Markus P. Brodmann · Fred Rohrer

Zahlentheorie

für Studierende des Lehramtes der Sekundarstufe I

Universität Zürich/Pädagogische Hochschule Zürich

Inhaltsverzeichnis

Abbildungsverzeichnis

Einleitung

Das vorliegende Skript ist konzipiert als Begleittext zur Vorlesung „Zahlentheorie“ für Studierende des Lehramtes der Sekundarstufe I an der Pädagogischen Hochschule Zürich. Das Skript enthält mehr Material, als in dieser zweistündigen Vorlesung gründlich behandelt werden kann. Dadurch soll den Studierenden die Möglichkeit geboten werden, den Vorlesungsstoff aus eigener Initiative zu vertiefen, was durchaus auch selektiv geschehen darf. Aus diesem Grund haben wir versucht, das Skript so zu gestalten, dass es auch zum Selbststudium benutzt werden kann. Der Aufbau und die Abfolge der Themen entspricht aber dem der Vorlesung, damit das Skript seiner Funktion als Begleittext genügt.

Die Vorlesung und das Skript sollen in erster Linie vertieftes Hintergrundwissen für den Arithmetikunterricht auf der Sekundarstufe I vermitteln. Entsprechend gehen wir beim behandelten Stoff wenig über das hinaus, was im Bereich der Arithmetik schon an der Sekundar- und Mittelschule zur Sprache kommt. Dafür soll mit grösserer Strenge und Systematik vorgegangen werden, als dies in der Schule möglich ist. Auf diese Weise soll versucht werden, durch Vertiefen „Bekanntes zu festigen“. Wir gehen allerdings nicht so weit, die Arithmetik aus ihren Axiomen aufzubauen. Vielmehr wagen wir einen „Einstieg auf halber Höhe“, indem wir einiges, was von der Schule her geläufig ist, als Grundlage voraussetzen, auf der wir dann in strenger Weise aufbauen.

Natürlich soll auch dem Aspekt „Neues kennenlernen“ Rechnung getragen werden. Ausgehend vom Chinesischen Restsatz führen wir in zwei Stufen an die Restklassenarithmetik heran. Auf diese Weise soll die Brücke zwischen der Arithmetik und der „abstrakten“ Algebra (d.h. der „Lehre von den algebraischen Strukturen“) geschlagen werden. Die diophantischen Gleichungen werden wir zum Anlass nehmen, uns mit den rationalen Punkten auf Quadriken zu befassen. Mit diesem ersten Blick in die „arithmetische Geometrie“ wird die äusserst wichtige Verbindung zwischen der Arithmetik und der (algebraischen) Geometrie beispielhaft geknüpft. Was an wesentlich Neuem behandelt wird, ordnet sich also stark dem Gesichtspunkt „interdisziplinär denken“ unter. Es fehlt (vorerst noch?) ein Thema, welches die wichtige Beziehung zwischen der Arithmetik und der Analysis zur Darstellung bringt, also ein Thema aus der „analytischen Zahlentheorie“.

Skript und Vorlesung sind aufgegliedert in vier Teile.

- Teil A: Vergleichen und Zählen
- Teil B: Teiler, Reste und Primzahlen
- Teil C: Von der Arithmetik zur Algebra: Restklassen
- Teil D: Von der Arithmetik zur Geometrie: diophantische Gleichungen und rationale Punkte auf Kurven

Jeder dieser vier Teile wird eingeleitet mit einer kurzen Zusammenfassung und mit einer Liste von Tipps zum Selbststudium. Die Teile A und D bestehen je aus 3 Kapiteln, die Teile B und C aus je 2 Kapiteln. Zu Beginn jedes Kapitels wird ein kurzer Überblick über den zu behandelnden Stoff gegeben. Zu jedem Themenkreis werden verschiedenartige Übungsaufgaben angeführt. Das Skript umfasst einen fünften Teil, in welchem Lösungen zu einer Auswahl dieser Aufgaben zu finden sind.

Gemäss der „klassischen“ Auffassung von Vorlesung wird unser Vorgehen in erster Linie bestimmt von der Leitidee der „systematischen Einführung“. Das „episodische“ Element, das in der Zahlentheorie sehr ausgeprägt ist und ihr auch einen ganz besonderen Reiz verleiht, wird dabei natürlich etwas zu kurz kommen. Zum Ausleich wird dieses Element in den Übungsaufgaben stärker gepflegt. Wir hoffen, auf diese Weise auch diejenigen Studierenden anzusprechen, die sich den Zahlen lieber durch Knobeln und Tüfteln nähern wollen, als auf begrifflichem Wege. Die Zahlentheorie lässt Raum für beide Zugänge und erhält aus deren Zusammenspiel auch auf dem Niveau der heutigen Forschung immer wieder neue Impulse.

Wir hoffen, mit dieser Vorlesung den zukünftigen Lehrpersonen der Sekundarstufe I einen gewissen Eindruck davon zu vermitteln, dass das „Grundmaterial der Arithmetik“ – die ganzen Zahlen – ein Gegenstand von grosser Reichhaltigkeit und Tiefe ist, der noch weit davon entfernt ist, erforscht zu sein.

Unser besonderer Dank geht an Franziska Robmann, für die sorgfältige Erstellung des LaTeX-Files und für die sehr ansprechende Umsetzung der Handskizzen zu den Illustrationen.

Teil A
Vergleichen und Zählen

ZUSAMMENFASSUNG

In diesem ersten Teil der Vorlesung werden die folgenden drei Kapitel behandelt:

- Was ist Zahlentheorie?
- Das Prinzip der kleinsten Zahl
- Vollständige Induktion

Im ersten dieser Kapitel werfen wir einige Schlaglichter auf das Gebiet der elementaren Zahlentheorie, wobei auch philosophische und prämathematische Fragen gestellt werden. Wir stellen zudem eine Reihe von Übungsaufgaben, welche auf Themen ausgerichtet sind, die später zur Sprache kommen werden. Wir legen schliesslich einige grundlegende Sprech- und Schreibweisen fest – aber auch unsere „Arbeitsphilosophie".

Mit dem *Prinzip der kleinsten Zahl* greifen wir das Thema des *Vergleichens* natürlicher Zahlen auf. Das genannte Prinzip werden wir als Axiom einführen und damit ein starkes Hilfsmittel für alle folgenden Überlegungen zur Verfügung haben. Wir werden dies auch gleich am Beispiel eines ersten Satzes demonstrieren, den wir mit dem Prinzip der kleinsten Zahl beweisen werden. Schliesslich führen wir *endliche Mengen von natürlichen Zahlen* ein – und zwar als beschränkte Mengen natürlicher Zahlen. Dieser auf dem Konzept des Vergleichens beruhende Endlichkeitsbegriff befriedigt allerdings noch nicht und wird später nochmals aufgegriffen.

Vom Prinzip der kleinsten Zahl ist es ein kleiner Schritt bis zum *Prinzip der vollständigen Induktion*. Ohne das fundamentale Beweisprinzip der vollständigen Induktion „wäre die Mathematik nichts als eine grosse Tautologie" (H. Poincaré). Deshalb schrecken wir nicht davor zurück, dieses Prinzip hier (nochmals) einzuführen, es mit Beispielen zu illustrieren und mit Übungsaufgaben zu vertiefen. Mit dem Induktionsprinzip sind wir aber auch bei der Idee des *Zählens* angelangt. Wir werden diese an sich noch prämathematische Idee präzise fassen und dann ein kleines Wegstück in der „Theorie des Zählens" beschreiten,

allerdings ohne uns in den Bereich der Kombinatorik vorzuwagen, in welchem aus der „Theorie“ eine „Kunst“ wird.

TIPPS FÜR DAS SELBSTSTUDIUM

- *Kapitel 1:* Nehmen Sie die Sache nicht zu ernst! Wenn Ihnen die Übungen grössere Schwierigkeiten bereiten, denken Sie daran: Unverzagtheit gehört genauso zum Betreiben von Mathematik wie Hartnäckigkeit. Zudem kommen die Themen der Übungsaufgaben später in der Vorlesung nochmals eingehender zur Sprache.

- *Kapitel 2:* Dieses Kapitel sollten Sie möglichst vollständig durcharbeiten. Das Thema ist für die Mathematik grundlegend. Zudem werden Sie hier konfrontiert mit typisch mathematischen Denk- und Vorgehensweisen: strenge Definitionen, eindeutig formulierte Sätze, logisch geführte Beweise. Sehen Sie die Übungsaufgaben als Denkschulung an.

- *Kapitel 3:* Wenn Sie glauben, das Thema „vollständige Induktion“ bereits zu kennen (aus der Schule oder aus der Vorlesung „Grundbegriffe“), können Sie dieses Kapitel überhüpfen oder überfliegen. Empfohlene Zwischenlandungen bei 3.4–3.8 („Fitnesstest“) und im Bereich 3.12–3.26 („Weiss ich schon, was Zählen ist?“).

Kapitel 1

Was ist Zahlentheorie?

Überblick

Die elementare Zahlentheorie ist die Lehre von den ganzen Zahlen. Sie fragt also nach den Gesetzmässigkeiten, die sich hinter dem Vergleichen von und dem Rechnen mit ganzen Zahlen verbergen.

Einige dieser Gesetzmässigkeiten wollen wir in dieser Vorlesung genauer kennenlernen. Dabei lassen wir uns von drei Anliegen leiten:

- *Bekanntes festigen:* Aus der Schularithmetik schon bekannte Begriffe (Teiler, Divisionsreste, grösster gemeinsamer Teiler, kleinstes gemeinsames Vielfaches, Primzahlen, ...) und Sätze (Chinesischer Restsatz, eindeutige Zerlegung in Primfaktoren, ...) sollen mit mathematischer Strenge behandelt werden.

- *Neues kennenlernen:* Einige Begriffe der nächsthöheren Abstraktionsstufe (Restklassen, Restklassenarithmetik, ...) sollen eingeführt, untersucht und durch Beispiele und Übungsaufgaben „konkretisiert“ werden.

- *Interdisziplinär denken:* Es soll aufgezeigt werden, dass die Arithmetik kein isoliertes Teilgebiet der Mathematik ist, sondern eng mit anderen Disziplinen – wie etwa der Algebra und der Geometrie – zusammenhängt (Restklassenringe und -körper, diophantische Gleichungen, rationale Punkte auf Kurven, ...).

In diesem einführenden Kapitel wollen wir einige Schlaglichter auf verschiedene Fragen werfen, die sich auf ganze Zahlen beziehen. Dabei stören wir uns nicht daran, dass philosophisches, prämathematisches und auch schon mathematisches in bunter Mischung zur Sprache kommt. Ein Grossteil der hier aufgegriffenen Fragen weist auf Dinge hin, die später in der Vorlesung noch eingehender behandelt werden.

Im Einzelnen kommen folgende Punkte zur Sprache:

- *Bezeichnungen und Festsetzungen,*
- *Einige Fragen und Probleme,*
- *Zwischen Arithmetik und Geometrie: ein Beispiel,*
- *Ausblick,*
- *Vorkenntnisse.*

Bezeichnungen und Festsetzungen

Bevor wir mit unseren Ausführungen beginnen, legen wir einige Bezeichnungs- und Sprechweisen fest, welche wir später dauernd verwenden werden.

Notationen 1.1. A) $\mathbb{R}$ bezeichne die *Menge aller reellen Zahlen*. Es gelten also etwa $1 \in \mathbb{R}$, $\frac{3}{17} \in \mathbb{R}$, $\sqrt{7} \in \mathbb{R}$, $\pi \in \mathbb{R} \ldots$ Die Menge $\mathbb{R}$ veranschaulicht man oft durch eine Gerade, die *Zahlengerade*.

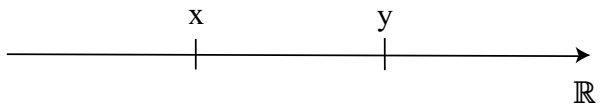


Abbildung 1.1: Zahlengerade

Dabei soll jede Zahl $x \in \mathbb{R}$ durch genau einen Punkt der Zahlengeraden dargestellt werden. Meist sprechen wir der Einfachheit halber nicht vom „Punkt, der x darstellt“, sondern nur vom „Punkt x“. Sind $x, y \in \mathbb{R}$ mit $x < y$ (x *kleiner als* y), so soll der Punkt x „links“ vom Punkt y liegen.

B) $\mathbb{Z}$ bezeichne die *Menge aller ganzen Zahlen*, also $\mathbb{Z} := \{0, \pm 1, \pm 2, \ldots\}$. Natürlich gilt $\mathbb{Z} \subseteq \mathbb{R}$, d.h. jede ganze Zahl ist auch eine reelle Zahl. Mit der üblichen Vereinbarung, dass die Distanz zwischen den Punkten x und $x+1$ auf der Zahlengeraden für alle $x \in \mathbb{R}$ gleich gross sein soll, erhält man für die Menge $\mathbb{Z}$ die folgende Veranschaulichung, bei der $\mathbb{Z}$ als ein „Zahlengitter“ (mit Maschenweite 1) erscheint.

C) $\mathbb{N}$ bezeichne die *Menge aller natürlichen Zahlen*, d.h. die Menge der positiven ganzen Zahlen

$$\mathbb{N} := \{1, 2, 3, \ldots\} = \{n \in \mathbb{Z} | n > 0\}.$$

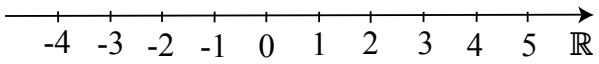


Abbildung 1.2: Gitter der ganzen Zahlen

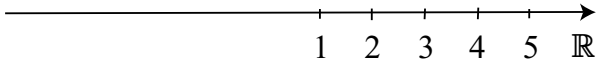


Abbildung 1.3: Halbgitter der natürlichen Zahlen

Anschaulich präsentiert sich die Menge $\mathbb{N}$ als ein rechtsseitiges Halbgitter, das bei 1 beginnt. Natürlich gilt $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{R}$.

D) $\mathbb{N}_0$ bezeichne die *Menge aller nichtnegativen ganzen Zahlen*

$$\mathbb{N}_0 := \{0, 1, 2, \ldots\} = \{0\} \cup \mathbb{N} = \{n \in \mathbb{Z} | n \geq 0\}.$$

Auch diese Menge erscheint auf der Zahlengeraden als rechtsseitiges Halbgitter, das nun allerdings bei 0 beginnt.

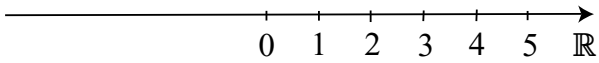


Abbildung 1.4: Halbgitter der nichtnegativen ganzen Zahlen

E) $\mathbb{Q}$ bezeichne die *Menge aller rationalen Zahlen*, d.h. aller Brüche,

$$\mathbb{Q} := \left\{ \frac{m}{n} \middle| \, m \in \mathbb{Z}, \ n \in \mathbb{N} \right\}.$$

Direkt anschaulich lässt sich die Menge $\mathbb{Q}$ nicht mehr als Teilmenge der Zahlengeraden charakterisieren. •

Einige Fragen und Probleme

Von alters her und von Kindsbeinen an stellt sich der Mensch Fragen über Zahlen wie etwa:

Fragen 1.2. A) Was heisst es zu zählen? Was ist überhaupt eine Zahl? „Gibt es“ Zahlen überhaupt?

B) Gibt es eine grösste Zahl?

C) Ist denn

$$10^{10^{10^{10^{10^{10}}}}}$$

überhaupt eine natürliche Zahl?

D) Gibt es gleichviele ganze Zahlen wie natürliche Zahlen?

E) Gibt es mehr Brüche als natürliche Zahlen?

F) Gibt es mehr reelle Zahlen als Brüche? •

Aufgabe 1.3. Machen Sie sich Gedanken zu den obigen Fragen! Fassen Sie in Stichworten zusammen. •

Die obigen Fragen sind eher philosophischer als mathematischer Art. Keine kann im mathematischen Sinn direkt beantwortet werden, ohne dass vorher alle auftretenden Begriffe streng gefasst werden. Andererseits hat jede dieser Fragen Anlass zu umwälzenden Entwicklungen in der Mathematik gegeben.

Aus dem Umgang mit arithmetischen Aufgaben ergeben sich naturgemäss vielerlei Fragen, wie etwa die folgenden:

Fragen 1.4. A) Warum „funktioniert“ die Neunerprobe?

B) Gibt es eine natürliche Zahl, welche beim Teilen durch 19 den Rest 4 und beim Teilen durch 8 den Rest 5 lässt? Wie findet man solche (oder alle diese) Zahlen?

C) Wie kann ich $1+2+3+\cdots+129$ schnell ausrechnen, oder wie $1+2^2+3^2+\cdots+87^2$?

D) Kann man beliebige natürliche Zahlen miteinander multiplizieren, wenn man nur addieren, subtrahieren und verdoppeln kann?

E) Wie hätte ein Römer die Zahl 71 528 193 310 471 geschrieben? •

Bei Fragen dieser Art geht es im Grunde immer um Algorithmen der Arithmetik, nämlich um die Fragen:

- Leistet ein gegebener Algorithmus das Erwartete? (A)
- Gibt es einen Algorithmus, der ein gegebenes Problem löst? (B), (C), (D), (E)
- Gibt es einen „schnellen“ Algorithmus zu einem an sich lösbaren Problem? (C), (E)

Fragen dieser Art gehören eindeutig in den mathematischen Bereich, selbst wenn sie nicht mit mathematischer Strenge formuliert sind. (Was ist ein „schneller“ Algorithmus?)

Aufgaben 1.5. A) Beantworten Sie Frage 1.4 B).

