 1 = \text{ggT}(b, m)$ und $[c] = [a] \cdot [b]$. Dann muss auch $\text{ggT}(c, m) = 1$ gelten, denn aus $c \equiv (a \cdot b) \pmod{m}$ folgt: $m | (c - a \cdot b)$. Gilt aber $k | c$ und $k | m \Rightarrow k | (c - a \cdot b) \Rightarrow k | a \cdot b$. Dann folgt: Entweder $k | a$, also $k = 1$ weil $\text{ggT}(a, m) = 1$, oder $k | b$, also $k = 1$ weil $\text{ggT}(b, m) = 1$, oder $k = k_1 \cdot k_2$ mit $k_1 | a$ und $k_2 | b$, hier muss dann mit demselben Argument $k_1 = k_2 = 1$ gelten.

Seien jetzt $P = \{[x_1], [x_2], \dots, [x_k]\}$ die Menge der Restklassen modulo m mit $\text{ggT}(m, x_j) = 1$, **Warum muss $k \leq m - 1$ gelten? Wann gilt $k = m - 1$?**

und a sei fest mit $\text{ggT}(a, m) = 1$. Dann gilt mit dem oben Gezeigten: Die Abbildung

$$[x_j] \mapsto [a] \cdot [x_j]$$

bildet P in sich ab, und diese Abbildung ist injektiv. Denn gilt $[a] \cdot [x_j] = [a] \cdot [x_l]$, also $a \cdot x_j \equiv a \cdot x_l \pmod{m}$, $\Rightarrow m | (a \cdot x_j - a \cdot x_l) \Rightarrow m | a \cdot (x_j - x_l)$, also $m | (x_j - x_l)$, also $[x_j] = [x_l]$.

Da P endlich ist, ist die Abbildung auch surjektiv. Da aber auch $[1] \in P$ gilt, haben wir genau ein $[x_j] \in P$ mit $[a] \cdot [x_j] = 1$. Gilt jetzt $[a] \cdot [x] = 1$ für beliebiges $[x] \in R_m$, so ist k ein Teiler von x und von m , dann muss k auch ein Teiler von 1 sein (wegen $m|(1 - ax)$), also $k = 1$. Damit muss $x \in P$ gelten, also muss dieses x schon das x_j von oben gewesen sein.

Zu 2. Angenommen, sie hätte eine, dann folgt: $[0] = [a] \cdot [x] \cdot [b] = [1] \cdot [b] = [b]$, also $b = km$, das kann nicht sein. ■

Nochmal ein Beispiel: mit MAPLE

Und wie findet Maple das Inverse mod m?

Wie findet man z.B. eine Zahl $b \in \{1, \dots, 23\}$, so dass $5 \cdot b \equiv 1 \pmod{23}$ gilt? Zu lösen ist also: $5 \cdot x - 1 = k \cdot 23 \longrightarrow 5 \cdot x - k \cdot 23 = 1$, d.h. zu lösen ist eine diophantische Gleichung. (Vergleiche Abschnitt 13 von Teil 1)

Das Argument von oben kann man verallgemeinern: Gibt es Elemente $a, b \neq 0$ in einem Ring mit $a \cdot b = 0$, (sogenannte *Nullteiler*) dann gilt die Kürzungsregel (KR) der Multiplikation nicht, denn in solchen Ringen gilt dann ja: $a \cdot b = 0 \cdot b$, aber es folgt nicht $a = 0$. Aus solchen Ringen kann man keinen Körper machen.

Das Ergebnis bezüglich der Restklassen fassen wir zusammen:

Satz 3.14 Sei R_m wie oben als Menge von Restklassen definiert

1. Es gilt immer: $(R_m, +)$ ist eine Gruppe. Für $a \in \{0, 1, 2, \dots, m - 1\}$ gilt

$$a + (m - a) \equiv 0 \pmod{m},$$

somit ist die Klasse $[m - a] = [-a]$ das Inverse bez. + zu $[a]$. Nimmt man noch die Verknüpfung \cdot hinzu, so ist $(R_m, +, \cdot)$ immer ein kommutativer Ring mit Eins.

2. (R_m, \cdot) ist eine Gruppe $\Leftrightarrow m$ ist eine Primzahl.
3. $(R_m, +, \cdot)$ ist ein Körper $\Leftrightarrow m$ ist eine Primzahl.

Beweis 1. ist klar.

Zu 2. „ \Rightarrow “ Sei (R_m, \cdot) eine Gruppe. Wäre m keine Primzahl, dann gilt $a \cdot b = m$, mit geeigneten Zahlen $1 < a, b < m$. Dann gilt aber: $[a]$ hat kein Inverses bez. \cdot nach Teil 2 von Satz 3.13.

„ \Leftarrow “ Ist m eine Primzahl, dann hat nach Teil 1 von Satz 3.13 jede Restklasse ein Inverses bez. \cdot ,

3. folgt aus 2. (denn ein kommutativer Ring mit Eins ist R_m ja immer.)

Im Zusammenhang mit Restklassenringen wollen wir noch eine für die Zahlentheorie wichtige Funktion definieren. In Satz 3.13 hatten wir gesehen: Ist $\text{ggT}(a, m) = 1$, dann existiert b mit $a \cdot b \equiv 1 \pmod{m}$, und $\text{ggT}(b, m) = 1$. Betrachten wir jetzt für ein solches a die Menge $\{[a], [a]^2, \dots, [a]^{-1}\}$, so erhalten wir eine zyklische Gruppe bezüglich der Multiplikation in R_m , selbst wenn m keine Primzahl ist. Welche Ordnung hat diese Gruppe?

Die Bestimmung der Ordnung führt uns auf eine wichtige Funktion in der Zahlentheorie.

Definition 3.15 Ist $m \in \mathbb{N}$, dann sei $\varphi(m) =$ Anzahl der zu m teilerfremden Zahlen zwischen 1 und m . Diese Funktion $\varphi : \mathbb{N} \rightarrow \mathbb{N}_0$ heißt **Euler-Funktion**.

Beispiele

1. $\varphi(1) = 0, \varphi(2) = 1, \varphi(4) = 2 = \varphi(3), \varphi(10) = 4$.
2. Ist p eine Primzahl, dann ist $\varphi(p) = p - 1$, und für $n \in \mathbb{N}$ ist dann $\varphi(p^n) = p^n - p^{n-1}$, denn von den Zahlen zwischen 1 und p^n ist $p, 2p, 3p, \dots, p^2, (p + 1)p, \dots, p^n$ durch p teilbar.
3. $p = 7, q = 5 \Rightarrow \varphi(7) = 6, \varphi(5) = 4, \varphi(35)$: von den 34 Zahlen bis 35 alle wegnehmen, die durch 5 teilbar sind: das sind 6, und alle, die durch 7 teilbar sind, das sind 4, also $\varphi(35) = 24 = \varphi(5)\varphi(7)$. Das gilt auch allgemein: Sind p, q verschiedene Primzahlen, dann ist $\varphi(pq) = \varphi(p)\varphi(q)$.

