Kapitel A

Aufbau des Zahlensystems

Mathematics teaches us not so much
what to think, but how to think!

(anonyme Weisheit)

Inhalt dieses Kapitels A

Ein einführendes Beispiel

Aufgabe: (Tomatensalat, Aufgabe für Klasse 5, DIE ZEIT 15.10.2020)

Eine Gemüsehändlerin kauft im Großmarkt 150kg *Tomaten für* $2€/\text{kg}$*. In ihrem Laden verkauft sie Packungen zu* 500g*, am ersten Tag für* $2€$*, am zweiten Tag für* $1.60€$*. (a) Übrig bleiben* 12kg*. Wie viele Packungen hat die Händlerin verkauft? (b) Die Händlerin macht* $220€$ *Gewinn. Wie viele Packungen hat sie zu* $2€$ *verkauft, wie viele zu* $1.60€$*?*

Wie gehen Sie diese Frage an? Wie formulieren Sie Ihren Lösungsweg? Es gibt viele kreative Lösungsmöglichkeiten, probieren Sie es selbst! Mögliche Werte x, y raten und prüfen? als Schleife programmieren? Graphisch als Schnittpunkt von zwei Geraden in der x–y–Ebene?

Eine bewährte, universelle Methode sind lineare Gleichungssysteme:

$$\left\{\begin{array}{rcrcl} 0.5x & + & 0.5y & = & 138 \\ 2.0x & + & 1.6y & = & 520 \end{array}\right.$$

 Mit einer guten Methode gelingt die Rechnung leicht und routiniert. Mathematische Abstraktion hilft, strukturiert und vereinfacht!

Ein einführendes Beispiel

Lösung mit einem allgemeinen Verfahren: der Gauß–Algorithmus!

$$\left\{\begin{array}{rcrcl} 0.5x & + & 0.5y & = & 138 \\ 2.0x & + & 1.6y & = & 520 \end{array}\right.$$

Zeilenoperation $R_1 \leftarrow 2R_1$, multipliziere Zeile 1 mit dem Faktor 2.

$$\left\{\begin{array}{rcrcl} x & + & y & = & 276 \\ 2.0x & + & 1.6y & = & 520 \end{array}\right.$$

Zeilenoperation $R_2 \leftarrow R_2 - 2R_1$, addiere (-2) mal Zeile 1 zu Zeile 2:

$$\left\{\begin{array}{rcrcl} x & + & y & = & 276 \\ & - & 0.4y & = & -32 \end{array}\right.$$

Zeilenoperation $R_2 \leftarrow (-0.4)^{-1}R_2$, multipliziere Zeile 2 mit -2.5.

$$\left\{\begin{array}{rcrcl} x & + & y & = & 276 \\ & & y & = & 80 \end{array}\right.$$

Zeilenoperation $R_1 \leftarrow R_1 - R_2$, addiere (-1) mal Zeile 2 zu Zeile 1:

$$\left\{\begin{array}{rcrcl} x & & & = & 196 \\ & & y & = & 80 \end{array}\right.$$

Motivation und Vorgehensweise

Wir wollen lineare Gleichungssysteme in voller Allgemeinheit verstehen, mit beliebigen, endlichen Anzahlen von Unbekannten und Gleichungen. Das ist der algebraische Ursprung der Linearen Algebra, zusammen mit der analytischen Geometrie: Wir rechnen systematisch in Koordinaten!

Dazu gehören zunächst die folgenden grundlegenden Fragen:

0. Wo liegen die Koeffizienten? Wo suchen wir die Lösungen?
   Welche arithmetischen Operationen stehen uns zur Verfügung?
1. Was genau ist ein lineares Gleichungssystem, ganz allgemein?
   Wie können wir es präzise definieren und effizient codieren?
2. Wie können wir systematisch alle Lösungen berechnen?
   Wie aufwändig ist diese algorithmische Berechnung?
3. Wie viele Lösungen gibt es? Welche Kriterien helfen uns hier?
   Gibt es mindestens eine Lösung? Gibt es höchstens eine Lösung?

Die Fragen 1,2,3 klären wir detailliert im nächsten Kapitel B.
In diesem ersten Kapitel A werden wir zunächst Frage 0 klären. . .

Motivation und Vorgehensweise

In praktischen Anwendungen sind Gleichungssysteme oft sehr groß. Wir müssen dabei den Überblick behalten und systematisch vorgehen.

Es lohnt sich, Mathematik zu verstehen, statt planlos herumzurechnen. Theoretische Grundlagen bereiten den Weg zur effizienten Anwendung.

Die nötigen Begriffe und Methoden werden uns schnell in luftige Höhen führen. Abstraktion ist hilfreich und effizient, gute Beispiele aber auch!

Aus der Erfahrung zahlreicher Beispiele wie dem obigen wissen wir: Zur Formulierung eines linearen Gleichungssystems benötigen wir Addition und Multiplikation, zur Lösung zudem Subtraktion und Division.

Grundlage der Linearen Algebra sind daher die vier Grundrechenarten: Addition $(a,b) \mapsto a+b$ und Multiplikation $(a,b) \mapsto a \cdot b$, sowie ihre Umkehrungen Negation $a \mapsto -a$ und Inversion $a \mapsto a^{-1}$.

Wir wollen daher zuerst diese vier Grundrechenarten klären!
Die mathematischen Begriffe hierzu sind **Ringe und Körper**.

Motivation und Vorgehensweise

Wir haben einen gemeinsamen Weg vor uns, steil doch wunderschön.
Bitte haben Sie Geduld (mit sich & uns) und Vertrauen (in uns & sich)!

Geben Sie sich zu Beginn Ihres Studiums eine faire Chance auf Erfolg:
kooperativ und kommunikativ, offen und neugierig, ehrlich und fleißig.

Es ist wie in der Grundschule, als Sie Lesen und Schreiben lernten.
Auch das benötigt Geduld und Vertrauen. Und nützt ein Leben lang!

☹ *„Bevor ich meine Zeit mit diesem sogenannten A verschwende, will ich erst mal wissen, wozu dieses A überall gebraucht wird!“*

☹ *„Dieses A ist nur ein theoretisches Detail für Spezialisten, in der Wirklichkeit da draußen benötigt das niemand.“*

Über das Lesen und Schreiben und seinen Nutzen hört man das selten, über das Mathematik-Lernen hingegen allzu oft. Das ist nicht recht.

☺ Widerstehen Sie engstirniger Ungeduld und ignoranten Vorurteilen.
Pflegen Sie Ihre angeborene Neugier und Ihre Freude am Lernen!

Motivation und Vorgehensweise

James Montgomery Flagg, Library of Congress

Wenn du ein Schiff bauen willst,
lehre deine Leute nicht nur ihr Handwerk,
sondern erwecke ihre Sehnsucht nach dem Meer!

Was sind und was sollen die Zahlen?

Seit Urzeiten nutzen Menschen Zahlen und entwickeln das Rechnen.
Doch was genau sind Zahlen? Und woher kommen die Rechenregeln?

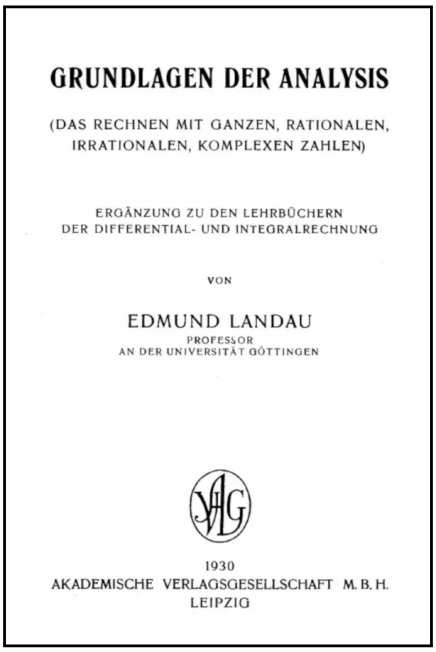

RICHARD DEDEKIND

Was sind und was sollen die Zahlen?

Zehnte Auflage

Stetigkeit und Irrationale Zahlen

Siebente Auflage


GRUNDLAGEN DER ANALYSIS

(DAS RECHNEN MIT GANZEN, RATIONALEN, IRRATIONALEN, KOMPLEXEN ZAHLEN)

ERGÄNZUNG ZU DEN LEHRBÜCHERN DER DIFFERENTIAL- UND INTEGRALRECHNUNG

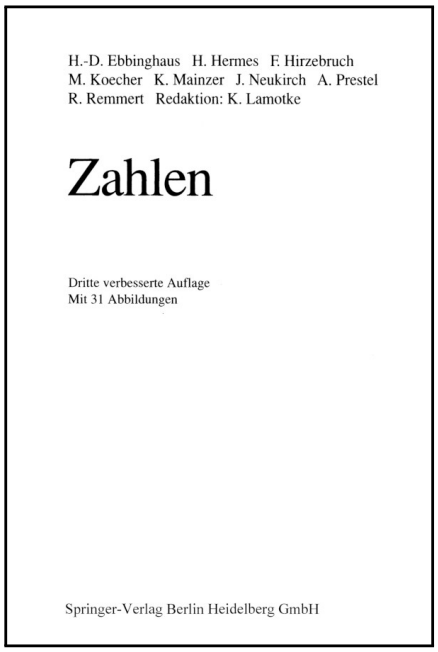
VON

EDMUND LANDAU

PROFESSOR AN DER UNIVERSITÄT GÖTTINGEN

1930

AKADEMISCHE VERLAGSGESELLSCHAFT M. B. H. LEIPZIG


H.-D. Ebbinghaus H. Hermes F. Hirzebruch
M. Koecher K. Mainzer J. Neukirch A. Prestel
R. Remmert Redaktion: K. Lamotke

Zahlen

Dritte verbesserte Auflage
Mit 31 Abbildungen

Springer-Verlag Berlin Heidelberg GmbH

Bitte vergiss alles, was Du auf der Schule gelernt hast; denn Du hast es nicht gelernt. Bitte denke bei allem an die entsprechenden Stellen des Schulpensums; denn Du hast es doch nicht vergessen. (Landau, Vorwort für den Lernenden)

Was sind und was sollen die Zahlen?

Solide Grundlagen. Allen Studierenden der Mathematik empfehle ich, lieber früher als später, den Aufbau des Zahlensystems zu studieren.

Richard Dedekind hat sich schon 1888 sehr gründlich mit dem Aufbau der natürlichen Zahlen $\mathbb{N}$ und ihrer Arithmetik auseinandergesetzt. Als logische Grundlage für sein Unterfangen nutzte er gewinnbringend die damals gerade entstehende Mengenlehre. Diese trägt bis heute!

Edmund Landaus Lehrbuch von 1930 ist ein Klassiker. Hier wurde zum ersten Mal der Aufbau des Zahlensystems von den natürlichen Zahlen zu den rationalen, den reellen und schließlich den komplexen Zahlen systematisch und präzise ausgeführt. Es ist berühmt für Landaus (selbst so genannten) „unbarmherzigen Telegrammstil“ und oft zitiert dank seiner beiden prägnanten Vorworte „Vorwort für den Lernenden“ und „Vorwort für den Kenner“. Landaus Büchlein ist nach wie vor erhellend!

Beide Klassiker sind in kommentierten Neuauflagen gut zugänglich. Heutige Studierende finden vielleicht neuere Lehrbücher sympathischer. Ich empfehle das wunderschöne Buch *Zahlen* von Ebbinghaus *et al.*

Aufbau des Zahlensystems $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$

Die Grundlage aller Mathematik ist das Zahlensystem:

natürliche Zahlen	$\mathbb{N} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \dots \}$
ganze Zahlen	$\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$
rationale Zahlen	$\mathbb{Q} = \{ z/n \mid z, n \in \mathbb{Z},\ n \neq 0 \}$
reelle Zahlen	$\mathbb{R} =$ „$\mathbb{Q}$ und alle Grenzwerte“
komplexe Zahlen	$\mathbb{C} = \{ x + \mathrm{i}y \mid x, y \in \mathbb{R} \}$

Wie erklären / definieren / konstruieren wir diese Zahlbereiche?

P Pia, die pragmatische Physikerin: „Wie kann ich damit *rechnen*? Ich will Modelle und Werkzeuge, die meine Experimente beschreiben.“

I Ida, die innovative Informatikerin: „Wie *implementiere* ich Elemente und Operationen in jedem dieser Bereiche korrekt und effizient?“

L Lea, die lernbegeisterte Lehrerin: „Wie kann ich das gut *verstehen* und *vermitteln*, mathematisch korrekt und didaktisch geschickt?“

M Mia, die methodische Mathematikerin: „Wie kann ich diese Objekte definieren und konstruieren und ihre Eigenschaften *beweisen*?“

Aufbau des Zahlensystems $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$

Aller Anfang ist schwer! Das gilt besonders für Ihr Mathematikstudium. Glücklicherweise ist es nicht nur Anfang, sondern auch Fortsetzung: Sie haben Vorkenntnisse aus der Schule, darauf bauen wir auf.

In diesem Kapitel werden Sie viele alte Bekannte wiedertreffen, die Sie schon lange kennen, zum Teil seit der Grundschule: Zahlen, ihre Rechenregeln und die Lösung von Gleichungen.

Ausgehend von den natürlichen Zahlen $\mathbb{N}$ konstruieren wir die ganzen Zahlen $\mathbb{Z}$ und die rationalen Zahlen $\mathbb{Q}$. Wir erklären den Polynomring $\mathbb{Q}[X]$ und den Körper $\mathbb{Q}(X)$ der gebrochen-rationalen Funktionen.

Die Sichtweise ist jedoch neu und für Sie vermutlich ungewohnt: Wir verhandeln diese Objekte in mathematisch präziser Sprache. Insbesondere wollen wir Eigenschaften und Rechenregeln beweisen.

Das ist anfangs etwas mühsam, bietet aber wunderbar Lernmaterial. Zudem bietet es konkrete Anschauung für spätere Abstraktionen. Die Ideen, Begriffe und Techniken werden wir später erneut aufgreifen und vertiefen. Hier will ich die prominentesten Akteure vorstellen.

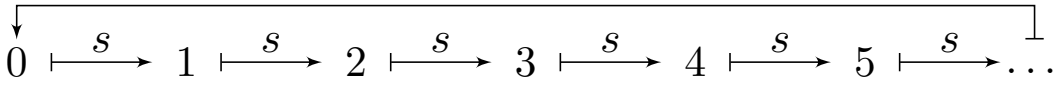
Die natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

Anschaulich: Die natürlichen Zahlen $\mathbb{N}$ nutzen wir zum Zählen gemäß

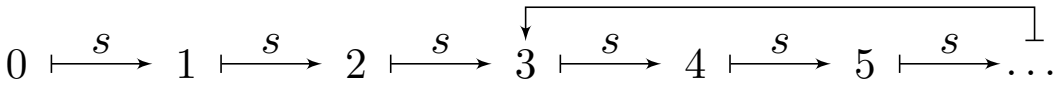
$$0 \overset{s}{\longmapsto} 1 \overset{s}{\longmapsto} 2 \overset{s}{\longmapsto} 3 \overset{s}{\longmapsto} 4 \overset{s}{\longmapsto} 5 \overset{s}{\longmapsto} \ldots$$

Die Abbildung $s : \mathbb{N} \to \mathbb{N}$ ordnet jeder Zahl n ihre Nachfolgerin $s(n)$ zu.
Ist damit alles klar? Aber nein, das Problem liegt in den drei Pünktchen!
Wir müssen unmissverständlich definieren, wie es weitergehen soll.

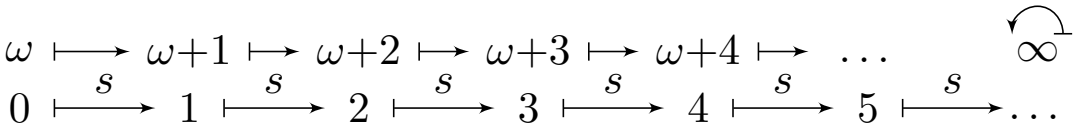
Der Zählprozess startet bei 0 und durchläuft jede Zahl genau einmal.
Situationen wie die folgenden wollen wir also ausschließen:



¬D0



¬D1



¬D2

Die natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

Auf diese Weise können wir beliebig viele Beispiele vorführen, aber eben nur endlich viele! Wie beschreiben wir *alle* natürlichen Zahlen?

Drei kleine Pünktchen sind bequem und berüchtigt, gar gefährlich.
Sie haben eine völlig andere Bedeutung in folgenden Kontexten:

- „Die Jahreszeiten sind Frühling, Sommer, Herbst, Winter, . . . “
- „Die Wochentage sind Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, . . . “ und immer so weiter?!?

Vielleicht sagen Sie: „Das ist doch Haarspalterei! Ich weiß doch wie es weitergeht.“ Wirklich? Ich glaube nicht, dass wir Menschen weit blicken.

Auf 8-Bit-Computern gilt $s(255) = 0$, auf 16-Bit-Computern $s(65535) = 0$, auf 32-Bit-Computern $s(4294967295) = 0$. Das ist ein reales Problem.
Da die meisten Menschen nicht so weit zählen oder vorausschauen, würden sie keinen Unterschied vermuten. Doch wehe dem Überlauf!
Das ist keine Haarspalterei, sondern ein gefürchteter Programmierfehler.
Wir erinnern uns an das Jahr-2000-Problem oder das vermeintliche Weltende 2012 laut Maya-Kalender. Soviel zu den Pünktchen „. . . “.

Die natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

Wir müssen also immer neue Zahlen generieren, ohne Wiederholung!
Das ist keineswegs selbstverständlich, wie Sie aus Kindertagen wissen.

Wie sehen konkrete Modelle aus? Am elegantesten ist das Binärsystem.
Wir nutzen die Ziffern 0 und 1 und bilden damit endliche Zeichenketten:

$$0 \mapsto 1 \mapsto 10 \mapsto 11 \mapsto 100 \mapsto 101 \mapsto 110 \mapsto 111 \mapsto 1000 \mapsto \ldots$$

Führende Nullen dürfen dabei beliebig ergänzt oder gelöscht werden.
Die Nachfolgerabbildung ist $s(*0) = *1$ und $s(*01\ldots1) = *10\ldots0$

Genauso gelingt dies im vertrauten Dezimalsystem, zur Basis Zehn:

$$\begin{aligned}
0 &\mapsto 1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 6 \mapsto 7 \mapsto 8 \mapsto 9 \mapsto \\
10 &\mapsto 11 \mapsto 12 \mapsto 13 \mapsto 14 \mapsto 15 \mapsto 16 \mapsto 17 \mapsto 18 \mapsto 19 \mapsto \\
20 &\mapsto 21 \mapsto 22 \mapsto 23 \mapsto \quad \ldots \quad \mapsto 97 \mapsto 98 \mapsto 99 \mapsto \\
100 &\mapsto 101 \mapsto 102 \mapsto 103 \mapsto \ldots
\end{aligned}$$

Hier lautet die Regel entsprechend: Erhöhe die letzte Ziffer wie in der ersten Zeile gezeigt, bei Übertrag $*9 \mapsto *0$ erhöhe die Ziffer davor, usw.

Die natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

So können wir immer neue Zahlen generieren, ohne Wiederholung.
Beispiele und Gegenbeispiele wie die obigen illustrieren eindringlich:
Selbst bei einfachen Definitionen benötigen wir Sorgfalt und Präzision!

Die drei kleinen Pünktchen „. . . “ sind meist das extreme Gegenteil:
Sind sich Sender und Empfänger einig, so ist das kein Problem.
Aber diese Hoffnung ist oft keine belastbare Vereinbarung!

Die Auslassung ist oft bequem als erste Idee, das hilft manchmal, und so habe ich es oben genutzt. Oft jedoch stecken dahinter weniger edle Motive: An solchen Stellen hat der Autor die redliche Mühe gescheut und überlässt dies dem Leser oder der Phantasie jedes einzelnen.

In obigen Modellen habe ich daher den Zählprozess s explizit erklärt.
Auch über Ziffern und endliche Zeichenketten können wir noch genauer nachdenken, aber darin liegt keine grundsätzliche Schwierigkeit mehr.

Beide Modelle sind übrigens *isomorph*: Es gibt eine Übersetzung von Binär in Dezimal und zurück, sodass keine Information verloren geht:
Es genügt, beide Zählprozesse parallel laufen zu lassen. (Satz F2C)

Rechenoperationen für natürliche Zahlen

Die drei Daten $(\mathbb{N}, 0, s)$ erfüllen die **Dedekind–Peano–Axiome**:

- D0: Null ist kein Nachfolger: $0 \notin s(\mathbb{N})$, also $\forall n \in \mathbb{N} : s(n) \neq 0$.
- D1: Die Abbildung s ist injektiv: $\forall p, q \in \mathbb{N} : p \neq q \Rightarrow s(p) \neq s(q)$.
  Äquivalent hierzu: $\forall p, q \in \mathbb{N} : s(p) = s(q) \Rightarrow p = q$.
- D2: Prinzip der **vollständigen Induktion**: Vorgelegt sei $E \subseteq \mathbb{N}$ mit $0 \in E$, und für jedes $n \in E$ gilt $s(n) \in E$. Dann gilt bereits $E = \mathbb{N}$.

Dies definiert eindeutig, was wir unter dem Zählprozess verstehen.

Definition A1A: Rechenoperationen für natürliche Zahlen

Hieraus konstruieren wir rekursiv Addition, Multiplikation und Potenz:

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (a, b) \mapsto a + b, \quad a + 0 := a, \quad a + s(n) := s(a + n)$$

$$\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (a, b) \mapsto a \cdot b, \quad a \cdot 0 := 0, \quad a \cdot s(n) := (a \cdot n) + a$$

$$\hat{} : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (a, b) \mapsto a^b, \quad a^0 := 1, \quad a^{s(n)} := a^n \cdot a$$

Damit gilt $s(n) = n + 1$, denn $n + 1 \overset{\text{Def}}{=} n + s(0) \overset{\text{Def}}{=} s(n + 0) \overset{\text{Def}}{=} s(n)$.