B) Was wissen Sie zur Frage 1.4 C)?

p	x	y
0	13	21
13	13	20
13	26	10
13	52	5
65	52	4
65	104	2
65	208	1
273	208	0

C) Im Pyramidengrab eines ägyptischen Infanten wurde eine in Stein gemeisselte Darstellung einer Schulstunde entdeckt. Die Darstellung zeigt unter anderem die folgende Tabelle (Ziffern ins Arabische übertragen), in welcher die Lösung einer Rechnungsaufgabe gezeigt wird.

Welche Rechnungsaufgabe wurde hier gelöst und mit welchem Algorithmus? (*Hinweis:* $p + xy =?$) Es besteht ein Zusammenhang zu einer der Fragen aus 1.4. Zu welcher?

D) Schreiben Sie Ihr Geburtsjahr mit arabischen und römischen Ziffern. •

Zwischen Arithmetik und Geometrie: ein Beispiel

Seit der Antike wurden immer wieder Zusammenhänge zwischen der Arithmetik und der Geometrie entdeckt und untersucht. Sehr oft ging es dabei um Anwendungen (Landvermessung etc.); dazu ein historisches Beispiel aus dem Grenzbereich Arithmetik/Geometrie, welches schon in der Antike bekannt war.

Beispiel und Aufgaben 1.6. (*Aufrollbares Winkelmass*)

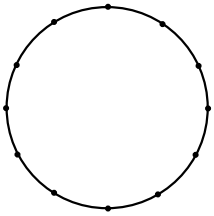


Abbildung 1.5: Schnur mit 12 Knoten

A) In einer geschlossenen Schnur sind in gleicher Entfernung voneinander $s = 12$ Knoten angebracht. Markieren Sie 3 Knoten so, dass ein Winkelmass (zum Messen rechter Winkel) entsteht.

B) Geben Sie zwei weitere Zahlen s an so, dass bei gleichmässigem Anbringen von s Knoten auf einer kreisförmig geschlossenen Schnur ein Winkelmass (zum Messen rechter Winkel) entsteht. Dabei soll s jeweils nicht durch 12 teilbar sein.

C) Geben Sie eine Knotenzahl s an, bei der zwei (wesentlich) verschiedene Winkelmasse möglich sind.

D) Ein Hersteller von aufrollbaren Winkelmassen möchte wissen, für welche Knotenzahlen s überhaupt ein Winkelmass möglich ist. Formulieren Sie das mathematische Problem, das dazu gelöst werden muss. •

Im obigen Beispiel hilft die Arithmetik ein geometrisches Problem zu verstehen. Das Umgekehrte ist aber ebenfalls möglich, wie die folgende Aufgabe nahelegt.

Aufgaben 1.7. (*Rationale Punkte auf dem Einheitskreis*) Wir betrachten den Einheitskreis

$$\mathbb{S} := \{(u, v) \in \mathbb{R}^2 | u^2 + v^2 = 1\} \subseteq \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}.$$

Sei $(u, v) \in \mathbb{S}$ mit $0 \leq v < 1$. Wir legen eine Gerade g durch die Punkte $(0, 1)$ und (u, v). Der Schnittpunkt von g mit der u-Achse sei $(t, 0)$.

A) Skizzieren Sie die oben beschriebene Situation.

B) Drücken Sie t durch u und v aus.

C) Drücken Sie u und v aus durch t.

D) Zeigen Sie: $u, v \in \mathbb{Q} \Longleftrightarrow t \in \mathbb{Q}$.

E) Konstruieren Sie zu jedem positiven Bruch t drei natürliche Zahlen

$$x = x(t), y = y(t), z = z(t) \text{ mit } x^2 + y^2 = z^2.$$

(*Hinweis:* Mit dem gemeinsamen Nenner von u und v multiplizieren.)

F) Formulieren Sie einen Zusammenhang zwischen Teil E) und 1.6 D). •

Frage 1.8. Können Sie Aufgabe 1.7 leicht und selbständig lösen? Wenn

ja: Haben Sie auch schon an ein Mathematikstudium gedacht?

nein: Keine Angst, das Thema wird später eingehender behandelt (s. Kapitel 9). •

Typisch für das Denken der Mathematiker ist der Hang zur Verallgemeinerung. So gelangt man, ausgehend von 1.6 D) oder 1.7 F) durch Verallgemeinerung ziemlich natürlich zur folgenden Frage:

Frage 1.9. Sei n eine natürliche Zahl mit $n \geq 3$. Gibt es natürliche Zahlen x, y, z so, dass

$$x^n + y^n = z^n?$$ •

Aufgaben 1.10. A) Haben Sie schon von der Frage 1.9 gehört? Wenn ja, fassen Sie in Stichworten zusammen.

B) Worin besteht die Verallgemeinerung beim Übergang von 1.6 D) und 1.7 F) zu 1.9? •

Ausblick

Der nachfolgende Kommentar will einen ersten Ausblick auf unsere Vorlesung und das Gebiet der Zahlentheorie überhaupt geben.

Kommentar 1.11. Wissen wir nun was Zahlentheorie ist? Wohl kaum! Kein Mathematiker könnte den Begriff „Zahlentheorie“ abschliessend fassen. Trotzdem besteht eine grosse Übereinstimmung der Meinungen über die Bedeutung und das Wesen der Zahlentheorie:

- Die Zahlentheorie ist die „Königin der mathematischen Disziplinen“.
- Die Zahlentheorie ist die faszinierendste Disziplin der Mathematik.
- Die Zahlentheorie ist die schwierigste Disziplin der Mathematik.
- ...

Wenige Mathematiker würden wohl diesen Aussagen widersprechen. Doch was bleibt für uns in dieser Vorlesung?

Die Zahlen, genauer die ganzen Zahlen, bilden das Fundament der Arithmetik. Sie sind das „Arbeitsmaterial“ mit dem im Mathematikunterricht an der Schule täglich umgegangen wird. Für zukünftige Lehrpersonen ist es also naheliegend, sich ein paar „nichtalltägliche“ Gedanken über dieses Arbeitsmaterial zu machen.

Dabei wird man mit etwas Fleiss und Hartnäckigkeit bald entdecken, dass das „Arbeitsmaterial ganze Zahlen“ alles andere als eintönig oder langweilig ist. Dringt man etwas in die Welt der Zahlen ein, so erweist sich diese bald als ein hervorragendes Turn- und Trainingsgerät zur Denkschulung, das einlädt zum Knobeln, Ausprobieren, sich Wundern und Philosophieren. Wenn diese Vorlesung dazu beiträgt, dass nur ein Funke dieses Geistes in den Arithmektikunterricht auf der Sekundarstufe I überspringt, so hat sie ihren Zweck erfüllt. Dieser Geist des Vermutens und Staunens ist nicht etwa „unwissenschaftlich“, sondern vielmehr der eigentliche Antrieb für jede mathematische Forschungstätigkeit. Kaum eine mathematische Disziplin ist so geeignet wie die Zahlentheorie, diese neugierig forschende Denkweise zu fördern; denn schon die Beherrschung der arithmetischen Grundfähigkeiten genügt, um weiterreichende „Entdeckungsreisen“ im Bereich der ganzen Zahlen zu unternehmen. Aber auch für den Mathematiker ist die Zahlentheorie noch voller Rätsel und Geheimnisse. Wohl in keinem anderen Bereich des menschlichen Denkens treten so viele Probleme auf, die zwar einfach zu stellen, aber nur mit viel Aufwand oder überhaupt (noch) nicht lösbar sind.

In diesem Sinne hoffen wir, mit unserer Vorlesung nicht nur Hintergrundwissen für den Schulunterricht zu vermitteln, sondern auch die Neugier und die Entdeckerfreude zu wecken. •

Vorkenntnisse

Bevor wir uns auf den Weg in die Zahlentheorie machen, sollten wir unser „Basislager“ beziehen und mindestens umreissen, von welchen Voraussetzungen wir ausgehen. Diese Festlegung können wir nicht allzu streng vornehmen und sie eher als Grundlage einer „Arbeitsphilophie“ für diese Vorlesung verstehen. In der folgenden Serie von Bemerkungen fassen wir dazu einiges zusammen. Wir verweisen dazu auch ausdrücklich auf die Vorlesung „Grundbegriffe“.

Bemerkungen 1.12. A) (*Grundbegriffe der Mengenlehre*) Wir setzen diese im Umfang der Mittelschule als bekannt voraus. Besonders wichtig sind für uns Abbildungen zwischen Mengen, so etwa die Begriffe der injektiven, der surjektiven und der bijektiven Abbildung, aber auch der Begriff der Komposition zweier Abbildungen oder der Begriff der Umkehrabbildung einer (bijektiven) Abbildung.

Wir haben in diesem Kapitel zwar schon stillschweigend die aus der Schule bekannten Schreibweisen der Mengenlehre verwendet. Wir wollen aber trotzdem nochmals kurz an diese erinnern:

$x \in \mathbb{M}$ steht für die Aussage „x ist ein Element der Menge $\mathbb{M}$“ ; $x \notin \mathbb{M}$ steht entsprechend für die Verneinung dieser Aussage.

$\mathbb{M} \subseteq \mathbb{P}$ steht für die Aussage „$\mathbb{M}$ ist eine Teilmenge von $\mathbb{P}$“ ; $\mathbb{M} \nsubseteq \mathbb{P}$ steht entsprechend für die Verneinung dieser Aussage.

$\mathbb{M} \cap \mathbb{P}$ und $\mathbb{M} \cup \mathbb{P}$ stehen für den Durchschnitt resp. die Vereinigung der Mengen $\mathbb{M}$ und $\mathbb{P}$, $\mathbb{M} \backslash \mathbb{P}$ für die Komplementärmenge von $\mathbb{P}$ in $\mathbb{M}$.

Weiter steht $\mathbb{M} \times \mathbb{P}$ für das kartesische Produkt (d.h. die Paarmenge) von $\mathbb{M}$ und $\mathbb{P}$.

Die leere Menge wird mit $\emptyset$ bezeichnet.

Sind $\mathbb{M}$ eine Menge und $\mathcal{A}$ eine Eigenschaft, die auf Elemente $x \in \mathbb{M}$ zutrifft oder nicht, so steht $\{x \in \mathbb{M} | \mathcal{A}(x)\}$ für die Menge aller Elemente x aus $\mathbb{M}$, für welche $\mathcal{A}$ zutrifft.

B) (*Formale Logik*) Wir verwenden einige von der Schule her bekannte Grundbegriffe und Schreibweisen. Insbesondere bezeichnen $\wedge, \vee, \neg, \Longrightarrow$ und $\Longleftrightarrow$ die Konjunktion, die Disjunktion, die Negation, die Implikation resp. die Äquivalenz von Aussagen. Genauer: Sind $\mathcal{A}$ und $\mathcal{B}$ zwei Aussagen, so stehen $\mathcal{A} \wedge \mathcal{B}$ für die Aussage „$\mathcal{A}$ und $\mathcal{B}$“, $\mathcal{A} \vee \mathcal{B}$ für die Aussage „$\mathcal{A}$ oder $\mathcal{B}$“, $\neg \mathcal{A}$ für die Aussage „nicht $\mathcal{A}$“, $\mathcal{A} \Longrightarrow \mathcal{B}$ für die Aussage „gilt $\mathcal{A}$, so gilt auch $\mathcal{B}$“ und $\mathcal{A} \Longleftrightarrow \mathcal{B}$ für die Aussage „$\mathcal{A}$ gilt genau dann, wenn $\mathcal{B}$ gilt“.

Mit $\forall$ und $\exists$ bezeichnen wir den Allquantor resp. den Existenzquantor. Ist $\mathcal{A}(x)$ eine Aussage in der Variablen x, und ist $\mathbb{M}$ eine Menge, so stehen $\forall x \in \mathbb{M} : \mathcal{A}(x)$ also für die Aussage „für alle Elemente x von $\mathbb{M}$ gilt $\mathcal{A}(x)$“ und $\exists x \in \mathbb{M} : \mathcal{A}(x)$ für die Aussage „es gibt ein Element x von $\mathbb{M}$ so, dass $\mathcal{A}(x)$ gilt“.

Schliesslich verwenden wir in Definitionen immer wieder die Schreibweisen $:=$ und $:\Longleftrightarrow$ für die Gleichheit resp. die Äquivalenz „gemäss Definition“. So bedeuten $f := g$ also „f ist nach Definition gleich g“ und $\mathcal{A} :\Longleftrightarrow \mathcal{B}$ „$\mathcal{A}$ ist nach Definition äquivalent zu $\mathcal{B}$“. Der Doppelpunkt steht dabei immer auf der Seite des definierten Objekts oder Begriffs.

C) (*Grundbegriffe der Arithmetik*) Wir haben in 1.1 bereits vorausgesetzt, dass die Zahlbereiche $\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$ bekannt sind und in diesen auch schon gerechnet. Dabei wollen wir natürlich bleiben. Insbesondere setzen wir die vier Grundoperationen in $\mathbb{R}$ und den Umgang mit diesen als bekannt voraus.

Etwas formalistischer gesagt: Wir setzen den „Körper der reellen Zahlen“, den „Unterkörper der rationalen Zahlen“ und den „Ring der ganzen Zahlen“ als bekannt voraus. (Diese Sprechweise wird später noch erläutert werden.) Für uns ist wichtig:

- *Summen, Differenzen, Produkte und Quotienten rationaler Zahlen sind wieder rationale Zahlen.*

- *Summen, Differenzen und Produkte ganzer Zahlen sind wieder ganze Zahlen.*
- *Summen und Produkte natürlicher Zahlen sind wieder natürliche Zahlen.*

D) (*Die Grösser-kleiner-Relation*) Auch diese setzen wir als bekannt voraus, z. B. die Tatsache, dass zwischen zwei reellen Zahlen x, y immer eine der drei Beziehungen

$$x = y, x < y \text{ oder } y < x$$

gilt. Stillschweigend werden wir auch immer wieder die folgenden Regeln verwenden:

- $$x < y \Longrightarrow x + z < y + z;$$
- $$x < y \wedge 0 < a \Longrightarrow ax < ay.$$

E) Mehr als das oben Umrissene wollen wir nicht voraussetzen. Insbesondere setzen wir den Begriff des Zählens nicht voraus. Vielmehr wollen wir diesen später mit Hilfe der gemäss A), B), C) und D) erlaubten Mittel mathematisch streng fassen. Dies tun wir, weil sich der Begriff des Zählens nicht nur auf Zahlen bezieht, sondern auch auf andere Objekte. In diesem Sinne wird dann das „Gedankenkonstrukt“ des Zahlengitters $\mathbb{N}$ zum „Massstab“, mit dem wir Objekte zählen. •

Einen vollständig axiomatischen Aufbau der Zahlentheorie zu geben ist im Rahmen dieser Einführung nicht möglich und wäre auch wenig sinnvoll. Wir vertrauen vielmehr darauf, dass die oben umrissenen Vorkenntnisse eine hinreichend stabile Unterlage bilden, von der aus wir dann logisch weiterargumentieren können.

Kapitel 2

Das Prinzip der kleinsten Zahl

Überblick

Wir lernen die vielleicht wichtigste Aussage der ganzen Mathematik kennen, das sogenannte *Prinzip der kleinsten Zahl*:

- *In jeder nichtleeren Menge von natürlichen Zahlen gibt es eine kleinste Zahl.*

Dieses Prinzip ist so einleuchtend, dass wir es als Axiom, d.h. als nicht zu beweisende Grundannahme betrachten.

Das Prinzip der kleinsten Zahl bezieht sich auf den Grösser-kleiner-Vergleich von natürlichen Zahlen. Entsprechend werden wir in diesem Kapitel einige grundlegende Themen behandeln, welche alle mit dem Vergleichen von Zahlen zusammenhängen:

- *der Begriff des Minimums,*
- *das Prinzip der kleinsten Zahl als Axiom und Beweismethode,*
- *der Begriff des Maximums,*
- *endliche Mengen natürlicher Zahlen.*

Der Begriff des Minimums

Um unser Auge für das Prinzip der kleinsten Zahl zu schärfen, holen wir etwas aus und fragen nach der Existenz kleinster Zahlen in beliebigen Mengen reeller Zahlen. Dies führt zum Begriff des Minimums.

Definition und Bemerkung 2.1. A) Sei $\emptyset \neq \mathbb{M} \subseteq \mathbb{R}$ und sei $x \in \mathbb{R}$. Wir sagen, x sei eine *kleinste Zahl von* $\mathbb{M}$, wenn x zu $\mathbb{M}$ gehört und $x \leq y$ für jede weitere Zahl $y \in \mathbb{M}$ gilt. Formal geschrieben:

$$x \text{ ist eine kleinste Zahl von } \mathbb{M} :\Longleftrightarrow (x \in \mathbb{M}) \wedge \ (\forall y \in \mathbb{M} : x \leq y).$$

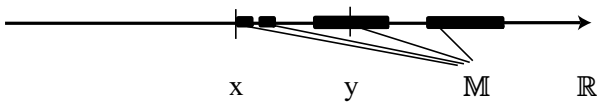


Abbildung 2.1: Kleinste Zahl einer Menge reeller Zahlen

B) Wichtig ist folgende Beobachtung:

Besitzt $\mathbb{M}$ *überhaupt eine kleinste Zahl* x*, so ist diese eindeutig bestimmt.*

Ist nämlich x' eine weitere kleinste Zahl von $\mathbb{M}$, so folgt $x' \in \mathbb{M}$. Weil x eine kleinste Zahl von $\mathbb{M}$ ist, gelten $x \in \mathbb{M}$ und $x \leq x'$. Weil x' eine kleinste Zahl von $\mathbb{M}$ ist, folgt $x' \leq x$. Es gilt also $x = x'$ und die behauptete Eindeutigkeit ist bewiesen.