Satz 3.16 Für die Eulersche φ -Funktion gelten folgende Aussagen:

1. Ist $\text{ggT}(a, b) = 1$, dann ist $\varphi(ab) = \varphi(a)\varphi(b)$.
2. Sind p_1, p_2, \dots, p_k die verschiedenen Primteiler einer Zahl a , so gilt

$$\varphi(a) = a \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

3. **Satz von Euler Fermat** Ist $\text{ggT}(a, m) = 1$, dann ist $a^{\varphi(m)} \equiv 1 \pmod{m}$, insbesondere gilt für den Fall, dass m eine Primzahl ist: $a^{m-1} \equiv 1 \pmod{m}$.
4. $\text{ggT}(a, m) = 1, \Rightarrow \text{ord}_m(a) | \varphi(m)$. Hierbei ist $\text{ord}_m(a)$ die kleinste Zahl k mit $a^k \equiv 1 \pmod{m}$, also die Ordnung der von a in (R_m, \cdot) erzeugten zyklischen Gruppe.

Beweis: Scheid, Elemente der Arithmetik und Algebra, pp 52 ff.

Beispiele:

1. Was ist $\text{ord}_{10}(7)$? $\varphi(10) = 4$, also kann die Ordnung nur 2 oder 4 sein. $7^2 \equiv 9 \pmod{10}$, also ist die Ordnung 4.
2. Was ist $\text{ord}_{17}(10)$? $\varphi(17) = 16$. $T(16) = \{2, 4, 8, 16\}$. Testen mit MAPLE:
3. Wir benutzen den Satz von Euler Fermat, um $2^{1000} \pmod{9}$ auszurechnen: $\varphi(9) = 6$. Also gilt:

$$2^{k \cdot 6} \equiv 1 \pmod{9} \quad \forall k \in \mathbb{N}.$$

Da $1000 \equiv 4 \pmod{6}$, ist $2^{1000} \equiv 2^4 \pmod{9} = 7 \pmod{9}$.

Das Rechnen mit Kongruenzen hat viele Anwendungen, auch durchaus praktische, einige werden wir noch kennenlernen. Erinnerung sei in diesem Zusammenhang auch an das „Erkennen“ von Quadratzahlen aus Teil I.

In diesem Zusammenhang betrachten wir folgendes Problem. Bei der Suche nach beliebig großen Primzahlen gibt es zwei besondere Gruppen von Kandidaten:

1. Zahlen von der Form $a = 2^n - 1$. Hier gilt: a ist Primzahl $\Rightarrow n$ ist Primzahl. Ist nämlich $n = u \cdot v$, also keine Primzahl, dann ist nach Satz 15.1 aus Teil 1 die Zahl $a = 2^{uv} - 1 = (2^u)^v - 1$ durch $2^u - 1$ teilbar. Die Zahlen $2^p - 1$, p Primzahl, heißen Mersenne Zahlen (Mersenne Primzahlen, falls man wirklich eine Primzahl hat.)
2. Zahlen von der Form $b = 2^n + 1$. Gilt: b ist Primzahl $\Rightarrow n$ ist eine Potenz von 2, d.h. $n = 2^k$ mit einer geeigneten Zahl k . **siehe Übungsaufgabe!** Zahlen von der Form $F_k = 2^{2^k} + 1$ heißen Fermat'sche Zahlen, entsprechend heißen sie Fermat'sche Primzahlen, wenn sie welche sind.

Beispiele mit MAPLE

Wie wir gesehen haben, ist also F_5 keine Primzahl. Wir zeigen jetzt, dass sie durch 641 teilbar ist. Es gilt $641 = 5 \cdot 2^7 + 1$, damit

$$\begin{aligned} 5 \cdot 2^7 &\equiv -1 \pmod{641} &\Rightarrow \text{mit der Regel } [a]^4 &= [a^4] \\ 5^4 \cdot 2^{28} &\equiv 1 \pmod{641} &\text{weil } (-1)^4 &= 1, \end{aligned}$$

Wegen $641 = 5^5 + 2^4 \Rightarrow 5^4 \equiv -2^4 \pmod{641}$. Einsetzen in die obige Gleichung \Rightarrow

$$-2^{32} \equiv 1 \pmod{641} \quad \Rightarrow \quad 2^{32} + 1 \equiv 0 \pmod{641}.$$

3.7 Noch mehr Ringe: Matrixringe

Wir erinnern uns an die 2×2 - Matrizen. Auch Matrizen kann man addieren, ist

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} =: \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}.$$

Die Matrizen bilden bezüglich $+$ eine Gruppe: das neutrale Element:

$$\mathbb{O} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \text{ und } \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix} = \mathbb{O}$$

Matrizen kann man auch miteinander multiplizieren, und man kann sich davon überzeugen, dass die Distributivgesetze $A \cdot (B + C) = A \cdot B + A \cdot C$, sowie $(A + B) \cdot C = A \cdot C + B \cdot C$ mit beliebigen 2×2 -Matrizen A, B, C gelten. Es gibt auch eine Eins: die Einheitsmatrix. Allerdings bilden die Matrizen keinen Körper, und es gibt Nullteiler: z.B:

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix} = \mathbb{O}.$$

Man kann aber darüber nachdenken, ob man mit „vernünftig“ ausgesuchten Teilmengen etwas anstellen kann.

siehe [Übungsaufgabe](#)

4 Zahlbereichserweiterungen II: die reellen und komplexen Zahlen

4.1 Die reellen Zahlen, Vollständigkeit

Betrachtet man ein Quadrat mit der Seitenlänge 1, so kann man der Länge der Diagonale ebenfalls eine Zahl zuordnen. Nennen wir diese Länge d , so gilt nach dem Satz des Pythagoras

$$1^2 + 1^2 = d^2, \quad \text{also } d^2 = 2.$$

Wie kann man diese Zahl näher beschreiben? Angenommen, d wäre ein Bruch, d.h.

$$\begin{aligned} d = \frac{p}{q}, \quad p, q \text{ teilerfremd} &\Rightarrow 2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2 \Rightarrow 2|p^2 \\ \Rightarrow 2|p &\Rightarrow p = 2k \Rightarrow 2q^2 = 4k^2 \Rightarrow q^2 = 2k^2 \Rightarrow 2|q. \end{aligned}$$

Also sind p, q nicht teilerfremd, somit kann dieses d nicht in \mathbb{Q} sein.