Rechenoperationen für natürliche Zahlen

Übung: Berechnen Sie so das kleine Einmaleins, zuvor Einspluseins.

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	10
2	2	3	4	5	6	7	8	9	10	11
3	3	4	5	6	7	8	9	10	11	12
4	4	5	6	7	8	9	10	11	12	13
5	5	6	7	8	9	10	11	12	13	14
6	6	7	8	9	10	11	12	13	14	15
7	7	8	9	10	11	12	13	14	15	16
8	8	9	10	11	12	13	14	15	16	17
9	9	10	11	12	13	14	15	16	17	18

·	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	10	12	14	16	18
3	0	3	6	9	12	15	18	21	24	27
4	0	4	8	12	16	20	24	28	32	36
5	0	5	10	15	20	25	30	35	40	45
6	0	6	12	18	24	30	36	42	48	54
7	0	7	14	21	28	35	42	49	56	63
8	0	8	16	24	32	40	48	56	64	72
9	0	9	18	27	36	45	54	63	72	81

Die rekursive Rechnung ist etwas gewöhnungsbedürftig, aber lehrreich. Genau so haben Sie es in der Grundschule gelernt! Dort natürlich an Beispielen ohne Definition. Hier sehen Sie, was genau dahinter steckt. Zudem erkennen wir erste Rechenregeln wie die Kommutativität...

Rechenregeln für natürliche Zahlen

Die Addition erfreut sich folgender Eigenschaften für alle $a, b, c \in \mathbb{N}$:

Kommutativität,	**Com**$(\mathbb{N}, +)$:	$a + b = b + a$
Assoziativität,	**Ass**$(\mathbb{N}, +)$:	$(a + b) + c = a + (b + c)$
Neutrales,	**Ntr**$(\mathbb{N}, +, 0)$:	$0 + a = a$ und $a + 0 = a$

Wir sagen dazu: $(\mathbb{N}, +, 0)$ ist ein **kommutatives Monoid**.

Die Multiplikation erfreut sich folgender Eigenschaften für alle $a, b, c \in \mathbb{N}$:

Kommutativität,	**Com**$(\mathbb{N}, \cdot)$:	$a \cdot b = b \cdot a$
Assoziativität,	**Ass**$(\mathbb{N}, \cdot)$:	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
Neutrales,	**Ntr**$(\mathbb{N}, \cdot, 1)$:	$1 \cdot a = a$ und $a \cdot 1 = a$

Wir sagen dazu: $(\mathbb{N}, \cdot, 1)$ ist ein **kommutatives Monoid**.

Die Multiplikation ist distributiv über die Addition für alle $a, b, c \in \mathbb{N}$:

Distributivität links,	**DL**$(\mathbb{N}, +, \cdot)$:	$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
Distributivität rechts,	**DR**$(\mathbb{N}, +, \cdot)$:	$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

☺ Dies sind acht grundlegende und vertraute Rechenregeln.
Wir sagen dazu: $(\mathbb{N}, +, 0, \cdot, 1)$ ist ein **kommutativer Halbring**.

Rechenregeln für natürliche Zahlen

Darauf beruhen alle Rechenverfahren, die Sie aus der Schule kennen. Solide Begründung und effiziente Handhabung der natürlichen Zahlen sind keineswegs leicht oder gar selbstverständlich. Stellenschreibweise und zugehörige Rechenverfahren sind monumentale Erfindungen; die Menschheit hat dafür ein paar Jahrtausende intellektuelle Entwicklung benötigt. Die erfreuliche Tatsache, dass Sie dies seit der Grundschule kennen und nutzen, darf Sie nicht über die Raffinesse hinwegtäuschen.

By relieving the brain of all unnecessary work, a good notation sets it free to concentrate on more advanced problems [...] Before the introduction of the Arabic notation, multiplication was difficult, and the division of integers called into play the highest mathematical faculties. Probably nothing in the modern world would have more astonished a Greek mathematician than to learn that, under the influence of compulsory education, a large proportion of the population of Western Europe could perform the operation of division for the largest numbers. Our modern power of easy reckoning with decimal fractions is the almost miraculous result of the gradual discovery of a perfect notation.

Alfred North Whitehead (1861–1947), *An Introduction to Mathematics* (1911)

Der Halbring $(\mathbb{N}, +, 0, \cdot, 1)$ der natürlichen Zahlen

Satz A1B: Eigenschaften der natürlichen Zahlen

Die natürlichen Zahlen $(\mathbb{N}, +, 0, \cdot, 1)$ sind ein kommutativer Halbring.

Als charakteristische Eigenschaft erfüllt die Nachfolgerabbildung $s : n \mapsto n + 1$ die zugrundeliegenden **Dedekind–Peano–Axiome**:

- D0: Null ist kein Nachfolger: $0 \notin s(\mathbb{N})$, also $\forall n \in \mathbb{N} : n + 1 \neq 0$.
- D1: Die Abbildung s ist injektiv: $\forall p, q \in \mathbb{N} : p \neq q \Rightarrow p + 1 \neq q + 1$.
- D2: Prinzip der **vollständigen Induktion**: Vorgelegt sei $E \subseteq \mathbb{N}$ mit $0 \in E$, und für jedes $n \in E$ gilt $n + 1 \in E$. Dann gilt bereits $E = \mathbb{N}$.

Die Addition ist kürzbar, das heißt $a + c = b + c$ impliziert $a = b$.
Die Multiplikation ist kürzbar: $a \cdot c = b \cdot c$ und $c \neq 0$ implizieren $a = b$.

Die Potenz erfreut sich folgender Eigenschaften / Potenzgesetze:

$$a^0 = 1 \text{ und } a^1 = a \text{ sowie } a^{m+n} = a^m \cdot a^n \text{ und } a^{m \cdot n} = (a^m)^n.$$

Für alle $n \in \mathbb{N} \setminus \{0\}$ gilt: $a^n = b^n$ impliziert $a = b$.
Für alle $a \in \mathbb{N} \setminus \{0, 1\}$ gilt: $a^m = a^n$ impliziert $m = n$.

Nachweis der Eigenschaften durch vollständige Induktion

Beweis: Alle Behauptungen rechnen wir geduldig nach. Ich zeige dies ausführlich für die Addition, analog gelingen Multiplikation und Potenz.

(1) Zur Assoziativität **Ass**$(\mathbb{N}, +)$ betrachten wir die Erfüllungsmenge

$$E := \left\{ n \in \mathbb{N} \;\middle|\; a + (b + n) = (a + b) + n \text{ für alle } a, b \in \mathbb{N} \right\}.$$

Wir zeigen nun $E = \mathbb{N}$ durch vollständige Induktion.

Induktionsanfang: Es gilt $0 \in E$, denn

$$a + (b + 0) \overset{\text{Def}}{=} a + b \overset{\text{Def}}{=} (a + b) + 0.$$

Induktionsschritt: Gilt $n \in E$, dann auch $s(n) \in E$, denn

$$\begin{aligned} a + (b + s(n)) &\overset{\text{Def}}{=} a + s(b + n) \overset{\text{Def}}{=} s(a + (b + n)) \\ &\overset{n \in E}{=} s((a + b) + n) \overset{\text{Def}}{=} (a + b) + s(n). \end{aligned}$$

Per Induktion gilt $E = \mathbb{N}$. Die Addition $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ ist also assoziativ.

Nachweis der Eigenschaften durch vollständige Induktion

(2) Nach Definition gilt $n + 0 = n$. Wir zeigen nun $0 + n = n$. Hierzu sei

$$E := \{\, n \in \mathbb{N} \mid 0 + n = n \,\}.$$

Wir haben $0 + 0 = 0$, also $0 \in E$. Gilt $n \in E$, dann auch $s(n) \in E$, denn

$$0 + s(n) \overset{\text{Def}}{=} s(0 + n) \overset{n \in E}{=} s(n).$$

Per Induktion gilt $E = \mathbb{N}$. Das Element 0 ist also beidseitig neutral.

(3) Nach Definition gilt $n + 1 = s(n)$. Wir zeigen $1 + n = s(n)$. Hierzu sei

$$E := \{\, n \in \mathbb{N} \mid 1 + n = s(n) \,\}.$$

Es gilt $0 \in E$, denn $1 + 0 = 1 = s(0)$. Gilt $n \in E$, dann auch $s(n) \in E$:

$$1 + s(n) \overset{\text{Def}}{=} s(1 + n) \overset{n \in E}{=} s(s(n)).$$

Per Induktion gilt $E = \mathbb{N}$. Also gilt $1 + n = n + 1$ für alle $n \in \mathbb{N}$.

Nachweis der Eigenschaften durch vollständige Induktion

(4) Zum Beweis der Kommutativität $\mathbf{Com}(\mathbb{N}, +)$ betrachten wir

$$E := \{\, n \in \mathbb{N} \mid a + n = n + a \text{ für alle } a \in \mathbb{N} \,\}.$$

Induktionsanfang: In (2,3) haben wir bereits $0 \in E$ und $1 \in E$ gezeigt.
Induktionsschritt: Gilt $n \in E$, dann auch $s(n) \in E$, denn

$$\begin{aligned} a + s(n) &\overset{\text{Def}}{=} s(a + n) \overset{n \in E}{=} s(n + a) \overset{\text{Def}}{=} n + s(a) \\ &\overset{(3)}{=} n + (1 + a) \overset{(1)}{=} (n + 1) + a \overset{\text{Def}}{=} s(n) + a. \end{aligned}$$

Per Induktion gilt $E = \mathbb{N}$. Also ist die Addition kommutativ.
(5) Zur Kürzbarkeit schließlich betrachten wir

$$E := \{\, n \in \mathbb{N} \mid \text{für alle } a, b \in \mathbb{N} \text{ mit } a + n = b + n \text{ folgt } a = b \,\}$$

Es gilt $0 \in E$. Gilt $n \in E$, dann auch $s(n) \in E$, denn für alle $a, b \in \mathbb{N}$ gilt:

$$a + s(n) = b + s(n) \overset{\text{Def}}{\Longrightarrow} s(a + n) = s(b + n) \overset{\text{Inj}}{\Longrightarrow} a + n = b + n \overset{n \in E}{\Longrightarrow} a = b$$

Per Induktion gilt $E = \mathbb{N}$. Also ist die Addition kürzbar. QED

Von den natürlichen Zahlen $\mathbb{N}$ zu den ganzen Zahlen $\mathbb{Z}$

In $\mathbb{N}$ können wir Gleichungen wie $3 = 5 + x$ formulieren, aber nicht lösen.
Hierzu erweitern wir die natürlichen Zahlen $\mathbb{N}$ zu den ganzen Zahlen

$$\mathbb{Z} = \{\, z = [a-b] \mid a, b \in \mathbb{N} \,\}.$$

Auf dieser Menge $\mathbb{Z}$ vereinbaren wir die folgenden Operationen:

Vergleich:	$[a-b] = [c-d]$ in $\mathbb{Z}$	$\Leftrightarrow$	$a+d = c+b$ in $\mathbb{N}$
Addition:	$[a-b] + [c-d]$	$=$	$[(a+c)-(b+d)]$
Negation:	$-[a-b]$	$=$	$[b-a]$
Multiplikation:	$[a-b] \cdot [c-d]$	$=$	$[(ac+bd)-(ad+bc)]$

Wir haben die Einbettung $\mathbb{N} \hookrightarrow \mathbb{Z} : n \mapsto [n-0]$ und schreiben kurz $\mathbb{N} \subset \mathbb{Z}$.
Genauer gilt $(\mathbb{N}, +_{\mathbb{N}}, \cdot_{\mathbb{N}}) \subset (\mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}})$; alles wird von $\mathbb{N}$ auf $\mathbb{Z}$ fortgesetzt.

Normalform: Für jedes $z \in \mathbb{Z}$ gilt $z = n$ oder $z = -n$ für ein $n \in \mathbb{N}$.

Beispiel: Die Gleichung $3 = 5 + x$ hat keine Lösung $x \in \mathbb{N}$.
In $\mathbb{Z}$ hingegen finden wir die Lösung $x = [3-5] = [0-2] = -2$.

Von den natürlichen Zahlen $\mathbb{N}$ zu den ganzen Zahlen $\mathbb{Z}$

Wir nutzen die Konvention **Punkt vor Strich**, um Klammern zu sparen.
Wo möglich lassen wir meist auch das Produktzeichen weg:

$$(a \cdot c) + (b \cdot d) = ac + bd$$

Die natürlichen Zahlen erweitern wir zu den ganzen Zahlen $\mathbb{Z}$: Addition und Multiplikation setzen wir fort und gewinnen zudem die Negation.

Dies definiert die Operationen, begründet oder motiviert sie aber nicht.
Genau so haben Sie es in der Schule gelernt und erfolgreich genutzt:
„Hier sind die Rechenregeln, damit können Sie arbeiten.“

P „Ok, damit bin ich zufrieden, damit kann ich konkret rechnen.“
I „Zur effizienten Implementierung muss ich noch genauer arbeiten.“
M „Sind unsere Konstruktionen einwandfrei und ohne Widersprüche?“
L „Warum vereinbaren wir diese Operationen? Woher kommen sie?“

Die Motivation erwächst erst aus den folgenden Rechenregeln und dem abschließenden Satz: Wir wollen den Halbring $\mathbb{N}$ zum Ring $\mathbb{Z}$ erweitern.
Dies gelingt auf genau eine Weise, nämlich wie hier gezeigt.

Der Ring $(\mathbb{Z}, +, 0, -, \cdot, 1)$ der ganzen Zahlen

Die Addition erfreut sich folgender Eigenschaften für alle $a, b, c \in \mathbb{Z}$:

Kommutativität,	**Com**$(\mathbb{Z}, +)$:	$a + b = b + a$
Assoziativität,	**Ass**$(\mathbb{Z}, +)$:	$(a + b) + c = a + (b + c)$
Neutrales,	**Ntr**$(\mathbb{Z}, +, 0)$:	$0 + a = a$ und $a + 0 = a$
Negatives,	**Inv**$(\mathbb{Z}, +, 0, -)$:	$(-a) + a = 0$ und $a + (-a) = 0$

Wir sagen dazu: $(\mathbb{Z}, +, 0, -)$ ist eine **kommutative Gruppe**.

Die Multiplikation erfreut sich folgender Eigenschaften für alle $a, b, c \in \mathbb{Z}$:

Kommutativität,	**Com**$(\mathbb{Z}, \cdot)$:	$a \cdot b = b \cdot a$
Assoziativität,	**Ass**$(\mathbb{Z}, \cdot)$:	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
Neutrales,	**Ntr**$(\mathbb{Z}, \cdot, 1)$:	$1 \cdot a = a$ und $a \cdot 1 = a$

Wir sagen dazu: $(\mathbb{Z}, \cdot, 1)$ ist ein **kommutatives Monoid**.

Die Multiplikation ist distributiv über die Addition für alle $a, b, c \in \mathbb{Z}$:

Distributivität links,	**DL**$(\mathbb{Z}, +, \cdot)$:	$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
Distributivität rechts,	**DR**$(\mathbb{Z}, +, \cdot)$:	$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

☺ Dies sind neun grundlegende und vertraute Rechenregeln.
Wir sagen dazu: $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ist ein **kommutativer Ring**.

Der Ring $(\mathbb{Z}, +, 0, -, \cdot, 1)$ der ganzen Zahlen

Jede Gleichung $a = x + b$ mit $a, b \in \mathbb{Z}$ hat genau eine Lösung $x \in \mathbb{Z}$, nämlich $x = a - b$. Zu $a \in \mathbb{Z}$ ist das Negative die Lösung zu $a + x = 0$; somit lässt sich die Negation $a \mapsto -a$ aus $(\mathbb{Z}, +, 0)$ rekonstruieren.

Statt $(\mathbb{Z}, +, 0, -)$ schreiben wir daher auch $(\mathbb{Z}, +, 0)$ oder kurz $(\mathbb{Z}, +)$.
Wie üblich nutzen wir die Abkürzung $a - b = a + (-b)$.

Zusammenfassung unserer Konstruktion:

Satz A1c: Die ganzen Zahlen erweitern die natürlichen Zahlen.

Die ganzen Zahlen $(\mathbb{Z}, +, 0, \cdot, 1)$ sind ein kommutativer Ring mit $\mathbb{Z} \supset \mathbb{N}$.

Genauer gesagt enthält der Ring $(\mathbb{Z}, +, 0, \cdot, 1)$ den Halbring $(\mathbb{N}, +, 0, \cdot, 1)$ und jede ganze Zahl $z \in \mathbb{Z}$ ist eine Differenz $z = a - b$ mit $a, b \in \mathbb{N}$.

Dies ist der einzige Ring mit diesen Eigenschaften.

Die Multiplikation ist kürzbar: $a \cdot c = b \cdot c$ und $c \neq 0$ implizieren $a = b$.
Insbesondere ist $\mathbb{Z}$ nullteilerfrei: Aus $a \neq 0$ und $b \neq 0$ folgt $a \cdot b \neq 0$.

Von den ganzen Zahlen $\mathbb{Z}$ zu den rationalen Zahlen $\mathbb{Q}$

In $\mathbb{Z}$ können wir Gleichungen wie $3 = 6 \cdot x$ formulieren, aber nicht lösen.
Hierzu erweitern wir die ganzen Zahlen $\mathbb{Z}$ zu den rationalen Zahlen

$$\mathbb{Q} = \{\, q = [a/b] \mid a, b \in \mathbb{Z},\ b \neq 0 \,\}.$$

Auf dieser Menge $\mathbb{Q}$ vereinbaren wir die folgenden Operationen:

Vergleich:	$[a/b] = [c/d]$ in $\mathbb{Q}$	$\Leftrightarrow$	$ad = cb$ in $\mathbb{Z}$
Addition:	$[a/b] + [c/d]$	$=$	$[(ad + cb)/(bd)]$
Negation:	$-[a/b]$	$=$	$[-a/b]$
Multiplikation:	$[a/b] \cdot [c/d]$	$=$	$[(ac)/(bd)]$
Inversion:	$[a/b]^{-1}$	$=$	$[b/a]$ falls $a \neq 0$

Wir haben die Einbettung $\mathbb{Z} \hookrightarrow \mathbb{Q} : z \mapsto [z/1]$ und schreiben kurz $\mathbb{Z} \subset \mathbb{Q}$.
Genauer gilt $(\mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}) \subset (\mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}})$; alles wird von $\mathbb{Z}$ auf $\mathbb{Q}$ fortgesetzt.

Normalform: Für $q \in \mathbb{Q}$ gilt $q = [a/b]$ mit $\operatorname{ggT}(a, b) = 1$ und $b \geq 1$;
dies nennen wir die Darstellung von q als gekürzten Bruch.

Beispiel: Die Gleichung $3 = 6 \cdot x$ hat keine Lösung $x \in \mathbb{Z}$.
In $\mathbb{Q}$ hingegen finden wir die Lösung $x = [3/6] = [1/2] = 2^{-1}$.

Von den ganzen Zahlen $\mathbb{Z}$ zu den rationalen Zahlen $\mathbb{Q}$

Die rationalen Zahlen $\mathbb{Q}$ erweitern die ganzen Zahlen $\mathbb{Z}$: Addition und Multiplikation setzen wir fort und gewinnen zudem die Inversion.

Dies definiert die Operationen, begründet oder motiviert sie aber nicht.
Genau so haben Sie es in der Schule gelernt und erfolgreich genutzt:
„Hier sind die Rechenregeln, damit können Sie arbeiten.“

P „Ok, damit bin ich zufrieden, damit kann ich konkret rechnen.“
I „Zur effizienten Implementierung muss ich noch genauer arbeiten.“
M „Sind unsere Konstruktionen einwandfrei und ohne Widersprüche?“
L „Warum vereinbaren wir diese Operationen? Woher kommen sie?“

Die Motivation erwächst erst aus den folgenden Rechenregeln und dem abschließenden Satz: Wir wollen den Ring $\mathbb{Z}$ zum Körper $\mathbb{Q}$ erweitern.
Dies gelingt auf genau eine Weise, nämlich die hier gezeigt.

☺ *Fun fact:* Wir vergleichen die Erweiterungen $\mathbb{N} \hookrightarrow \mathbb{Z}$ und $\mathbb{Z} \hookrightarrow \mathbb{Q}$:
Für Differenzen $[a - b]$ ist die Addition leichter als die Multiplikation.
Für Brüche $[a/b]$ ist die Multiplikation leichter als die Addition.

Der Körper $(\mathbb{Q}, +, 0, -, \cdot, 1, ^{-1})$ der rationalen Zahlen

Die Addition erfreut sich folgender Eigenschaften für alle $a, b, c \in \mathbb{Q}$:

Kommutativität,	**Com**$(\mathbb{Q}, +)$:	$a + b = b + a$
Assoziativität,	**Ass**$(\mathbb{Q}, +)$:	$(a + b) + c = a + (b + c)$
Neutrales,	**Ntr**$(\mathbb{Q}, +, 0)$:	$0 + a = a$ und $a + 0 = a$
Negatives,	**Inv**$(\mathbb{Q}, +, 0, -)$:	$(-a) + a = 0$ und $a + (-a) = 0$

Wir sagen dazu: $(\mathbb{Q}, +, 0, -)$ ist eine **kommutative Gruppe**.

Die Multiplikation erfreut sich folgender Eigenschaften für alle $a, b, c \in \mathbb{Q}$:

Kommutativität,	**Com**$(\mathbb{Q}, \cdot)$:	$a \cdot b = b \cdot a$
Assoziativität,	**Ass**$(\mathbb{Q}, \cdot)$:	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
Neutrales,	**Ntr**$(\mathbb{Q}, \cdot, 1)$:	$1 \cdot a = a$ und $a \cdot 1 = a$
Inverses,	**Inv**$(\mathbb{Q}^*, \cdot, 1, ^{-1})$:	$a \cdot a^{-1} = 1$ und $a^{-1} \cdot a = 1$

Letzteres gilt nur für $a \neq 0$, also für alle $a \in \mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$.
Wir sagen dazu: $(\mathbb{Q}^*, \cdot, 1, ^{-1})$ ist eine **kommutative Gruppe**.