C) Nehmen wir nun an, $\mathbb{M}$ besitze eine kleinste Zahl x. Nach Teil B) ist diese dann eindeutig festgelegt durch $\mathbb{M}$. Wir nennen x dann *die (!) kleinste Zahl* oder das *Minimum von* $\mathbb{M}$ und schreiben $x = \min(\mathbb{M})$. Also:

$$x = \min(\mathbb{M}) \Longleftrightarrow (x \in \mathbb{M}) \wedge (\forall y \in \mathbb{M} : x \leq y).$$

•

Beispiele 2.2. A) Das Intervall

$$[0, 1[:= \{x \in \mathbb{R} | 0 \leq x < 1\}$$

hat offenbar die kleinste Zahl 0, d.h. es gilt

$$\min([0, 1[\ ) = 0.$$

B) Das Intervall

$$]0, 1[:= \{x \in \mathbb{R} | 0 < x < 1\}$$

hat gar keine kleinste Zahl. Wäre nämlich x eine kleinste Zahl von $]0, 1[$, so gälte $x \in]0, 1[$, also $0 < x < 1$. Dann folgte aber $0 < \frac{x}{2} < x < 1$. Es ergäben sich $\frac{x}{2} \in]0, 1[$ und $\frac{x}{2} < x$, und somit wäre x nicht die kleinste Zahl von $]0, 1[$. Widerspruch! •

Aufgaben 2.3. A) Zeigen Sie, dass die Menge $\mathbb{M} := \{x \in \mathbb{Q} | x > 1\}$ keine kleinste Zahl besitzt.

B) Zeigen Sie, dass die Menge $\mathbb{U} := \{\frac{1}{n} | n \in \mathbb{N}\}$ kein Minimum besitzt.

C) Zeigen Sie, dass $\mathbb{M} := \{x^2 - x + 2 | x \in \mathbb{R}\}$ ein Minimum besitzt und bestimmen Sie dieses.

D) Sei $a \in \mathbb{R}$ und sei $\mathbb{Q}_{\geq a} := \{q \in \mathbb{Q} | a \leq q\}$. Zeigen Sie folgende Aussagen:

a) $a \in \mathbb{Q} \Longrightarrow a = \min(\mathbb{Q}_{\geq a})$.

b) $a \notin \mathbb{Q} \Longrightarrow \min(\mathbb{Q}_{\geq a})$ existiert nicht.

(*Hinweis zu b):* Verwenden Sie Folgendes: Ist $a < q$, so gibt es ein $q' \in \mathbb{Q}$ mit $a < q' < q$.)

E) Seien $\mathbb{U}, \mathbb{V} \subseteq \mathbb{R}$ zwei Mengen, welche ein Minimum haben. Zeigen Sie, dass

$$\min(\mathbb{U} \cup \mathbb{V}) = \min\{\min(\mathbb{U}), \min(\mathbb{V})\}.$$

F) Geben Sie zwei Mengen $\mathbb{U}, \mathbb{V} \subseteq \mathbb{R}$ an so, dass gleichzeitig folgende Aussagen gelten:

$\min(\mathbb{U})$ und $\min(\mathbb{V})$ existieren, $\mathbb{U} \cap \mathbb{V} \neq \emptyset$ und $\min(\mathbb{U} \cap \mathbb{V})$ existiert nicht. •

Das Prinzip der kleinsten Zahl als Axiom

Wir haben oben gesehen (vgl. 2.2 B)), dass beliebige nichtleere Teilmengen positiver Zahlen kein Minimum haben müssen. Für die natürlichen Zahlen sieht dies anders aus, denn es gilt ja das schon genannte Prinzip der kleinsten Zahl. Wir wollen dieses Prinzip jetzt zu einer Grundannahme erklären und postulieren deshalb:

Axiom 2.4. *(Prinzip der kleinsten Zahl)*

Jede nichtleere Menge $\mathbb{T} \subseteq \mathbb{N}$ besitzt eine kleinste Zahl.

Bemerkung 2.5. Einen mathematischen Beweis für das oben formulierte Prinzip der kleinsten Zahl können wir nicht geben. Das Prinzip ist aber derart einleuchtend, dass wir es gerne für richtig halten, besonders wenn wir einmal gesehen haben, wie viel dieses Prinzip einbringt. Deshalb erklären wir es (in Übereinstimmung mit der grossen Mehrheit der Mathematiker) zum Axiom. •

Beispiel 2.6. (*Kleinster Nenner eines Bruches*) Sei $q \in \mathbb{Q}$. Für eine Zahl $n \in \mathbb{N}$ sind die folgenden beiden Aussagen gleichbedeutend:

(i) Es gibt ein $m \in \mathbb{Z}$ so, dass $q = \frac{m}{n}$;

(ii) $nq \in \mathbb{Z}$.

Genügt eine Zahl $n \in \mathbb{N}$ diesen beiden Bedingungen, so heisst n ein *Nenner von* q. Mit $N(q)$ wollen wir die Menge aller Nenner von q bezeichnen, also

$$N(q) := \left\{ n \in \mathbb{N} \,\middle|\, \exists m \in \mathbb{Z} : q = \frac{m}{n} \right\} = \{n \in \mathbb{N} | nq \in \mathbb{Z}\}.$$

Weil q ein Bruch ist, besitzt q einen Nenner. Also ist $\emptyset \neq N(q) \subseteq \mathbb{N}$. Nach 2.4 besitzt $N(q)$ also eine kleinste Zahl, wobei diese nach 2.1 B) eindeutig bestimmt ist. Diese kleinste Zahl von $N(q)$ nennen wir den *kleinsten Nenner von* q. Wir bezeichnen diesen kleinsten Nenner von q mit $\eta(q)$. Also:

$$\eta(q) := \min\{n \in \mathbb{N} | nq \in \mathbb{Z}\} \ ; \ (q \in \mathbb{Q}). \qquad \bullet$$

Aufgaben 2.7. A) Bestimmen Sie die Menge

$$\{q \in \mathbb{Q} | 0 \leq q \leq 1 \wedge \eta(q) = 36\}.$$

B) Bestimmen Sie $\eta(1{,}648)$ und $\eta(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{7})$. $\bullet$

Das Prinzip der kleinsten Zahl als Beweismethode

Wir wollen nun demonstrieren, wie das Prinzip der kleinsten Zahl als Beweismethode eingesetzt werden kann.

Wir beweisen nämlich den nachfolgenden Satz über die Wurzeln natürlicher Zahlen, der sich auch mit Hilfe der „eindeutigen Zerlegung in Primfaktoren“ beweisen liesse. Die Zerlegung in Primfaktoren wollen wir aber erst später behandeln. Wir werden dann auch nochmals auf unseren Satz zu sprechen kommen.

Satz 2.8. *Sei $n \in \mathbb{N}$. Dann gilt entweder $\sqrt{n} \in \mathbb{N}$ oder $\sqrt{n} \in \mathbb{R}\backslash\mathbb{Q}$.*

Anders gesagt: Die Quadratwurzel einer natürlichen Zahl ist entweder wieder eine natürliche Zahl oder irrational.

Beweis: Wir nehmen an, unsere Behauptung wäre falsch. Dann gibt es eine Zahl $n \in \mathbb{N}$ so, dass weder $\sqrt{n} \in \mathbb{N}$ noch $\sqrt{n} \in \mathbb{R}\backslash\mathbb{Q}$. Für diese Zahl n gilt dann $\sqrt{n} \notin \mathbb{N}$ und $\sqrt{n} \in \mathbb{Q}$. Wegen $\sqrt{n} \in \mathbb{Q}$ besitzt $\sqrt{n}$ einen kleinsten Nenner $\eta(\sqrt{n}) \in \mathbb{N}$. Zur Vereinfachung schreiben wir $r := \eta(\sqrt{n})$. Es gelten dann

$$(\alpha) \qquad r\sqrt{n} \in \mathbb{Z};$$

$$(\alpha') \qquad r'\sqrt{n} \notin \mathbb{Z} \text{ für alle } r' \in \mathbb{N} \text{ mit } r' < r.$$

Wegen $\sqrt{n} \notin \mathbb{N}$ ist $r \neq 1$, also $r > 1$. Wegen $\sqrt{n} \notin \mathbb{N}$ ist $n \neq 1$, d.h. $n > 1$, also $\sqrt{n} > 1$. Es folgt $r\sqrt{n} > r$ und damit

$$(\beta) \qquad r\sqrt{n} - r > 0.$$

Beidseitige Multiplikation mit $\sqrt{n}$ liefert $rn - r\sqrt{n} = (r\sqrt{n} - r)\sqrt{n} > 0$, d.h.

$$(\beta') \qquad r\sqrt{n} - nr < 0.$$

Wir betrachten nun die Menge

$$\mathbb{T} := \{s \in \mathbb{N} | r\sqrt{n} - sr \leq 0\}.$$

Gemäss (β') ist $n \in \mathbb{T}$, also $\emptyset \neq \mathbb{T} \subseteq \mathbb{N}$. Nach 2.4 besitzt $\mathbb{T}$ also eine kleinste Zahl t. Gemäss (β) ist $1 \notin \mathbb{T}$. Insbesondere ist $t \neq 1$, also $t > 1$. Es folgt $t - 1 \in \mathbb{N}$. Wegen $t - 1 < t$ und $t = \min(\mathbb{T})$ ist $t - 1 \notin \mathbb{T}$. Schreiben wir $w := t - 1$, so gelten also

$$(\gamma) \qquad w \in \mathbb{N}\backslash\mathbb{T};$$

$$(\gamma') \qquad w + 1 = t \in \mathbb{T}.$$

Gemäss (γ') gilt $r\sqrt{n} - (w + 1)r \leq 0$, also $r\sqrt{n} - wr \leq r$. Dabei kann $r\sqrt{n} - wr = r$ nicht gelten, denn sonst wäre ja $\sqrt{n} = w + 1 \in \mathbb{N}$ im Widerspruch zu unserer Annahme. Deshalb muss $r\sqrt{n} - wr < r$ gelten. Schreiben wir $r' := r\sqrt{n} - wr$, so folgt

$$(\delta) \qquad r' < r.$$

Wegen $r\sqrt{n} \in \mathbb{Z}$ (s. (α)) und $w, r \in \mathbb{Z}$ gilt auch $r' = r\sqrt{n} - wr \in \mathbb{Z}$. Wegen $w \notin \mathbb{T}$ (s. (γ)) ist $r' = r\sqrt{n} - wr > 0$. Insgesamt gilt also

$$(\delta') \qquad r' \in \mathbb{N}.$$

Schliesslich gilt $r'\sqrt{n} = (r\sqrt{n} - wr)\sqrt{n} = r\sqrt{n}^2 - wr\sqrt{n} = rn - w(r\sqrt{n})$ und wegen $r, n, w \in \mathbb{Z}$ und $r\sqrt{n} \in \mathbb{Z}$ (s. (α)) folgt

$$(\delta'') \qquad r'\sqrt{n} \in \mathbb{Z}.$$

Aber (δ), (δ') und (δ'') ergeben zusammen einen Widerspruch zu (α'). Unsere Annahme (d.h. die Annahme, dass unser Satz falsch ist), führt also auf einen Widerspruch. Damit ist die Annahme falsch, also unser Satz richtig. ■

Wir haben unseren Satz nach dem Prinzip der *Reductio ad absurdum* (Rückführung auf das Absurde) geführt: Aus der Annahme, unser Satz wäre falsch, haben wir etwas Absurdes, d.h. „einen Widerspruch“ hergeleitet. In sehr vielen Beweisen wird – wie in unserem Fall – das Prinzip der kleinsten Zahl mit dem Prinzip der Reductio ad absurdum kombiniert.

Bemerkung 2.9. Sei $\mathcal{E}$ eine Eigenschaft, welche auf natürliche Zahlen zutrifft oder nicht. Das Prinzip vom kleinsten Element lässt sich dann auch so formulieren:

> *Gibt es überhaupt eine natürliche Zahl mit der Eigenschaft $\mathcal{E}$, so gibt es eine (eindeutig bestimmte) kleinste natürliche Zahl mit der Eigenschaft $\mathcal{E}$.*

Um die Richtigkeit dieser Aussage zu überprüfen, wende man einfach 2.4 auf die Menge

$$\mathbb{T} := \{n \in \mathbb{N} | n \text{ hat die Eigenschaft } \mathcal{E}\}$$

an. •

Frage 2.10. Was ist überhaupt gemeint mit einer Eigenschaft, die auf natürliche Zahlen zutrifft oder nicht? •

Aufgaben 2.11. A) Bestimmen Sie die kleinste natürliche Zahl n, für welche die Menge $\{q \in \mathbb{Q} | q \geq \sqrt{n}\}$ keine kleinste Zahl besitzt. (*Hinweis:* 2.3 D) verwenden.)

B) Bestimmen Sie die kleinste natürliche Zahl $n > 23$ derart, dass $\{q \in \mathbb{Q} | q \geq \sqrt{n-4}\}$ eine kleinste Zahl besitzt.(*Hinweis:* 2.3 D) verwenden.)

C) Seien $m, n \in \mathbb{N}$ mit $m \neq n$. Zeigen Sie:

a) $\sqrt{m} + \sqrt{n} \in \mathbb{Q} \iff \sqrt{m} - \sqrt{n} \in \mathbb{Q}$.

b) $\sqrt{m} + \sqrt{n} \in \mathbb{Q} \iff \sqrt{m}, \sqrt{n} \in \mathbb{N}$. •

Aufgaben 2.12. A) Halten Sie in Stichworten fest, was Sie zur Frage 2.10 wissen.

B) Sei $\mathcal{E}$ eine Eigenschaft, die auf natürliche Zahlen zutrifft oder nicht. Die *charakteristische Funktion von $\mathcal{E}$* ist definiert durch

$$\chi_{\mathcal{E}} : \mathbb{N} \to \{0, 1\};\ \chi_{\mathcal{E}}(n) := \begin{cases} 1, & \text{falls } \mathcal{E} \text{ für } n \text{ zutrifft;} \\ 0, & \text{sonst .} \end{cases}$$

Sei $\mathcal{F}$ eine weitere Aussage, die auf natürliche Zahlen zutrifft oder nicht. Drücken Sie $\chi_{\mathcal{E}\wedge\mathcal{F}}, \chi_{\mathcal{E}\vee\mathcal{F}}$ und $\chi_{\neg\mathcal{E}}$ durch $\chi_{\mathcal{E}}$ und $\chi_{\mathcal{F}}$ aus. •

Der Begriff des Maximums

Genauso wie man sich für die kleinste Zahl einer Menge $\mathbb{M}$ interessieren kann, ist auch die Frage nach einer grössten Zahl dieser Menge sinnvoll. Wir werden so zur nachfolgenden Begriffsbildung geführt.

Definition und Bemerkung 2.13. Sei $\emptyset \neq \mathbb{M} \subseteq \mathbb{R}$. Wir sagen x sei eine *grösste Zahl von* $\mathbb{M}$, wenn $x \in \mathbb{M}$ und wenn für jede weitere Zahl $y \in \mathbb{M}$ gilt $y \leq x$.

Genau wie in 2.1 B) überlegt man sich: Besitzt $\mathbb{M}$ eine grösste Zahl x, so ist diese eindeutig bestimmt. In diesem Fall nennen wir x die *grösste Zahl* oder das *Maximum von* $\mathbb{M}$ und schreiben $x = \max(\mathbb{M})$. Also:

$$x = \max(\mathbb{M}) \Longleftrightarrow (x \in \mathbb{M}) \wedge (\forall y \in \mathbb{M} : y \leq x).$$

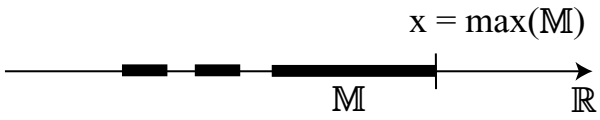


Abbildung 2.2: Maximum einer Menge $\mathbb{M}$

•

Aufgaben 2.14. A) Zeigen Sie, dass die Menge $\mathbb{M} := [0,1[= \{x \in \mathbb{R} | 0 \leq x < 1\}$ kein Maximum besitzt.

B) Für $a \in \mathbb{R}$ sei $\mathbb{Q}_{\leq a} := \{q \in \mathbb{Q} | q \leq a\}$. Zeigen Sie:

a) $a \in \mathbb{Q} \Longrightarrow a = \max(\mathbb{Q}_{\leq a})$.

b) $a \notin \mathbb{Q} \Longrightarrow \max(\mathbb{Q}_{\leq a})$ existiert nicht.

(*Hinweis zu b):* Verwenden Sie: Ist $q < a$, so gibt es ein $q' \in \mathbb{Q}$ mit $q < q' < a$.)

C) Bestimmen Sie alle natürlichen Zahlen $n \leq 20$ für welche $\mathbb{Q}_{\leq \sqrt{n}}$ ein Maximum hat, und geben Sie jeweils dieses Maximum an.

D) Formulieren und lösen Sie die zu 2.3 E) analoge Aufgabe mit „max“ statt „min“.

E) Formulieren und lösen Sie die zu 2.3 F) analoge Aufgabe mit „max“ statt „min“. •

Endliche Mengen natürlicher Zahlen

Nun begehen wir eine Provokation: Wir definieren, was eine endliche Menge (natürlicher Zahlen) ist. Dabei ist aber sicher jedermann klar, was gemeint ist, wenn wir von endlich vielen Zahlen (oder Punkten etc.) reden. Aber ein Begriff, der einleuchtet, ist deswegen noch nicht streng definiert.