Wir versuchen, diesem d durch Probieren näher zu kommen: Wenn wir uns diese Zahl als Diagonalenlänge veranschaulicht vorstellen, brauchen wir nur in positiven Zahlen zu suchen. Dann überlegen wir uns, was wir über die Funktion $f : \mathbb{Q}_+ \rightarrow \mathbb{Q}_+, x \mapsto x^2$ wissen. Haben wir zwei positive rationale Zahlen mit

$$\begin{aligned} b > a &\Rightarrow b = a + (b - a), \text{ wobei } (b - a) > 0 \Rightarrow \\ b^2 &= a^2 + (b - a)^2 + 2b(b - a) > a^2 \text{ weil 2 positive Summanden weggelassen werden.} \end{aligned}$$

Also erhalten wir: $a < b \Rightarrow f(a) < f(b)$.

Diese Eigenschaft drückt man so aus: Die Funktion f ist **monoton steigend** auf \mathbb{Q}_+ .

Wenn wir uns vorstellen, dass wir das unbekannte d irgendwo „zwischen“ den rationalen Zahlen unterbringen können, was die anschauliche Vorstellung als Länge der Diagonalen nahelegt, dann können wir jetzt experimentieren:

$$\begin{aligned} 1^2 < 2, \quad 2^2 = 4 &\Rightarrow 1 < d < 2 \\ 1.5^2 = 2.25 &\Rightarrow 1 < d < 1.5 \\ (1 + 1.5)/2 = 1.25, \quad 1.25^2 = 1.5625 < 2 &\Rightarrow 1.25 < d < 1.5 \\ &\vdots \end{aligned}$$

Experiment mit MAPLE

Wir sperren also die unbekannte Zahl d ein zwischen Folgen von rationalen Zahlen. Wir stellen fest: Nach 6 Schritten unterscheiden sich die beiden ersten Stellen der oberen und der unteren Schranken nicht mehr (beides 1.4), und nach $[n]$ weiteren Schritten bleiben

die nächsten Stellen fest. Wir erhalten so eine Dezimalbruchentwicklung, die weder periodisch noch abbrechend ist (sonst hätten wir ja einen Bruch). Das Verfahren, dass wir hier verwendet haben, nennt man **Intervallhalbierungsverfahren**.

Mit diesem Verfahren erhalten wir eine Folge von Intervallen $I_k = [a_k, b_k]$, für die folgendes gilt:

1. Für alle k gilt: $I_k \supset I_{k+1}$
In unserem Beispiel war

$$\begin{aligned} [1, 2] &= I_0 \supset [1, 1.5] = I_1 \supset [1.25, 1.5] = I_2 \supset [1.375, 1.5] = I_3 \supset \\ &\supset [1.375, 1.4375] = I_4 \supset [1.40625, 1.4375] = I_5 \dots \end{aligned}$$

2. Die Länge der Intervalle wird beliebig klein: Für jede kleine Fehlervorgabe $\varepsilon > 0$ finden wir ein k mit $|I_k| = b_k - a_k < \varepsilon$.
In unserem Beispiel kann man die Länge der Intervalle leicht bestimmen: Da wir ja immer halbieren, und $|I_0| = 1 \Rightarrow$:

$$|I_1| = \frac{1}{2}, \quad |I_2| = \frac{1}{4} = \frac{1}{2^2}, \quad \dots, \quad |I_k| = \frac{1}{2^k}$$

Eine solche Folge von Intervallen mit den Eigenschaften 1. und 2. nennt man eine **Intervallschachtelung**. Solche Intervallschachtelungen kann man sich auch mit beliebigen Anfangsintervallen konstruieren, und dann z.B. Münzen werfen:

0. Schritt: Wähle ein Anfangsintervall I_0 , und finde den Mittelpunkt.

1. Schritt: Münze werfen, Zahl: linkes Teilintervall = I_1 , Bild: (auf Euro Münzen gibt es nicht nur Köpfe): Rechtes Teilintervall = I_1 .

2. Schritt: Halbiere I_1 , Münze werfen, Zahl: linkes Teilintervall = $I_2 \dots$

(Genauso kann man sich an die Straße setzen: Auto von links, \dots , Auto von rechts \dots)

Man kann dann zusehen, (bis man die Geduld verliert), wie sich die Intervalle „auf einen Punkt zusammen ziehen“. In der Regel wird man damit Zahlen erwischen, die keine periodische Dezimalbruchentwicklung haben, und diese Zahlen schließen die „Lücken in \mathbb{Q} “. Mathematisch korrekt kann man das so formulieren:

(IA) Hat man eine Intervallschachtelung $\{I_k\}_{k \in \mathbb{N}}$ wie oben, so gibt ein d mit $d \in I_k$ für alle k , d.h. $d \in \bigcap_{k \in \mathbb{N}} I_k$.

Es läßt sich außerdem noch sagen: Es gibt genau ein $d \in \bigcap_{k \in \mathbb{N}} I_k$ – nicht zwei oder mehr, denn bei zwei verschiedenen d, d' , z.B. mit $d < d'$ müßte auch das „Zwischenstückgrqq $[d, d']$ im Durchschnitt $\bigcap_{k \in \mathbb{N}} I_k$ liegen, dann könnte aber die Länge der Intervalle nicht beliebig klein werden, sie müßte ja mindestens $d' - d$ betragen.

Damit lassen sich die reellen Zahlen \mathbb{R} wie folgt charakterisieren

Definition 4.1 Bei den reellen Zahlen handelt es sich um eine Menge \mathbb{R} , auf der es zwei Verknüpfungen, $+$, \cdot , gibt mit folgenden Eigenschaften:

Axiome der reellen Zahlen

1. $(\mathbb{R}, +, \cdot)$ ist ein Körper.
2. Es gibt eine Relation $<$ auf \mathbb{R} , für die gilt
(O1) Für $r \in \mathbb{R}$ gilt genau eine der drei Möglichkeiten:

$$r > 0, \quad r = 0, \quad -r > 0. \quad \text{Trichotomiegesetz}$$

(O2) $r > 0, s > 0 \Rightarrow r + s > 0$. Bezeichnung: $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$.

(O3) $r > 0, s > 0 \Rightarrow r \cdot s > 0$.

3. Es gilt das Archimedische Axiom
(AA) Zu $r, s \in \mathbb{R}_+$ gibt es immer ein $m \in \mathbb{N}$ mit $m \cdot r > s$.
4. Es gilt das sogenannte Intervallschachtelungsaxiom (IA).