Die Multiplikation ist distributiv über die Addition, es gilt also **DL** und **DR**.

☺ Dies sind zehn grundlegende und vertraute Rechenregeln.
Wir sagen dazu: $(\mathbb{Q}, +, 0, -, \cdot, 1, ^{-1})$ ist ein **Körper**.

Der Körper $(\mathbb{Q}, +, 0, -, \cdot, 1, ^{-1})$ der rationalen Zahlen

Jede Gleichung $a = xb$ mit $a, b \in \mathbb{Q}$, $b \neq 0$ hat genau eine Lösung $x \in \mathbb{Q}$:

$$a = x \cdot b \implies a \cdot b^{-1} = (x \cdot b) \cdot b^{-1} = x \cdot (b \cdot b^{-1}) = x \cdot 1 = x$$
$$x = a \cdot b^{-1} \implies x \cdot b = (a \cdot b^{-1}) \cdot b = a \cdot (b \cdot b^{-1}) = a \cdot 1 = a$$

Zu jedem Element $a \in \mathbb{Q}^*$ ist das Inverse die Lösung zu $a \cdot x = 1$;
somit lässt sich die Inversion $a \mapsto a^{-1}$ aus $(\mathbb{Q}, \cdot, 1)$ rekonstruieren.
Statt $(\mathbb{Q}, \cdot, 1, ^{-1})$ schreiben wir daher auch $(\mathbb{Q}, \cdot, 1)$ oder kurz $(\mathbb{Q}, \cdot)$.
Wie üblich nutzen wir die Abkürzung $a/b = a \cdot b^{-1}$

Zusammenfassung unserer Konstruktion:

Satz A1D: Die rationalen Zahlen erweitern die ganzen Zahlen.

Die rationalen Zahlen $(\mathbb{Q}, +, 0, \cdot, 1)$ sind ein Körper mit $\mathbb{Q} \supset \mathbb{Z}$.

Genauer gesagt enthält der Körper $(\mathbb{Q}, +, 0, \cdot, 1)$ den Ring $(\mathbb{Z}, +, 0, \cdot, 1)$ und jede rationale Zahl $q \in \mathbb{Q}$ ist Quotient $q = z/n$ mit $z, n \in \mathbb{Z}$, $n \neq 0$.

Dies ist der einzige Körper mit den genannten Eigenschaften.

Die vier Grundrechenarten und ihre Rechenregeln

Definition A1E: Ringe und Körper

Wir nennen $(K,+,0,-,\cdot,1,^{-1})$ mit $0\neq 1$ einen **Körper**, wenn die obigen zehn Rechenregeln / Forderungen / Axiome gelten. Für abgeschwächte Forderungen vereinbaren und nutzen wir folgende Bezeichnungen:

Struktur $(K,+,\cdot)$		$(K,+)$				$(K,+,\cdot)$		$(K,\cdot)$			
Name	Beispiele	Ass	Ntr	Inv	Com	DL	DR	Ass	Ntr	Inv*	Com
Körper	$\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}_p$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CRing	$\mathbb{Z},\mathbb{Z}_n,\mathbb{Q}[X]$	✓	✓	✓	✓	✓	✓	✓	✓		✓
DRing	$\mathbb{H}\subset\mathbb{C}^{2\times 2}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Ring	$\mathbb{Z}^{2\times 2}$, $\mathbb{R}^{2\times 2}$	✓	✓	✓	✓	✓	✓	✓	✓		
Rng	$\left(\begin{smallmatrix}\mathbb{R} & \mathbb{R}\\ 0 & 0\end{smallmatrix}\right)$	✓	✓	✓	✓	✓	✓	✓			
KRng	$2\mathbb{Z}$, $\mathscr{C}_c(\mathbb{R})$	✓	✓	✓	✓	✓	✓	✓			✓
Halbkörper	$\mathbb{Q}_{\geq 0}$, $\mathbb{R}_{\geq 0}$	✓	✓		✓	✓	✓	✓	✓	✓	✓
Halbring, Rig	$\mathbb{N}$, $[0,\infty]$	✓	✓		✓	✓	✓	✓	✓		

Die vier Grundrechenarten und ihre Rechenregeln

Körper sind die strengsten und schönsten dieser Strukturen: Hier gelten alle Rechenregeln. Für einen **Divisionsring**, kurz DRing, verzichten wir auf Kommutativität **Com**$(K,\cdot)$ der Multiplikation; auch das kommt vor. Einen nicht-kommutativen Divisionsring nennt man **Schiefkörper**.

Für einen **kommutativen Ring**, kurz CRing, verzichten wir stattdessen auf Invertierbarkeit **Inv**$(K^*,\cdot,1)$ der Multiplikation, noch allgemeiner für einen **Ring** auch auf Kommutativität **Com**$(K,\cdot)$. Ein (kommutativer) Ring $(R,+,0,-,\cdot,1)$ besteht also aus einer kommutativen Gruppe $(R,+,0,-)$ und einem (kommutativen) Monoid $(R,\cdot,1)$ und ist beidseitig distributiv.

Die untere Hälfte der Tabelle dient zur Abrundung nützlicher Begriffe. Uns begegnen öfters „Ringe ohne Eins“, engl. „ring without identity“, daher das Wortspiel **Rng**, für „Ringe ohne Negation“ entsprechend **Rig**.

Auch (nicht/kommutative) Halbkörper treten natürlich auf, etwa $\mathbb{Q}_{\geq 0}$: Hier ist zwar die Multiplikation invertierbar, aber nicht die Addition.

Halbringe sind mit die schwächsten dieser Strukturen. Allerdings sind die natürlichen Zahlen $\mathbb{N}$ sehr wichtig, daher stehen sie hier zu Recht.

Anordnung der ganzen Zahlen

Aufgabe: Wie erklären Sie die Anordnung $\leq$ der natürlichen Zahlen $\mathbb{N}$?

Lösung: Für $a, b \in \mathbb{N}$ definieren wir die Relation $a \leq b$ durch die Bedingung $a + x = b$ für ein $x \in \mathbb{N}$. Damit gilt für alle $a, b, c \in \mathbb{N}$:

Reflexivität,	**Refl**$(\mathbb{N}, \leq)$:	$a \leq a$.
Antisymmetrie,	**Asym**$(\mathbb{N}, \leq)$:	Aus $a \leq b$ und $b \leq a$ folgt $a = b$.
Transitivität,	**Tran**$(\mathbb{N}, \leq)$:	Aus $a \leq b$ und $b \leq c$ folgt $a \leq c$.

Aufgabe: Wie erklären Sie die Anordnung $\leq$ der ganzen Zahlen $\mathbb{Z}$? Was sind die grundlegenden Rechenregeln? Wie beweist man sie?

Lösung: Für $a, b \in \mathbb{Z}$ definieren wir $a \leq b$ durch $b - a \in \mathbb{N}$. Damit gilt $a \leq a$. Aus $a \leq b$ und $b \leq a$ folgt $a = b$. Aus $a \leq b$ und $b \leq c$ folgt $a \leq c$.

Entsprechend definieren wir die Relation $a < b$ durch $a \leq b$ und $a \neq b$. Symmetrisch hierzu schreiben wir $a \geq b$ für $b \leq a$ und $a > b$ für $b < a$.

Damit ist $(\mathbb{Z}, +, \cdot, \leq)$ ein **angeordneter Ring**:
(0) Für je zwei Zahlen $a, b \in \mathbb{Z}$ gilt entweder $a = b$ oder $a < b$ oder $a > b$.
(1) Aus $a \leq b$ folgt $a + c \leq b + c$. (2) Aus $a \leq b$ und $0 \leq c$ folgt $ac \leq bc$.

Anordnung der rationalen Zahlen

Aufgabe: Wie erklären Sie die Anordnung $\leq$ der rationalen Zahlen $\mathbb{Q}$? Was sind die grundlegenden Rechenregeln? Wie beweist man sie?

Lösung: Die Menge der nicht-negativen rationalen Zahlen ist

$$P = \mathbb{Q}_{\geq 0} := \{\, z/n \mid z, n \in \mathbb{N},\ n \neq 0 \,\}.$$

Sie erfüllt $P \cap (-P) = \{0\}$ und $P \cup (-P) = \mathbb{Q}$ sowie $P + P \subseteq P$ und $P \cdot P \subseteq P$, das heißt, aus $a, b \in P$ folgt $a + b \in P$ und $a \cdot b \in P$.

Für $a, b \in \mathbb{Q}$ definieren wir die Relation $a \leq b$ durch $b - a \in P$. Damit gilt $a \leq a$. Aus $a \leq b$ und $b \leq a$ folgt $a = b$. Aus $a \leq b$ und $b \leq c$ folgt $a \leq c$.

Entsprechend definieren wir die Relation $a < b$ durch $a \leq b$ und $a \neq b$. Symmetrisch hierzu schreiben wir $a \geq b$ für $b \leq a$ und $a > b$ für $b < a$.

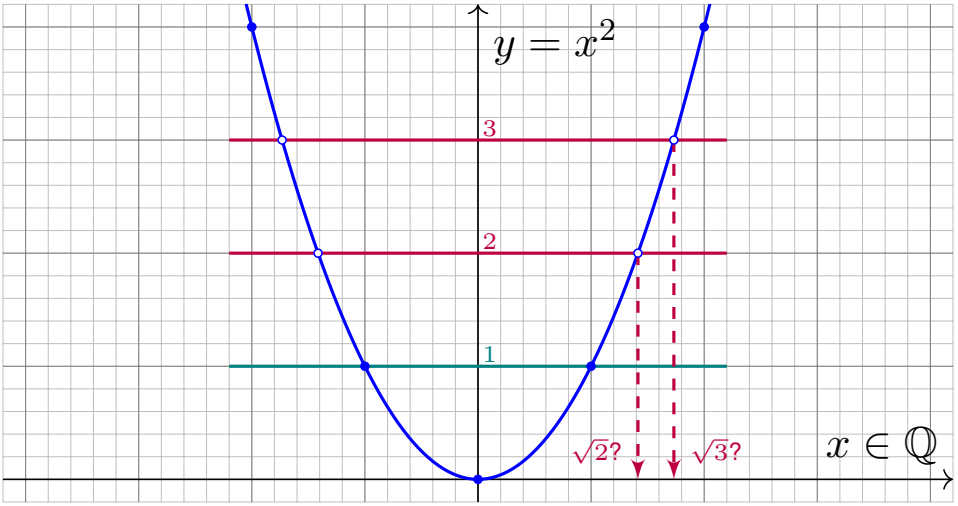
Damit ist $(\mathbb{Q}, +, \cdot, \leq)$ ein **angeordneter Körper**:
(0) Für je zwei Zahlen $a, b \in \mathbb{Q}$ gilt entweder $a = b$ oder $a < b$ oder $a > b$.
(1) Aus $a \leq b$ folgt $a + c \leq b + c$. (2) Aus $a \leq b$ und $0 \leq c$ folgt $ac \leq bc$.

Wir definieren den **Absolutbetrag**

$$|-| : \mathbb{Q} \to \mathbb{Q}_{\geq 0} : x \mapsto |x| = \begin{cases} x & \text{falls } x \geq 0, \\ -x & \text{falls } x \leq 0. \end{cases}$$

Die rationalen Zahlen haben erhebliche Lücken!

In $\mathbb{Q}$ können wir Gleichungen wie $x^2 = 2$ formulieren, aber nicht lösen.



Die Funktion $f : \mathbb{Q} \to \mathbb{Q} : x \mapsto x^2$ trifft die Werte $0 = f(0)$ und $1 = f(\pm 1)$ und $4 = f(\pm 2)$, sogar jeweils zweimal, aber nicht die Werte 2 und 3.

☹ Anschaulich: Der geordnete Körper $(\mathbb{Q}, +, \cdot, \leq)$ hat noch erhebliche Lücken! Diese wollen wir möglichst schließen, je nach Bedarf.

☺ Ideale Lösung ist der Körper $(\mathbb{R}, +, \cdot, \leq)$ der reellen Zahlen (A3A). Doch wir wollen nicht gleich mit Kanonen auf Spatzen schießen...

Logik Beweise

Beispiele für irrationale Zahlen

In $\mathbb{Q}$ können wir Gleichungen wie $x^2 = 2$ formulieren, aber nicht lösen.

Satz A1F: Irrationalität von $\sqrt{2}$, Euklid ca. 300 v.Chr.

Es gibt keine rationale Zahl $r \in \mathbb{Q}$ mit der Eigenschaft $r^2 = 2$.

Beweis: Angenommen, es gäbe $r \in \mathbb{Q}$ mit $r^2 = 2$.
Rational bedeutet $r = a/b$ mit $a, b \in \mathbb{Z}$ und $b \neq 0$.
Zudem sei der Bruch a/b vollständig gekürzt.

Aus der Gleichung $(a/b)^2 = 2$ folgt $a^2 = 2b^2$.
Daher ist a^2 gerade, also auch a, das heißt $a = 2\overline{a}$ mit $\overline{a} \in \mathbb{Z}$.

Einsetzen in $a^2 = 2b^2$ ergibt $4\overline{a}^2 = 2b^2$, also $2\overline{a}^2 = b^2$.
Daher ist b^2 gerade, also auch b, das heißt $b = 2\overline{b}$ mit $\overline{b} \in \mathbb{Z}$.

Somit ließe sich $a/b = \overline{a}/\overline{b}$ weiter kürzen. Das ist ein Widerspruch!
Also gibt es keine rationale Zahl $r \in \mathbb{Q}$ mit der Eigenschaft $r^2 = 2$. QED

Übung: Ebenso sind $\sqrt[3]{2}, \sqrt[4]{2}, \ldots$ und $\sqrt{3}, \sqrt[3]{3}, \sqrt[4]{3}, \ldots$ irrational.
Denken Sie sich weitere Beispiele aus und beweisen Sie diese!

Rechnen in $\mathbb{Q}[\sqrt{2}]$: Motivation

Wir möchten mit dem Halb/Ring / Körper $\mathbb{K} = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ und $\sqrt{2}$ rechnen.
Wir wünschen uns einen Halb/Ring / Körper $\mathbb{K}[\sqrt{2}] \supset \mathbb{K}$ der Form

$$\mathbb{K}[\sqrt{2}] = \{\, z = x + y\sqrt{2} \mid x, y \in \mathbb{K} \,\}.$$

Wie sehen die Operationen aus? Falls $\mathbb{K}[\sqrt{2}]$ existiert, so erwarten wir:

Vergleich: $x + y\sqrt{2} = u + v\sqrt{2}$ in $\mathbb{K}[\sqrt{2}] \;\Leftrightarrow\; x = u$ und $y = v$ in $\mathbb{K}$

Addition: $(x + y\sqrt{2}) + (u + v\sqrt{2}) = (x + u) + (y + v)\sqrt{2}$

Multiplikation: $(x + y\sqrt{2}) \cdot (u + v\sqrt{2}) = (xu + 2yv) + (xv + yu)\sqrt{2}$

Über $\mathbb{K} = \mathbb{Z}, \mathbb{Q}$ haben wir zu jedem Element $z = x + y\sqrt{2}$ in $\mathbb{K}[\sqrt{2}]$
das Negative $-z = (-x) + (-y)\sqrt{2}$ und das Konjugierte $\overline{z} = x - y\sqrt{2}$.
Ist jedes Element $z \neq 0$ invertierbar? Über $\mathbb{K} = \mathbb{Q}$ gelingt dies:

$$\frac{1}{x + y\sqrt{2}} = \frac{1}{x + y\sqrt{2}} \cdot \frac{x - y\sqrt{2}}{x - y\sqrt{2}} = \frac{x}{x^2 - 2y^2} - \frac{y}{x^2 - 2y^2}\sqrt{2}$$

Wann gilt $x^2 - 2y^2 = 0$? Aus $y \neq 0$ folgt $(x/y)^2 = 2$; das ist für $x, y \in \mathbb{Q}$
unmöglich (A1F). Also gilt $y = 0$ und somit $x = 0$, das heißt $x + y\sqrt{2} = 0$.

Rechnen in $\mathbb{Q}[\sqrt{2}]$: Konstruktion

kartesisches Produkt

Ist das erlaubt? Wie können wir die Menge $\mathbb{Q}[\sqrt{2}]$ und ihre Operationen
einwandfrei erklären? Wir nutzen die Menge $\mathbb{Q}^2 = \{\, (x, y) \mid x, y \in \mathbb{Q} \,\}$
aller Paare (x, y) mit $x, y \in \mathbb{Q}$ und $\mathbb{Q}^2 \to \mathbb{Q}[\sqrt{2}] : (x, y) \mapsto x + y\sqrt{2}$.

Satz A1G: Konstruktion des Körpers $\mathbb{Q}[\sqrt{2}]$, siehe B137

Auf der Menge $E = \mathbb{Q}^2$ definieren wir Addition und Multiplikation durch

$$+ : E \times E \to E : (x, y) + (u, v) := (x + u, y + v),$$
$$\cdot : E \times E \to E : (x, y) \cdot (u, v) := (xu + 2yv, xv + yu).$$

Damit ist $(E, +, \cdot)$ ein Körper. Hierin ist $(\mathbb{Q}, +, \cdot)$ ein Teilkörper
dank der Einbettung $\mathbb{Q} \hookrightarrow E : x \mapsto (x, 0)$. Wir schreiben kurz $\mathbb{Q} \subset E$.

Im Körper E erfüllt das Element $\xi = (0, 1)$ die Eigenschaft $\xi^2 = 2$.
Jedes Element $z \in E$ schreibt sich eindeutig $z = x + y\xi$ mit $x, y \in \mathbb{Q}$.

Die Konjugation $\overline{} : E \to E : (x, y) \mapsto (x, -y)$ erfüllt $\overline{z + w} = \overline{z} + \overline{w}$
und $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$. Für $z \in E$ gilt $\overline{z} = z$ genau dann, wenn $z \in \mathbb{Q}$.

Diese Konstruktion des Körpers E rechtfertigt die Schreibweise $\mathbb{Q}[\sqrt{2}]$.

Rechnen in $\mathbb{Q}[\mathrm{i}]$: Motivation

Für jede rationale Zahl $x \in \mathbb{Q}$ gilt $x^2 \geq 0$, also $x^2 + 1 > 0$. Daher können wir Gleichungen wie $x^2 + 1 = 0$ in $\mathbb{Q}$ zwar formulieren, aber nicht lösen.

Können wir eine Lösung $\mathrm{i} = \sqrt{-1}$ erfinden und damit sinnvoll rechnen? Versuchen wir es! Dazu betrachten wir den Ring / Körper $\mathbb{K} = \mathbb{Z}, \mathbb{Q}$, später $\mathbb{K} = \mathbb{R}$. Wir wünschen uns einen Ring / Körper $\mathbb{K}[\mathrm{i}]$ der Form

$$\mathbb{K}[\mathrm{i}] = \{\, z = x + y\mathrm{i} \mid x, y \in \mathbb{K} \,\}.$$

Wie sehen die Operationen aus? Falls $\mathbb{K}[\mathrm{i}]$ existiert, so erwarten wir:

Vergleich:	$x + y\mathrm{i} = u + v\mathrm{i}$ in $\mathbb{K}[\mathrm{i}]$	$\Leftrightarrow$	$x = u$ und $y = v$ in $\mathbb{K}$
Addition:	$(x + y\mathrm{i}) + (u + v\mathrm{i})$	$=$	$(x + u) + (y + v)\mathrm{i}$
Multiplikation:	$(x + y\mathrm{i}) \cdot (u + v\mathrm{i})$	$=$	$(xu - yv) + (xv + yu)\mathrm{i}$

Über $\mathbb{K} = \mathbb{Z}, \mathbb{Q}$ haben wir zu $z = x + y\mathrm{i}$ das Negative $-z = (-x) + (-y)\mathrm{i}$ und das Konjugierte $\overline{z} = x - y\mathrm{i}$. Dabei gilt $z\overline{z} = x^2 + y^2$, über $\mathbb{Q}$ also

$$\frac{1}{x + y\mathrm{i}} = \frac{1}{x + y\mathrm{i}} \cdot \frac{x - y\mathrm{i}}{x - y\mathrm{i}} = \frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2}\mathrm{i}$$

Für jedes Element $x + y\mathrm{i} \neq 0$ gilt $x \neq 0$ oder $y \neq 0$, also $x^2 + y^2 > 0$.

Rechnen in $\mathbb{Q}[\mathrm{i}]$: Konstruktion

kartesisches Produkt

Ist das erlaubt? Wie können wir die Menge $\mathbb{Q}[\mathrm{i}]$ und ihre Operationen einwandfrei erklären? Wir nutzen $\mathbb{Q}^2 \to \mathbb{Q}[\mathrm{i}] : (x, y) \mapsto x + y\mathrm{i}$.

Satz A1H: Konstruktion des Körpers $\mathbb{Q}[\mathrm{i}]$, siehe B137

Auf der Menge $E = \mathbb{Q}^2$ definieren wir Addition und Multiplikation durch

$$+ : E \times E \to E : (x, y) + (u, v) := (x + u, y + v),$$
$$\cdot : E \times E \to E : (x, y) \cdot (u, v) := (xu - yv, xv + yu).$$

Damit ist $(E, +, \cdot)$ ein Körper. Hierin ist $(\mathbb{Q}, +, \cdot)$ ein Teilkörper dank der Einbettung $\mathbb{Q} \hookrightarrow E : x \mapsto (x, 0)$. Wir schreiben kurz $\mathbb{Q} \subset E$.

Im Körper E erfüllt das Element $\mathrm{i} = (0, 1)$ die Eigenschaft $\mathrm{i}^2 = -1$. Jedes Element $z \in E$ schreibt sich eindeutig $z = x + y\mathrm{i}$ mit $x, y \in \mathbb{Q}$.