In der Mathematik darf man zwar Axiome einführen, weil sie einleuchtend erscheinen, solange man bei der Formulierung dieser Axiome ausschliesslich streng definierte Begriffe verwendet. Dies haben wir im Fall des Axioms 2.4 eingehalten: In der Formulierung traten nur der (als bekannt vorausgesetzte) Begriff der nichtleeren Menge und der in 2.1 definierte Begriff des Minimums einer Menge von Zahlen auf. Führt man andererseits einen neuen Begriff ein – wie wir dies jetzt tun wollen – so muss dieser mit Hilfe von bereits definierten Begriffen beschrieben werden. Nur die strengste Einhaltung dieses Prinzips kann nämlich garantieren, was die Mathematik in erster Linie anstrebt: absolut eindeutige (nicht „wahre“ oder „richtige“) Aussagen zu machen.

Genauso wollen wir jetzt vorgehen und den Begriff der endlichen Menge natürlicher Zahlen mit (möglichst einfachen) schon definierten Begriffen definieren.

Definition 2.15. Eine Menge $\mathbb{S} \subseteq \mathbb{N}$ natürlicher Zahlen heisst *endlich*, wenn es eine Zahl $m \in \mathbb{N}$ so gibt, dass $n \leq m$ für alle $n \in \mathbb{S}$. In diesem Fall heisst m eine *obere Schranke von* $\mathbb{S}$.

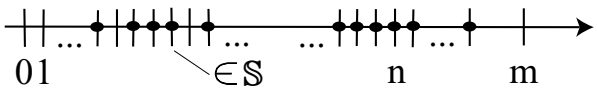


Abbildung 2.3: Endliche Menge mit oberer Schranke

•

Es scheint uns einleuchtend, dass eine nichtleere, (im Sinne von 2.15) endliche Menge eine grösste Zahl enthält (also ein Maximum besitzt). Es wäre deshalb naheliegend, diese Tatsache wieder als Axiom einzuführen. Aber genau das ist nun nicht mehr nötig: Man kann nämlich die Existenz des fraglichen Maximums mit Hilfe des Prinzips der kleinsten Zahl beweisen. Genauer gilt der folgende Satz.

Satz 2.16. *Sei* $\emptyset \neq \mathbb{S} \subseteq \mathbb{N}$. *Dann sind äquivalent:*

(i) $\mathbb{S}$ *ist endlich;*

(ii) $\mathbb{S}$ *besitzt eine grösste Zahl.*

Beweis: „(i) ⇒ (ii)“ : Sei $\mathbb{S}$ endlich. Dann gibt es eine obere Schranke $m \in \mathbb{N}$ von $\mathbb{S}$. Also gibt es eine kleinste natürliche Zahl n mit der Eigenschaft, obere Schranke von $\mathbb{S}$ zu sein (s. 2.9).

Ist $n = 1$, so gilt $1 \leq s \leq n = 1$, also $s = 1$ für jedes $s \in \mathbb{S}$. Dann ist 1 die (einzige und damit) grösste Zahl von $\mathbb{S}$.

Ist $n > 1$, so ist $n - 1 \in \mathbb{N}$ und $n - 1 < n$. Also ist $n - 1$ keine obere Schranke von $\mathbb{S}$. Es gibt also ein $s \in \mathbb{S}$ mit $n - 1 < s$, d.h. mit $n \leq s$. Weil n obere Schranke von $\mathbb{S}$ ist, gilt auch $s \leq n$. Es folgt $s = n$, also $n \in \mathbb{S}$. Also ist n eine obere Schranke von $\mathbb{S}$ und es gilt $n \in \mathbb{S}$. Damit ist aber $n = \max(\mathbb{S})$.

„(ii) ⇒ (i)“ : Sei $s = \max(\mathbb{S})$. Dann ist s eine obere Schranke von $\mathbb{S}$. Damit ist $\mathbb{S}$ endlich. ■

Fragen 2.17. A) Wir haben definiert, was eine endliche Menge natürlicher Zahlen ist. Muss man das?

B) Ist $\emptyset$ eine endliche Menge natürlicher Zahlen? •

Aufgaben 2.18. A) Halten Sie in Stichworten fest, was Ihnen zur Frage 2.17 A) einfällt.

B) Beantworten Sie die Frage 2.17 B) im Sinne von 2.15.

C) Zeigen Sie: $\mathbb{S} := \{1, 7, 412, 10^{28}, 14, 11, 2^{101}, 3^{67}\}$ ist im Sinne von 2.15 endlich. Bestimmen Sie dazu $\max(\mathbb{S})$, möglichst ohne Verwendung des Rechners. •

Rein „technisch“ gesehen lässt sich mit dem in 2.15 definierten Endlichkeitsbegriff offenbar gut arbeiten. Andererseits entspricht dieser Endlichkeitsbegriff nicht der „natürlichen“ Vorstellung, dass man die Elemente einer endlichen Menge zählen kann. Wir werden später auf diese Frage zurückkommen und Resultate beweisen, welche dieser natürlichen Vorstellung entgegenkommen.

Kapitel 3

Vollständige Induktion

Überblick

Das Prinzip der kleinsten Zahl führt uns zur zweifellos grundlegendsten Beweismethode der Mathematik – der Methode der vollständigen Induktion. Diese beruht auf dem sogenannten *Induktionsprinzip*. Dieses Prinzip bezieht sich auf eine Aussage $\mathcal{A}(x)$, für welche es sinnvoll ist, anstelle von x eine beliebige natürliche Zahl n einzusetzen, d.h. auf eine Ausage, die für jede natürliche Zahl $x = n$ zutrifft oder nicht. Es besagt:

- *Gilt $\mathcal{A}(1)$ und folgt aus der Richtigkeit von $\mathcal{A}(n)$ immer die Richtigkeit von $\mathcal{A}(n+1)$, so gilt $\mathcal{A}(n)$ für jede natürliche Zahl n.*

Wie wir gleich sehen werden, ergibt sich dieses neue Prinzip leicht aus dem Prinzip der kleinsten Zahl. Mit dem Übergang vom Prinzip der kleinsten Zahl zum Induktionsprinzip sind wir vom „Vergleichen“ zum „Zählen“ gelangt.

Im Einzelnen werden wir in diesem Kapitel behandeln:

- *das Prinzip der vollständigen Induktion,*
- *Anwendungsbeispiele zur vollständigen Induktion,*
- *der Begriff des Zählens,*
- *abzählbar endliche Mengen,*
- *die Invarianz der Anzahl,*
- *der Begriff der Kardinalität,*
- *einige Resultate über Kardinalitäten.*

Dieses Kapitel hat primär Vertiefungscharakter, da wir eigentlich nur über Dinge reden, die schon aus der Schule bekannt oder direkt einleuchtend sind. Neu dürfte höchstens die Betrachtungsweise und die Strenge des Vorgehens sein. Dieses Kapitel will entsprechend primär als „kleine Schule des mathematischen Denkens“ verstanden sein.

Das Prinzip der vollständigen Induktion

Wir wollen das Prinzip der vollständigen Induktion auf dem Prinzip der kleinsten Zahl begründen. Dazu beweisen wir:

Satz 3.1. *(Induktivitätssatz) Sei* $\mathbb{T} \subseteq \mathbb{N}$ *so, dass* $1 \in \mathbb{T}$ *und so, dass aus* $n \in \mathbb{T}$ *immer* $n+1 \in \mathbb{T}$ *folgt. Dann gilt* $\mathbb{T} = \mathbb{N}$.

Beweis: Nehmen wir an, es wäre $\mathbb{T} \neq \mathbb{N}$. Dann gibt es natürliche Zahlen n mit $n \notin \mathbb{T}$. Nach 2.9 gibt es also eine kleinste natürliche Zahl n mit $n \notin \mathbb{T}$.

Wegen $1 \in \mathbb{T}$ ist $n \neq 1$, also $n > 1$. Also ist $n-1 \in \mathbb{N}$. Wegen $n-1 < n$ gilt demnach $n-1 \in \mathbb{T}$. Nach Voraussetzung folgt $(n-1)+1 \in \mathbb{T}$, also $n = (n-1)+1 \in \mathbb{T}$, ein Widerspruch. Also war unsere Annahme falsch, d.h. es gilt $\mathbb{T} = \mathbb{N}$. ■

Bemerkungen 3.2. A) Eine Menge $\mathbb{T} \subseteq \mathbb{N}$, welche die Voraussetzung von 3.1 erfüllt, heisst *induktiv*. Wir können also 3.1 auch aussprechen in der Form:

Ist $\mathbb{T} \subseteq \mathbb{N}$ *induktiv, so folgt* $\mathbb{T} = \mathbb{N}$.

B) Sei nun $\mathcal{A}(x)$ eine Aussage, die für jede natürliche Zahl $x = n$ zutrifft oder nicht. Will man zeigen, dass $\mathcal{A}(n)$ für alle natürlichen Zahlen n zutrifft, so muss man zeigen, dass die Menge

$$\mathbb{T} := \{n \in \mathbb{N} | \mathcal{A}(n) \text{ trifft zu } \}$$

gerade mit ganz $\mathbb{N}$ übereinstimmt. Nach dem im Teil A) Gesagten genügt es zu zeigen, dass $\mathbb{T}$ induktiv ist. Dazu muss man die folgenden zwei Dinge beweisen:

a) $\mathcal{A}(1)$ *trifft zu*;

b) *trifft* $\mathcal{A}(n)$ *zu, so trifft auch* $\mathcal{A}(n+1)$ *zu* $(n \in \mathbb{N})$.

Das ist aber genau das, was nach dem Induktionsprinzip zu tun ist.

Das Nachprüfen von a) nennt man die *Induktionsverankerung*, das Nachprüfen von b) nennt man den *Induktionsschritt*. Das ganze hier beschriebene Beweisverfahren nennt man die *Methode der (vollständigen) Induktion.* •

Anwendungsbeispiele zur vollständigen Induktion

Wir beweisen nun zur Demonstration drei Resultate mit Hilfe der vollständigen Induktion. Auf die ersten beiden dieser Resultate werden wir wiederholt zurückgreifen.

Beispiele 3.3. A) Sei b eine positive reelle Zahl, d.h. $b \in \mathbb{R}$ und $b > 0$. Mit Hilfe der Methode der vollständigen Induktion wollen wir zeigen, dass für alle $n \in \mathbb{N}$ gilt:

$$(1+b)^n \geq 1 + nb; \quad (\textit{Bernoulliungleichung}).$$

Die Aussage $\mathcal{A}(x)$ aus 3.2 B) kann hier als die Aussage $(1+b)^x \geq 1 + xb$ verstanden werden. Zunächst müssen wir die Induktionsverankerung vornehmen, also zeigen, dass unsere Aussage gilt, wenn wir $x = n = 1$ wählen. Dies ist aber klar, weil ja $(1+b)^1 = 1 + b = 1 + 1b$ gilt. Nun kommen wir zum Induktionsschritt. Wir nehmen also an, $\mathcal{A}(n)$ treffe für ein $n \in \mathbb{N}$ zu und müssen zeigen, dass dann auch $\mathcal{A}(n+1)$ gilt. Anders gesagt: Wir nehmen an, dass für ein beliebiges, aber festes $n \in \mathbb{N}$ die Ungleichung $(1+b)^n \geq 1 + nb$ gilt und müssen zeigen, dass daraus auch die Ungleichung $(1+b)^{n+1} \geq 1 + (n+1)b$ folgt. Genau dies wollen wir nun tun. Weil wir voraussetzen, dass $(1+b)^n \geq 1 + nb$, können wir (wegen $b > 0$)

$$\begin{aligned}(1+b)^{n+1} &= (1+b)^n(1+b) \geq (1+nb)(1+b) = \\ &= 1 + nb + b + nb^2 \geq 1 + nb + b = \\ &= 1 + (n+1)b\end{aligned}$$

schreiben und erhalten $(1+b)^{n+1} \geq 1 + (n+1)b$, was zu zeigen war. Damit ist der Induktionsschritt beendet und der ganze Beweis geführt.

B) Sei $q \in \mathbb{R}\backslash\{1\}$. Wir wollen zeigen, dass für alle $n \in \mathbb{N}$ gilt:

$$1 + q + q^2 + \cdots + q^n = \frac{1 - q^{n+1}}{1 - q}; \quad (\textit{Teilsummenformel für geometrische Reihen}).$$

Wir tun dies durch vollständige Induktion. Für $n = 1$ lautet die linke Seite der behaupteten Gleichung einfach $1 + q$, die rechte Seite aber $\frac{1-q^2}{1-q}$. Wegen

$$\frac{1 - q^2}{1 - q} = \frac{(1-q)(1+q)}{1-q} = 1 + q$$

ergibt sich die behauptete Gleichung für $n = 1$. Damit ist die Induktionsverankerung gemacht.

Gilt für ein beliebiges $n \in \mathbb{N}$ bereits die Gleichung

$$1 + q + q^2 + \cdots + q^n = \frac{1 - q^{n+1}}{1 - q},$$

so folgt

$$\begin{aligned}1+q+q^2+\cdots+q^{n+1} &= (1+q+\cdots+q^n)+q^{n+1} = \\ &= \frac{1-q^{n+1}}{1-q}+q^{n+1} = \frac{1-q^{n+1}+(1-q)q^{n+1}}{1-q} = \\ &= \frac{1-q^{n+1}+q^{n+1}-qq^{n+1}}{1-q} = \frac{1-q^{n+2}}{1-q} = \frac{1-q^{(n+1)+1}}{1-q}\ ,\end{aligned}$$

also

$$1+q+q^2+\cdots+q^{n+1} = \frac{1-q^{(n+1)+1}}{1-q}.$$

Die behauptete Gleichung gilt also auch, wenn wir n durch $n+1$ ersetzen. Dies beendet den Induktionsschritt. Damit ist der Beweis geführt.

C) Wir möchten gerne zeigen, dass für beliebige $n \in \mathbb{N}$ gilt:

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots+\frac{1}{n^2} < 2.$$

Leider gelingt dies nicht so direkt und wir beweisen deshalb durch vollständige Induktion die stärkere Aussage, dass für alle $n \in \mathbb{N}$ gilt:

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots+\frac{1}{n^2} \leq 2-\frac{1}{n}.$$

Wegen $1 \leq 2-1 = 2-\frac{1}{1}$ gilt unsere Ungleichung, falls $n=1$. Dies erledigt die Induktionsverankerung.

Gilt unsere Ungleichung bereits für ein bestimmtes $n \in \mathbb{N}$, so folgt

$$\begin{aligned}1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots+\frac{1}{n^2}+\frac{1}{(n+1)^2} &= \\ = \left(1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{n^2}\right)+\frac{1}{(n+1)^2} &\leq \left(2-\frac{1}{n}\right)+\frac{1}{(n+1)^2} = \\ = 2-\frac{1}{n}+\frac{1}{(n+1)^2} = 2-\left(\frac{1}{n}-\frac{1}{(n+1)^2}\right) &= \\ = 2-\frac{(n+1)^2-n}{n(n+1)^2} = 2-\frac{n^2+2n+1-n}{n(n+1)^2} &= \\ = 2-\frac{n^2+n+1}{n(n+1)^2} \leq 2-\frac{n^2+n}{n(n+1)^2} = 2-\frac{n(n+1)}{n(n+1)^2} = 2-\frac{1}{n+1},&\end{aligned}$$

also

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots+\frac{1}{(n+1)^2} \leq 2-\frac{1}{n+1}.$$

Der Induktionsschritt ist damit ebenfalls beendet. •

Aufgaben 3.4. A) Zeigen Sie durch vollständige Induktion, dass für alle $n \in \mathbb{N}$ gilt:

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

B) Zeigen Sie durch vollständige Induktion, dass für alle $n \in \mathbb{N}$gilt:

$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

C) Zeigen Sie durch vollständige Induktion, dass für alle $n \in \mathbb{N}$ gilt: $2^{n-1} \leq n!$ (*Hinweis:* $1! = 1, (n+1)! = n!(n+1)$.)

D) Zeigen Sie, dass für alle $n \in \mathbb{N}$ gilt: $n! < 2^{n^2}$. (*Hinweis:* Zeigen Sie zuerst mit 3.3 A), dass $(n+1) \leq 2^n$ gilt.)

E) Seien $e_1 := 1$ und $e_n := e_{n-1} \cdot n + 1$ für $n > 1$. Zeigen Sie, dass $e_n = n! \left(\frac{1}{1!} + \frac{1}{2!} + \cdots \frac{1}{n!}\right)$ für alle $n \in \mathbb{N}$.

F) Holen Sie ein Beispiel aus http://www.research.att.com/∼njas/sequences/, das für die vollständige Induktion „etwas hergibt“ und beschreiben Sie dieses. •

Aufgaben 3.5. A) Zeigen Sie mit 3.3 A), dass $\sqrt{n} < \left(1 + \frac{1}{\sqrt{n}}\right)^n$ für alle $n \in \mathbb{N}$.

B) Zeigen Sie mit Teil A), dass für jedes $n \in \mathbb{N}$ gilt: $\sqrt[n]{n} < \left(1 + \frac{1}{\sqrt{n}}\right)^2 \leq 1 + \frac{3}{\sqrt{n}}$.

C) Zeigen Sie mit Teil B), dass $\lim_{n\to\infty} \sqrt[n]{n} = 1$. •.

Aufgaben 3.6. Gegeben seien n Geraden $g_1, \cdots, g_n$ in der Ebene $\mathbb{E}$. Je zwei dieser Geraden schneiden sich. Es kommt nicht vor, dass sich drei oder mehr der Geraden in einem Punkt schneiden.

A) Skizzieren Sie die Situation für $n = 1, 2, 3, 4$.

B) Bestimmen Sie die Anzahl der Geradenschnittpunkte.

C) Zeigen Sie durch Induktion, dass die Ebene $\mathbb{E}$ durch die Geraden g_i in $\frac{n^2+n+2}{2}$ Gebiete zerlegt wird. (Hinweis: g_n wird durch $g_1, \cdots, g_{n-1}$ in n Teile zerlegt. Jeder dieser Teile zerlegt ein Flächengebiet.)