Da 1.-3. auch in \mathbb{Q} gelten, liegt der entscheidende Unterschied in dem Intervallschachtelungsaxiom, dass in \mathbb{Q} offensichtlich nicht gilt. Betrachtet man in unserem Beispiel die Folge $\{a_k \mid k \in \mathbb{N}_0\}$ der unteren Intervallgrenzen, so „sieht“ man: Diese Zahlenfolge reicht schon aus, um die Dezimalstellen von d mit $d^2 = 2$ zu bestimmen. Wir können uns überlegen, wieviel Schritte wir brauchen, um die ersten 10 Stellen hinter dem Komma exakt zu haben. Da entweder $a_{k+1} = a_k$ oder $a_{k+1} = (a_k + b_k)/2$ und $|b_k - a_k| = 2^{-k}$ gilt, ändert sich an den vorderen Stellen nichts mehr, wenn $2^{-k} < 10^{-11}$ oder $2^k > 10^{11}$ gilt. Da $2^4 = 16$, ist klar, dass man spätestens nach 4 Schritten eine Dezimalstelle weiter ist. Ausprobieren liefert: Hier reichen 37 Halbierungen.

Für unser gesuchtes d mit $d^2 = 2$ geht es aber auch schneller: Wir betrachten folgende Zahlenfolge:

$$x_0 = 1, x_1 = \frac{1}{2}\left(x_0 + \frac{2}{x_0}\right), \quad \dots, \quad x_{k+1} = \frac{1}{2}\left(x_k + \frac{2}{x_k}\right)$$

(So etwas nennt man eine **rekursiv definierte Folge**. Warum diese Folge gegen d konvergiert, erfordert mehr Argumente, als wir hier zur Verfügung haben, wird aber auf Wunsch erläutert.)

MAPLE

Wenn wir unser gesuchtes $d = \sqrt{2}$ nennen, so stellen wir uns in beiden Fällen vor: Der Betrag $|\sqrt{2} - a_k|$ wird beliebig klein, wenn der Index k groß wird. Dieses Verhalten halten wir in folgender Definition fest:

Definition 4.2 Eine Folge $\{x_k\}$ von reellen Zahlen heißt **konvergent gegen eine Zahl** x , falls für jede noch so kleine Fehlerschranke $\varepsilon > 0$ ein Index K existiert, ab dem $|x - x_k| < \varepsilon$ gilt, (d.h. $|x - x_k| < \varepsilon \forall k > K$).

Speziell in unserem Beispiel können wir allerdings dieses x nicht sehen, (es sei denn, man betrachtet ein Quadrat), noch deutlicher wird dies, wenn man eine Zahl wie oben „auswürfelt“ wird. Tatsächlich beobachten können wir folgendes: Immer mehr Dezimalstellen nach dem Komma bleiben unverändert. Beim Intervallhalbierungsverfahren für $\sqrt{2}$ haben wir gesehen: ab $k = 4$ bleiben die ersten beiden Stellen der linken Intervallgrenzen fest, (1.4), das kann man auch so ausdrücken:

$$\forall l, m > 4 \text{ gilt } : |a_m - a_l| < 1/10.$$

Ab $k = 8$ bleiben die ersten 3 Stellen fest (1.41)

$$\forall l, m > 8 \text{ gilt } : |a_m - a_l| < 1/100.$$

Bei der anderen Folge ging das wesentlich schneller:

$$\forall l, m > 4 \text{ gilt } : |x_m - x_l| < 10^{-4}.$$

$$\forall l, m > 6 \text{ gilt } : |x_m - x_l| < 10^{-23}.$$

Was wir also beobachten, ist: Für jede kleine Fehlerschranke $\varepsilon > 0$ findet sich ein Index $k(\varepsilon)$, ab dem gilt: $|x_l - x_m| < \varepsilon$, falls die Indizes $l, m > k(\varepsilon)$ sind. Solche Folgen heißen **Cauchy-Folgen**.

Wir können jetzt den Unterschied zwischen \mathbb{Q} und \mathbb{R} auch so formulieren: In \mathbb{R} gilt das **Vollständigkeitsaxiom**

(VA) Jede Cauchy-Folge ist konvergent.

In \mathbb{Q} gilt (VA) nicht, abgesehen von den Beispielen, die gegen $\sqrt{2}$ konvergieren – ohne dass wir das hier jetzt wirklich bewiesen haben – kann man sich hierzu beliebige weitere Gegenbeispiele „auswürfeln“.

ACHTUNG Es reicht nicht, dass $|a_k - a_{k+1}|$ beliebig klein wird!

Betrachte dazu die Folge $x_1 = 1, x_2 = 1 + \frac{1}{2}, x_3 = 1 + \frac{1}{2} + \frac{1}{3}$, allgemein $x_k = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{k}$. Hier gilt:

$$|x_{k+1} - x_k| = \frac{1}{k+1} \quad \text{aber: } x_k \text{ wird beliebig groß!}$$

Das sieht man so ein:

$$\begin{array}{cccccc} \frac{1}{2} + & \underbrace{\frac{1}{3} + \frac{1}{4}}_V & + & \underbrace{\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}}_V & + & \underbrace{\frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \dots + \frac{1}{16}}_V & + \dots > \\ & \frac{1}{2} & & + \frac{1}{2} & & + \frac{1}{2} & & + \dots \end{array}$$

Die reellen Zahlen lassen sich aus \mathbb{Q} mit Hilfe einer Äquivalenzrelation konstruieren.

(womit sonst? Hartgesottene Hörer dürfen nach der Vorlesung nachfragen, wie das geht.)

Begonnen haben wir mit der Betrachtung von \mathbb{R} dadurch, dass wir die Gleichung $x^2 = 2$ lösen wollten. Man kann allgemein das Problem betrachten: Wie finde ich Nullstellen eines Polynoms? (Am liebsten natürlich mit Formeln!) Zahlen, die als Nullstellen von Polynomen mit ganzzahligen Koeffizienten auftauchen, heißen **algebraisch**. In \mathbb{R} gibt es aber auch solche, die das nicht tun: solche Zahlen heißen **transzendent**, das sind die Zahlen, die sich nicht mit Hilfe von Zirkel und Lineal konstruieren lassen.

Berühmtestes Beispiel: die Zahl π . Die Transzendenz von π wurde aber erst 1882 von Carl Louis Ferdinand von Lindemann bewiesen, und damit ein Schlußstrich unter ein Jahrtausende altes Problem gezogen. Man kann einen Kreis nicht mit Hilfe von Zirkel und Lineal in ein flächengleiches Quadrat verwandeln – obwohl es immer mal wieder Leute gibt, die behaupten, genau das zu tun.