Die Konjugation $\overline{} : E \to E : (x, y) \mapsto (x, -y)$ erfüllt $\overline{z + w} = \overline{z} + \overline{w}$ und $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$. Für $z \in E$ gilt $\overline{z} = z$ genau dann, wenn $z \in \mathbb{Q}$.

⚠ Es gibt keine Anordnung auf $\mathbb{Q}[\mathrm{i}]$ zu einem geordneten Körper $(\mathbb{Q}[\mathrm{i}], +, \cdot, \leq)$, denn in jedem geordneten Körper gilt $x^2 \geq 0$ für alle x.

Kurzschreibweise für Produkte und Summen

Im Folgenden seien a_i Elemente in einem kommutativen Monoid, additiv geschrieben wie $(\mathbb{Q}, +, 0)$ oder multiplikativ wie $(\mathbb{Q}, \cdot, 1)$. Mehrfache Summen und Produkte kürzen wir wie folgt ab:

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n := (\ldots(a_1 + a_2) + \ldots) + a_n$$

$$\prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdot \cdots \cdot a_n := (\ldots(a_1 \cdot a_2) \cdot \ldots) \cdot a_n$$

☺ Dank Assoziativität können wir beliebig umklammern, dank Kommutativität zudem beliebig umordnen.

Allgemein für die Grenzen $k, \ell \in \mathbb{Z}$ vereinbaren wir:

$$\sum_{i=k}^{\ell} a_i := \begin{cases} a_k + a_{k+1} + \cdots + a_\ell & \text{falls } k \leq \ell, \\ 0 \quad \text{(leere Summe)} & \text{falls } k > \ell. \end{cases}$$

$$\prod_{i=k}^{\ell} a_i := \begin{cases} a_k \cdot a_{k+1} \cdot \cdots \cdot a_\ell & \text{falls } k \leq \ell, \\ 1 \quad \text{(leeres Produkt)} & \text{falls } k > \ell. \end{cases}$$

Kurzschreibweise für Produkte und Summen

Sei $n \in \mathbb{N}$. Im Sonderfall $a_1 = a_2 = a_3 = \cdots = a_n =: a$ erhalten wir

$$a \cdot n := \sum_{i=1}^{n} a = \begin{cases} 0 \quad \text{(leere Summe)} & \text{falls } n = 0, \\ a + a + \cdots + a \quad \text{(mit } n \text{ Summanden)} & \text{falls } n \geq 1. \end{cases}$$

$$a^n := \prod_{i=1}^{n} a = \begin{cases} 1 \quad \text{(leeres Produkt)} & \text{falls } n = 0, \\ a \cdot a \cdot \cdots \cdot a \quad \text{(mit } n \text{ Faktoren)} & \text{falls } n \geq 1. \end{cases}$$

☺ Das stimmt mit unserer bisherigen Definition A1A überein.
Ist $-a$ das Negative zu a, so setzen wir $a \cdot (-n) := (-a) \cdot n$.
Ist a^{-1} das Inverse zu a, so setzen wir $a^{-n} := (a^{-1})^n$.

Ist $I = \{i_1, i_2, \ldots, i_n\}$ eine n–elementige Menge, so schreiben wir

$$\sum_{i \in I} a_i := \sum_{k=1}^{n} a_{i_k} \quad \text{und} \quad \prod_{i \in I} a_i := \prod_{k=1}^{n} a_{i_k}.$$

Eine Umnummerierung der Elemente ändert das Ergebnis nicht.

Sei J eine Menge und $I \subseteq J$ endlich, sodass $a_i = 0$ für alle $i \in J \setminus I$. Dann definieren wir $\sum_{i \in J} a_i := \sum_{i \in I} a_i$ als endliche Summe wie oben.

Polynome

Sei K ein Körper, wie $\mathbb{Q}$, oder allgemein ein kommutativer Ring, wie $\mathbb{Z}$.
Wir betrachten Polynome in der Unbestimmten X mit Koeffizienten in K:

$$K[X] = \left\{ P = p_0 + p_1 X + \cdots + p_n X^n \;\middle|\; n \in \mathbb{N},\ p_0, p_1, \ldots, p_n \in K \right\}.$$

Wir schreiben kurz $P = \sum_{i=0}^{n} p_i X^i$. Im Falle $p_n \neq 0$ ist $\deg(P) := n$ der Grad von P und $\mathrm{lc}(P) := p_n$ der Leitkoeffizient. Wir schreiben noch kürzer $P = \sum_i p_i X^i$ und vereinbaren $p_i = 0$ für alle $i < 0$ und alle $i > n$.

Im Sonderfall $P = 0$ setzen wir $\deg(0) := -\infty$ und $\mathrm{lc}(0) := 0$.
Wir schreiben $K[X]_n$ und $K[X]_{\leq n}$ und $K[X]_{<n}$ für die Menge der Polynome $P \in K[X]$ vom Grad genau / höchstens / kleiner n

Wir übertragen die Operationen von K auf $K[X]$:

Vergleich: $\sum_i p_i X^i = \sum_i q_i X^i$ in $K[X] \;\Leftrightarrow\; p_i = q_i$ in K für alle i
Addition: $\left[\sum_i p_i X^i\right] + \left[\sum_i q_i X^i\right] = \sum_i (p_i + q_i) X^i$
Multiplikation: $\left[\sum_i p_i X^i\right] \cdot \left[\sum_j q_j X^j\right] = \sum_k r_k X^k,\ r_k = \sum_{i+j=k} p_i q_j$

Die letzte Summe durchläuft alle Paare $(i, j) \in \mathbb{N}^2$ mit $i + j = k$.

Polynome

Ein **Integritätsring**, kurz IRing, ist ein kommutativer Ring $(K, +, 0, \cdot, 1)$ mit $0 \neq 1$ sodass für alle $a, b \in K$ gilt: Aus $a \neq 0$ und $b \neq 0$ folgt $a \cdot b \neq 0$.
Das heißt: Ein Produkt ab ist genau dann null, wenn ein Faktor null ist.
Multiplikation mit $a \neq 0$ ist kürzbar: $ab = ac \;\Leftrightarrow\; a(b - c) = 0 \;\Leftrightarrow\; b = c$

Satz A11: der Polynomring $K[X]$

Ist $(K, +, 0, \cdot, 1)$ ein kommutativer Ring, so auch $(K[X], +, 0, \cdot, 1)$.
Ist zudem K ein Integritätsring, so auch $K[X]$; genauer gilt nämlich

$$\begin{aligned} \deg(P \cdot Q) &= \deg(P) + \deg(Q) && \text{in } \mathbb{N} \cup \{-\infty\}, \\ \mathrm{lc}(P \cdot Q) &= \mathrm{lc}(P) \cdot \mathrm{lc}(Q) && \text{in } K. \end{aligned}$$

Jedes Polynom $P(X) = \sum_{i=0}^{n} p_i X^i$ in $K[X]$ definiert seine zugehörige Polynomfunktion $f_P : K \to K : x \mapsto P(x) = \sum_{i=0}^{n} p_i x^i$ durch Einsetzen.
Wir unterscheiden also sorgsam den formalen Ausdruck $P(X) \in K[X]$ und seine Anwendung $f_P : x \mapsto P(x)$ auf Elemente $x \in K$. Über einem unendlichen Körper wie $\mathbb{Q}$ besteht kein großer Unterschied, über einem endlichen Körper hingegen ist die Unterscheidung ganz wesentlich!

Bruchkörper und gebrochen-rationale Funktionen

Sei R ein Integritätsring, etwa $\mathbb{Z}$ oder $\mathbb{Q}[X]$. Wie / Können wir mit Brüchen sinnvoll rechnen? Versuchen wir es! Dazu betrachten wir

$$K = \operatorname{Frac}(R) := \left\{ q = [a/b] \;\middle|\; a, b \in R,\ b \neq 0 \right\}.$$

Auf dieser Menge K vereinbaren wir die folgenden Operationen:

Vergleich:	$[a/b] = [c/d]$ in K	$\Leftrightarrow$	$ad = cb$ in R
Addition:	$[a/b] + [c/d]$	$=$	$[(ad + cb)/(bd)]$
Negation:	$-[a/b]$	$=$	$[-a/b]$
Multiplikation:	$[a/b] \cdot [c/d]$	$=$	$[(ac)/(bd)]$
Inversion:	$[a/b]^{-1}$	$=$	$[b/a]$ falls $a \neq 0$

Wir haben die Einbettung $R \hookrightarrow K : a \mapsto [a/1]$ und schreiben kurz $R \subseteq K$.

Satz A1J: Bruchkörper zu einem Integritätsring

Ist $(R, +, 0, \cdot, 1)$ ein Integritätsring, so ist $(K, +, 0, \cdot, 1)$ ein Körper.

☺ So erhalten wir insbesondere die rationalen Zahlen $\mathbb{Q} = \operatorname{Frac}(\mathbb{Z})$ und die gebrochen-rationalen Funktionen $\mathbb{Q}(X) = \operatorname{Frac}(\mathbb{Q}[X])$.

Bruchkörper und gebrochen-rationale Funktionen

Die Erweiterung $\mathbb{Q} \supset \mathbb{Z}$ erhalten wir durch die Bildung von Brüchen:

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \neq 0 \right\}$$

Auch $\mathbb{Q}(X) \supset \mathbb{Q}[X]$ erhalten wir durch die Bildung von Brüchen:

$$\mathbb{Q}(X) = \left\{ \frac{A}{B} = \frac{a_m X^m + \cdots + a_1 X + a_0}{b_n X^n + \cdots + b_1 X + b_0} \;\middle|\; A, B \in \mathbb{Q}[X],\ B \neq 0 \right\}$$

Genau so kennen Sie diese Brüche aus der Schule, dort allerdings eher pragmatisch-experimentell durch *learning by doing*. Hier schauen wir die Voraussetzungen genauer an und entdecken ein allgemeines Prinzip:

Ist R ein Integritätsring, also ein kommutativer Ring ohne Nullteiler, so können wir den Bruchkörper $K = \operatorname{Frac}(R)$ wie oben konstruieren. Das ist eine vollkommen natürliche und allgemeine Konstruktion.

Alles liegt explizit vor, Sie können es nachrechnen! Dahinter stecken jedoch einige scharfsinnige Fragen: Ist der Vergleich „=“ wirklich eine Äquivalenzrelation, also reflexiv, symmetrisch und vor allem: transitiv? Sind die Operationen $+$ und $\cdot$ wohldefiniert, also unabhängig von den Repräsentanten? Wir kommen darauf später noch genauer zurück.

Arithmetik ganzer Zahlen: Division mit Rest

In den ganzen Zahlen $\mathbb{Z}$ haben wir neben den drei Grundrechenarten $+, -, \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ auch die **Division mit Rest**. Einfaches Beispiel:

„Teile 372 ganzzahlig durch 25“: $\quad 372 = 25 \cdot q + r = 25 \cdot 14 + 22$

Gelingt das immer? Ist das Ergebnis eindeutig? Glücklicherweise ja!

Satz A2A: euklidische / ganzzahlige Division mit Rest

Sei $b \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ und $\mathbb{Z}_b = \{\, r \in \mathbb{Z} \mid 0 \leq r < |b| \,\} = \{0, 1, \ldots, |b|-1\}$.
Jede ganze Zahl $a \in \mathbb{Z}$ schreibt sich eindeutig als **Division mit Rest**

$$a = bq + r \quad \text{mit } q \in \mathbb{Z} \text{ und } r \in \mathbb{Z}_b.$$

Wir nennen diese Zerlegung die **euklidische Division** von a durch b mit **Quotient** q und **Rest** r. Dies definiert die beiden Operationen

$$(\mathrm{quo}, \mathrm{rem}) \,:\, \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Z} \times \mathbb{N} \,:\, (a, b) \mapsto (q, r).$$

Wir schreiben kurz $q = a \operatorname{quo} b$ und $r = a \operatorname{rem} b$.

Übung: M Wie beweisen Sie dies? I Wie berechnen Sie es effizient?

Arithmetik ganzer Zahlen: Division mit Rest

Wenn Sie bereits Erfahrung oder gar Routine haben, dann werden Sie ausrufen „Das ist klar per Induktion!“. Wenn Sie Sorgfalt und Technik anfangs noch üben wollen, so ist dies eine wunderbare Gelegenheit.

Aufgabe: Beweisen Sie Existenz und Eindeutigkeit der Lösung (q, r).

Lösung: Wir fixieren den Divisor $b \in \mathbb{Z} \setminus \{0\}$. Zur Vereinfachung dürfen wir $b > 0$ annehmen, denn $a = bq + r = (-b)(-q) + r$.

Existenz: Für $a = 0$ genügt $(q, r) = (0, 0)$. Ist $a = bq + r$ mit $q \in \mathbb{N}$ und $r \in \mathbb{Z}_b$ gegeben, dann folgt $a + 1 = bq + (r + 1) = bq' + r'$: Für $r + 1 < b$ wähle $(q', r') = (q, r + 1)$. Für $r + 1 = b$ wähle $(q', r') = (q + 1, 0)$. Voilà.

Für negatives $a \in \mathbb{Z}_{<0}$ haben wir $-a = bq + r$ mit $q \in \mathbb{N}$ und $r \in \mathbb{Z}_b$, also $a = b(-q) + (-r)$. Im Falle $r \neq 0$ also $a = b(-q - 1) + (b - r)$.

Eindeutigkeit: Sei $a = bq + r = bq' + r'$ mit $q, q' \in \mathbb{Z}$ und $r, r' \in \mathbb{Z}_b$.
Subtraktion ergibt $0 = (bq' + r') - (bq + r') = b(q' - q) + (r' - r)$.
Also teilt b die Differenz $r' - r \in \{1 - b, \ldots, -1, 0, 1, \ldots, b - 1\}$.
Daraus folgt $r' - r = 0$, also $r' = r$ und schließlich $q' = q$. QED

Arithmetik ganzer Zahlen: Zifferndarstellung in Basis B

Satz A2B: Zifferndarstellung in Basis B

Wir fixieren $B \in \mathbb{N}_{\geq 2}$, etwa $B = 2$ (binär) oder $B = 10$ (dezimal).
Als Ziffernmenge nutzen wir entsprechend $\mathbb{Z}_B = \{0, 1, \ldots, B-1\}$.

Jede natürliche Zahl $n \in \mathbb{N}$ schreibt sich eindeutig in Basis B gemäß

$$n = n_{\ell-1}B^{\ell-1} + n_{\ell-2}B^{\ell-2} + \cdots + n_2B^2 + n_1B + n_0$$

mit Länge $\ell \in \mathbb{N}$ und Ziffern $n_0, n_1, n_2, \ldots, n_{\ell-2}, n_{\ell-1} \in \mathbb{Z}_B$, $n_{\ell-1} \neq 0$.

$$\begin{array}{ccccc} \text{natürliche Zahlen} & \mathbb{N} & \underset{\sigma_B}{\overset{\rho_B}{\underset{\longleftarrow}{\overset{\longrightarrow}{\cong}}}} & \mathbb{Z}_B^{(\mathbb{N})} & \text{Zifferndarstellung} \\ n_{\ell-1}B^{\ell-1} + \cdots + n_1B + n_0 & & \longmapsto \; \longmapsto & (n_0, n_1, \ldots, n_{\ell-1}, 0, 0, 0, \ldots) & \end{array}$$

Diese Bijektion nennen wir die **Zifferndarstellung in Basis B**.

Übung: M Wie erklären Sie die schriftliche Addition und Multiplikation?
I Wie implementieren Sie diese Operationen möglichst effizient?
Überraschung: Die Schulmethode ist nicht die schnellste!

Arithmetik ganzer Zahlen: Zifferndarstellung in Basis B

Hier ist $\mathbb{Z}_B^{(\mathbb{N})} = \{\, f : \mathbb{N} \to \mathbb{Z}_B \mid \operatorname{supp}(f) \text{ endlich} \,\}$ die Menge aller Folgen f mit endlichem Träger, also $f_k = 0$ für alle $k \geq \ell$ ab einem gewissen Index $\ell \in \mathbb{N}$; dies entspricht der endlichen Folge $(f_0, f_1, \ldots, f_{\ell-1})$ in $\mathbb{Z}_B^\ell$.

Zur Basis $B = 10$ ist dies die allgegenwärtige Dezimaldarstellung, die sie seit der Grundschule kennen und täglich überall verwenden. Sie benötigen dazu nur zehn Ziffern: $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Das ist wunderbar handlich und bequem. Im Gegensatz dazu ist die römische Zahlschreibweise hoffnungslos unhandlich und verwirrend.

Binäre Computer nutzen die Basis $B = 2$ und kommen daher bereits mit zwei Ziffern aus: $\mathbb{Z}_2 = \{0, 1\}$. Das ist minimalistisch und effizient. Für größere Speichereinheiten fasst man je 8 (oder 16, 32) Bits zu einem Wort zusammen und rechnet dann zur Basis $B = 2^8$ (oder 2^{16}, 2^{32}). Auch das Hexadezimalsystem zur Basis $B = 16$ ist gebräuchlich.

Die Reihenfolge der Ziffern rechts-nach-links oder links-nach-rechts aufsteigend ist eine Konvention, wie so oft: wichtig aber willkürlich. Im Computer-Jargon sagt man *big-endian* und *little-endian*.

Arithmetik ganzer Zahlen: schriftliche Addition

Übung: Wie funktioniert die schriftliche Addition $\oplus : \mathbb{Z}_B^{(\mathbb{N})} \times \mathbb{Z}_B^{(\mathbb{N})} \to \mathbb{Z}_B^{(\mathbb{N})}$? Wie viele Rechenschritte sind nötig? Schreiben Sie es explizit aus!

Lösung: Als **elementaren Rechenschritt** nutzen wir die Addition $a + b$ von zwei Ziffern $a, b \in \mathbb{Z}_B$ und einem **Übertrag** $c \in \{0, 1\}$, engl. *carry*:

$$\begin{aligned} \mathrm{Add} : \mathbb{Z}_B \times \mathbb{Z}_B \times \{0,1\} &\to \{0,1\} \times \mathbb{Z}_B \\ (a, b, c) &\mapsto (d, e) \quad \text{mit } a + b + c = dB + e \end{aligned}$$

Algo A2C: schriftliche Addition in Basis B

Eingabe: zwei Zifferndarstellungen $x, y \in \mathbb{Z}_B^\ell$
Ausgabe: die Darstellung $z = x \oplus y \in \mathbb{Z}_B^{\ell+1}$ der Summe

1: $c \leftarrow 0$
2: for k from 0 to $\ell - 1$ do $(c, z_k) \leftarrow \mathrm{Add}(x_k, y_k, c)$
3: return $z = (z_0, z_1, \ldots, z_{\ell-1}, c)$

☺ Dieser Algorithmus verwendet genau ℓ Ziffernoperationen (hier Add). Besser geht es nicht: Mindestens ℓ Schritte sind nötig allein zum Lesen.

Arithmetik ganzer Zahlen: schriftliche Multiplikation

Wie funktioniert die schriftliche Multiplikation $\odot : \mathbb{Z}_B^{(\mathbb{N})} \times \mathbb{Z}_B^{(\mathbb{N})} \to \mathbb{Z}_B^{(\mathbb{N})}$? Wie viele Rechenschritte sind nötig? Schreiben Sie es explizit aus!

(1) Als **elementaren Rechenschritt** nutzen wir die Multiplikation $a \cdot b$ von zwei Ziffern $a, b \in \mathbb{Z}_B$ und zudem einem **Übertrag** $c \in \mathbb{Z}_B$:

$$\begin{aligned} \mathrm{Mul} : \mathbb{Z}_B \times \mathbb{Z}_B \times \mathbb{Z}_B &\to \mathbb{Z}_B \times \mathbb{Z}_B \\ (a, b, c) &\mapsto (d, e) \quad \text{mit } a \cdot b + c = dB + e \end{aligned}$$

Algo A2D: kleine Multiplikation in Basis B

Eingabe: eine Zifferndarstellung $x \in \mathbb{Z}_B^\ell$ und $y \in \mathbb{Z}_B$
Ausgabe: die Darstellung $z = x \odot y \in \mathbb{Z}_B^{\ell+1}$ des Produkts

1: $c \leftarrow 0$
2: for k from 0 to $\ell - 1$ do $(c, z_k) \leftarrow \mathrm{Mul}(x_k, y, c)$
3: return $z = (z_0, z_1, \ldots, z_{\ell-1}, c)$

☺ Dieser Algorithmus verwendet genau ℓ Ziffernoperationen (hier Mul). Besser geht es nicht: Mindestens ℓ Schritte sind nötig allein zum Lesen.

Arithmetik ganzer Zahlen: schriftliche Multiplikation

(2) Die Multiplikation $x \odot y$ setzen wir aus $x \odot y_k$ zusammen mit der Verschiebung $\mathrm{Shift} : \mathbb{Z}_B^{(\mathbb{N})} \to \mathbb{Z}_B^{(\mathbb{N})} : (f_0, f_1, f_2, \dots) \mapsto (0, f_0, f_1, f_2, \dots)$.