D) (*Türme von Hanoi*)

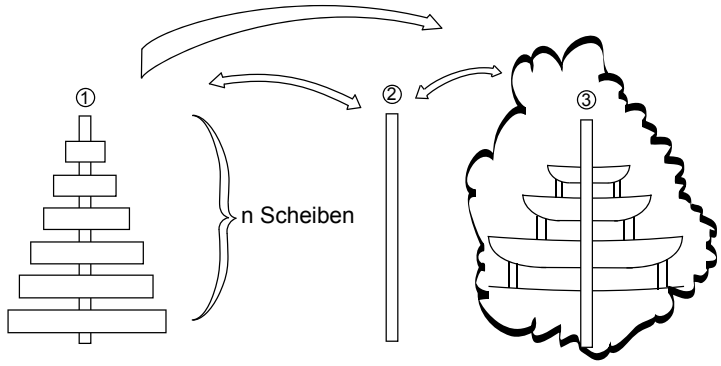


Abbildung 3.1: Türme von Hanoi

Gegeben sind drei auf einem Brett befestigte Stöcke mit den Nummern 1, 2 und 3. Aufgesteckt auf Stock 1 befinden sich n in der Mitte durchbohrte runde Scheiben, wobei der Durchmesser der Scheiben nach oben abnimmt. Der Scheibenturm soll von Stock 1 auf Stock 3 umgeschichtet werden. Stock 2 darf als „Zwischenlager“ verwendet werden. Während des ganzen Umschichtungsprozesses darf nie eine grössere Scheibe auf eine kleinere zu liegen kommen. Zeigen Sie, dass man die Aufgabe mit $(2^n - 1)$-maligem Umstecken einzelner Scheiben lösen kann. •

Frage 3.7. Gibt es Aussagen $\mathcal{A}(x)$, für welche der Induktionsschritt durchführbar ist, aber nicht die Induktionsverankerung? •

Aufgabe 3.8. Geben Sie ein Beispiel einer Aussage, welches die Frage 3.7 im bejahenden Sinn beantwortet. •

Bemerkung 3.9. In den bisherigen Induktionsbeweisen haben wir immer ausdrücklich auf die Induktionsverankerung und den Induktionsschritt verwiesen. Im „Alltag“ wird dies oft nicht mehr getan. Auch haben wir bis jetzt bei der Durchführung des Induktionsschrittes immer „von n auf $n + 1$“ geschlossen. Viel praktischer ist in den meisten Fällen allerdings der *Schluss von* $n - 1$ *auf* n:

- *Man nimmt an, es sei* $n > 1$ *und macht die („Induktions“ -)Voraussetzung, dass die Behauptung für* $n - 1$ *bereits gilt. Dann zeigt man, dass die Behauptung auch für* n *gilt.* •

Der Begriff des Zählens

Vom Prinzip der kleinsten Zahl – bei dem es ausschliesslich um den Grössenvergleich natürlicher Zahlen geht – sind wir in diesem Kapitel zum Induktionsprinzip gelangt, bei dem es um das andauernde Fortschreiten von einer natürlichen Zahl zur nächsthöheren geht. Damit sind wir von der Idee des Vergleichens zur Idee des Zählens vorgestossen, allerdings erst in prämathematischer Weise: Das anschauliche Konzept des Zählens muss nämlich noch durch ein geeignetes mathematisches Modell beschrieben werden, damit es streng fassbar wird. Genau dies wollen wir im Folgenden tun. Zunächst eine Vorbereitung:

Definition 3.10. Ist $n \in \mathbb{N}$, so schreiben wir

$$\mathbb{N}_{\leq n} := \{m \in \mathbb{N} | m \leq n\}$$

und nennen $\mathbb{N}_{\leq n}$ den *n-ten Anfangsabschnitt der natürlichen Zahlen.* •

Bemerkungen 3.11. A) Sei $n \in \mathbb{N}$. Natürlich gilt dann

$$\max(\mathbb{N}_{\leq n}) = n.$$

Insbesondere können wir damit sagen, dass die Menge $\mathbb{N}_{\leq n}$ im Sinne unserer Definition 2.15 endlich ist (s. 2.17 A)).

B) Intuitiv-anschaulich ist $\mathbb{N}_{\leq n}$ die Menge „der ersten n natürlichen Zahlen“ oder die „Menge der natürlichen Zahlen von 1 bis n“. Entsprechend dieser Vorstellung verwenden wir auch die Notation (!)

$$\{1, 2, \ldots, n\} := \mathbb{N}_{\leq n}.$$

Auf der Zahlengeraden kann diese Menge wie folgt veranschaulicht werden:

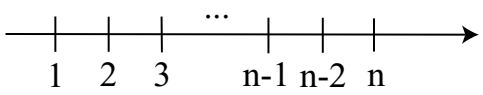


Abbildung 3.2: Anfangsabschnitt der natürlichen Zahlen

•

Nun können wir aussprechen, wie wir den Begriff des Zählens mathematisch modellieren (vgl. 1.2 A)):

- *Die Elemente einer Menge* $\mathbb{M}$ *zu zählen heisst, eine Bijektion* $\varphi : \mathbb{N}_{\leq n} \to \mathbb{M}$ *zwischen einem Anfangsabschnitt der natürlichen Zahlen und der Menge* $\mathbb{M}$ *anzugeben.*

Abzählbar endliche Mengen

Wir haben den Begriff einer endlichen Menge $\mathbb{M}$ von natürlichen Zahlen bereits definiert. Für beliebige Mengen $\mathbb{M}$ scheint es naheliegend zu sagen:

- *Eine Menge* $\mathbb{M}$ *ist endlich, wenn man ihre Elemente zählen kann.*

Dies führt uns zur folgenden Festsetzung.

Definition 3.12. Eine Menge $\mathbb{M} \neq \emptyset$ heisst *endlich im abzählenden Sinne* oder *abzählbar endlich*, wenn es eine Zahl $n \in \mathbb{N}$ und eine bijektive Abbildung $\varphi : \mathbb{N}_{\leq n} \to \mathbb{M}$ gibt. Die Menge $\emptyset$, d.h. die leere Menge, betrachten wir ebenfalls als abzählbar endlich. •

Mit dieser Definition haben wir uns allerdings eine Pflicht auferlegt: Wir sollten zeigen, dass eine Menge $\mathbb{M} \subseteq \mathbb{N}$ genau dann abzählbar endlich ist, wenn sie im Sinne der Definition 2.15 endlich ist. Um dies zu tun, zeigen wir zunächst das folgende Hilfsresultat:

Lemma 3.13. *Ist* $n \in \mathbb{N}$ *und ist* $\varphi : \mathbb{N}_{\leq n} \to \mathbb{R}$ *eine Abbildung, so enthält* $\varphi(\mathbb{N}_{\leq n})$ *eine kleinste und eine grösste Zahl.*

Beweis: (*Vollständige Induktion bezüglich* n). Ist $n = 1$, so gilt $\varphi(\mathbb{N}_{\leq n}) = \varphi(\mathbb{N}_{\leq 1}) = \varphi(\{1\}) = \{\varphi(1)\}$. Insbesondere ist $\varphi(1)$ die kleinste und die grösste Zahl von $\varphi(\mathbb{N})_{\leq n}$. Sei also $n > 1$. Gemäss Induktionsvoraussetzung gilt unsere Behauptung bereits für die Einschränkung $\varphi\restriction: \mathbb{N}_{\leq n-1} \to \mathbb{N}$ von φ auf $\mathbb{N}_{\leq n-1}$. Das heisst, $\varphi(\mathbb{N}_{\leq n-1}) = \varphi\restriction(\mathbb{N}_{\leq n-1})$ besitzt sowohl ein Minimum als auch ein Maximum. Wir schreiben

$$a := \min\left(\varphi(\mathbb{N}_{\leq n-1})\right), \ b := \max\left(\varphi(\mathbb{N}_{\leq n-1})\right).$$

Natürlich gelten $a \leq b$ und $\varphi(\mathbb{N}_{\leq n}) = \varphi(\mathbb{N}_{\leq n-1}) \cup \{\varphi(n)\}$. Nun erhält man aber sofort:

$$\min\left(\varphi(\mathbb{N}_{\leq n})\right) = \begin{cases} \varphi(n), & \text{wenn } \varphi(n) < a; \\ a, & \text{wenn } \varphi(n) \geq a, \end{cases}$$

$$\max\left(\varphi(\mathbb{N}_{\leq n})\right) = \begin{cases} \varphi(n), & \text{wenn } \varphi(n) > b; \\ b, & \text{wenn } \varphi(n) \leq b. \end{cases}$$

■

Bevor wir unser nächstes Resultat beweisen, erinnern wir an den folgenden Begriff:

Definition 3.14. Seien $\mathbb{U}, \mathbb{V} \subseteq \mathbb{R}$ und sei $f : \mathbb{U} \to \mathbb{V}$ eine Abbildung. Wir sagen, f sei *(streng) wachsend*, wenn für alle $a, b \in \mathbb{U}$ gilt:

$$a < b \Longrightarrow f(a) \leq f(b) \quad (\text{resp. } \ f(a) < f(b)).$$ •

Satz 3.15. *Ist $\emptyset \neq \mathbb{M} \subseteq \mathbb{N}$ und enthält $\mathbb{M}$ eine grösste Zahl, so gibt es eine natürliche Zahl $n \in \mathbb{N}$ und eine wachsende, bijektive Abbildung $\varphi : \mathbb{N}_{\leq n} \to \mathbb{M}$.*

Beweis: (*Vollständige Induktion bezüglich* $m := \max(\mathbb{M})$) Sei $m = 1$. Dann ist $\mathbb{M} = \{1\}$. Wir wählen $n = 1$ und definieren $\varphi : \mathbb{N}_{\leq 1} = \{1\} \to \mathbb{M} = \{1\}$ durch $\varphi(1) := 1$. Sei also $m > 1$. Wir setzen $\mathbb{M}' := \mathbb{M} \backslash \{m\}$. Ist $\mathbb{M}' = \emptyset$, so ist $\mathbb{M} = \{m\}$. In diesem Fall setzen wir $n = 1$ und definieren $\varphi : \mathbb{N}_{\leq 1} = \{1\} \to \mathbb{M} = \{m\}$ durch $\varphi(1) := m$.

Sei also $\mathbb{M}' \neq \emptyset$. Wegen $\mathbb{M}' \subseteq \mathbb{M}$ ist m eine obere Schranke von $\mathbb{M}'$. Also ist $\mathbb{M}'$ eine nichtleere endliche Menge natürlicher Zahlen. Nach 2.16 existiert nun $m' := \max(\mathbb{M}')$. Wegen $m' \in \mathbb{M}' \subseteq \mathbb{M}$ ist $m' \leq m$. Wegen $m \notin \mathbb{M}'$ ist $m' \neq m$. Deshalb gilt $m' < m$.

Nach Induktionsvoraussetzung gibt es also ein $n' \in \mathbb{N}$ und eine wachsende, bijektive Abbildung $\varphi' : \mathbb{N}_{\leq n'} \to \mathbb{M}'$. Sei $n := n' + 1$. Wir definieren eine Abbildung $\varphi : \mathbb{N}_{\leq n} \to \mathbb{M}$ durch

$$\varphi(k) := \begin{cases} \varphi'(k)\ , & \text{falls } k \leq n-1; \\ m\ , & \text{falls } k = n. \end{cases}$$

Dann gilt $\varphi(\mathbb{N}_{\leq n}) = \varphi(\mathbb{N}_{\leq n'}) \cup \{\varphi(n)\} = \varphi'(\mathbb{N}_{\leq n'}) \cup \{m\} = \mathbb{M}' \cup \{m\} = \mathbb{M}$. Also ist φ surjektiv. Für alle $k, l \in \mathbb{N}_{\leq n}$ mit $k < l < n$ gilt $\varphi(k) = \varphi'(k) < \varphi'(l) = \varphi(l) < \varphi(n) = m$. Daraus folgt, dass φ streng wachsend und bijektiv ist. ■

Nun sind wir an unserem ersten Ziel angelangt:

Korollar 3.16. *Eine Menge $\mathbb{M} \subseteq \mathbb{N}$ ist endlich im Sinne der Definition 2.15 dann und nur dann, wenn sie es im Sinne der Definition 3.12 ist.*

Beweis: Ist $\mathbb{M}$ endlich im Sinne der Definition 2.15, so ist $\mathbb{M}$ abzählbar endlich. Die Umkehrung folgt sofort mit 3.13 und 2.16. ■

Insbesondere müssen wir also die beiden Endlichkeitsbegriffe nicht mehr unterscheiden. Wir setzen deshalb fest

- *Abzählbar endliche Mengen nennen wir ab jetzt nur noch endliche Mengen.*

Die Invarianz der Anzahl

Eines der wichtigsten „Naturphänomene“ im Bereich des Zählens blieb bis jetzt unausgesprochen, nämlich:

- *(Invarianz der Anzahl) Die Anzahl der Elemente einer Menge $\mathbb{M}$ hängt nicht davon ab, in welcher Reihenfolge diese Elemente gezählt werden.*

Diese Aussage wollen wir nun in strenger Form beweisen. Insbesondere müssen wir dazu den Begriff der Anzahl der Elemente einer Menge definieren. Wir beginnen mit dem folgenden Hilfsresultat.

Lemma 3.17. *Seien $m, n \in \mathbb{N}$ und sei $\varphi : \mathbb{N}_{\leq n} \to \mathbb{N}_{\leq m}$ eine injektive Abbildung. Dann gilt $n \leq m$.*

Beweis: (*Vollständige Induktion bezüglich n*). Sei zunächst $n = 1$. Dann ist $\mathbb{N}_{\leq n} = \mathbb{N}_{\leq 1} = \{1\}$ und $1 \leq \varphi(1) \leq m$. Dies erledigt den Fall $n = 1$. Sei also $n > 1$. Nehmen wir zunächst an, es sei

$$(\alpha) \qquad \varphi(t) < m \text{ für alle } t \leq n-1.$$

Durch Einschränken von φ erhalten wir dann eine injektive Abbildung $\varphi\restriction: \mathbb{N}_{\leq n-1} \to \mathbb{N}_{\leq m-1}$. Aus der Induktionsvoraussetzung folgt dann $n-1 \leq m-1$, also $n \leq m$. Damit ist der Fall erledigt, in dem (α) gilt.

Sei also (α) falsch. Dann gibt es ein Element $t \in \mathbb{N}_{\leq n-1}$ mit $\varphi(t) = m$. Weil φ injektiv ist, folgt $\varphi(s) \neq m$ für alle $s \in \mathbb{N}_{\leq n} \backslash \{t\}$. Wegen $\varphi(\mathbb{N}_{\leq n}) \subseteq \mathbb{N}_{\leq m}$ erhalten wir

$$(\beta) \qquad \varphi(s) \in \mathbb{N}_{\leq m-1} \text{ für alle } s \in \mathbb{N}_{\leq n-1} \backslash \{t\}.$$

Insbesondere ist $\varphi(n) \in \mathbb{N}_{\leq m-1}$. Jetzt können wir die folgende Abbildung definieren:

$$\psi : \mathbb{N}_{\leq n-1} \to \mathbb{N}_{\leq m-1} \ ; \ \psi(s) := \begin{cases} \varphi(s) \ , & \text{falls } s \neq t; \\ \varphi(n) \ , & \text{falls } s = t. \end{cases}$$

Seien $s, s' \in \mathbb{N}_{\leq n-1}$ mit $s \neq s'$. Gelten $s \neq t$ und $s' \neq t$, so erhalten wir wegen $s \neq s'$ sofort $\psi(s) = \varphi(s) \neq \varphi(s') = \psi(s')$, also $\psi(s) \neq \psi(s')$. Gilt $s = t$, so erhalten wir wegen $s' \neq n$ offenbar $\psi(s) = \psi(t) = \varphi(n) \neq \varphi(s')$, also wieder $\psi(s) \neq \psi(s')$. Gilt $s' = t$, so folgt genau gleich, dass $\psi(s) \neq \psi(s')$. Also ist ψ injektiv. Gemäss der Induktionsvoraussetzung folgt daraus $n-1 \leq m-1$ und damit $n \leq m$. ■

Nun können wir die angekündigte Invarianzaussage formulieren und beweisen:

Satz 3.18. *Sei $\mathbb{M}$ eine Menge, seien $m, n \in \mathbb{N}$ und seien $\varphi : \mathbb{N}_{\leq n} \to \mathbb{M}$ und $\psi : \mathbb{N}_{\leq m} \to \mathbb{M}$ bijektive Abbildungen. Dann gilt $m = n$.*

Beweis: Sei $\varphi^{-1} : \mathbb{M} \to \mathbb{N}_{\leq n}$ die Umkehrabbildung von φ. Natürlich ist φ^{-1} bijektiv. Also ist die Komposition $\varphi^{-1} \circ \psi : \mathbb{N}_{\leq m} \to \mathbb{N}_{\leq n}$ der beiden bijektiven Abbildungen ψ und φ^{-1} bijektiv. Insbesondere ist $\varphi^{-1} \circ \psi : \mathbb{N}_{\leq m} \to \mathbb{N}_{\leq n}$ injektiv. Nach 3.17 folgt $m \leq n$. Genau gleich erhält man $n \leq m$. ■

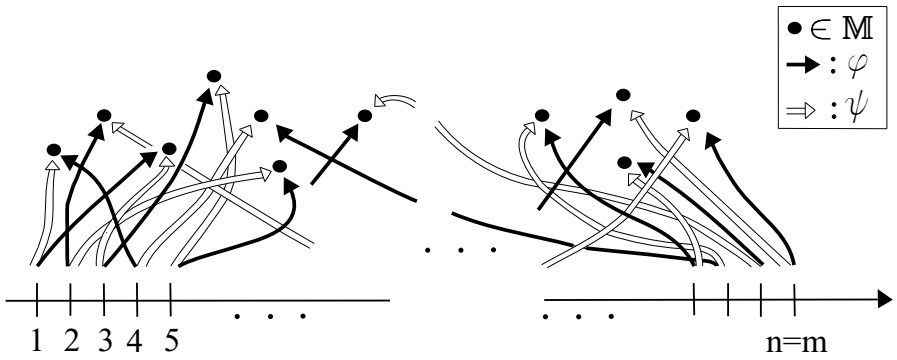


Abbildung 3.3: Zwei Abzählungen einer Menge

Der Begriff der Kardinalität

Bedenkt man, dass das Zählen der Elemente einer Menge $\mathbb{M}$ in der Angabe einer Bijektion $\varphi : \mathbb{N}_{\leq n} \to \mathbb{M}$ besteht, so besagt 3.18, dass die Anzahl der Elemente, die man beim Abzählen erhält (nämlich n) nur von $\mathbb{M}$, aber nicht von der Abzählung abhängt.