4.2 Mehr über Potenzen und Wurzeln und wie man damit rechnet

Bevor wir uns im nächsten Abschnitt ein wenig damit beschäftigen, wie und warum die Mathematiker auf komplexe Zahlen gekommen sind, wollen wir uns Potenzen und Wurzeln noch ein wenig genauer ansehen. Aus dem Axiomensystem für die reellen Zahlen \mathbb{R} kann man folgendes herleiten:

Satz 4.3 Für jedes $y \in \mathbb{R}$ mit $y \geq 0$ gibt es genau ein $x \geq 0$ mit $x^2 = y$. Bezeichnung: $x = \sqrt{y}$.

Beweis: Zwei Dinge sind zu zeigen: Es gibt \sqrt{y} (*Existenz*) und es gibt nicht zwei oder mehr (*Eindeutigkeit*). Zuerst erledigen wir $y = 0$. Da $0^2 = 0$, und aus $x^2 = 0$ folgt: $x = 0$, ist dieser Fall schon ok. Jetzt brauchen wir nur $y > 0$ zu betrachten.

Wir zeigen zuerst die Eindeutigkeit. Angenommen, es gäbe $a \neq b$, beide > 0 mit $a^2 = b^2 = y$. Wenn $a \neq b$, können wir o.B.d.A. annehmen, dass $a < b$. Dann ist aber $a^2 < b^2$ – mit der gleichen Argumentation wie in \mathbb{Q} , Widerspruch!

Die Existenz von \sqrt{y} zeigen wir mit dem Interhalbierungsverfahren. Aus dem Axiom (AA) angewandt auf $y (= r)$ und $1 (= s)$ folgt: Es gibt $m \in \mathbb{N}$ mit $m > y$, damit auch $m^2 > y$.

Wir setzen unser Startintervall $I_0 = [0, m] =: [a_0, b_0]$.

Im ersten Schritt testen wir: $(\frac{m}{2})^2 \leq y?$, dann setzen wir $\frac{m}{2} = a_1$ und $b_0 = b_1$.

Falls $(\frac{m}{2})^2 > y$, dann setzen wir $\frac{m}{2} = b_1$ und $a_1 = a_0$.

Im k -ten Schritt haben wir ein Intervall $I_{k-1} = [a_{k-1}, b_k]$ mit $a_{k-1}^2 \leq y \leq b_{k-1}^2$. Wir testen wir wieder:

$$\text{Mit } M = \frac{1}{2}(a_{k-1} + b_{k-1}) : \quad \begin{array}{l} M^2 \leq y? \Rightarrow I_k = [a_k, b_k] =: [M, b_{k-1}], \\ M^2 > y? \Rightarrow I_k = [a_k, b_k] =: [a_{k-1}, M]. \end{array}$$

Wir erhalten eine Intervallschachtelung, auf die wir (IA) anwenden können: $\bigcap I_k = \{x\}$, und wir wissen:

$$a_k \leq x \leq b_k \quad \Rightarrow \quad a_k^2 \leq x \leq b_k^2, \quad \text{und} \quad a_k^2 \leq y \leq b_k^2. \quad (4.1)$$

Wir haben aber auch die folgende Intervallschachtelung $\tilde{I}_k =: [a_k^2, b_k^2]$. Dass $\tilde{I}_k \supset \tilde{I}_{k+1}$, ist klar, und die Länge der Intervalle läßt sich abschätzen: Wegen $a_k, b_k \leq m$ gilt

$$b_k^2 - a_k^2 = (b_k + a_k)(b_k - a_k) \leq 2m(b_k - a_k) \leq 2m \cdot m \cdot 2^{-k} = \frac{m^2}{2^{k-1}},$$

also werden auch hier die Intervalle beliebig klein. Damit wissen wir: $\bigcap \tilde{I}_k$ besteht aus genau einem Element: Wegen (4.1) muss dieses Element sowohl y als auch x^2 sein, somit $x^2 = y$. ■

Mit einer ähnlichen Konstruktion zeigt man

Satz 4.4 Sei $n \in \mathbb{N}$ beliebig vorgegeben. Für jedes $y \in \mathbb{R}$, mit $y \geq 0$ gibt es genau ein $x \geq 0$ mit $x^n = y$. Bezeichnung: $x = \sqrt[n]{y}$.

Ein Kommentar zum Beweis: Um die Monotonie der Funktion $f : \mathbb{R}_+ \rightarrow \mathbb{R}_+; x \mapsto x^n$ nachzuweisen, kann man statt der binomischen Formel den allgemeinen binomischen Lehrsatz benutzen:

$$(a + b)^n = a^n + na^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \dots + \binom{n}{k}a^{n-k}b^k + \dots + nab^{n-1} + b^n.$$

Die Koeffizienten

$$\binom{n}{k} = \binom{n}{n-k} =: \frac{n!}{k!(n-k)!}$$

heißen Binomialkoeffizienten und man kann sie mit Hilfe des sogenannten Pascal'schen Dreiecks ausrechnen.

$$\begin{array}{rcccccc} n = 0 : & & & & & & 1 \\ n = 1 : & & & & & 1 & 1 \\ n = 2 : & & & & 1 & 2 & 1 \\ n = 3 : & & & 1 & 3 & 3 & 1 \\ n = 4 : & & 1 & 4 & 6 & 4 & 1 \\ n = 5 : & & & & \dots & & \end{array}$$

Weiterhin braucht man die Formel

$$b_k^n - a_k^n = (b_k - a_k)(b_k^{n-1} + b_k^{n-2}a_k + \dots + b_k a_k^{n-2} + a_k^{n-1}).$$

Dann funktioniert der Beweis genauso wie bei der Quadratwurzel. ■

Bemerkung 4.5 Die Bezeichnung $\sqrt[n]{}$ wurde 1525 von Christoph Rudolff eingeführt, er schrieb allerdings noch $\sqrt[3]{}$ für die 3. Wurzel und $\sqrt[4]{}$ für die 4. Wurzel.