Algo A2E: schriftliche Multiplikation in Basis B

Eingabe: zwei Zifferndarstellungen $x \in \mathbb{Z}_B^p$ und $y \in \mathbb{Z}_B^q$
Ausgabe: die Darstellung $z = x \odot y \in \mathbb{Z}_B^{p+q+1}$ des Produkts

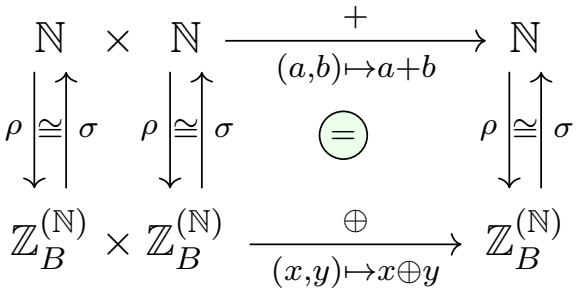
1: $z \leftarrow 0$
2: for k from 0 to $q-1$ do $z \leftarrow z \oplus \mathrm{Shift}^k(x \odot y_k)$
3: return z

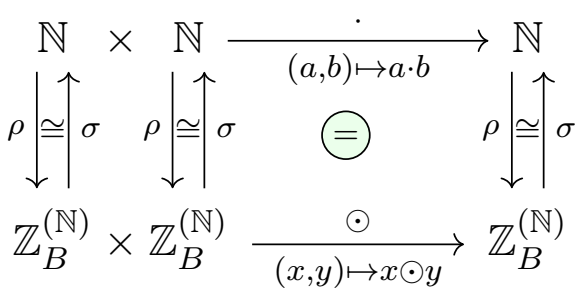
🙂 ☹ Dieser Algorithmus verwendet pq mal Add und pq mal Mul. Speziell für $B = 2$ ist $x \odot y_k$ trivial, es bleiben nur die pq Additionen. Das ist für kleine Eingabelängen p und q noch ausreichend effizient, aber für große Eingaben wird diese Methode spürbar zeitaufwändig.

⚠ Die schriftliche Addition hat nur **linearen** Zeitaufwand (optimal), die schriftliche Multiplikation hingegen hat **quadratischen** Aufwand. Können wir das Produkt $x \odot y$ raffinierter und schneller berechnen?

Arithmetik ganzer Zahlen: schriftliche Multiplikation

Übung: Weisen Sie nach, dass die obigen Algorithmen korrekt sind, also tatsächlich Summe und Produkt in $\mathbb{N}$ richtig abbilden. Ausführlich:





Übung: Implementieren Sie dies in Ihrer Lieblingsprogrammiersprache. Testen Sie es ausführlich auf zahlreichen, immer größeren Beispielen. Wie macht sich die lineare vs quadratische Laufzeit bemerkbar?

Übung: Formulieren und implementieren Sie die euklidische Division ebenso als Algorithmus $(x, y) \mapsto (q, r)$. Wer's kann, verdient Respekt!

🙂 Bibliotheken wie GMP (*GNU Multiple Precision Arithmetic Library*, `gmplib.org`) implementieren diese Arithmetik – hochgradig optimiert!

Schnelle Multiplikation nach Karatsuba

Even fairly good students, when they have obtained the solution of the problem and written down neatly the argument, shut their books and look for something else. Doing so, they miss an important and instructive phase of the work. [...]
A good teacher should understand and impress on his students the view that no problem whatever is completely exhausted.
George Pólya (1887–1985), *How to Solve It* (1945)

Um 1956 formulierte Andrey Kolmogorov seine Vermutung, dass die Multiplikation ganzer Zahlen nicht schneller als quadratisch gelingen kann. Im Herbst 1960 organisierte er an der Lomonossov–Universität in Moskau ein Seminar zur Kybernetik und Fragen der Komplexität.

Der 23-jährige Anatoly Karatsuba widerlegte Kolmogorovs Vermutung innerhalb einer Woche: Er fand die weltweit erste schnelle Multiplikation!

Damit begann eine neue Forschungsrichtung *Fast Arithmetic*, die seither sehr aktiv ist und sensationelle Erfolge erreicht hat. Diese Grundlagenforschung steckt in allen modernen Computern.

📖 Gathen, Gerhard: *Modern Computer Algebra.* Cambridge CUP 2013

Schnelle Multiplikation nach Karatsuba

Wieviel Zeit kostet die Verknüpfung von Zahlen $a, b \in \mathbb{N}$ mit $\leq \ell$ Ziffern?

- Addition? Der Aufwand ist $\leq \text{const} \cdot \ell$, und linear ist optimal.
- Multiplikation? Aufwand $\leq \text{const} \cdot \ell^2$. Geht es schneller? Ja!

Zur Multiplikation vorgelegt seien $a, b \in \mathbb{N}$ mit $\leq 2n$ Ziffern in Basis B:

$$a = a_0 + a_1 B^n \quad \text{und} \quad b = b_0 + b_1 B^n \quad \text{mit} \quad a_0, a_1, b_0, b_1 < B^n$$
$$a \cdot b = (a_0 \cdot b_0) + (a_0 \cdot b_1 + a_1 \cdot b_0) B^n + (a_1 \cdot b_1) B^{2n}$$

Wir wollen hierzu das Produkt berechnen: Dies gelingt wie gezeigt mit vier Multiplikationen der Länge n. So weit, so klar, so langweilig. Karatsubas genialer Trick benötigt statt vier nur drei Multiplikationen:

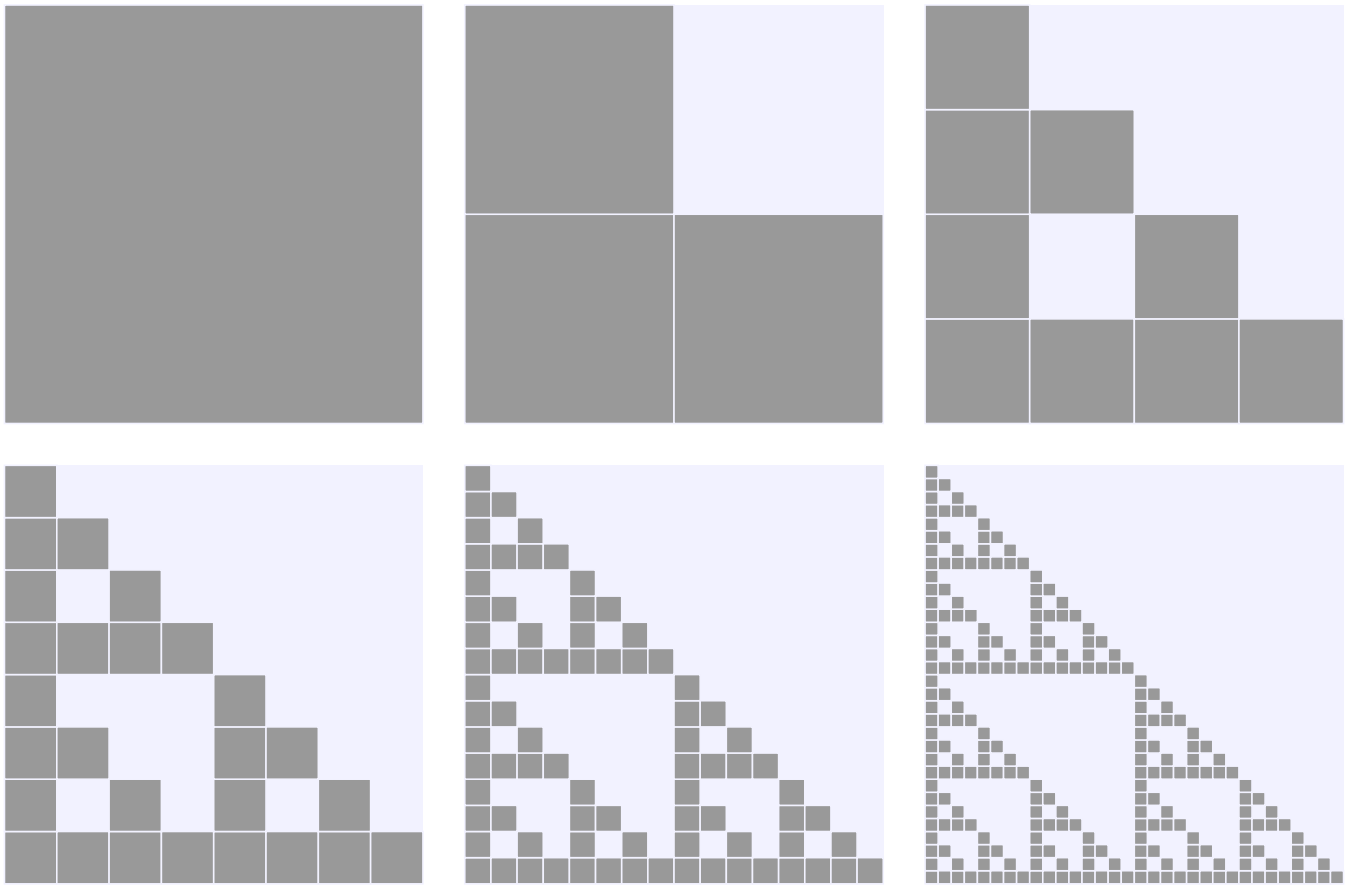
$$s := a_0 \cdot b_0, \quad t := a_1 \cdot b_1, \quad u := (a_0 + a_1) \cdot (b_0 + b_1) - s - t$$

Es gilt $u = a_0 \cdot b_1 + a_1 \cdot b_0$, somit erhalten wir $a \cdot b = s + uB^n + tB^{2n}$. Somit genügen drei Multiplikationen und zwei (billige!) Subtraktionen. Das macht sich bezahlt: Wir können diesen Trick rekursiv anwenden!

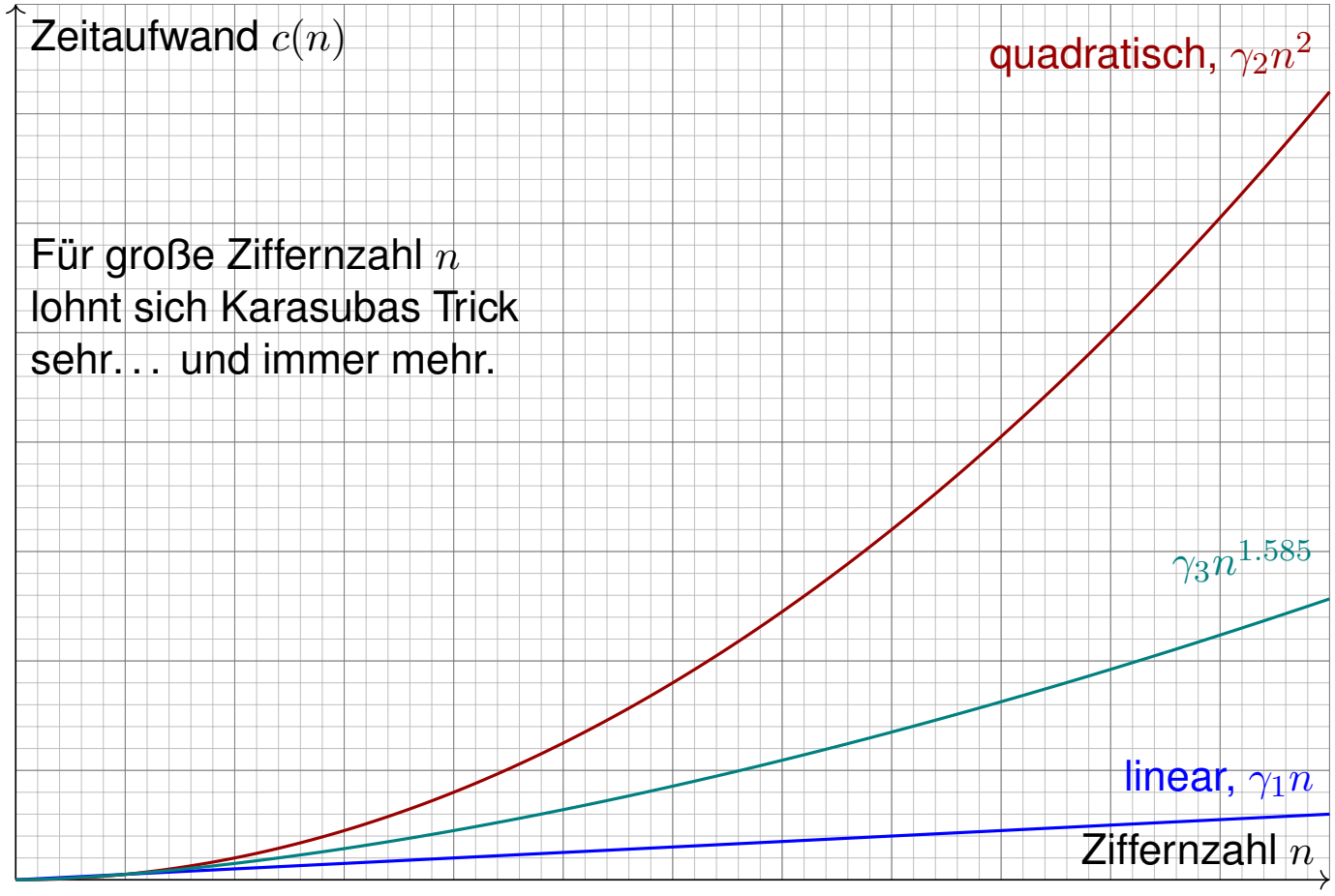
🙂 Der Aufwand beträgt nur $c(2n) \leq 3c(n) + \alpha n$.

Karatsubas Multiplikation ist subquadratisch.

Visualisierung der Rekursion: Kosten (grau) und Ersparnis (blau).



Karatsubas Multiplikation ist subquadratisch.



Schnelle Multiplikation nach Karatsuba

Karatsubas Idee ist ein Musterbeispiel des Prinzips **Teile und herrsche**. Wir zerlegen ein großes Problem in kleinere, leichtere Teilprobleme.

Seine Methode ist ebenso einfach wie genial: Zu multiplizieren seien $a, b \in \mathbb{N}$ mit $a, b < B^{2n}$. Diese sind gegeben als Zifferndarstellungen in Basis B. Wir zerlegen $a = a_0 + a_1 B^n$ und $b = b_0 + b_1 B^n$ in die n niedrigen Ziffern a_0, b_0 und die n hohen Ziffern a_1, b_1. Das Produkt

$$a \cdot b = (a_0 \cdot b_0) + (a_0 \cdot b_1 + a_1 \cdot b_0)B^n + (a_1 \cdot b_1)B^{2n}$$

benötigt augenscheinlich vier Multiplikationen. Es geht aber besser: Karatsubas genialer Trick benötigt statt vier nur drei Multiplikationen!

$$s \leftarrow a_0 \cdot b_0, \quad t \leftarrow a_1 \cdot b_1, \quad u \leftarrow (a_0 + a_1) \cdot (b_0 + b_1) - s - t$$

Es gilt $u = a_0 \cdot b_1 + a_1 \cdot b_0$, somit erhalten wir $ab = s + uB^n + tB^{2n}$.

☺ Auf den ersten Blick scheint das keine große Ersparnis zu sein. Im Gegenteil können die ungewohnten Formeln den Anschein erwecken, Karatsubas Methode wäre sogar komplizierter als die Schulmethode. Wir rechnen den Zeitaufwand und die Ersparnis daher sorgfältig nach.

Schnelle Multiplikation nach Karatsuba

Sei $c(n)$ die maximale Laufzeit für Karatsubas Multiplikation bei n Ziffern. Wir messen sie zum Beispiel in Sekunden auf einem Referenzcomputer, noch besser hardwareunabhängig als Anzahl der Ziffernoperationen. Die Umrechnung ist dann nur ein Faktor: die Hardwarekonstante.

Wir wenden Karatsubas Multiplikation rekursiv an, daher finden wir:

$$c(2n) \leq 3c(n) + \alpha n$$

Für eine Multiplikation der Länge $2n$ benötigen wir drei Multiplikationen der Länge n, jeweils mit Aufwand $c(n)$, sowie vier Additionen und zwei zusätzliche Subtraktionen, alle mit linearem Aufwand $\leq \alpha n$, $\alpha \in \mathbb{R}_{\geq 0}$.

Alle Ziffern liegen bereits im Speicher vor, die Aufteilung in niedrige und hohe Ziffern kostet nahezu nichts. Multiplikation mit B^n und B^{2n} ist nur eine Verschiebung der Ziffern, also ebenso vernachlässigbar billig.

☺ Diese rekursive, implizite Ungleichung können wir explizit auflösen! Der folgende Satz zeigt, dass Karatsubas Algorithmus tatsächlich eine wesentliche Verbesserung ist. Der Satz ist ein einfacher Spezialfall des **Master Theorems**, das rekursive Laufzeitanalysen zusammenfasst.

Karatsubas Multiplikation ist subquadratisch.

Satz A2F: Zeitaufwand von Karatsubas Multiplikation

Vorgelegt sei $c : \mathbb{N} \to \mathbb{R}$ monoton wachsend. Zudem gelte

$$\text{(1)} \qquad c(2n) \leq 3c(n) + \alpha n \quad \text{und} \quad c(1) \leq \beta$$

für alle $n \in \mathbb{N}$. Hierbei sind $\alpha, \beta \in \mathbb{R}_{\geq 0}$ Konstanten. Dann folgt:

$$\text{(2)} \qquad c(2^k) \leq 3^k(\alpha + \beta) - 2^k\alpha \quad \text{für alle } k \in \mathbb{N}$$

$$\text{(3)} \qquad c(n) < 3(\alpha + \beta)\, n^{\log_2(3)} \quad \text{für alle } n \in \mathbb{N}$$

Dank $\log_2(3) \approx 1.585 < 2$ ist dies wesentlich besser als $\text{const} \cdot n^2$.

Beweis: Ungleichung (2) folgt per Induktion über k. Die Abschätzung (3) folgt aus der Monotonie von c dank $n \leq 2^k$ für $k = \lceil \log_2 n \rceil < 1 + \log_2 n$.

☺ Stehen die Formeln schon da, so ist ihr formaler Beweis relativ leicht: Es gelingt mit vollständiger Induktion und sorgfältigem Nachrechnen.

☺ Geeignete Ungleichungen zu finden, ist schwieriger; es gelingt gut durch Ausprobieren kleiner Fälle bis zum Auffinden eines Musters.

Karatsubas Multiplikation ist subquadratisch.

Aufgabe: Führen Sie den skizzierten Beweis des Satzes aus.

Lösung: Ungleichung (2) gilt für $k = 0$, denn $c(0) = \beta = 3(\alpha + \beta) - 2\alpha$. Wir nehmen an, die Ungleichung (2) gilt für k, und zeigen sie für $k + 1$:

$$\begin{aligned} c(2^{k+1}) &\overset{(1)}{\leq} 3c(2^k) + \alpha 2^k \\ &\overset{(2)}{\leq} 3^{k+1}(\alpha + \beta) - 3 \cdot 2^k\alpha + 2^k\alpha \\ &= 3^{k+1}(\alpha + \beta) - 2^{k+1}\alpha \end{aligned}$$

Die vereinfachende Abschätzung (3) für alle $n \in \mathbb{N}$ folgt aus $n \leq 2^k$ für $k = \lceil \log_2 n \rceil < 1 + \log_2 n$. Dank der Monotonie von c gilt:

$$\begin{aligned} c(n) \;\leq\; c(2^k) &\overset{(2)}{\leq} 3^k(\alpha + \beta) - 2^k\alpha \;<\; 3^k(\alpha + \beta) \\ &< 3 \cdot 3^{\log_2(n)}(\alpha + \beta) \;=\; 3(\alpha + \beta)\, n^{\log_2(3)} \end{aligned}$$

Damit sind beide Ungleichungen des Satzes bewiesen. QED

☺ Allein die Konstanten α und β hängen von der Implementierung ab, von der Geschwindigkeit der Hardware, von lokalen Optimierungen, etc. Der entscheidende Exponent $\log_2(3) \approx 1.585$ hingegen ist immer gleich.

Teilbarkeit in ganzen Zahlen

Wir wollen in den ganzen Zahlen $\mathbb{Z}$ effizient rechnen. Ein typisches Problem ist, den größten gemeinsamen Teiler ggT zu bestimmen.

$$\mathrm{GT}(18,24) = \{\pm1, \pm2, \pm3, \pm6\},\ \mathrm{GGT}(18,24) = \{\pm6\},\ \mathrm{ggT}(18,24) = 6$$

Wir benötigen eine präzise Definition und effiziente Algorithmen.

Definition A2G: größter gemeinsamer Teiler in $\mathbb{Z}$

Seien $a, b \in \mathbb{Z}$. Wir sagen a **teilt** b **in** $\mathbb{Z}$, oder b ist ein Vielfaches von a, falls es $a' \in \mathbb{Z}$ gibt mit $aa' = b$. Dies schreiben wir $a \mid_{\mathbb{Z}} b$ oder kurz $a \mid b$. Andernfalls sagen wir a teilt nicht b, geschrieben $a \nmid_{\mathbb{Z}} b$ oder kurz $a \nmid b$.

Die Menge der **gemeinsamen Teiler** von $a_1, \ldots, a_n \in \mathbb{Z}$ ist

$$\mathrm{GT} = \mathrm{GT}_{\mathbb{Z}}(a_1, \ldots, a_n) := \left\{ t \in \mathbb{Z} \;\middle|\; t \mid_{\mathbb{Z}} a_1, \ldots, t \mid_{\mathbb{Z}} a_n \right\}.$$

Die Menge der **größten gemeinsamen Teiler** definieren wir durch

$$\mathrm{GGT} = \mathrm{GGT}_{\mathbb{Z}}(a_1, \ldots, a_n) := \left\{ t \in \mathrm{GT} \;\middle|\; \forall s \in \mathrm{GT} : s \mid_{\mathbb{Z}} t \right\}.$$

Ist GGT nicht leer, so gilt $\mathrm{GGT} = \{\pm g\}$, und wir setzen $\mathrm{ggT} := |g|$.

Teilbarkeit in ganzen Zahlen

⚠ Beachten Sie, dass „größer“ im Sinne der Teilbarkeit definiert ist: Ein ggT von $a_1, \ldots, a_n$ ist ein Teiler, der von allen Teilern geteilt wird.

Im geordneten Ring $(\mathbb{Z}, +, \cdot, \leq)$ ist der positive ggT das größte Element bezüglich $\leq$, das ist jedoch eine Folgerung und nicht Teil der Definition.

(0) Teilbarkeit ist eine (Prä)Ordnung. Das heißt, für alle $a, b, c \in \mathbb{Z}$ gilt:

Reflexivität,	**Refl**$(\mathbb{Z}, \mid)$:	Es gilt $a \mid a$.
Antisymmetrie,	**Asym**$(\mathbb{Z}, \mid)$:	Aus $a \mid b$ und $b \mid a$ folgt $a = \pm b$.
Transitivität,	**Tran**$(\mathbb{Z}, \mid)$:	Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$.