Natürlich sind diese Ausführungen prämathematischer Art. In der Sprache der Mathematik können wir 3.18 wie folgt kommentieren.

Das soeben bewiesene Ergebnis 3.18 berechtigt zu folgenden Definitionen:

Definitionen 3.19. Ist $\mathbb{M}$ eine Menge, ist $n \in \mathbb{N}$ und besteht eine bijektive Abbildung $\varphi : \mathbb{N}_{\leq n} \to \mathbb{M}$, so heisst n die *Mächtigkeit* oder *Kardinalität* oder die *Anzahl der Elemente von* $\mathbb{M}$. Wir schreiben dann $\sharp\mathbb{M} := n$. Weiter setzen wir fest, dass $\sharp\emptyset := 0$.

Ist die Menge $\mathbb{M}$ nicht endlich, d.h. ist $\mathbb{M} \neq \emptyset$ und gibt es zu keinem $n \in \mathbb{N}$ eine Bijektion $\varphi : \mathbb{N}_{\leq n} \to \mathbb{M}$, so sagen wir $\mathbb{M}$ sei eine *unendliche Menge* und schreiben $\sharp\mathbb{M} = \infty$. Dabei verabreden wir, dass $n < \infty$ für alle $n \in \mathbb{N}_0$.

Um auszudrücken, dass eine Menge $\mathbb{M}$ endlich ist, schreiben wir $\sharp\mathbb{M} < \infty$. •

Der Satz 3.18 liefert eine erste Bestätigung dafür, dass wir mit unserer mathematischen Formulierung des Begriffs des Zählens erfolgreich waren: Tatsachen, die uns nur aus der Erfahrung geläufig waren, können wir nun streng beweisen. Beflügelt von diesem Erfolg wollen wir noch einige Schritte in die gleiche Richtung tun. Zuerst beweisen wir, dass die Anzahl der Elemente einer Menge nicht nur durch Zählen, sondern auch durch Vergleichen mit einer andern Menge bestimmt werden kann.

Satz 3.20. *Seien* $\mathbb{M}$ *und* $\mathbb{M}'$ *zwei nichtleere Mengen. Dann gelten:*

a) *Besteht eine bijektive Abbildung* $\varphi : \mathbb{M} \to \mathbb{M}'$*, so folgt* $\sharp\mathbb{M} = \sharp\mathbb{M}'$*.*

b) *Gilt* $\sharp\mathbb{M} = \sharp\mathbb{M}' < \infty$*, so besteht eine bijektive Abbildung* $\varphi : \mathbb{M} \to \mathbb{M}'$*.*

Beweis: „a)“ : Setzen wir voraus, es gebe eine bijektive Abbildung $\varphi : \mathbb{M} \to \mathbb{M}'$. Wir schreiben $m := \sharp\mathbb{M}$ und $m' := \sharp\mathbb{M}'$. Sei zunächst $m < \infty$. Dann ist $m \in \mathbb{N}$ und es besteht eine bijkektive Abbildung $\psi : \mathbb{N}_{\leq m} \to \mathbb{M}$. Dann ist aber $\varphi \circ \psi : \mathbb{N}_{\leq m} \to \mathbb{M}'$ ebenfalls bijektiv und aus 3.18 folgt $\sharp\mathbb{M}' = m$, d.h. $m' = m$.

Ist $m' < \infty$, so folgt $m = m'$, wenn man das eben Gesagte auf die bijektive Abbildung $\varphi^{-1} : \mathbb{M}' \to \mathbb{M}$ anwendet. Insbesondere folgt aus $m = \infty$ auch $m' = \infty$.

„b)“ : Sei $m := \sharp\mathbb{M} = \sharp\mathbb{M}' < \infty$. Dann bestehen bijektive Abbildungen $\alpha : \mathbb{N}_{\leq m} \to \mathbb{M}$ und $\beta : \mathbb{N}_{\leq m} \to \mathbb{M}'$. Es genügt, $\varphi := \beta \circ \alpha^{-1}$ zu setzen. ■

Einige Resultate über Kardinalitäten

Das nächste Resultat bringt eine Grundvorstellung zum Ausdruck, die wir vom „*Zusammenzählen*“ haben:

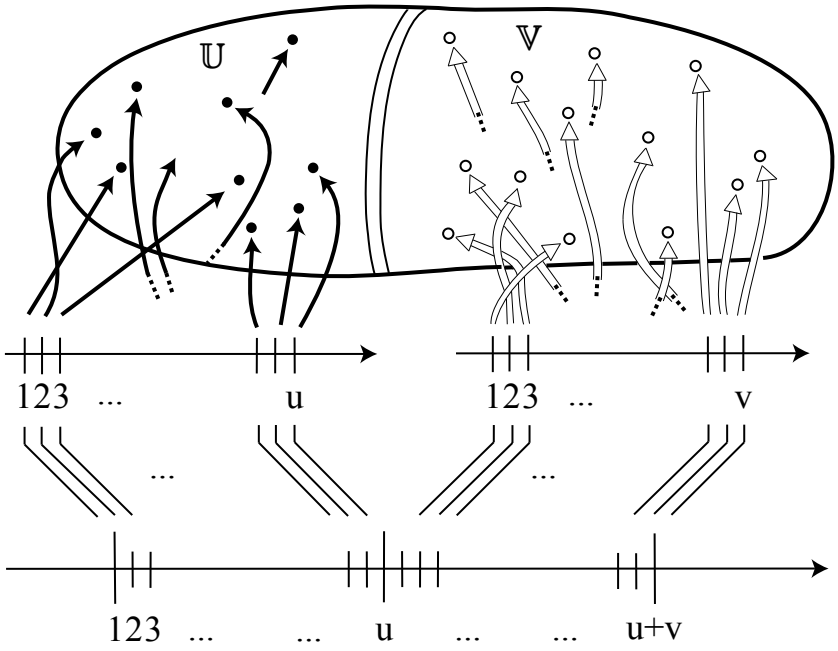


Abbildung 3.4: Zusammenzählen zweier Mengen

Satz 3.21. *Sei $\mathbb{T}$ eine Menge und seien $\mathbb{U}, \mathbb{V} \subseteq \mathbb{T}$ endliche Teilmengen so, dass $\mathbb{U} \cap \mathbb{V} = \emptyset$. Dann ist $\mathbb{U} \cup \mathbb{V}$ eine endliche Menge und es gilt*

$$\sharp(\mathbb{U} \cup \mathbb{V}) = \sharp\mathbb{U} + \sharp\mathbb{V}.$$

Beweis: Ist $\mathbb{U} = \emptyset$ oder $\mathbb{V} = \emptyset$ ist alles klar. Seien also $\mathbb{U} \neq \emptyset$ und $\mathbb{V} \neq \emptyset$. Seien $u := \sharp\mathbb{U}$ und $v := \sharp\mathbb{V}$. Dann bestehen Bijektionen

$$\alpha : \mathbb{N}_{\leq u} \to \mathbb{U};\ \beta : \mathbb{N}_{\leq v} \to \mathbb{V}.$$

Wir definieren nun eine Abbildung

$$\gamma : \mathbb{N}_{\leq (u+v)} \to \mathbb{U} \cup \mathbb{V}$$

durch die Vorschrift

$$\gamma(k) := \begin{cases} \alpha(k), & \text{falls } 0 \leq k \leq u\ ; \\ \beta(k-u)\ , & \text{falls } u < k \leq u+v. \end{cases}$$

(Die Vorschrift ist sinnvoll, weil aus $u < k \leq u + v$ folgt, dass $k - u \in \mathbb{N}_{\leq v}$.)

Wir zeigen, dass γ bijektiv ist:

„γ ist injektiv“ : Seien $k, l \in \mathbb{N}_{\leq (u+v)}$ mit $k \neq l$. Wir müssen zeigen, dass $\gamma(k) \neq \gamma(l)$. Ohne weiteres können wir annehmen, es sei $k < l$. Durch Fallunterscheidung schliessen wir nun wie folgt:

Ist $k < l \leq u$, so gelten $\gamma(k) = \alpha(k)$ und $\gamma(l) = \alpha(l)$. Weil α injektiv ist, gilt $\alpha(l) \neq \alpha(k)$, also $\gamma(k) \neq \gamma(l)$.

Ist $k \leq u < l$, so gelten $\gamma(k) = \alpha(\gamma) \in \mathbb{U}$ und $\gamma(l) = \beta(l-u) \in \mathbb{V}$, also $\gamma(k) \neq \gamma(l)$.

Ist $u < k < l$, so gelten $\gamma(k) = \beta(k-u)$ und $\gamma(l) = \beta(l-u)$. Weil β injektiv ist und $k - u \neq k - v$ gilt, folgt $\beta(k-u) \neq \beta(l-u)$, also $\gamma(k) \neq \gamma(l)$.

„γ ist surjektiv“ : Sei $m \in \mathbb{U} \cup \mathbb{V}$. Dann ist $m \in \mathbb{U}$ oder $m \in \mathbb{V}$. Ist $m \in \mathbb{U} = \alpha(\mathbb{N}_{\leq u})$, so gibt es ein $k \in \mathbb{N}_{\leq u}$ mit $\alpha(k) = m$. Wegen $k \leq u$ ist aber $\gamma(k) = \alpha(k)$. Es folgt $\gamma(k) = m$.

Ist $m \in \mathbb{V} = \beta(\mathbb{N}_{\leq v})$, so gibt es ein $h \in \mathbb{N}_{\leq v}$ mit $m = \beta(h)$. Wegen $u < u + h \leq u + v$ gilt $\gamma(u + h) = \beta(h)$, also $\gamma(u + h) = m$.

Damit ist gezeigt, dass γ bijektiv ist und es folgt, dass $\mathbb{U} \cup \mathbb{V}$ endlich ist mit $\sharp(\mathbb{U} \cup \mathbb{V}) = u + v = \sharp\mathbb{U} + \sharp\mathbb{V}$. ■

Wir beweisen zwei Konsequenzen:

Korollar 3.22. *Sei $\mathbb{M}$ eine endliche Menge und sei $\mathbb{U} \subseteq \mathbb{M}$. Dann sind die Mengen $\mathbb{U}$ und $\mathbb{M}\backslash\mathbb{U}$ endlich, wobei gilt:*

$$\sharp\mathbb{U} + \sharp(\mathbb{M}\backslash\mathbb{U}) = \sharp\mathbb{M}.$$

Beweis: Wir zeigen zuerst, dass $\mathbb{U}$ endlich ist. Ist $\mathbb{U} = \emptyset$, ist dies klar. Sei also $\mathbb{U} \neq \emptyset$. Wir wissen, dass $\mathbb{M}$ endlich und nichtleer ist. Setzen wir $m := \sharp\mathbb{M}$, so besteht also eine Bijektion $\varphi : \mathbb{N}_{\leq m} \to \mathbb{M}$. Durch Einschränkung von φ erhält man nun eine Bijektion $\varphi\restriction: \varphi^{-1}(\mathbb{U}) \to \mathbb{U}$. Weil m eine obere Schranke von $\varphi^{-1}(\mathbb{U})$ ist, ist $\varphi^{-1}(\mathbb{U})$ endlich (s. 2.15).Die Bijektion $\varphi\restriction$ zeigt nun aber auch, dass $\mathbb{U}$ eine endliche Menge ist.

Genau gleich folgt, dass $\mathbb{V} := \mathbb{M}\backslash\mathbb{U}$ endlich ist. Jetzt schliesst man mit 3.21. ■

Korollar 3.23. *Sei $\mathbb{M}$ eine endliche Menge und sei $\mathbb{U} \subseteq \mathbb{M}$. Dann ist auch $\mathbb{U}$ eine endliche Menge, wobei $\sharp\mathbb{U} \leq \sharp\mathbb{M}$. Dabei gilt $\sharp\mathbb{U} = \sharp\mathbb{M}$ genau dann, wenn $\mathbb{U} = \mathbb{M}$.*

Beweis: Klar aus 3.22 unter Beachtung der Tatsache, dass $\mathbb{U} = \mathbb{M}$ gleichbedeutend mit $\sharp(\mathbb{M}\backslash\mathbb{U}) = 0$ ist. ■

Kardinalitäten endlicher Mengen lassen sich nicht nur mit Hilfe von Bijektionen vergleichen, wie dies in Satz 3.20 getan wird. Es gilt nämlich:

Satz 3.24. *Sei $\mathbb{M}$ eine endliche Menge, und seien $\varphi : \mathbb{U} \to \mathbb{M}$ eine injektive und $\psi : \mathbb{M} \to \mathbb{V}$ eine surjektive Abbildung. Dann gelten:*

a) $\mathbb{U}$ *ist endlich mit $\sharp\mathbb{U} \leq \sharp\mathbb{M}$, wobei Gleichheit genau dann gilt, wenn φ bijektiv ist.*

b) $\mathbb{V}$ *ist endlich mit $\sharp\mathbb{V} \leq \sharp\mathbb{M}$, wobei Gleichheit genau dann gilt, wenn ψ bijektiv ist.*

Beweis: „a)“ : Es besteht die Bijektion $\varphi : \mathbb{U} \to \varphi(\mathbb{U})$. Nach 3.20 gilt also $\sharp\mathbb{U} = \sharp\varphi(\mathbb{U})$. Jetzt schliesst man mit 3.23, angewandt auf die Menge $\varphi(\mathbb{U}) \subseteq \mathbb{M}$.

„b)“ : Sei $m := \sharp\mathbb{M}$. Dann besteht eine Bijektion $\alpha : \mathbb{N}_{\leq m} \to \mathbb{M}$. Insbesondere besteht die Surjektion $\psi \circ \alpha : \mathbb{N}_{\leq m} \to \mathbb{V}$. Zu jedem $v \in \mathbb{V}$ gibt es also ein $k \in \mathbb{N}_{\leq m}$ mit $\psi(\alpha(k)) = \psi \circ \alpha(k) = v$. Wir setzen deshalb

$$\varphi(v) := \alpha\left(\min\{k \in \mathbb{N}_{\leq m} | \psi(\alpha(k)) = v\}\right).$$

Auf diese Weise erhalten wir eine Abbildung $\varphi : \mathbb{V} \to \mathbb{M}$. Dabei gilt jeweils

$$(\alpha) \qquad \psi(\varphi(v)) = v\ , \quad (\forall v \in \mathbb{V}).$$

Dies zeigt, dass φ injektiv ist.

Nach Teil a) folgt also $\sharp\mathbb{V} \leq \sharp\mathbb{M}$, wobei Gleichheit genau dann gilt, wenn φ bijektiv ist, d.h. genau dann, wenn φ surjektiv ist. Die Beziehung (α) zeigt aber, dass dies dann und nur dann der Fall ist, wenn ψ injektiv, d.h. bijektiv ist. ■

Schliesslich möchten wir noch die *aufzählende Schreibweise* für endliche Mengen kurz erwähnen.

Notation und Bemerkungen 3.25. A) Sei $n \in \mathbb{N}$, sei $\mathbb{T}$ eine Menge und sei $\varphi : \mathbb{N}_{\leq n} \to \mathbb{T}$ eine Abbildung. Dann besteht die surjektive Abbildung $\varphi : \mathbb{N}_{\leq n} \to \varphi(\mathbb{M}) := (\mathbb{N}_{\leq n})$. Nach 3.24 ist dann $\mathbb{M}$ eine endliche Menge mit $\sharp\mathbb{M} \leq n$. Dabei gilt $\sharp\mathbb{M} = n$ genau dann, wenn $\varphi : \mathbb{N}_{\leq n} \to \mathbb{M}$ bijektiv ist, also genau dann, wenn $\varphi : \mathbb{N}_{\leq n} \to \mathbb{T}$ injektiv ist.

Ist $k \in \mathbb{N}_{\leq n}$, so schreiben wir $m_k := \varphi(k)$. Die Menge $\mathbb{M}$ besteht dann aus den Elementen $m_1, \cdots, m_n$. Deshalb führt man die Schreibweise

a) $$\{m_1, \cdots, m_n\} := \{m_k | k = 1, \cdots, n\} = \mathbb{M}$$

ein, die *aufzählende Schreibweise*.

B) Natürlich lässt sich jede endliche Menge in der Form a) schreiben. Nach dem oben Bemerkten ist dann sofort klar:

> $\sharp\{m_1, \cdots, m_n\} \leq n$, *wobei Gleichheit genau dann gilt, wenn die Elemente* $m_1, \cdots, m_n$ *paarweise verschieden sind, d.h. wenn* $m_i \neq m_j$ *für alle* $i, j \in \mathbb{N}_{\leq n}$ *mit* $i \neq j$.