Aus diesem Satz ergeben sich jetzt Konsequenzen für das Rechnen mit Wurzeln, hierzu erinnern wir an die Rechenregeln für Potenzen, die aus der Definition der Potenzen und den Körperaxiomen folgen. Sind $c, d \in \mathbb{R}$, $n, m \in \mathbb{N}$, dann gilt:

$$(cd)^m = c^m d^m, \quad c^{m+n} = c^m c^n, \quad (c^m)^n = c^{mn}$$

$$c^{-n} := \frac{1}{c^n} \quad \Rightarrow \quad c^{m-n} = \frac{c^m}{c^n}.$$

Man sieht hieran: Für jedes feste $c > 0$ bildet die Abbildung: $e : \mathbb{Z} \rightarrow \mathbb{Q}_+, m \mapsto c^m$ die Gruppe $(\mathbb{Z}, +)$ in die Gruppe (\mathbb{Q}_+, \cdot) ab, in der folgenden Art und Weise:

$$\underbrace{e(m+n)}_{\text{Operation in } (\mathbb{Z}, +)} = \underbrace{e(m) \cdot e(n)}_{\text{Operation in } (\mathbb{Q}, \cdot)}$$

Folgerung 4.6 Sind $a, b \in \mathbb{R}$, $a, b \geq 0$, $n, m \in \mathbb{N}$, dann gilt:

$$\sqrt{ab} = \sqrt{a}\sqrt{b}, \quad \sqrt[n]{ab} = \sqrt[n]{a}\sqrt[n]{b}, \quad (4.2)$$

$$\sqrt[m]{a^m} = (\sqrt{a})^m, \quad \sqrt[n]{a^m} = (\sqrt[n]{a})^m, \quad (4.3)$$

$$\sqrt{\frac{1}{a}} = \frac{1}{\sqrt{a}}, \quad \sqrt[n]{\frac{1}{a}} = \frac{1}{\sqrt[n]{a}}, \quad (4.4)$$

$$\sqrt[n]{\sqrt[m]{a}} = \sqrt[nm]{a} \quad (4.5)$$

Beweis Die Formeln (4.2) folgen aus den Rechengesetzen für Potenzen $(cd)^2 = c^2 d^2$, allgemein $(cd)^m = c^m d^m$:

Wir setzen $c = \sqrt{a}$, $d = \sqrt{b} \Rightarrow$

$$(\sqrt{a}\sqrt{b})^2 = \sqrt{a}^2 \sqrt{b}^2 = ab \quad \Rightarrow \quad \sqrt{ab} = \sqrt{a}\sqrt{b},$$

weil es nur eine nichtnegative Wurzel gibt (und wir haben sie „vorgezeigt“).

Analog argumentiert man bei der $\sqrt[n]{\cdot}$.

Die Formel (4.3) zeigt man mit Hilfe der ersten durch Induktion nach m .

(Übungsaufgabe!)

Zu (4.4):

$$\left(\frac{1}{\sqrt{a}}\right)^2 = \frac{1}{(\sqrt{a})^2} = \frac{1}{a} \Rightarrow \text{Beh.},$$

analog für die m te Wurzel.

Zu (4.5): Da aus der Definition der Potenzen folgt: $(c^m)^n = c^{mn} = (c^n)^m \Rightarrow$

$$\left(\sqrt[n]{\sqrt[m]{a}}\right)^{nm} = \left(\left(\sqrt[m]{a}\right)^n\right)^m = \left(\sqrt[n]{a}\right)^m = a.$$

Jetzt erhalten wir die Behauptung wieder mit der Eindeutigkeit der nm -ten Wurzel, da wir eine Zahl c mit $c^{nm} = a$ „vorgezeigt“ haben, nämlich $c = \sqrt[n]{\sqrt[m]{a}}$. ■

Diese Rechenregeln, zusammen mit den Rechenregeln für Potenzen, legen die Schreibweise nahe: Für $a > 0, p, q \in \mathbb{N}$

$$\sqrt[q]{a} := a^{\frac{1}{q}}, \text{ somit (4.3) } \Leftrightarrow a^{\frac{p}{q}} = (\sqrt[q]{a})^p = \sqrt[q]{a^p}.$$

Damit lassen sich auch die anderen Rechengesetze viel leichter behalten:

$$(4.2) \quad \Leftrightarrow \quad (ab)^{\frac{1}{n}} = a^{\frac{1}{n}} b^{\frac{1}{n}}$$

$$(4.4) \quad \Leftrightarrow \quad (a^{-1})^{\frac{1}{n}} = (a^{\frac{1}{n}})^{-1} (= a^{-\frac{1}{n}})$$

$$(4.5) \quad \Leftrightarrow \quad ((a)^{\frac{1}{n}})^{\frac{1}{m}} = a^{\frac{1}{nm}}$$

Problem Was ist

$$\sqrt[3]{a^7} \sqrt[6]{a^4}?$$

Mit den gebrochenen Hochzahlen ganz einfach:

$$a^{\frac{7}{3}} a^{\frac{4}{6}} = a^{\frac{7}{3} + \frac{2}{3}} = a^{\frac{9}{3}} = a^3.$$

Dazu muss man folgende Regel noch beweisen:

Satz 4.7 Für $a \in \mathbb{R}_+, q, q' \in \mathbb{N}, p, p' \in \mathbb{Z}$ gilt:

$$\sqrt[q]{a^p} \sqrt[q']{a^{p'}} = \sqrt[qq']{a^{pq'+qp'}} \quad (\Leftrightarrow \quad a^{\frac{p}{q}} a^{\frac{p'}{q'}} = a^{\frac{pq'+qp'}{qq'}}).$$

Beweis

$$\begin{aligned} (\sqrt[q]{a^p} \sqrt[q']{a^{p'}})^{qq'} &= (\sqrt[q]{a^p})^{qq'} (\sqrt[q']{a^{p'}})^{qq'} \\ &= (\sqrt[q]{a^{pq}})^{q'} (\sqrt[q']{a^{p'q'}})^q = (a^p)^{q'} (a^{p'})^q \\ &= a^{pq'} a^{p'q} = a^{pq'+p'q}. \end{aligned}$$

Jetzt können wir wieder das Argument benutzen, dass es nur eine positive qq' -te Wurzel aus $a^{pq'+p'q}$ gibt, und die haben wir vorgezeigt.

Auch hier erhalten wir: Die Abbildung $g : \mathbb{Q} \rightarrow \mathbb{R}_+, x \mapsto a^x$ bildet die Gruppe $(\mathbb{Q}, +)$ strukturerhaltend auf (\mathbb{R}_+, \cdot) ab, denn $g(x+y) = g(x) \cdot g(y)$ – so etwas nennt man einen **Gruppenhomomorphismus**.

Folgerung 4.8 $a^0 = 1$ für alle $a \in \mathbb{R}_+$.

Beweis $a^0 = a^{1-1} = a \cdot a^{-1} = 1.$

4.3 Die komplexen Zahlen

Die ersten, die sich systematisch mit dem Lösen von quadratischen Gleichungen befassten, waren die Araber beginnend mit al-Hwarizmi (1. Hälfte 9. Jahrhundert). Al-Hwarizmi nannte die dabei auftretenden irrationalen Zahlen, (die er auch am liebsten vermied) „taube Wurzeln“, daher hießen diese auch bis zum 18. Jahrhundert taube Zahlen.