(1) Die Ordnung $\mid$ ist partiell, nicht total, zum Beispiel $2 \nmid 3$ und $3 \nmid 2$.
Es gilt $1 \mid a$ und $a \mid 0$, das heißt 1 ist kleinstes Element und 0 ist größtes.
Es gilt $0 \mid a$ genau dann wenn $a = 0$, und $a \mid 1$ genau dann wenn $a = \pm 1$.

(2) Teilbarkeit ist verträglich mit Addition und Multiplikation:
Aus $a \mid b$ und $a \mid c$ folgt $a \mid b + c$, allgemein $a \mid bu + cv$ für alle $u, v \in \mathbb{Z}$.
Aus $a \mid b$ und $c \mid d$ folgt $ac \mid bd$, insbesondere dank $c \mid c$ auch $ac \mid bc$.
Kürzungsregel: Für $c \neq 0$ sind $ac \mid bc$ und $a \mid b$ äquivalent.

Übung: Beweisen Sie die Aussagen (0–2).

Der euklidische Algorithmus

Für alle $a, b, c \in \mathbb{Z}$ gilt $\mathrm{GT}(a, b) = \mathrm{GT}(b, a - bc)$ und $\mathrm{GGT}(a, 0) = \{\pm a\}$.

$$\mathrm{GT}\begin{bmatrix}138\\24\end{bmatrix} = \mathrm{GT}\begin{bmatrix}24\\18\end{bmatrix} = \mathrm{GT}\begin{bmatrix}18\\6\end{bmatrix} = \mathrm{GT}\begin{bmatrix}6\\0\end{bmatrix} \quad\Longrightarrow\quad \mathrm{ggT}\begin{bmatrix}138\\24\end{bmatrix} = 6$$

Das beschert uns folgenden Satz mit Algorithmus:

Satz A2H: Euklid in $\mathbb{Z}$

(1) Zu je zwei ganzen Zahlen $a, b \in \mathbb{Z}$ existiert ein ggT in $\mathbb{Z}$.
(2) Der folgende Algorithmus berechnet den positiven ggT.

Algo A2H: Berechnung des ggT in $\mathbb{Z}$

Eingabe: zwei ganze Zahlen $a_0, b_0 \in \mathbb{Z}$
Ausgabe: der größte gemeinsame Teiler $a = \mathrm{ggT}(a_0, b_0)$

1: $\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right] \leftarrow \left[\begin{smallmatrix}a_0\\b_0\end{smallmatrix}\right]$ // $\mathrm{GT}(a, b) = \mathrm{GT}(a_0, b_0)$
2: while $b \neq 0$ do $\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right] \leftarrow \left[\begin{smallmatrix}b\\a \operatorname{rem} b\end{smallmatrix}\right]$ // $\mathrm{GT}(a, b) = \mathrm{GT}(b, a - qb)$
3: return $|a|$ // $\mathrm{GGT}(a, 0) = \{\pm a\}$

Der euklidische Algorithmus

Wir müssen zeigen, dass der angegebene Algorithmus korrekt ist, also dass die Methode tatsächlich liefert, was die Spezifikation verspricht.

Die Methode terminiert: Der Wert $|b|$ nimmt in jedem Schritt ab, bis schließlich $b = 0$ erreicht ist und der Algorithmus endet.

Das gelieferte Ergebnis erfüllt die geforderten Bedingungen:
Die Initialisierung $(a, b) \leftarrow (a_0, b_0)$ garantiert $\mathrm{GT}(a, b) = \mathrm{GT}(a_0, b_0)$. Jede Iteration erhält $\mathrm{GT}(a, b) = \mathrm{GT}(b, a - qb)$. Zum Schluss gilt also $\mathrm{GT}(a_0, b_0) = \mathrm{GT}(a, 0)$ und somit $\mathrm{GGT}(a_0, b_0) = \mathrm{GGT}(a, 0) = \{\pm a\}$. Demnach ist $|a|$ der positive ggT von a_0, b_0. QED

🙂 Das ist genial-einfach und einfach-genial. Zudem ist die Methode sehr effizient, das heißt, auch für große Eingaben (a_0, b_0) geeignet.

⚠ Vielleicht kennen Sie ein weiteres Verfahren: Wenn Sie zu a, b die Primfaktorzerlegungen $a = \pm p_1^{a_1} \dots p_n^{a_n}$ und $b_0 = \pm p_1^{b_1} \dots p_n^{b_n}$ kennen, so gilt $\mathrm{ggT}(a, b) = p_1^{t_1} \dots p_n^{t_n}$ mit $t_i = \min\{a_i, b_i\}$ und $\mathrm{kgV}(a, b) = p_1^{v_1} \dots p_n^{v_n}$ mit $v_i = \max\{a_i, b_i\}$. Für große Eingaben a, b ist die Primfaktorzerlegung jedoch hoffnungslos aufwändig. Euklid ist dagegen blitzschnell.

Der erweiterte euklidische Algorithmus nach Bézout

Satz A2I: Bézout in $\mathbb{Z}$

(1) Zu je zwei Zahlen $a, b \in \mathbb{Z}$ existieren $u, v \in \mathbb{Z}$ mit $au + bv = \mathrm{ggT}(a, b)$.
(2) Das ist ein Zertifikat: Aus $d = au + bv \in \mathrm{GT}(a, b)$ folgt $d \in \mathrm{GGT}(a, b)$.
(3) Der folgende Algorithmus berechnet solche **Bézout–Koeffizienten**.

Algo A2I: Berechnung des ggT mit Bézout–Koeffizienten

Eingabe: zwei ganze Zahlen $a_0, b_0 \in \mathbb{Z}$
Ausgabe: drei Zahlen $a, u, v \in \mathbb{Z}$ mit $a = a_0u + b_0v = \mathrm{ggT}(a_0, b_0)$

1: $\left[\begin{smallmatrix} a & u & v \\ b & s & t \end{smallmatrix}\right] \leftarrow \left[\begin{smallmatrix} a_0 & 1 & 0 \\ b_0 & 0 & 1 \end{smallmatrix}\right]$ // Invariante $\left\{\begin{smallmatrix} a=a_0u+b_0v \\ b=a_0s+b_0t \end{smallmatrix}\right.$
2: while $b \neq 0$ do $q \leftarrow a \operatorname{quo} b$ // euklidische Division
3: $\left[\begin{smallmatrix} a & u & v \\ b & s & t \end{smallmatrix}\right] \leftarrow \left[\begin{smallmatrix} b & s & t \\ a-qb & u-qs & v-qt \end{smallmatrix}\right]$ // Invariante $\left\{\begin{smallmatrix} a=a_0u+b_0v \\ b=a_0s+b_0t \end{smallmatrix}\right.$
4: if $a < 0$ then $(a, u, v) \leftarrow -(a, u, v)$ // normiere das Vorzeichen
5: return (a, u, v) // $\mathrm{ggT}(a_0, b_0) = a = a_0u + b_0v$

Beweis: In der ersten Spalte wird der euklidische Algorithmus A2H ausgeführt. Die Invarianten garantieren $a = a_0u + b_0v$. QED

Der erweiterte euklidische Algorithmus nach Bézout

Bemerkung: Die Operationen $q \leftarrow a \operatorname{quo} b$ und

$$\begin{bmatrix} a & u & v \\ b & s & t \end{bmatrix} \leftarrow \begin{bmatrix} b & s & t \\ a - qb & u - qs & v - qt \end{bmatrix}$$

sind Zeilenoperationen, hier für die Invarianten $a = a_0u + b_0v$ und $b = a_0s + b_0t$. Ausführlich: $R_1 \leftrightarrow R_2$, wir tauschen die beiden Zeilen; $R_2 \leftarrow R_2 - qR_1$, von der zweiten Zeile ziehen wir q mal die erste ab.

Numerisches Beispiel: Für $a_0 = 138$ und $b_0 = 24$ erhalten wir:

init		138	1	0	Invariante:	$138 = 1\,a_0 + 0\,b_0$
init		24	0	1	Invariante:	$24 = 0\,a_0 + 1\,b_0$
$q = 5$	$\Rightarrow$	18	1	-5	Invariante:	$18 = 1\,a_0 - 5\,b_0$
$q = 1$	$\Rightarrow$	6	-1	6	Invariante:	$6 = -1\,a_0 + 6\,b_0$
$q = 3$	$\Rightarrow$	0	4	-23	Invariante:	$0 = 4\,a_0 - 23\,b_0$

Somit gilt $\mathrm{ggT}(a_0, b_0) = 6 = ua_0 + vb_0$ mit $u = -1$ und $v = 6$.

Übung: Erfinden und erproben Sie selbst weitere Beispiele!

Algorithmus = Spezifikation + Methode

Unsere ersten Beispiele geben uns wichtiges Anschauungsmaterial.
Ein Algorithmus besteht, wie oben gesehen, immer aus zwei Teilen:

- eine Spezifikation: Was soll er erreichen?
- eine Methode: Wie führt er es aus?

Die Spezifikation erklärt, welche Eingaben erlaubt sind und welche Ausgabe garantiert wird. Am besten verstehen Sie dies als Vertrag: Zum Aufruf des Algorithmus müssen die Vorbedingungen erfüllt sein, bei der Rückgabe sichert der Algorithmus die Nachbedingungen zu.

Jeder Algorithmus, der etwas auf sich hält, muss bewiesen werden!
Zur Korrektheit sind die Angaben der Spezifikation wesentlich:

- Terminiert die angegebene Methode für jede erlaubte Eingabe?
- Liefert die Methode als Ausgabe, was die Spezifikation verspricht?

Nach der Korrektheit können und sollten wir nach den Kosten fragen: Welche Ressourcen (Laufzeit, Speicher, etc.) benötigt der Algorithmus?

Algorithmen und Komplexität sind faszinierende Gebiete der Informatik, und sowohl theoretisch als auch praktisch von überragender Bedeutung.

Satz = Aussage + Beweis

Spezifikation und Methode verhalten sich wie Aussage und Beweis:
Die Methode führt schrittweise von der Eingabe zur Ausgabe.
Der Beweis führt von der Voraussetzung zur Schlussfolgerung.

Die Trennung in Spezifikation und Methode dient der Arbeitsteilung:

- Für die aufrufende Instanz ist allein die Spezifikation maßgeblich, die Methode hingegen ist Privatsache der ausführenden Instanz.
- Ebenso bei einem Satz: Die Nutzerin verlässt sich auf die Aussage, die Mathematikerin garantiert seine Richtigkeit durch einen Beweis.

In sehr vielen Fällen werden Sie Sätze / Algorithmen dankbar nutzen und sich auf deren sorgsame Beweise / Implementierungen verlassen. Ihr Studium gibt Ihnen glücklicherweise die Werkzeuge für beide Seiten, als Nutzer und Hersteller mathematischer Ergebnisse und Methoden.

 In der Mathematik lernen sie viele schöne Ideen und Techniken, nicht zuletzt auch algorithmisches Denken und sorgfältiges Beweisen. Damit erkennen Sie Zusammenhänge und Lösungen, wo andernfalls nur heillose Verwirrung und planloses Herumprobieren möglich wären.

Der Fundamentalsatz der Arithmetik

Gilt $a = b \cdot c$ in $\mathbb{Z}$, so sagen wir a ist **zerlegbar** in die Faktoren b und c. Die **trivialen Zerlegungen** sind $a = (\pm 1) \cdot (\pm a) = (\pm a) \cdot (\pm 1)$; sind dies die einzigen, so nennen wir a **unzerlegbar** (vorsichtig… später „prim“).

Jede natürliche Zahl $a \geq 1$ können wir zerlegen, bis es nicht weiter geht, zum Beispiel $60 = 6 \cdot 10 = (2 \cdot 3) \cdot (2 \cdot 5)$ oder $60 = 4 \cdot 15 = (2 \cdot 2) \cdot (3 \cdot 5)$. Die Wege sind verschieden, aber das Ergebnis ist umgeordnet dasselbe!

Satz A2J: Fundamentalsatz der Arithmetik

(1) Jede natürliche Zahl $a \in \mathbb{N}_{\geq 1}$ können wir zerlegen in ein Produkt

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_\ell$$

der Länge $\ell \in \mathbb{N}$ mit unzerlegbaren Faktoren $p_1, p_2, \ldots, p_\ell \in \mathbb{N}_{\geq 2}$.

(2) Diese Zerlegung ist eindeutig bis auf Umordnung: Gilt

$$p_1 \cdot p_2 \cdot \ldots \cdot p_\ell = q_1 \cdot q_2 \cdot \ldots \cdot q_k$$

mit unzerlegbaren Faktoren $p_1 \leq p_2 \leq \cdots \leq p_\ell$ und $q_1 \leq q_2 \leq \cdots \leq q_k$ in $\mathbb{N}$, so folgt $\ell = k$ und $p_i = q_i$ für alle $i = 1, 2, \ldots, \ell$.

Der Fundamentalsatz: Existenz einer Zerlegung

Für „Produkt unzerlegbarer Faktoren in $\mathbb{N}$“ sage ich kurz UProdukt.

(1) Existenz: Jede natürliche Zahl $a \in \mathbb{N}_{\geq 1}$ ist ein UProdukt

(2) Eindeutigkeit: … auf genau eine Weise (bis auf Umordnung).

Beweis der Existenz (1): Wir führen Induktion und betrachten

$$E = \left\{ n \in \mathbb{N}_{\geq 1} \;\middle|\; \begin{array}{c} \text{Jede natürliche Zahl } a \text{ mit} \\ 1 \leq a \leq n \text{ ist ein UProdukt} \end{array} \right\}$$

Es gilt $1 \in E$: Die Zahl $a = 1$ ist das leere UProdukt der Länge $\ell = 0$.

Sei $n \in E$ und $a = n + 1$. Entweder a ist unzerlegbar: Dann ist a ein UProdukt der Länge 1. Oder a ist zerlegbar gemäß $a = bc$ mit $b, c \geq 2$: Dann gilt $b, c \leq n$, also sind b und c UProdukte der Längen k und ℓ und somit $a = b \cdot c$ ein UProdukt der Länge $k + \ell$. Wir schließen $n + 1 \in E$.

Somit gilt $E = \mathbb{N}_{\geq 1}$: Jede natürliche Zahl $a \geq 1$ ist ein UProdukt. QED

⚠ Die Eindeutigkeit (2) ist schwieriger, interessanter und nützlicher!

Die möglichen Rechenwege bis zu einem UProdukt sind verschieden. Wir müssen zeigen, dass im Endergebnis die unzerlegbaren Faktoren immer dieselben sind bis auf Umordnung. Das ist tatsächlich knifflig.

Fundamentalsatz: unzerlegbar vs prim

Zur weiteren Untersuchung benötigen wir zwei grundlegende Begriffe:

Definition A2K: unzerlegbar / irreduzibel vs prim

Eine ganze Zahl $a \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$ heißt **unzerlegbar** in $\mathbb{Z}$, falls gilt:
Für alle $b, c \in \mathbb{Z}$ folgt aus $a = b \cdot c$ entweder $b = \pm 1$ oder $c = \pm 1$.

Hingegen nennen wir $a \in \mathbb{Z} \smallsetminus \{\pm 1\}$ **prim** in $\mathbb{Z}$, falls gilt:
Für alle $b, c \in \mathbb{Z}$ folgt aus $a \mid b \cdot c$ stets $a \mid b$ oder $a \mid c$.

⚠ Oft wird beides „prim“ genannt. Es sind jedoch zwei verschiedene Eigenschaften, sie verdienen daher auch zwei verschiedene Namen.

Beispiele: Die Elemente $2, 3, 5, 7, 11, 13, 17, 19, \ldots$ sind unzerlegbar.
Die Elemente $4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, \ldots$ sind echt zerlegbar.
Die Elemente 0 und ± 1 sind speziell, weder zerlegbar noch unzerlegbar.

Die Zahl 0 ist prim: $0 \mid ab$ bedeutet $ab = 0$, also $a = 0$ oder $b = 0$.
Die Zahl 2 ist prim: Ist ab gerade, so muss a oder b gerade sein.
Es gilt $10 \mid 4 \cdot 25$, aber $10 \nmid 4$ und $10 \nmid 25$. Somit ist 10 nicht prim.

Fundamentalsatz: unzerlegbar vs prim

🙂 Wir möchten hoffen, dass unzerlegbar und prim in $\mathbb{Z}$ dasselbe sind.
Ist das klar oder müssen wir es beweisen? Wir müssen es beweisen!
Warum müssen wir es beweisen? Schon nebenan in $1 + 4\mathbb{N}$ gilt es nicht:

Beispiel A2L: Hilbert–Monoid

Wir betrachten $(H, \cdot)$ mit $H = 1 + 4\mathbb{N} = \{1, 5, 9, 13, 17, 21, \ldots\}$.
In $(H, \cdot)$ ist 9 unzerlegbar, aber nicht prim: $9 \mid_H 21 \cdot 21$, aber $9 \nmid_H 21$.

Es kommt sogar noch schlimmer: In $(H, \cdot)$ sind $441 = 21 \cdot 21 = 9 \cdot 49$ zwei verschiedene Zerlegungen der Zahl 441 in unzerlegbare Faktoren.

Übung: In Lufthansa-Flugzeugen fehlen die Reihen 13 und 17.
Finden Sie im Monoid $(M, \cdot)$ mit $M = \mathbb{N}_{\geq 1} \smallsetminus \{13, 17\}$ die kleinste Zahl, die mehr als eine Zerlegung in unzerlegbare Faktoren erlaubt.

Übung: In $\mathbb{N}[X]$ gilt $(1 + X + X^2)(1 + X^3) = (1 + X)(1 + X^2 + X^4)$.
Die Faktoren sind unzerlegbar in $\mathbb{N}[X]$, doch zerlegbar in $\mathbb{Z}[X]$.

Für $(\mathbb{Z}, \cdot)$ wollen wir zeigen, dass solche Pathologien nicht auftreten!
Obige Gegenbeispiele zeigen, dass hier ernsthaft etwas zu tun ist.

Fundamentalsatz: die Lemmata von Gauß und Euklid

Lemma A2M: Lemma von Euklid für $\mathbb{Z}$

(0) Jedes Primelement $p \in \mathbb{Z}^*$ ist unzerlegbar in $\mathbb{Z}$.
(1) Jedes unzerlegbare Element p in $\mathbb{Z}$ ist prim in $\mathbb{Z}$.

Beweis: (0) Sei $p \neq 0$ prim und $p = ab$ in $\mathbb{Z}$. Daraus folgt $p \mid a$ oder $p \mid b$. Nehmen wir $p \mid a$ an, also $a = pp'$ für ein $p' \in \mathbb{Z}$. Damit gilt $p = ab = pp'b$, nach Kürzung $1 = p'b$, also $b = \pm 1$. Analog folgt aus $p \mid b$, dass $a = \pm 1$.

(1) Sei $p > 0$ unzerlegbar und $p \mid ab$. Wir müssen $p \mid a$ oder $p \mid b$ zeigen. Hierzu sei $d = \operatorname{ggT}(p, a)$. Es gilt $d \mid p$; da p unzerlegbar ist, gilt entweder $d = 1$ oder $d = p$. (1a) Im Falle $d = p$ gilt dank $d \mid a$ sofort $p \mid a$.
(1b) Im Falle $d = 1$ folgt $p \mid b$ mit dem Lemma von Gauß. QED

Lemma A2N: Lemma von Gauß für $\mathbb{Z}$

Seien $p, a, b \in \mathbb{Z}$ mit $\operatorname{ggT}(p, a) = 1$. Dann folgt aus $p \mid ab$ bereits $p \mid b$.

Beweis: Dank Bézout A2I existieren $u, v \in \mathbb{Z}$, sodass $pu + av = 1$. Die Teilbarkeit $p \mid ab$ bedeutet $ab = pq$ für ein $q \in \mathbb{Z}$. Daraus folgt $b = (pu + av)b = pub + abv = p(ub + qv)$, also $p \mid b$. QED

Fundamentalsatz: die Lemmata von Gauß und Euklid

Diese beiden Lemmata sind der harte Kern des Fundamentalsatzes: Sie besagen, dass unzerlegbar und prim ($\neq 0$) in $\mathbb{Z}$ dasselbe sind! Daraus folgt, wie wir anschließend sehen, die ersehnte Eindeutigkeit der Primfaktorzerlegung im Ring $\mathbb{Z}$ der ganzen Zahlen.

Ich betone nochmals, dass dies keineswegs selbstverständlich ist. Schon in benachbarten, sehr einfachen Beispielen wie $\mathbb{N}[X]$ oder $1 + 4\mathbb{N}$ (A2L) sind manche Elemente unzerlegbar, aber nicht prim, und die Zerlegung in unzerlegbare Faktoren ist nicht eindeutig.

Dass dies dennoch in $\mathbb{Z}$ gelingt, liegt an zwei wesentlichen Zutaten:

- Wir haben die euklidische Division mit Rest A2A.
- Der euklidische Algorithmus A2H berechnet den ggT.
- Der erweiterte Algorithmus A2I berechnet Bézout–Koeffizienten.

Ich habe den Beweis so organisiert, dass diese zentralen Eigenschaften möglichst klar hervortreten und sich später verallgemeinern lassen. Alle Argumente gelten wörtlich genauso für jeden Polynomring $K[X]$ über einem Körper K, und allgemein für sogenannte euklidische Ringe.

Fundamentalsatz: Eindeutigkeit der Zerlegung

Beweis der Eindeutigkeit (2): In $\mathbb{N}$ betrachten wir zwei UProdukte

$$a \;=\; p_1 p_2 \cdots p_n \;=\; q_1 q_2 \cdots q_m.$$

Wir zeigen, dass $n = m$ gilt und nach Umordnung $p_i = q_i$ für alle i. Sei

$$E = \left\{ n \in \mathbb{N} \;\middle|\; \begin{array}{l} \text{Jedes UProdukt der Länge } n \\ \text{ist im obigen Sinne eindeutig.} \end{array} \right\}$$

Es gilt $0 \in E$: Für $n = 0$ haben wir $a = 1$, somit auch $m = 0$.