C) Aufzählend geschrieben hat der Anfangsabschnitt $\mathbb{N}_{\leq n}$ (mit der Wahl $\varphi = \mathrm{id}_{\mathbb{N}_{\leq n}}$) gerade die Form

$$\mathbb{N}_{\leq n} = \{1, 2, \cdots, n\},$$

entsprechend der Schreibweise aus 3.11 B). •

Nun wollen wir unsere Ausführungen „über das Zählen“ beenden, nicht ohne zu bemerken, dass jetzt noch eine ganze Reihe von vertrauten Tatsachen über das Zählen und über die Anzahl der Elemente von Mengen zu beweisen wären. Exemplarisch schlagen wir dazu die folgenden Aufgaben vor:

Aufgaben 3.26. A) Sei $\mathbb{T}$ eine Menge und seien $\mathbb{U}, \mathbb{V} \subseteq \mathbb{T}$ zwei endliche Mengen. Zeigen Sie mit Hilfe von 3.21–3.23, dass die Mengen $\mathbb{U} \cap \mathbb{V}$ und $\mathbb{U} \cup \mathbb{V}$ endlich sind und dass gilt

$$\sharp(\mathbb{U} \cup \mathbb{V}) = \sharp\mathbb{U} + \sharp\mathbb{V} - \sharp(\mathbb{U} \cap \mathbb{V}).$$

B) Sei $\mathbb{T}$ eine Menge, sei $n \in \mathbb{N}$ und seien $\mathbb{M}_1, \cdots, \mathbb{M}_n \subseteq \mathbb{T}$ endliche Mengen so, dass $\mathbb{M}_i \cap \mathbb{M}_j = \emptyset$ für alle $i, j \in \{1, 2, \cdots, n\}$ mit $i \neq j$. Zeigen Sie mit Hilfe von 3.21 durch Induktion bezüglich n, dass

$$\sharp(\mathbb{M}_1 \cup \mathbb{M}_2 \cup \cdots \cup \mathbb{M}_n) = \sharp\mathbb{M}_1 + \sharp\mathbb{M}_2 + \cdots + \sharp\mathbb{M}_n.$$

C) Seien $\mathbb{T}, n$ und $\mathbb{M}_1, \cdots, \mathbb{M}_n$ wie in B), aber sei zusätzlich $r := \sharp\mathbb{M}_1 = \sharp\mathbb{M}_2 = \cdots = \sharp\mathbb{M}_n$. Zeigen Sie, dass $\sharp(\mathbb{M}_1 \cup \mathbb{M}_2 \cup \cdots \cup \mathbb{M}_n) = nr$.

D) Seien $\mathbb{U}$ und $\mathbb{V}$ zwei endliche Mengen. Zeigen Sie, dass auch die Paarmenge $\mathbb{U} \times \mathbb{V} = \{(u, v) | u \in \mathbb{U}, v \in \mathbb{V}\}$ endlich ist, wobei $\sharp(\mathbb{U} \times \mathbb{V}) = (\sharp\mathbb{U})(\sharp\mathbb{V})$. (*Hinweis:* Aufgabe C) verwenden.)

E) Sei $\{m_1, \cdots, m_n\} = \mathbb{M}$ eine endliche Menge mit $\sharp\mathbb{M} = n$. Sei $\mathbb{U}$ eine endliche Menge und sei $\varphi : \mathbb{U} \to \mathbb{M}$ eine Abbildung. Zeigen Sie, dass

$$\sharp\mathbb{U} = \sharp\varphi^{-1}(m_1) + \sharp\varphi^{-1}(m_2) + \cdots + \sharp\varphi^{-1}(m_n).$$

(*Hinweis:* Man kann Aufgabe B) verwenden.)

F) Sei $\mathbb{M} \subseteq \mathbb{R}$ mit $\sharp\mathbb{M} = n \in \mathbb{N}$. Folgen Sie der Beweisidee von 3.15 um zu zeigen, dass es eine wachsende, bijektive Abbildung $\varphi : \mathbb{N}_{\leq n} \to \mathbb{M}$ gibt.

G) Geben Sie n und eine monoton wachsende Bijektion $\varphi : \mathbb{N}_{\leq n} \to \mathbb{M}$ an für

$$\mathbb{M} = \{0, 1, \cdots, k\}, \mathbb{M} = \{-7, -6, \cdots, 0, \cdots, 23\}, \mathbb{M} = \{2k + 1 | k = -4, \cdots, 8\},$$

$$\mathbb{M} = \{(-2)^k | k = 2, 3, 4, 5, 6\} \text{ und } \mathbb{M} = \{\frac{1}{k} | k \in \mathbb{N}_{\leq n}\}.$$

•

Aufgaben 3.27. (*Etwas Kombinatorik*) A) Für zwei Mengen $\mathbb{M}, \mathbb{M}'$ stehe $\mathrm{Abb}(\mathbb{M}, \mathbb{M}')$ für die Menge aller Abbildungen $\varphi : \mathbb{M} \to \mathbb{M}'$. Sei weiter $n := \sharp\mathbb{M}' \in \mathbb{N}$. Zeigen Sie:

a) $\sharp\mathrm{Abb}(\mathbb{N}_{\leq 1}, \mathbb{M}') = n$.

b) Ist $k \in \mathbb{N}$, so gilt $\sharp\mathrm{Abb}(\mathbb{N}_{\leq k+1}, \mathbb{M}') = n \cdot \sharp\mathrm{Abb}(\mathbb{N}_{\leq k}, \mathbb{M}')$.

c) Ist $m \in \mathbb{N}$, so gilt $\sharp\mathrm{Abb}(\mathbb{N}_{\leq m}, \mathbb{M}') = n^m$ (*Hinweis:* Induktion bezüglich m; a), b) verwenden).

d) Ist $\sharp\mathbb{M} = m \in \mathbb{N}$, so gilt $\sharp\mathrm{Abb}(\mathbb{M}, \mathbb{M}') = n^m$.

B) Für je zwei Mengen $\mathbb{M}, \mathbb{M}'$ stehe $\mathrm{injAbb}(\mathbb{M}, \mathbb{M}')$ für die Menge aller injektiven Abbildungen $\varphi : \mathbb{M} \to \mathbb{M}'$. Sei wieder $n := \sharp\mathbb{M}' \in \mathbb{N}$. Zeigen Sie:

a) $\sharp\mathrm{injAbb}(\mathbb{N}_{\leq 1}, \mathbb{M}') = n$.

b) Ist $m \in \mathbb{N}$, so gilt:

$$\sharp\mathrm{injAbb}(\mathbb{N}_{\leq k+1}, \mathbb{M}') = \begin{cases} 0, & \text{falls } k \geq m; \\ (n - k) \cdot \sharp\mathrm{injAbb}(\mathbb{N}_{\leq k}, \mathbb{M}'), & \text{sonst.} \end{cases}$$

c) Ist $m \in \mathbb{N}$, so gilt:

$$\sharp\mathrm{injAbb}(\mathbb{N}_m, \mathbb{M}') = \begin{cases} 0, & \text{falls } m > n; \\ n(n-1)\cdots(n-m+1), & \text{falls } m \leq n. \end{cases}$$

(*Hinweis:* Induktion bezüglich m; a), b) verwenden.)

d) Ist $\sharp\mathbb{M} = m \in \mathbb{N}$, so gilt

$$\sharp\mathrm{injAbb}(\mathbb{M}, \mathbb{M}') = \begin{cases} 0, & \text{falls } m > n; \\ n(n-1)\cdots(n-m+1), & \text{falls } m \leq n. \end{cases}$$

e) Beschreiben Sie das Ergebnis von d) für den Fall $m = n$.

C) Seien $n := \sharp\mathbb{M}'$ und $m \in \{1, \cdots, n\}$. Sei $p_m(\mathbb{M}') := \{\mathbb{U} \subseteq \mathbb{M}' | \sharp\mathbb{U} = m\}$. Wir betrachten die Abbildung

$$\mathrm{injAbb}(\mathbb{N}_{\leq m}, \mathbb{M}') \stackrel{\mathrm{Im}}{\to} p_m(\mathbb{M}'),$$

welche einer injektiven Abbildung $\varphi : \mathbb{N}_{\leq m} \to \mathbb{M}'$ ihre Bildmenge $\mathrm{Im}(\varphi) := \varphi(\mathbb{N}_{\leq m})$ zuordnet.

a) Zeigen Sie, dass für jede Menge $\mathbb{U} \in p_m(\mathbb{M}')$ gilt: $\sharp\mathrm{Im}^{-1}(\mathbb{U}) = m! := m(m-1)(m-2)\cdots 3 \cdot 2 \cdot 1$. (*Hinweis:* Aufgabe B) e) beachten!)

b) Wenden Sie Aufgabe 3.26 E) auf die Abbildung $\mathrm{Im} : \mathrm{injAbb}(\mathbb{N}_{\leq m}, \mathbb{M}') \to p_m(\mathbb{M}')$ an und leiten Sie mit Hilfe der Teilaufgaben a) und B) c) eine Formel für $\sharp p_m(\mathbb{M}')$ her.

D) Sei $p(\mathbb{M}') := \{\mathbb{U} | \mathbb{U} \subseteq \mathbb{M}'\}$ die Menge aller Teilmengen von $\mathbb{M}'$.

a) Zeigen Sie, dass die durch $\varphi \mapsto \Sigma(\varphi) := \varphi^{-1}(1)$ definierte Abbildung

$$\Sigma : \mathrm{Abb}(\mathbb{M}', \{0, 1\}) \to p(\mathbb{M}')$$

bijektiv ist.

b) Verwenden Sie die Teilaufgaben a) und A) d), um eine Formel für $\sharp p(\mathbb{M}')$ herzuleiten.

c) Begründen Sie mit Aufgabe 3.26 B) die Formel

$$\sharp p(\mathbb{M}') = 1 + p_1(\mathbb{M}') + p_2(\mathbb{M}') + \cdots + p_n(\mathbb{M}')$$

und leiten Sie mit den Teilaufgaben b) und C) b) eine rein arithmetische Gleichheit her.

d) Begründen Sie die in Teil c) gefundene arithmetische Beziehung auf einem naheliegenden anderen Weg. •

Teil B
Teiler, Reste und Primzahlen

ZUSAMMENFASSUNG

Im zweiten Teil unserer Vorlesung werden die folgenden zwei Kapitel behandelt:

- Reste, Teiler und Vielfache
- Primzahlen

Im ersten dieser beiden Kapitel studieren wir die *Grundbegriffe der Teilbarkeitslehre*, die ja schon vom Arithmetikunterricht an der Schule bekannt sind. Im Unterschied zur Schule werden wir aber formale Strenge walten lassen, um auf diese Weise dem Aspekt der „Vertiefung von Bekanntem“ zu genügen. Diese Art der Vertiefung ist natürlich etwas anspruchsvoll. Wir hoffen aber, auf diese Weise an Objekten, die uns schon vertraut sind, die mathematische Denkweise zu schulen.

Das grundlegendste Resultat in Kapitel 4 ist zweifellos der *Euklidische Restsatz*, auf dem die Division mit Rest beruht. Besonderes Gewicht legen wir dabei auf die Begriffe des *grössten gemeinsamen Teilers* und der *Teilerfremdheit* zweier ganzer Zahlen. Daran anschliessend werden wir uns auch mit dem *kleinsten gemeinsamen Vielfachen* befassen. Dann werden wir den Blick für einen Moment über die elementare Arithmetik hinausgehen lassen und einen knappen Ausblick auf den *Idealbegriff* geben. In einer Folge von Übungsaufgaben werden wir zur Tatsache hinführen, dass in $\mathbb{Z}$ jedes Ideal ein *Hauptideal* ist. Am Schluss von Kapitel 4 kehren wir uns wieder der elementaren Arithmetik zu und behandeln die *Teilervielfachheit*.

In Kapitel 5 werden wir uns ausführlich mit den „Atomen“ der Teilbarkeitslehre befassen, den *Primzahlen*. Zuerst definieren wir den Begriff der Primzahl und beweisen ein einfaches *Primalitätskriterium*. Dann definieren wir den Begriff des *Primfaktors* oder *Primteilers* und befassen uns mit seinen Eigenschaften. Im Anschluss daran behandeln wir die *Teilerordnung bezüglich einer Primzahl*. Ausgehend von diesem Thema werden wir kurz den Begriff der *Bewertung* streifen – ein Begriff der schon jenseits der elementaren Arithmetik liegt, der aber für die „höhere Arithmetik“ (z. B. für die Theorie der algebraischen Zahlen und Funktionen) von fundamentaler Bedeutung ist.

Das zentrale Ergebnis von Kapitel 5 ist der Satz von der *eindeutigen Zerlegung in Primfaktoren*, den wir entsprechend seiner Bedeutung in einer gewissen Breite behandeln wollen. Dabei werden auch die auf der Primfaktorzerlegung beruhenden *Teilbarkeitskriterien* zur Sprache gebracht. Zum Schluss werden wir uns noch kurz mit der Tatsache befassen, dass es *unendlich viele Primzahlen* gibt.

Auch in diesem Kapitel bleiben wir in der Darstellung bei der Strenge des vorangehenden. Natürlich nehmen wir damit in Kauf, dass wir relativ wenig von dem unglaublich reichhaltigen und immer noch rätselvollen Gebiet der Primzahlen behandeln können. Als Kompensation für diesen Mangel stellen wir einige Übungsaufgaben, die zum Ausprobieren und „Tüfteln“ einladen können – und zur Suche im Internet. Wohl kein Thema der Mathematik ist im Netz so umfassend dokumentiert wie das der Primzahlen. Sich in dieser Fülle einmal umzuschauen und Verständliches herauszuholen lohnt sich im Sinne einer Übung jedenfalls.

TIPPS FÜR DAS SELBSTSTUDIUM

- *Kapitel 4:* Sicher kennen Sie die meisten Begriffe schon, die in diesem Kapitel zur Sprache kommen werden. Doch neu durchdenken (!) von schon Bekanntem ist ein sehr guter Weg zur Vertiefung. Genau aus diesem Grund sollten Sie sich in diesem Kapitel mit den Beweisen auseinandersetzen. Dabei bringt ein vertieftes Studium einiger ausgewählter Beweise vermutlich mehr ein als das rasche Durchgehen von vielen. Besonders empfehlenswert zum Selbststudium sind die Beweise von 4.2, 4.12 und 4.16 und 4.25.

- *Kapitel 5:* Was an Grundsätzlichem zu Kapitel 4 gesagt wurde, gilt auch hier. Zum Selbststudium empfehlen wir besonders die Beweise von 5.2, 5.8, 5.12, 5.15 und 5.20. Die Übungsaufgaben sind besonders wichtig in diesem Kapitel.

Kapitel 4

Reste, Teiler und Vielfache

Überblick

Im ersten Teil unserer Vorlesung haben wir uns mit dem Vergleichen und Zählen im Bereich der natürlichen Zahlen befasst. Nun wollen wir uns dem *Rechnen* mit den ganzen Zahlen, d.h. der Arithmetik in $\mathbb{Z}$ zuwenden. Dabei steht die *Teilbarkeitslehre* im Vordergrund. In diesem Kapitel wollen wir einige Grundbegriffe, die schon aus der Schule bekannt sind, auf ein tragfähiges Fundament stellen. Im Zentrum stehen dabei die Themen

- *die Division mit Rest,*
- *Teiler und Teilerverbände,*
- *der grösste gemeinsame Teiler,*
- *Teilerfremdheit,*
- *Charakterisierungen des grössten gemeinsamen Teilers,*
- *das kleinste gemeinsame Vielfache,*
- *die Teilervielfachheit.*

Die Division mit Rest

Das grundlegendste Konzept dieses Kapitels ist die Division mit Rest, der wir uns jetzt zuwenden wollen. Zunächst benötigen wir noch eine kleine Vorbereitung.

Notation und Bemerkung 4.1. A) Ist $n \in \mathbb{Z}$, so schreiben wir

$$\mathbb{Z}_{\geq n} := \{m \in \mathbb{Z} | m \geq n\}.$$

Es gelten insbesondere $\mathbb{Z}_{\geq 0} = \mathbb{N}_0$ und $\mathbb{Z}_{\geq 1} = \mathbb{N}$.

B) Das Prinzip der kleinsten Zahl 2.4 lässt sich nun wie folgt verallgemeinern:

Ist $n \in \mathbb{Z}$ und ist $\emptyset \neq \mathbb{M} \subseteq \mathbb{Z}_{\geq n}$, so besitzt $\mathbb{M}$ ein Minimum.

Ist nämlich $n \geq 1$, so schliessen wir mit 2.4, weil dann ja $\emptyset \neq \mathbb{M} \subseteq \mathbb{Z}_{\geq n} \subseteq \mathbb{N}$. Ist $n \leq 0$, so setzen wir $\mathbb{M}' := \{m - n + 1 | m \in \mathbb{M}\}$. Dann ist $\emptyset \neq \mathbb{M}' \subseteq \mathbb{N}$ und nach 2.4 existiert $m' := \min(\mathbb{M}')$. Sofort sieht man nun, dass $m' + n - 1 = \min(\mathbb{M})$. •

Nun formulieren und beweisen wir das grundlegende Resultat dieses Abschnittes, welches die „Division mit Rest“ überhaupt rechtfertigt.