Selbst bei quadratischen Gleichungen sieht man recht fix ein, dass man mit der Erweiterung von \mathbb{Q} auf \mathbb{R} zwar ein Stück weiterkommt, das löst aber nicht alle Probleme. Betrachten wir drei Beispiele:

$$\begin{aligned}x^2 + x - 6 &= 0 \\x^2 + x + 1/2 &= 0 \\x^2 + x + 6 &= 0\end{aligned}$$

Im ersten Fall haben wir zwei Lösungen: $x_1 = -3, x_2 = 2$, im zweiten Fall eine: $x = -1/2$, im dritten Fall gar keine reelle Lösung. (*Bildchen in der Vorlesung*)

Betrachten wir den allgemeinen Fall: $x^2 + px + q$, fast alle haben in Schule die folgende Formel gelernt:

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q},$$

mit dem Zusatz: es gibt zwei Lösungen, falls der Ausdruck unter der Wurzel > 0 ist, es gibt eine Lösung, falls der Ausdruck genau 0 ergibt, und wenn er < 0 ist, hat man Pech gehabt.

Was hat man eigentlich bei der Gleichung $x^2 = 2$ gemacht? Wenn man nur Brüche kennt, hat man ein Problem. Das kann man lösen, indem man die Zahl $\sqrt{2}$ „erfindet“ und zu den Zahlen dazu tut. Von $\sqrt{2}$ zu $-\sqrt{2}$ ist dann der Schritt nicht mehr so weit. Betrachtet man $x^2 = -2$, so kann man sich folgendes überlegen: Hält man die Rechenregeln für Wurzeln für vernünftig, dann hat man wegen $-2 = (-1) \cdot 2$ nur mit $\sqrt{-1}$ ein Problem. Niemand hindert uns daran, diese Zahl zu „erfinden“ und uns zu überlegen, wie man damit sinnvoll rechnen kann. Wir nennen diese Zahl i (eingeführt 1777 von Leonhard Euler):

$$\boxed{i = \sqrt{-1}}, \quad \boxed{i^2 = -1}.$$

Damit erhalten wir aus der p - q -Formel für das Beispiel $x^2 + x + 6 = 0$:

$$x_{1,2} = -\frac{1}{2} \pm \sqrt{\frac{1^2}{4} - 6} = -\frac{1}{2} \pm \sqrt{\frac{1^2 - 24}{4}} = -\frac{1}{2} \pm \frac{\sqrt{23}}{2}i.$$

Allgemein erhält man bei der p - q -Formel (mit $p, q \in \mathbb{R}$), sofern $\frac{p^2}{4} - q < 0$:

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{q - \frac{p^2}{4}}i,$$

also Ausdrücke in der Form $x = a + ib$. Wie soll man jetzt mit solchen Ausdrücken rechnen? Es ist sicher vernünftig, zu verlangen, dass die üblichen Gesetze der Addition und Multiplikation gelten, wie man sie in der Schule auch für das Rechnen mit Zahlen und Buchstaben benutzt, außerdem $i^2 = -1$, dann ist:

$$(3 + 4i) + (2 - 7i) = 5 - 3i, \quad 3 + 4i - (3 + 4i) = 0,$$

$$(3 + 4i) \cdot (2 - 7i) = 6 + 8i - 21i - 28i^2 = 6 - 13i + 28 = 34 - 13i.$$

Allgemein:

$$a + bi + a' + b'i = (a + a') + (b + b')i, \quad (a + bi) \cdot (a' + b'i) = aa' - bb' + (ab' + a'b)i.$$

Summen und Produkte von der Form $a + bi$ lassen sich also wieder in diese Form sortieren. Was soll aber

$$\frac{1}{3 + 4i}$$

darstellen? Wir stellen zunächst fest: $(3 + 4i)(3 - 4i) = 9 + 16 = 25$ (binomische Formel und $i^2 = -1$). Jetzt erweitern wir den Bruch

$$\frac{1}{3 + 4i} = \frac{3 - 4i}{(3 + 4i)(3 - 4i)} = \frac{3 - 4i}{25} = \frac{3}{25} - \frac{4}{25}i.$$

Das funktioniert auch allgemein, falls a oder b ungleich 0:

$$(a + bi)(a - bi) = a^2 + b^2, \quad \frac{1}{a + ib} = \frac{a - ib}{(a + bi)(a - bi)} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i.$$

Definition 4.9 Die Ausdrücke von der Form $a + bi$ mit $a, b \in \mathbb{R}$ heißen **komplexe Zahlen**. Bez: \mathbb{C} .

Mit der oben beschriebenen Addition und Multiplikation bildet \mathbb{C} einen Körper.

Ist $z =: a + bi \in \mathbb{C}$, so heißt a der Realteil der Zahl, b der Imaginärteil.

Die Zahl $a - ib =: \bar{z}$ heißt die zu z konjugiert komplexe Zahl.

Die reellen Zahlen kann man in natürlicher Weise als Teilmenge von \mathbb{C} auffassen, das sind die Zahlen mit Imaginärteil = 0. Gerechnet wurde mit Wurzeln aus negativen Zahlen bereits im 15. Jahrhundert, wobei offen blieb, was man sich darunter vorzustellen hatte, man ging einfach formal damit um – so wie wir es zu Beginn ja auch getan haben. Der Begriff „imaginäre“ Zahlen (1637) stammt von Descartes, dem Erfinder des kartesischen Koordinatensystems. Bei ihm war das allerdings ein abwertender Begriff, ihm waren allerdings auch negative Zahlen suspekt, die von den Mathematikern seiner Zeit längst akzeptiert wurden.

Wie kann man sich komplexe Zahlen veranschaulichen? Hieran versuchten sich in der zweiten Hälfte des 18. Jahrhunderts eine Reihe von Amateurmathematikern, die aber allesamt nicht so ganz ernst genommen wurden. Erst dem Mathematiker Carl Friedrich

Gauss gelang es, die geometrische Interpretation der komplexen Zahlen durchzusetzen – er führte auch 1831 den Begriff „komplexe“ Zahlen ein.

Eine Zahl $z = a + bi$ kann man sich als Punkt in der Ebene mit den Koordinaten (a, b) vorstellen, die Addition als Vektoraddition, (*Bildchen in der Vorlesung*), Multiplikation von z mit einer Zahl \tilde{z} als Drehstreckung.

Wie wir schon gesehen haben, ist für $z = a + bi$

$$z \cdot \bar{z} = a^2 + b^2 \Rightarrow \sqrt{a^2 + b^2} = \text{Abstand des Punktes } z \text{ von } 0.$$

Definition 4.10 (Weierstraß) Die Zahl $|z| = \sqrt{z\bar{z}}$ heißt **Betrag von z** .