Aus $n - 1 \in E$ folgt $n \in E$: Wir betrachten zwei UProdukte wie oben.
Der Faktor p_n ist unzerlegbar, somit auch prim dank Euklid A2M.
Also gilt $p_n \mid q_i$ für ein $i \in \{1, \ldots, m\}$. Nach Umordnung gilt $i = m$.
Da auch q_m unzerlegbar ist, folgt $p_n = q_m$. Kürzen ergibt

$$a/p_n \;=\; p_1 p_2 \cdots p_{n-1} p_n \;=\; q_1 q_2 \cdots q_{m-1} q_m.$$

Nach Voraussetzung $n - 1 \in E$ gilt für diese gekürzten Produkte
$n - 1 = m - 1$ und nach Umordnung $p_i = q_i$ für alle $i = 1, \ldots, n - 1$. QED

Fundamentalsatz: Eindeutigkeit der Zerlegung

Bitte schauen Sie sich diesen schönen raffinierten Beweis genau an.
Er ist lehrreiches Anschauungsmaterial für mathematische Arbeit.
Diese Argumentationskette selbst zu finden, ist sicherlich schwierig,
aber sie schrittweise nachzuvollziehen erfordert nur Beharrlichkeit.

Den Fundamentalsatz der Arithmetik kennen Sie vermutlich bereits
aus der Schule, wenn auch vielleicht nicht unter diesem Namen,
sondern vermutlich nur als „Erfahrungstatsache“ oder als ständig
wiederholte, niemals hinterfragte und nie bewiesene Behauptung.

Es ist ein Unterschied, ob Sie Mathematik nur nutzen und anwenden,
oder ob Sie Mathematik selbst machen, verstehen und vertiefen wollen.
Als Anwender/in genügt es, fertige Ergebnisse dankend zu übernehmen.
Als Mathematiker/in wollen Sie die Zusammenhänge genau verstehen.

Unsere obigen Gegenbeispiele belegen eindringlich, dass wir hier
tatsächlich etwas beweisen und akribisch argumentieren müssen.
Dank präziser Vorbereitung ist der Beweis am Ende nicht schwer.
Sorgfältige Arbeit kostet Zeit, doch unsere Mühe lohnt sich!

Rechnen mit Resten modulo 10

Aufgabe: Ich behaupte leichtfertig $13^{14} = 3\,937\,376\,385\,699\,291$.
Weisen Sie ohne Computer nach, dass dieses Behauptung falsch ist.

Lösung: Die Größenordnung 10^{15} stimmt ungefähr, das scheint ok.
Betrachten wir also die letzte Ziffer: Diese ist offensichtlich falsch!

$$1 \xmapsto{\cdot 13} 13 \xmapsto{\cdot 13} 169 \xmapsto{\cdot 13} 2197 \xmapsto{\cdot 13}$$
$$28561 \xmapsto{\cdot 13} 371293 \xmapsto{\cdot 13} 4826809 \xmapsto{\cdot 13} 62748517 \xmapsto{\cdot 13}$$
$$815730721 \xmapsto{\cdot 13} \ldots 3 \xmapsto{\cdot 13} \ldots 9 \xmapsto{\cdot 13} \ldots 7 \xmapsto{\cdot 13} \ldots$$

Die letzte Ziffer von 13^{14} ist demnach 9 und nicht 1.

☺ Die Berechnung der letzten Ziffer lässt sich einfach durchführen.
Wenn Sie den Trick erst einmal kennen, gelingt dies durch Kopfrechnen.
Da uns hier nur die letzte Ziffer interessiert, brauchen wir die vorderen Ziffern gar nicht zu berechnen. Warum ist das so? Gilt das immer?

☺ Dieser genial-einfache Trick heißt „Rechnen modulo 10“.
Diesen wollen wir nun zu einer allgemeinen Methode ausbauen!

Rechnen mit Resten modulo n

Sei $n \in \mathbb{N}_{\geq 2}$. Auf der Restemenge $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ definieren wir die Verknüpfungen $a +_n b := (a + b) \operatorname{rem} n$ und $a \cdot_n b := (a \cdot b) \operatorname{rem} n$.

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

Körper!

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Körper!

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

CRing!

$+_5$	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

$\cdot_5$	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

Körper!

Anwendungen modularer Arithmetik

☺ In der Linearen Algebra sind dies unsere ersten und wichtigsten Beispiele für endliche Körper. Die Klassifikation aller endlichen Körper ist ein schönes Kapitel der Algebra (ab dem dritten Semester).

☺ Auch überall sonst in der Mathematik und Informatik sind die Ringe $\mathbb{Z}_n$ nützlich und allgegenwärtig. Es lohnt sich, sie genau zu verstehen.

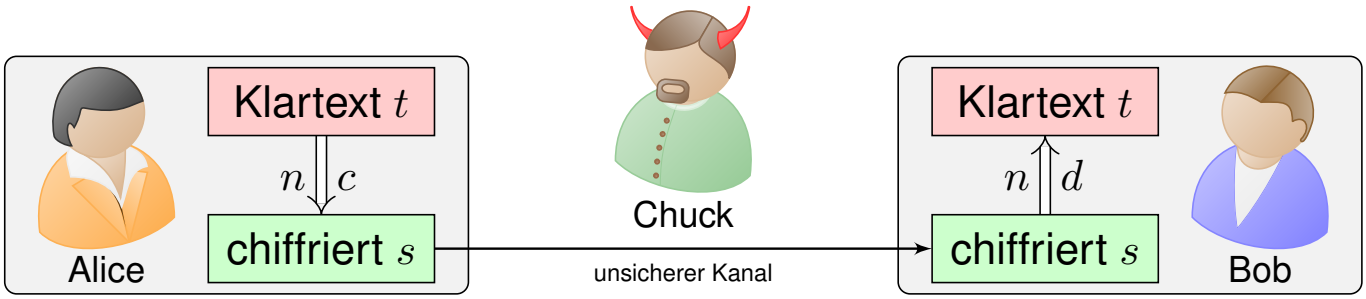
☺ Im Ring $(\mathbb{Z}_n, +_n, \cdot_n)$ können wir rechnen wir in $(\mathbb{Z}, +, \cdot)$, in vielfacher Hinsicht sogar noch besser und effizienter.

Ein Computer mit b Bit rechnet in $\mathbb{Z}_B$ wobei $B = 2^b$.
Wir haben oben schon die Zifferndarstellung diskutiert.

☺ Ich nenne eine spektakuläre Anwendung unter vielen:
Der **RSA–Cryptosystem** ist das erste *asymmetrische* Verschlüsselungsverfahren und bis heute weit verbreitet, siehe `en.wikipedia.org/wiki/RSA_(cryptosystem)`.

Ich werde das RSA–Verfahren hier nur ganz grob skizzieren und mich zusammenreißen, nicht zu viel zu verraten. Ausführen will ich aber die universelle arithmetische Grundlage: den Restklassenring $(\mathbb{Z}_n, +_n, \cdot_n)$.

Anwendung: das RSA–Cryptosystem



Das RSA–Verfahren wurde 1977 entwickelt von R. Rivest, A. Shamir und L. Adleman. Nachrichten werden dabei in $\mathbb{Z}_n$ codiert, mit sehr großem n. Ein vollständiger Schlüssel (n, c, d) besteht aus drei Zahlen $n, c, d \in \mathbb{N}$.

public key (n, c)	–	encrypt	$\mathbb{Z}_n \to \mathbb{Z}_n : t \mapsto s = t^c$
private key (n, d)	–	decrypt	$\mathbb{Z}_n \to \mathbb{Z}_n : s \mapsto t = s^d$

Jeder Schlüssel (n, c, d) wird dabei so konstruiert, dass folgendes gilt:

Korrektheit dank Bijektivität: Es gilt $(t^c)^d = t^{cd} = t$ für alle $t \in \mathbb{Z}_n$. Ver- und Entschlüsselung sind somit zueinander inverse Bijektionen.

Sicherheit dank Komplexität: Allein mit Kenntnis von n, c, s lässt sich der Klartext $t = s^d$ nur mit „unwirtschaftlich hohem Aufwand“ berechnen.

Der Restklassenring $\mathbb{Z}_n$

Sei $n \in \mathbb{N}_{\geq 2}$. Wir betrachten die Restemenge $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ mit der Projektion $p = p_n : \mathbb{Z} \twoheadrightarrow \mathbb{Z}_n : a \mapsto a \operatorname{rem} n$ und folgende Diagramme:

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow[(a,b)\mapsto a+b]{+} & \mathbb{Z} \\ {\scriptstyle p}\downarrow \quad {\scriptstyle p}\downarrow & = & {\scriptstyle p}\downarrow \\ \mathbb{Z}_n \times \mathbb{Z}_n & \xrightarrow[(r,s)\mapsto (r+s) \operatorname{rem} n]{+_n} & \mathbb{Z}_n \end{array} \qquad \begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow[(a,b)\mapsto a\cdot b]{\cdot} & \mathbb{Z} \\ {\scriptstyle p}\downarrow \quad {\scriptstyle p}\downarrow & = & {\scriptstyle p}\downarrow \\ \mathbb{Z}_n \times \mathbb{Z}_n & \xrightarrow[(r,s)\mapsto (r\cdot s) \operatorname{rem} n]{\cdot_n} & \mathbb{Z}_n \end{array}$$

Satz A2o: Konstruktion des Rings $(\mathbb{Z}_n, +_n, 0, \cdot_n, 1)$

(0) Für alle $a, b \in \mathbb{Z}$ gilt $p(a+b) = p(a) +_n p(b)$ und $p(a \cdot b) = p(a) \cdot_n p(b)$. Das bedeutet p ist ein Homomorphismus für Addition und Multiplikation.

(1) Somit ist $(\mathbb{Z}_n, +_n, 0, \cdot_n, 1)$ ein kommutativer Ring (CRing), und die Abbildung $p : \mathbb{Z} \to \mathbb{Z}_n$ ist ein Ringhomomorphismus.

(2) Invertierbare Elemente sind $\mathbb{Z}_n^\times = \{\, a \in \mathbb{Z}_n \mid \operatorname{ggT}(a, n) = 1 \,\}$. Explizite Inversion: Dank Bézout $au + nv = 1$ gilt $au \operatorname{rem} n = 1$.

(3) Genau dann ist $(\mathbb{Z}_n, +_n, 0, \cdot_n, 1)$ ein Körper, wenn $n \in \mathbb{N}_{\geq 2}$ prim ist. In diesem Falle schreiben wir zur Betonung auch $\mathbb{F}_n = \mathbb{Z}_n$ (engl. *field*).

Der Restklassenring $\mathbb{Z}_n$

Auf der Menge $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ der ganzen Zahlen haben wir die übliche Addition $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ und Multiplikation $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. Damit ist $(\mathbb{Z}, +, 0, \cdot, 1)$ ein kommutativer Ring (CRing). Auf der Menge $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ definieren wir nun zwei neue Verknüpfungen:

$$\begin{aligned} +_n &: \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n : (a, b) \mapsto a +_n b = (a + b) \operatorname{rem} n \\ \cdot_n &: \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n : (a, b) \mapsto a \cdot_n b \ = (a \cdot b) \operatorname{rem} n \end{aligned}$$

Diese sind verschieden von $+$ und $\cdot$, daher betonen wir sorgsam n. Die obigen Diagramme stellen die gesamte Situation übersichtlich dar. Dies führt uns zu einer ganz einfachen aber grundlegenden Frage:

Ist es egal, ob wir erst verknüpfen und dann den Rest mod n bilden oder umgekehrt erst Reste mod n bilden und diese dann verknüpfen?

☺ Alle Daten liegen explizit vor, jedes konkrete Beispiel können Sie damit ganz direkt nachrechnen: Führen Sie einige zur Übung aus!

☺ Das allgemeine Ergebnis ist überaus bemerkenswert: Es ist egal, jedes dieser Diagramme kommutiert! Das ist der Inhalt des Satzes.

Der Restklassenring $\mathbb{Z}_n$

Beweis: (0) Vorgelegt seien zwei beliebige ganze Zahlen $a, b \in \mathbb{Z}$.
Wir zerlegen $a = nq_a + r_a$ mit $r_a = p(a)$ und $b = nq_b + r_b$ mit $r_b = p(b)$.
Somit gilt $a + b = n(q_a + q_b) + r_a + r_b$, also $a + b \operatorname{rem} n = r_a + r_b \operatorname{rem} n$,
und $a \cdot b = n^2 q_a q_b + n(q_a r_b + r_a q_b) + r_a r_b$, also $a \cdot b \operatorname{rem} n = r_a \cdot r_b \operatorname{rem} n$.

(1) Wir müssen alle Axiome eines kommutativen Rings nachrechnen.

Wir zeigen zunächst **Ass**$(\mathbb{Z}_n, +_n)$. Vorgelegt seien hierzu $r_1, r_2, r_3 \in \mathbb{Z}_n$.
Hierzu existieren Urbilder $a_1, a_2, a_3 \in \mathbb{Z}$ mit $p(a_i) = r_i$. Damit finden wir:

$$(r_1 +_n r_2) +_n r_3 = \big[p(a_1) +_n p(a_2)\big] +_n p(a_3) = p\big[(a_1 + a_2) + a_3\big]$$
$$r_1 +_n (r_2 +_n r_3) = p(a_1) +_n \big[p(a_2) +_n p(a_3)\big] = p\big[a_1 + (a_2 + a_3)\big]$$

Aus **Ass**$(\mathbb{Z}, +)$ folgt **Ass**$(\mathbb{Z}_n, +_n)$. Ebenso alle anderen Ringaxiome!

☺ Jede Allaussage in $(\mathbb{Z}, +, 0, \cdot, 1)$ vererbt sich auf $(\mathbb{Z}_n, +_n, 0, \cdot_n, 1)$
dank des Homomorphismus $p : \mathbb{Z} \twoheadrightarrow \mathbb{Z}_n$: **Ntr**$(\mathbb{Z}_n, +_n, 0)$, **Com**$(\mathbb{Z}_n, +_n)$,
DL$(\mathbb{Z}_n, +_n, \cdot_n)$, **DR**$(\mathbb{Z}_n, +_n, \cdot_n)$, **Ass**$(\mathbb{Z}_n, \cdot_n)$, **Ntr**$(\mathbb{Z}_n, \cdot_n, 1)$, **Com**$(\mathbb{Z}_n, \cdot_n)$.
Was fehlt noch? Die Negation $-_n : \mathbb{Z}_n \to \mathbb{Z}_n$ ist gegeben durch $-_n 0 = 0$
und $-_n a = n - a$ für $a \in \mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$. Damit gilt **Inv**$(\mathbb{Z}_n, +_n, 0, -_n)$.

Der Restklassenring $\mathbb{Z}_n$

Logik Mengen

Im Ring $(\mathbb{Z}, +, \cdot)$ sind nur die Elemente ± 1 invertierbar:

$$\mathbb{Z}^\times = \{\, \pm 1 \,\}$$

Im Ring $(\mathbb{Z}_n, +_n, \cdot_n)$ ist die Situation viel interessanter:

$$\mathbb{Z}_n^\times = \{\, a \in \mathbb{Z}_n \mid \operatorname{ggT}(a, n) = 1 \,\}$$

(2a) Es gilt „$\supseteq$“: Zu $a \in \mathbb{Z}_n$ mit $\operatorname{ggT}(a, n) = 1$ existieren $u, v \in \mathbb{Z}$ mit
$au + nv = 1$ dank Bézout A2I. Also gilt $a \cdot_n u = 1$, somit $a \in \mathbb{Z}_n^\times$.

(2b) Es gilt „$\subseteq$“: Ist $a \in \mathbb{Z}_n$ invertierbar, so existiert $u \in \mathbb{Z}_n$ mit $a \cdot_n u = 1$.
Das bedeutet $a \cdot u + n \cdot v = 1$ für ein $v \in \mathbb{Z}$, also $\operatorname{ggT}(a, n) = 1$. (A2I)

(3a) Ist $n \in \mathbb{N}_{\geq 2}$ prim, also unzerlegbar (A2M), so gilt $\operatorname{ggT}(a, n) = 1$ für
alle $a \in \{1, \ldots, n-1\} = \mathbb{Z}_n \setminus \{0\}$. Dank (2a) ist a in $\mathbb{Z}_n$ invertierbar.
Also gilt $\mathbb{Z}^\times = \mathbb{Z}^*$, und $(\mathbb{Z}_n, +_n, \cdot_n)$ ist ein Körper.

(3b) Ist $n = a \cdot b$ zerlegbar in $a, b \in \mathbb{N}_{\geq 2}$, so gilt $a, b \in \mathbb{Z}_n \setminus \{0\}$, aber
$a \cdot_n b = 0$ in $\mathbb{Z}_n$. Somit sind a, b Nullteiler in $\mathbb{Z}_n$ und nicht invertierbar.
Also gilt $\mathbb{Z}^\times \subsetneq \mathbb{Z}^*$, und $(\mathbb{Z}_n, +_n, \cdot_n)$ ist kein Körper. QED

Die reellen Zahlen

Wir verfolgen den Aufbau des Zahlensystems $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$:

natürliche Zahlen	$\mathbb{N} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \dots \}$
ganze Zahlen	$\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$
rationale Zahlen	$\mathbb{Q} = \{ z/n \mid z, n \in \mathbb{Z},\ n \neq 0 \}$
reelle Zahlen	$\mathbb{R} =$ „$\mathbb{Q}$ und alle Grenzwerte“

Die **reellen Zahlen** $(\mathbb{R}, +, \cdot, \leq)$ sind ein vollständig geordneter Körper.

Vollständigkeit bedeutet: Zu jeder Teilmenge $M \subseteq \mathbb{R}$, die nicht-leer und nach oben beschränkt ist, existiert in $\mathbb{R}$ eine kleinste obere Schranke.

☺ Das ist die Grundlage der gesamten Analysis. Daraus erhalten wir Grenzwerte von Folgen und Reihen, Ableitungen und Integrale, usw.

Satz A3A: der Körper $\mathbb{R}$ der reellen Zahlen

Solche Körper $(\mathbb{R}, +, \cdot, \leq)$ existieren: Wir können Modelle konstruieren mit Cauchy–Folgen, Dedekind–Schnitten oder Intervallschachtelungen.

Je zwei sind isomorph bis auf einen eindeutigen Isomorphismus.

Die reellen Zahlen

In $\mathbb{Q}$ haben manche Intervallschachtelungen leeren Durchschnitt, etwa die Approximationen von $\sqrt{2} = 1.4142\dots$ oder $\mathrm{e} = 2.7182\dots$ oder $\pi = 3.1415\dots$. Dies sind keine Elemente von $\mathbb{Q}$, wir können sie bestenfalls annähern. Dieses grundlegende Ärgernis lösen wir durch die Erweiterung von den rationalen Zahlen $\mathbb{Q}$ zu den reellen Zahlen $\mathbb{R}$.

☺ Der Körper $(\mathbb{R}, +, \cdot, \leq)$ ist **topologisch vollständig**.

Erst mit $\mathbb{R}$ lassen sich viele fundamentale und praktische Probleme elegant und befriedigend lösen und eine tragfähige Grundlage finden: Zu $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} : x \mapsto x^n$ konstruieren wir die Umkehrfunktion $y \mapsto \sqrt[n]{y}$. In der Analysis entwickeln wir die Exponentialfunktion $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ und ihre Umkehrfunktion $\ln : \mathbb{R}_{>0} \to \mathbb{R}$, trigonometrische Funktionen $\sin, \cos : \mathbb{R} \to \mathbb{R}$ und viele weitere, und beweisen ihre Eigenschaften.

Die Konstruktion der reellen Zahlen $\mathbb{R}$ und der Aufbau der Theorie ist viel reichhaltiger, als ich es hier zusammenfassend skizzieren könnte. Diese wunderbaren Errungenschaften werden wir im Folgenden dankbar aus der Analysis importieren, wo immer sie nötig oder hilfreich sind.

Die komplexen Zahlen: Motivation

Für jede reelle Zahl $x \in \mathbb{R}$ gilt $x^2 \geq 0$, also $x^2 + 1 > 0$. Daher können wir Gleichungen wie $x^2 + 1 = 0$ in $\mathbb{R}$ zwar formulieren, aber nicht lösen.

Können wir eine Lösung $\mathrm{i} = \sqrt{-1}$ erfinden und damit sinnvoll rechnen? Versuchen wir es! Wir wünschen uns einen Körper $\mathbb{C} \supset \mathbb{R}$ der Form

$$\mathbb{C} = \{\, z = x + y\mathrm{i} \mid x, y \in \mathbb{R} \,\}.$$

Wie sehen die Operationen aus? Falls $\mathbb{C}$ existiert, so erwarten wir:

Vergleich:	$x + y\mathrm{i} = u + v\mathrm{i}$ in $\mathbb{C}$	$\Leftrightarrow$	$x = u$ und $y = v$ in $\mathbb{R}$
Addition:	$(x + y\mathrm{i}) + (u + v\mathrm{i})$	$=$	$(x + u) + (y + v)\mathrm{i}$
Multiplikation:	$(x + y\mathrm{i}) \cdot (u + v\mathrm{i})$	$=$	$(xu - yv) + (xv + yu)\mathrm{i}$

Zu jedem Element $z = x + y\mathrm{i}$ haben wir das Negative $-z = (-x) + (-y)\mathrm{i}$ und das Konjugierte $\overline{z} = x - y\mathrm{i}$. Dabei gilt $z\overline{z} = x^2 + y^2$, also

$$\frac{1}{z} = \frac{1}{x + y\mathrm{i}} = \frac{1}{x + y\mathrm{i}} \cdot \frac{x - y\mathrm{i}}{x - y\mathrm{i}} = \frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2}\mathrm{i} = \frac{\overline{z}}{z\overline{z}}$$

Für jedes Element $x + y\mathrm{i} \neq 0$ gilt $x \neq 0$ oder $y \neq 0$, also $x^2 + y^2 > 0$.

Die komplexen Zahlen: Konstruktion

kartesisches Produkt

Ist das erlaubt? Wie können wir die Menge $\mathbb{C}$ und ihre Operationen einwandfrei erklären? Wir nutzen das Modell $\mathbb{R}^2 \xrightarrow{\sim} \mathbb{C} : (x, y) \mapsto x + y\mathrm{i}$.

Satz A3B: Konstruktion des Körpers $\mathbb{C}$ der komplexen Zahlen

Auf der Menge $\mathbb{C} = \mathbb{R}^2$ definieren wir Addition und Multiplikation durch

$$+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C} : (x, y) + (u, v) := (x + u, y + v),$$
$$\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C} : (x, y) \cdot (u, v) := (xu - yv, xv + yu).$$

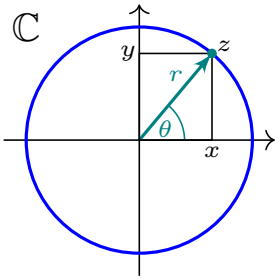
Damit ist $(\mathbb{C}, +, \cdot)$ ein Körper. Hierin ist $(\mathbb{R}, +, \cdot)$ ein Teilkörper dank der Einbettung $\mathbb{R} \hookrightarrow \mathbb{C} : x \mapsto (x, 0)$. Wir schreiben kurz $\mathbb{R} \subset \mathbb{C}$.

Im Körper $\mathbb{C}$ erfüllt das Element $\mathrm{i} = (0, 1)$ die Eigenschaft $\mathrm{i}^2 = -1$. Jedes Element $z \in \mathbb{C}$ schreibt sich eindeutig $z = x + y\mathrm{i}$ mit $x, y \in \mathbb{R}$.

Die Konjugation $\overline{} : \mathbb{C} \to \mathbb{C} : (x, y) \mapsto (x, -y)$ erfüllt $\overline{z + w} = \overline{z} + \overline{w}$ und $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$. Für $z \in \mathbb{C}$ gilt $\overline{z} = z$ genau dann, wenn $z \in \mathbb{R}$.

⚠ Auf $\mathbb{C}$ existiert keine Anordnung zu einem geordneten Körper $(\mathbb{C}, +, \cdot, \leq)$, denn in jedem geordneten Körper gilt $x^2 \geq 0$ für alle x.

Komplexe Zahlen: Polarkoordinaten



Auf $\mathbb{C}$ haben wir die **komplexe Exponentialfunktion**

$$\exp : \mathbb{C} \twoheadrightarrow \mathbb{C}^* : z = x + y\mathrm{i} \mapsto \mathrm{e}^z = \mathrm{e}^x (\cos y + \mathrm{i} \sin y)$$

Jede komplexe Zahl $z = x + y\mathrm{i} \in \mathbb{C}$ lässt sich damit in **Polarkoordinaten** darstellen vermöge

$$z = r\,\mathrm{e}^{\mathrm{i}\theta} = r\,(\cos\theta + \mathrm{i}\sin\theta)$$

mit dem **Betrag** $r = |z| = \sqrt{z\overline{z}} = \sqrt{x^2+y^2}$ und einem **Argument** $\theta \in \mathbb{R}$.
Dabei gilt $\mathrm{e}^{\mathrm{i}\theta} = \mathrm{e}^{\mathrm{i}\varphi}$ genau dann, wenn $\varphi = \theta + 2\pi k$ für ein $k \in \mathbb{Z}$.

Für die Funktionen $\exp$, $\cos$ und $\sin$ gelten **Additionstheoreme**.
Die Multiplikation mit $z \in \mathbb{C}$ erweist sich damit als **Drehstreckung**:

$$z = |z|\,\mathrm{e}^{\mathrm{i}\theta},\ w = |w|\,\mathrm{e}^{\mathrm{i}\varphi} \quad \Longrightarrow \quad z \cdot w = |z| \cdot |w| \cdot \mathrm{e}^{\mathrm{i}(\theta+\varphi)}$$

Aufgabe: In $\mathbb{C}$ hat jede Zahl $z \neq 0$ genau n verschiedene $n$te Wurzeln.

Lösung: Wir lösen die Gleichung $w^n = z$ für $z = r\,\mathrm{e}^{\mathrm{i}\theta}$ und $n \in \mathbb{N}_{\geq 2}$ elegant-explizit durch $w_k = \sqrt[n]{r} \cdot \mathrm{e}^{\mathrm{i}(\theta+2\pi k)/n}$ mit $k = 0, 1, \ldots, n-1$.

Komplexe Zahlen: Polarkoordinaten

Viele wichtige Funktionen lassen sich als **Potenzreihen** darstellen; die nötigen Begriffe und Techniken hierzu lernen Sie in der Analysis.

Dies gilt insbesondere für die Exponentialfunktion, Cosinus und Sinus:

$$\exp(z) = \sum_{k=0}^{\infty} \frac{z^k}{k!} = 1 + z + \frac{z^2}{2} + \frac{z^3}{3!} + \ldots$$

$$\cos(z) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!} z^{2k} = 1 - \frac{z^2}{2} + \frac{z^4}{4!} - \frac{z^6}{6!} + \ldots$$

$$\sin(z) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!} z^{2k+1} = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \frac{z^7}{7!} + \ldots$$

Jede dieser drei Reihen konvergiert für jeden Parameter $z \in \mathbb{C}$.
Wir erhalten so die zugehörigen Funktionen $\exp, \cos, \sin : \mathbb{C} \to \mathbb{C}$.

Mit konvergenten Potenzreihen können wir rechnen wie mit Polynomen: addieren und multiplizieren, differenzieren und integrieren, usw.

Komplexe Zahlen: Polarkoordinaten

Aus diesen Potenzreihen lesen wir die **Euler–Formel** ab:

$$\exp(\mathrm{i}z) = \cos z + \mathrm{i}\sin z, \quad \cos(z) = \frac{\mathrm{e}^{\mathrm{i}z} + \mathrm{e}^{-\mathrm{i}z}}{2}, \quad \sin(z) = \frac{\mathrm{e}^{\mathrm{i}z} - \mathrm{e}^{-\mathrm{i}z}}{2\mathrm{i}}$$

Hieraus folgt sofort die geometrisch nützliche Gleichung

$$\cos(z)^2 + \sin(z)^2 = 1.$$

Auch die Ableitungen lesen wir direkt aus den Potenzreihen ab, denn Potenzreihen dürfen wir termweise ableiten und erhalten so:

$$\exp' = \exp, \quad \sin' = \cos, \quad \cos' = -\sin$$

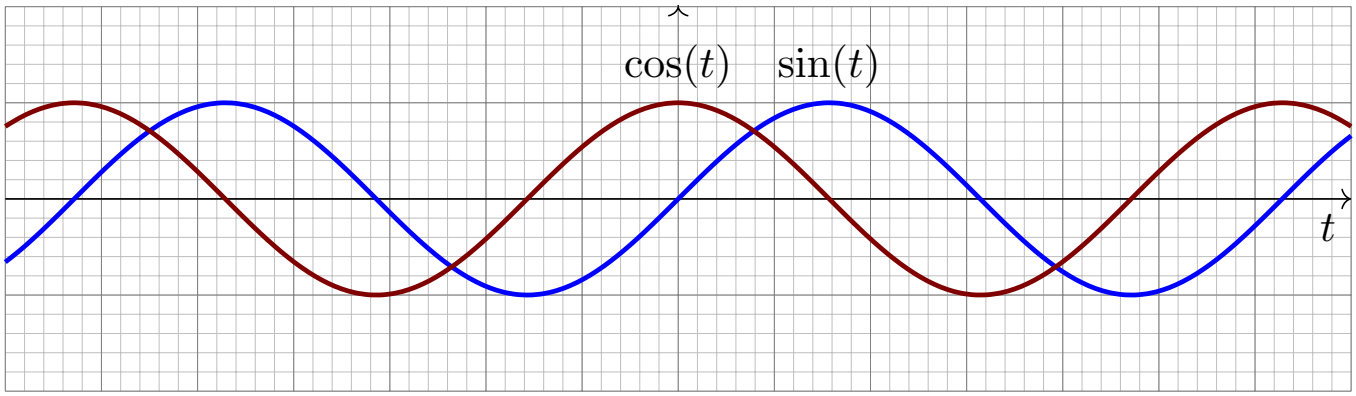
Diese Funktionen sind daher sehr oft nützlich, etwa bei der Integration als Stammfunktionen, als Lösungen von Differentialgleichungen, usw.

Aus der Reihe $\exp(z) = \sum_{k=0}^{\infty} \frac{z^k}{k!}$ folgt das **Additionstheorem**

$$\exp(z+w) = \exp(z) \cdot \exp(w) \quad \text{für alle } z, w \in \mathbb{C}.$$

Abkürzend schreiben wir $\mathrm{e}^z := \exp(z)$ mit $\mathrm{e} := \exp(1) = 2.71828182\ldots$.

Komplexe Zahlen: Polarkoordinaten



Die trigonometrischen Funktionen $\sin, \cos$ heißen **Kreisfunktionen**, denn $t \mapsto (\cos t, \sin t)$ parametrisiert die Kreislinie $x^2 + y^2 = 1$.

Sie sind periodisch, mit Periode 2π, wobei $\pi = 3.14159265\ldots$.
Somit ist auch $\exp : \mathbb{C} \to \mathbb{C}$ periodisch, mit Periode $2\pi\mathrm{i}$.

Für $\sigma, \theta \in \mathbb{R}$ gilt $\exp(\sigma + \mathrm{i}\theta) = \mathrm{e}^{\sigma}(\cos\theta + \mathrm{i}\sin\theta)$. Jede komplexe Zahl $z \in \mathbb{C}$ lässt sich damit in **Polarkoordinaten** darstellen vermöge

$$z = r\,\mathrm{e}^{\mathrm{i}\theta} = r\,(\cos\theta + \mathrm{i}\sin\theta)$$

mit $r = |z| \in \mathbb{R}_{\geq 0}$ und $\theta \in \mathbb{R}$. Im Falle $z = 0$ ist θ beliebig. Im Falle $z \neq 0$ ist θ eindeutig bis Addition eines ganzzahligen Vielfachen von 2π.

Komplexe Zahlen: Fundamentalsatz

Die Erweiterung $\mathbb{C} \supset \mathbb{R}$ beschert dem Polynom X^2+1 die Nullstellen $\pm\mathrm{i}$; damit zerfällt $X^2+1 = (X-\mathrm{i})(X+\mathrm{i})$ in Linearfaktoren über $\mathbb{C}$.

Erfreulicherweise gilt dies sogleich für *jedes* Polynom über $\mathbb{C}$:

Satz A3c: Fundamentalsatz der Algebra (der komplexen Zahlen)

Zu jedem Polynom $P(X) = X^n + c_1 X^{n-1} + \cdots + c_n$ mit $c_1, \ldots, c_n \in \mathbb{C}$ existieren Nullstellen $z_1, \ldots, z_n \in \mathbb{C}$ sodass $P(X) = (X-z_1)\cdots(X-z_n)$.

Für $n = 1$ ist das trivial, für $n = 2$ leicht dank Mitternachtsformel:

$$\begin{aligned} z^2 + 2pz + q = 0 \quad &\Longleftrightarrow \quad z^2 + 2pz + p^2 = p^2 - q \\ &\Longleftrightarrow \quad (z+p)^2 = p^2 - q \\ &\Longleftrightarrow \quad z \in \left\{ -p \pm \sqrt{p^2 - q} \right\} \end{aligned}$$

Wur nutzen hier: In $\mathbb{C}$ hat jede Zahl $\neq 0$ genau zwei Quadratwurzeln!
Für $n \geq 3$ ist der Beweis raffinierter, siehe Umlaufzahl in der Topologie.

Komplexe Zahlen: Fundamentalsatz

Nicht jedes Polynom $P \in \mathbb{R}[X]$ hat Nullstellen in $\mathbb{R}$, etwa $P = X^2+1$.
Über $\mathbb{C}$ hingegen zerfällt jedes Polynom $P \in \mathbb{C}[X]$ in Linearfaktoren.

🙂 Damit ist der Körper $\mathbb{C}$ **algebraisch abgeschlossen**. Dieser Satz vollendet den langen Marsch der Vervollständigung des Zahlensystems: faszinierend als Theorie und grundlegend für praktische Anwendungen.

Aufgabe: Zerlegen Sie das Polynom $X^2 - \mathrm{i}$ in Linearfaktoren über $\mathbb{C}$.

Lösung: Die Gleichung $z^2 = \mathrm{i}$ hat in $\mathbb{C}$ die Lösungen $\pm(1+\mathrm{i})/\sqrt{2}$.
In $\mathbb{C}[X]$ gilt demnach $X^2 - \mathrm{i} = (X - (1+\mathrm{i})/\sqrt{2})(X + (1+\mathrm{i})/\sqrt{2})$.

Aufgabe: Zerlegen Sie das Polynom $X^n - 1$ in Linearfaktoren über $\mathbb{C}$.

Lösung: Die Gleichung $z^n = 1$ hat in $\mathbb{C}$ die Lösungen $z_k = \mathrm{e}^{2\pi\mathrm{i}k/n}$, also

$$X^n - 1 = \textstyle\prod_{k=0}^{n-1} (X - \mathrm{e}^{2\pi\mathrm{i}k/n}).$$

Die komplexen Zahlen $z_0, z_1, \ldots, z_{n-1}$ sind die **$n$ten Einheitswurzeln**.
Sie bilden die Ecken eines regemäßigen n–Ecks auf dem Einheitskreis.
Polynome und ihre Nullstellen untersuchen wir genauer in Kapitel G.

Hamiltons Quaternionen

Definition A3D: Quaternionen erweitern die komplexen Zahlen.

Die **Quaternionen** $(\mathbb{H}, +, 0, \cdot, 1)$ sind ein Schiefkörper mit $\mathbb{H} \supset \mathbb{C} \supset \mathbb{R}$; dabei gilt $\mathbb{H} = \{\, q = \alpha + \beta\mathrm{i} + \gamma\mathrm{j} + \delta\mathrm{k} \mid \alpha, \beta, \gamma, \delta \in \mathbb{R} \,\}$ mit

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-\mathrm{j}$
j	j	$-\mathrm{k}$	-1	i
k	k	j	$-\mathrm{i}$	-1

kurz $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1$, $\mathrm{ijk} = -1$ und $\mathrm{ij} = -\mathrm{ji}$.

Jede reelle Zahl $\alpha \in \mathbb{R}$ kommutiert dabei mit $\mathrm{i}, \mathrm{j}, \mathrm{k}$, also mit jeder Quaternion.

Die Konjugation ist $\mathbb{H} \to \mathbb{H} : q = \alpha + \beta\mathrm{i} + \gamma\mathrm{j} + \delta\mathrm{k} \mapsto \overline{q} = \alpha - \beta\mathrm{i} - \gamma\mathrm{j} - \delta\mathrm{k}$.

Übung: Prüfen Sie die Ringaxiome nach (direkt oder später in B1G). Die Inversion in $\mathbb{H}$ ist erfreulich leicht. Ausmultiplizieren ergibt

$$q \cdot \overline{q} = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 =: |q|^2 \quad \in \quad \mathbb{R}_{\geq 0}.$$

Somit ist jede Quaternion $q \neq 0$ invertierbar und $q^{-1} = \overline{q}/|q|^2$.

Hamiltons Quaternionen

Die Körper $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ der rationalen, reellen und komplexen Zahlen werden Ihnen nahezu überall in der Mathematik begegnen, gar noch häufiger in ihren naturwissenschaftlich-technischen Anwendungen.

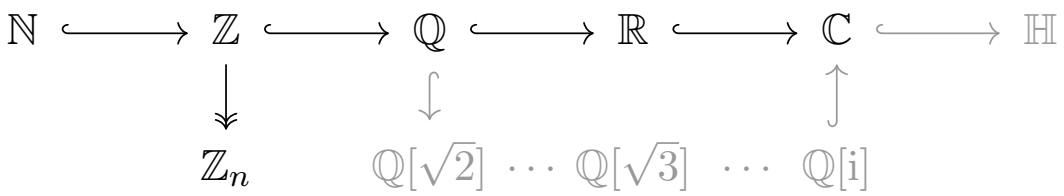
Der Schiefkörper $\mathbb{H}$ der Quaternionen ist weniger prominent und dient uns vor allem zur Illustration, als lockendes oder mahnendes Beispiel. Er zeigt eindrücklich, dass es auch „nicht-kommutative Körper“ gibt.

Ohne konkrete Beispiele und Gegenbeispiele könnten Sie allzu leicht dem Irrglauben verfallen, dass die hier vorgestellten Begriffe gar nicht realisierbar sind. Dagegen helfen am besten explizite Konstruktionen.

Ausgehend von $\mathbb{R}$ können Sie für $\mathbb{C}$ und $\mathbb{H}$ direkt die Körperaxiome nachrechnen; das ist eine gute Übung, aber leider auch etwas länglich. Später gelingt es mühelos mit dem allgemeinen Matrixkalkül (B1F, B1G).

Ein Repertoire an Gegen/Beispielen aufzubauen kostet Zeit und Mühe, doch es lohnt sich. Wie folgen unserer mathematischen Neugier, daran schulen Sie Ihre Anschauung und üben Ihre technische Ausführung.

Zusammenfassung: Aufbau des Zahlensystems



Die **natürlichen Zahlen** $(\mathbb{N}, +, 0, \cdot, 1)$ sind ein kommutativer Halbring; dabei erfüllt $(\mathbb{N}, 0, s)$ mit $s : n \mapsto n + 1$ die Dedekind–Peano–Axiome.

Die **ganzen Zahlen** $(\mathbb{Z}, +, 0, \cdot, 1)$ sind ein kommutativer Ring mit $\mathbb{N} \subset \mathbb{Z}$ als Teilhalbring und $\mathbb{Z} = \{\, z = a - b \mid a, b \in \mathbb{N} \,\}$.

Die **rationalen Zahlen** $(\mathbb{Q}, +, 0, \cdot, 1)$ sind ein Körper mit $\mathbb{Z} \subset \mathbb{Q}$ als Teilring und $\mathbb{Q} = \{\, q = z/n \mid z, n \in \mathbb{Z},\ n \neq 0 \,\}$.

Die **reellen Zahlen** $(\mathbb{R}, +, 0, \cdot, 1)$ sind ein Körper mit $\mathbb{Q} \subset \mathbb{R}$ und vollständig geordnet durch $x \leq y \ \Leftrightarrow\ \exists a \in \mathbb{R} : x + a^2 = y$.

Die **komplexen Zahlen** $(\mathbb{C}, +, 0, \cdot, 1)$ sind ein Körper mit $\mathbb{R} \subset \mathbb{C}$ dabei gilt $\mathbb{C} = \mathbb{R}[\mathrm{i}] = \{\, z = x + \mathrm{i}y \mid x, y \in \mathbb{R} \,\}$ mit $\mathrm{i}^2 = -1$.

Zusammenfassung: Aufbau des Zahlensystems

Dieses erste Kapitel ist eine Einführung und stellt Ihnen Themen vor, die in den folgenden Kapiteln genauer ausgeführt und vertieft werden. Dazu werden die Begriffe und Techniken hier zunächst motiviert und zugleich soweit erklärt, dass Sie damit sofort arbeiten können.

Wichtige Ergebnisse, Begriffe und Techniken dieses Kapitels:

- Sie sollten sicher in den folgenden Zahlbereichen rechnen können: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, K[X], \mathbb{Z}_n$. Einige sind Ihnen bekannt, andere noch neu.
- Irrationalität von $\sqrt{2}$ (A1F) und die Körpererweiterung $\mathbb{Q}[\sqrt{2}]$ (A1G)
- Kurzschreibweise für Summen $\sum_{i \in I} a_i$ und Produkte $\prod_{i \in I} a_i$ (A135)
- euklidische Division mit Rest in den ganzen Zahlen $\mathbb{Z}$ (A2A)
- Teilbarkeit, ggT und kgV, euklidischer Algorithmus (A2H)
- erweiterter euklidischer Algorithmus nach Bézout (A2I)
- Fundamentalsatz der Arithmetik (A2J) mit Beweis
- Fundamentalsatz der Algebra (A3C) ohne Beweis

Ausblick auf das erste Semester

Diese Einführung vermittelt einen ersten Überblick und erste Methoden, sodass Sie sofort einsteigen, damit üben und bereits arbeiten können:

- ehrliches Beispielmaterial zu den Grundlagen der Mathematik,
- präzise Definitionen und Konstruktionen, soweit bereits möglich,
- wichtige Sätze und instruktive Beweise in unmittelbarer Reichweite.

Das ist ein Sprung ins kalte Wasser, dafür anregend statt langatmig. Die benötigten Begriffe und Techniken werden wir in den nächsten Kapiteln gründlich aufarbeiten. Ich möchte Ihren Appetit und Ihre Neugier wecken, die Mathematik genauer verstehen zu wollen:

- Aussagenlogik und vollständige Induktion
- Mengen, Relationen und Abbildungen
- Monoide und Gruppen, Ringe und Körper

Die entsprechenden Stellen sind durch gelbe Merkzettel markiert, die auf die Ausführungen der folgenden Kapitel verweisen.

Ausblick auf das erste Semester

Mathematische Grundlagen	Algebraische Grundlagen	Lineare Strukturen
Mathematische Logik und Beweistechniken	Monoide und Gruppen	Lineare Räume und lineare Abbildungen
Mengen und Abbildungen	Ringe und Körper	Basis und Dimension
Kombinatorik und Quotienten	Polynomringe	Darstellung linearer Abbildungen durch Matrizen
Ordnungsrelationen und Kardinalität	Matrixringe	Signatur und Determinante