Aus der Definition folgt sofort für den Betrag die Rechenregel: Sind $z, w \in \mathbb{C}$, so gilt:

$$|zw| = \sqrt{zw\bar{z}\bar{w}} = \sqrt{z\bar{z}w\bar{w}} = |z||w|.$$

Wird $z = a + bi$ durch einen Punkt mit den kartesischen Koordinaten (a, b) dargestellt, so kann man daraus auch die Polarkoordinatendarstellung ablesen, ist nämlich φ der von der positiven reellen Achse und der Strecke $(0, 0), (a, b)$ eingeschlossene Winkel, so ist

$$a = |z| \cos \varphi, b = |z| \sin \varphi, \text{ also } z = |z|(\cos \varphi + i \sin \varphi).$$

Hieraus erhalten wir: Ist $z = |z|(\cos \varphi + i \sin \varphi)$, $w = |w|(\cos \alpha + i \sin \alpha)$, so gilt mit Hilfe der Additionstheoreme für die Winkelfunktionen (siehe Abschnitt 3.3 über Drehgruppen)

$$\begin{aligned} zw &= |z|(\cos \varphi + i \sin \varphi)|w|(\cos \alpha + i \sin \alpha) \\ &= |z||w| \left(\cos \varphi \cos \alpha - \sin \varphi \sin \alpha + i(\cos \varphi \sin \alpha + \sin \varphi \cos \alpha) \right) \\ &= |z||w|(\cos(\varphi + \alpha) + i \sin(\varphi + \alpha)). \end{aligned}$$

Fazit: Beim Multiplizieren zweier komplexer Zahlen werden die Beträge multipliziert und die Winkel addiert, wobei der Winkel hier im Bogenmaß genommen wird.

Weiterhin erhalten wir für $\frac{1}{z}$:

$$\frac{1}{z} = \frac{1}{z\bar{z}} = \frac{\bar{z}}{|z|^2} = \frac{1}{|z|} \left(\frac{a}{|z|} - i \frac{b}{|z|} \right) = \frac{1}{|z|}(\cos \varphi - i \sin \varphi) = \frac{1}{|z|}(\cos(-\varphi) + i \sin(-\varphi)).$$

Geometrisch bedeutet das: Wir nehmen den Vektor mit Betrag $1/|z|$ und Winkel φ und spiegeln ihn an der reellen Achse.

Eine Potenz einer komplexen Zahl hat somit die Form: $z^n = |z|^n(\cos(n\varphi) + i(\sin n\varphi))$, das gilt für alle $n \in \mathbb{Z}$ Geometrisch betrachtet, liegen diese Zahlen auf Spiralen.

Bildchen in der Vorlesung.

Betrachten wir noch folgendes Beispiel mit einer Zahl vom Betrag 1:

$$z = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i \Leftrightarrow z = \cos \frac{\pi}{4} + i \sin \frac{\pi}{4},$$

Wir erhalten

$$z^n = \cos \frac{n\pi}{4} + i \sin \frac{n\pi}{4}.$$

Da aber $\cos \alpha = \cos(\alpha + 2\pi)$, entsprechend beim sin, erhalten wir hier

$$z^n = z^m, \text{ falls } m \equiv n \pmod{8},$$

denn z.B ist $\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} = \cos(\frac{\pi}{4} + \frac{8\pi}{4}) + i \sin(\frac{\pi}{4} + \frac{8\pi}{4})$. Die Zahl $\cos \frac{\pi}{4} + i \sin \frac{\pi}{4}$ erzeugt beim Potenzieren eine zyklische Gruppe der Ordnung 8, da der Betrag hier immer erhalten bleibt. Beachte: $(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4})^8 = \cos \frac{8\pi}{4} + i \sin \frac{8\pi}{4} = 1 + 0i = 1$ Wir erhalten also eine Darstellung der Drehgruppe $D_{\pi/4}$ (vergl. Abschnitt 3.3)

Wie zieht man jetzt Wurzeln aus einer komplexen Zahl?

Beispiel: Gesucht ist $w \in \mathbb{C}$ mit $w^2 = z := -3 + 4i$. Hier gilt $|z| = 5$, $\cos \varphi = -3/5$, also $\varphi = \arccos \frac{5}{\sqrt{29}} \approx 2.214297436$. Für das gesuchte w muss gelten: $|w|^2 = 5$, also $|w| = \sqrt{5}$. Für den Winkel kommt man auf jeden Fall mit $\varphi_w = \varphi/21.107148718$ weiter, aber auch mit $\tilde{\varphi}_w = \varphi/2 + \pi$, denn es gilt:

$$\cos(2\varphi_w) = \cos(2\tilde{\varphi}_w), \quad \sin(2\varphi_w) = \sin(2\tilde{\varphi}_w).$$

Addieren wir noch ein π , so erhalten wir wieder $\varphi_w (= \varphi_w + 2\pi)$. Allgemein stellen wir fest:

Zu jeder Zahl $z \in \mathbb{C}$ mit $z \neq 0$ gibt es genau zwei $w \in \mathbb{C}$ mit $w^2 = z$, in Polarkoordinaten:

$$\begin{aligned} z &= |z|(\cos \varphi + i \sin \varphi) \Rightarrow w_1 = \sqrt{|z|}(\cos \varphi/2 + i \sin \varphi/2), \\ &= \sqrt{|z|}(\cos(\varphi/2 + \pi) + i \sin(\varphi/2 + \pi)) \\ &= \sqrt{|z|}(-\cos \varphi/2 - i \sin \varphi/2) = -w_1. \end{aligned}$$

Hat man speziell $z = -a$, $a \in \mathbb{R}$, $a > 0$, so ist $z = a(\cos \pi + i \sin \pi)$, somit erhalten wir auch über diese Formel die beiden Wurzeln aus $-a$

$$w_1 = \sqrt{a}(\cos \frac{\pi}{2} + i \sin \frac{\pi}{2}), w_2 = \sqrt{a}(\cos \frac{3\pi}{2} + i \sin \frac{3\pi}{2}), \text{ also } \sqrt{-a} = \pm i\sqrt{a}.$$

Wie funktioniert das mit $\sqrt[n]{z}$?

In \mathbb{C} ist man jetzt endültig alle Sorgen mit Nullstellen von Polynomen los, es gilt nämlich der

Satz 4.11 Fundamentalsatz der Algebra *Alle quadratischen Gleichungen besitzen genau zwei Lösungen in \mathbb{C} , wobei die Lösungen doppelt vorkommen können, d.h. man kann den quadratischen Term immer zerlegen in*

$$x^2 + px + q = (x - z_1)(x - z_2), \text{ mit } z_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q},$$

*($z_1 = z_2$ ist zulässig, man spricht dann von einer doppelten Nullstelle des Polynoms.)
Allgemein: Ein Polynom n -ter Ordnung besitzt immer n Nullstellen.*