Satz 4.2. *(Euklidischer Restsatz) Sei $n \in \mathbb{Z}$ und sei $m \in \mathbb{N}$. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ so, dass*

$$n = mq + r \text{ und } 0 \leq r < m.$$

Beweis: Zuerst zeigen wir die Eindeutigkeit von q und r. Seien also zwei weitere Zahlen $q', r' \in \mathbb{Z}$ so gegeben, dass $n = mq' + r'$ und $0 \leq r' < m$. Wir müssen zeigen, dass $r' = r$ und $q' = q$. Ohne Einschränkung können wir annehmen, es sei $r \leq r'$. Dann gelten $0 \leq r' - r < m$ und $mq' + r' = n = mq + r$, d.h. $r' - r = m(q - q')$. Es folgt $0 \leq m(q - q') < m$. Dies ist nur möglich, wenn $q - q' = 0$, also wenn $q' = q$. Dann ist auch $r' = r$.

Es bleibt zu zeigen, dass q und r existieren. Wir schreiben dazu

$$\mathbb{M} := \{n - mq | q \in \mathbb{Z}\} \cap \mathbb{N}_0.$$

Zuerst überlegen wir uns, dass $\mathbb{M} \neq \emptyset$. Wir müssen dazu ein $q \in \mathbb{Z}$ finden so, dass $n - mq \geq 0$. Ist $n \geq 0$, so genügt es $q = 0$ zu wählen. Ist $n < 0$, so kann man $q = n$ wählen, denn dann gilt ja $n - mq = n - mn = n(1 - m) \geq 0$. Also gilt

$$\emptyset \neq \mathbb{M} \subseteq \mathbb{N}_0 = \mathbb{Z}_{\geq 0}.$$

Nach 4.1 B) existiert deshalb die Zahl

$$r := \min(\mathbb{M}).$$

Mit geeignetem $q \in \mathbb{Z}$ gilt dann

$$r = n - mq, \text{ also } n = mq + r.$$

Es bleibt zu zeigen, dass $0 \leq r < m$. Wegen $r \in \mathbb{M} \subseteq \mathbb{N}_0$ ist $r \geq 0$. Es bleibt also zu zeigen, dass $r < m$. Nehmen wir das Gegenteil an! Dann ist $r \geq m$, d.h. $r - m \in \mathbb{N}_0$. Wegen $r-m = n-mq-m = n-m(q+1)$ folgt dann $r-m \in \mathbb{M}$, also $r-m \geq \min(\mathbb{M}) = r$, d.h. $m \leq 0$ – ein Widerspruch! ■

Definitionen und Bemerkung 4.3. A) Seien $n \in \mathbb{Z}$ und $m \in \mathbb{N}$. Gemäss 4.2 gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit $n = mq + r$ und $0 \leq r < m$. Die Zahl r nennen wir den *Rest bei der Division von n durch m* und schreiben

$$r = n \mod (m) \text{ („}n \text{ modulo } m\text{“)}.$$

Weiter nennen wir die Zahl q den *ganzen Teil des Quotienten* $\frac{n}{m}$ und schreiben

$$q = \left\lfloor \frac{n}{m} \right\rfloor.$$

B) Es gelten die Notationen von Teil A). Anschaulich bildet dann die Menge

$$\mathbb{Z}m := \{km | k \in \mathbb{Z}\}$$

ein „Zahlengitter der Maschenweite m“, welches den Nullpunkt enthält. Der Divisionsrest $r = n \mod (m)$ gibt an, wie weit rechts n vom letzten vorangehenden Gitterpunkt liegt. Der ganze Teil q des Quotienten ist die „Nummer“ dieses vorangehenden Gitterpunktes.

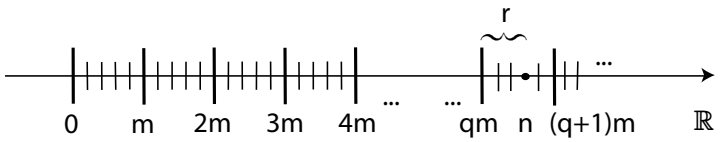


Abbildung 4.1: Division mit Rest

•

Aufgaben 4.4. A) Seien $P_0, \ldots, P_{11}$ die Ecken eines regulären 12-Ecks. Sei $\tau : \mathbb{Z} \to \{P_0, \ldots, P_{11}\}$ gegeben durch $n \mapsto P_{n \bmod (12)}$. Für $k \in \mathbb{N}$ sei $\mathbb{Z}k := \{nk | n \in \mathbb{Z}\}$. Bestimmen und skizzieren Sie $\tau(\mathbb{Z}k)$ für $k = 2, 3, 4, 5$.

B) Es gelten die Bezeichnungen von 4.3. Zeigen Sie:

a) $\left\lfloor \frac{n}{m} \right\rfloor \leq \frac{n}{m} < \left\lfloor \frac{n}{m} \right\rfloor + 1.$

b) $n \bmod (m) = n - m\left\lfloor \frac{n}{m} \right\rfloor.$

C) Sei $m \in \mathbb{Z}_{\geq 3}$. Zeigen Sie, dass für jedes $n \in \mathbb{N}$ die Gleichung $m^n \bmod (m-1) = 1$ gilt und dass $(km^n) \bmod (m-1) = k$ für $k = 0, 1, \ldots, m-2$ (vgl. 3.3 B)).

D) Begründen Sie mit C) die folgende Aussage, die aus dem Schulunterricht bekannt ist:

Eine (dezimal geschriebene) natürliche Zahl hat den gleichen Neunerrest wie ihre Ziffernsumme. •

Teiler und Teilerverbände

Nun wenden wir uns den Begriffen des Teilers und des Vielfachen zu:

Definitionen und Bemerkungen 4.5. A) Seien $m \in \mathbb{N}$ und $n \in \mathbb{Z}$. Wir sagen, m sei ein *Teiler von* n oder n sei ein *Vielfaches von* m, wenn es ein $q \in \mathbb{Z}$ so gibt, dass $n = mq$. Gleichbedeutend ist natürlich auch, dass $n \bmod (m) = 0$.

Ist m ein Teiler von n, so schreiben wir $m|n$. Ist m kein Teiler von n, so schreiben wir $m \nmid n$.

B) Für die Teilbarkeitsbeziehung $\cdot|\cdot$ gelten, wie man nachrechnen kann, die folgenden Regeln, wobei $k, m \in \mathbb{N}$ und $n, p \in \mathbb{Z}$:

a) $m|0;\ 1|n;\ m|m.$

b) $k|m \wedge m|n \Longrightarrow k|n.$

c) $m|n \Longleftrightarrow m|-n.$

d) $m|n \wedge m|p \Longrightarrow m|n+p.$

e) $m|n \Longrightarrow m|np.$

f) $k|m \wedge k \neq m \Longrightarrow k < m.$

g) $km|n \Longrightarrow m|n.$

C) Sei $n \in \mathbb{Z}$. Die Menge aller Teiler von n werde mit $\mathbb{T}(n)$ bezeichnet:

$$\mathbb{T}(n) := \{m \in \mathbb{N} \mid m|n\}.$$

Die Menge $\mathbb{T}(n)$ (versehen mit der Teilbarkeitsrelation $\cdot|\cdot$) nennt man auch den *Teilerverband von* n.

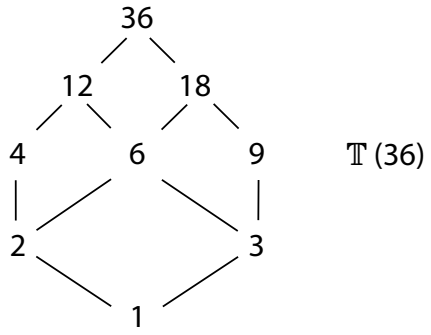


Abbildung 4.2: Ein Teilerverband

Man stellt den Teilerverband manchmal durch sein *„Hassediagramm“* dar, wie vorhergehend am Beispiel $n = 36$ illustriert.

D) Wir wollen einige Eigenschaften von Teilerverbänden festhalten. Sind $m \in \mathbb{N}$ und $n \in \mathbb{Z}$, so folgen aus den Aussagen B) a),b), c) leicht:

a) $\mathbb{T}(0) = \mathbb{N};\ 1 \in \mathbb{T}(n);\ \mathbb{T}(1) = \{1\}.$

b) $\mathbb{T}(n) = \mathbb{T}(-n).$

c) $\mathbb{T}(m) \subseteq \mathbb{T}(n) \Longleftrightarrow m|n.$

Mit Hilfe der Aussage B) f) sieht man sofort:

d) $m \in \mathbb{N} \Longrightarrow \max(\mathbb{T}(m)) = m.$

Zusammen mit Aussage a) ergibt sich daraus (s. 2.16):

e) $n \in \mathbb{Z}\backslash\{0\} \Longrightarrow \sharp\mathbb{T}(n) < \infty.$ •

Der grösste gemeinsame Teiler

Nun wenden wir uns den gemeinsamen Teilern zweier ganzer Zahlen zu. Dabei interessieren wir uns besonders für den grössten gemeinsamen Teiler.

Definitionen und Bemerkungen 4.6. A) Seien $n, p \in \mathbb{Z}$. Eine Zahl $m \in \mathbb{N}$ heisst *gemeinsamer Teiler von n und p*, wenn $m|n$ und $m|p$ gelten, d.h. wenn es Zahlen $k, l \in \mathbb{Z}$ so gibt, dass $n = km$ und $p = lm$.

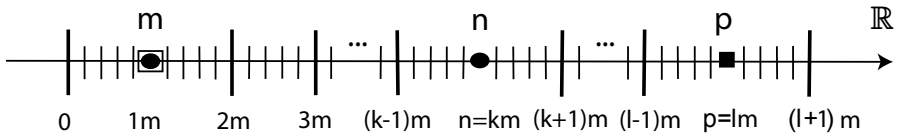


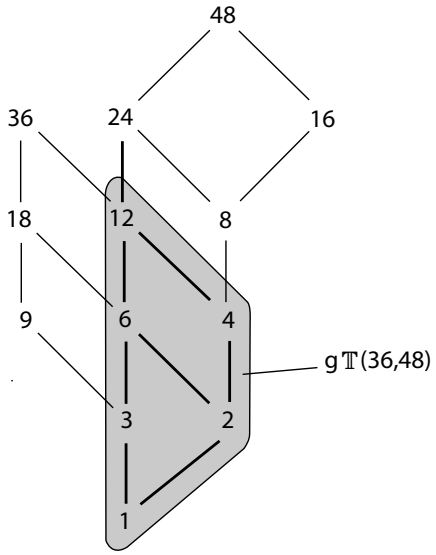
Abbildung 4.3: Gemeinsamer Teiler

B) Seien $n, p \in \mathbb{Z}$. Die Menge

$$g\mathbb{T}(n,p) := \{m \in \mathbb{N} \mid m|n \wedge m|p\}$$

der gemeinsamen Teiler von n und p (versehen mit der Teilbarkeitsrelation $\cdot|\cdot$) nennen wir den *gemeinsamen Teilerverband von n und p*. Natürlich gilt in den Notationen von 4.5 C):

a) $g\mathbb{T}(n,p) = \mathbb{T}(n) \cap \mathbb{T}(p)$.



Illustriert mit $n = 36$ und $p = 48$ ergibt sich die nebenstehende Situation.

Abbildung 4.4: Ein gemeinsamer Teilerverband

Sofort folgen nun (s. 4.5 D) a, b), e), 3.23):

b) $g\mathbb{T}(n,p) = g\mathbb{T}(p,n)$.

c) $g\mathbb{T}(0,p) = \mathbb{T}(p);\ 1 \in g\mathbb{T}(n,p)$.

d) $g\mathbb{T}(-n,p) = g\mathbb{T}(n,p)$.

e) $n \neq 0 \vee p \neq 0 \Longrightarrow \sharp \mathrm{g}\mathbb{T}(n,p) < \infty$.

C) Seien $n, p \in \mathbb{Z}$ mit $n \neq 0$ oder $p \neq 0$. Nach Aussage B) e) ist der gemeinsame Teilerverband $\mathrm{g}\mathbb{T}(n,p)$ endlich. Nach B) c) ist aber auch $\mathrm{g}\mathbb{T}(n,p) \neq \emptyset$. Wegen $\mathrm{g}\mathbb{T}(n,p) \subseteq \mathbb{N}$ enthält $\mathrm{g}\mathbb{T}(n,p)$ also eine grösste Zahl (s. 2.16). Diese heisst der *grösste gemeinsame Teiler von n und p* und wird mit $\mathrm{ggT}(n,p)$ bezeichnet. Also:

$$\mathrm{ggT}(n,p) := \max\left(\mathrm{g}\mathbb{T}(n,p)\right);\ (n,p \in \mathbb{Z}; n \neq 0 \text{ oder } p \neq 0).$$

Anschaulich gesagt, ist der grösste gemeinsame Teiler von n und p die grösste natürliche Zahl g so, dass n und p zum „0-zentrierten Zahlengitter mit Maschenweite g“ gehören, d.h. so, dass $n, p \in \mathbb{Z}g := \{kg | k \in \mathbb{Z}\}$.

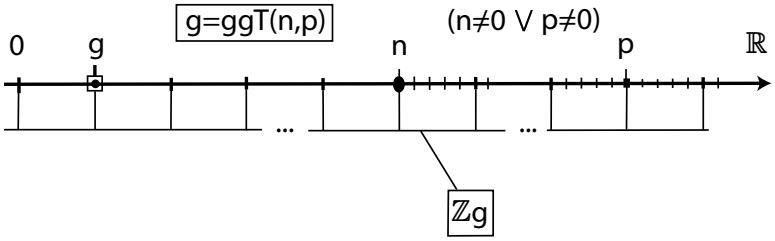


Abbildung 4.5: Grösster gemeinsamer Teiler

•

Bevor wir uns mit der Berechnung des ggT und seinen Anwendungen befassen, stellen wir einige Rechenregeln bereit.

Satz 4.7. *(Rechenregeln für den* ggT*) Sei $m \in \mathbb{N}$ und seien $n, p \in \mathbb{Z}$ so, dass $n \neq 0$ oder $p \neq 0$. Dann gelten die Regeln:*

a) $\mathrm{ggT}(n,p) = \mathrm{ggT}(p,n)$.

b) $\mathrm{ggT}(n,p) = \mathrm{ggT}(-n,p)$.

c) $\mathrm{ggT}(m,0) = m$.

d) $\mathrm{ggT}(m,n) = \mathrm{ggT}(m, n \bmod(m))$.

Beweis: „a)“ : Klar aus 4.6 B) b).

„b)“ : Klar aus 4.6 B) d).

„c)“ : Klar aus 4.6 B) c) und 4.5 D) d).

„d)“ : Sei $r := n \bmod (m)$. Dann ist $0 \leq r < m$, und es gibt ein $q \in \mathbb{Z}$ mit $n = mq + r$. Seien $g := \mathrm{ggT}(m, n)$ und $\overline{g} := \mathrm{ggT}(m, r)$. Wir müssen zeigen, dass $g = \overline{g}$.

Wegen $g|m$ und $g|n$ folgt $g|(n + m(-q)) = n - mq = r$ (s. 4.5 B) e), d)), und damit ist g ein gemeinsamer Teiler von m und r. Insbesondere ist $g \leq \overline{g}$.

Wegen $\overline{g}|m$ und $\overline{g}|r$ folgt $\overline{g}|(mq + r) = n$ (s. 4.5 B), e), d)), und damit ist $\overline{g}$ ein gemeinsamer Teiler von m und n. Insbesondere ist $\overline{g} \leq g$. Es folgt $g = \overline{g}$. ■

Nun können wir einen Algorithmus zur Berechnung des ggT angegeben.

Anwendung 4.8. (*Euklidischer Algorithmus zur Bestimmung des ggT*) Seien $m \in \mathbb{N}$ und $n \in \mathbb{Z}$. Die Rechenregeln 4.7 erlauben es, m und n durch fortgesetztes Divisionsrestbilden zu „reduzieren“, ohne den ggT zu verändern. Dies führt zu einer effizienten Methode zur Bestimmung des ggT, die wie folgt skizziert werden kann:

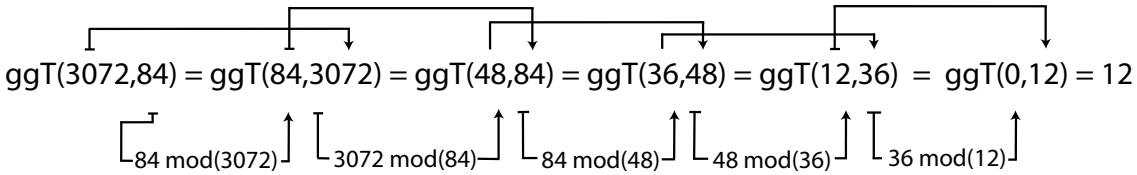
$$\mathrm{ggT}(m,n) = \mathrm{ggT}(r_1,m) = \mathrm{ggT}(r_2,r_1) = \ \ldots\ = \mathrm{ggT}(0,r_n) = r_n\ .$$

$$r_1 = n \bmod (m) \qquad r_2 = m \bmod (r_1) \qquad r_{n-1} \bmod (r_n)$$

$$(m > r_1 > r_2 > \ldots > r_n > 0\ ;\ r_i \in \mathbb{N})$$

•

Beispiel 4.9.



•

Aufgaben 4.10. A) Beweisen Sie einige der Aussagen 4.5 B) a)–g) (falls Sie dies nicht schon getan haben) und beweisen Sie die Aussagen 4.5 D) c), d).

B) Skizzieren Sie den Teilerverband $\mathbb{T}(n)$ für $n = 5, 8, 100, 120, 196, 1024$.

C) Skizzieren Sie gemäss Abbildung 4.4 den gemeinsamen Teilerverband $\mathrm{g}\mathbb{T}(n, p)$ als Durchschnitt der Teilerverbände $\mathbb{T}(n)$ und $\mathbb{T}(p)$ für die Zahlenpaare $(n, p) = (17, 35)$, $(2, 20)$, $(100, 40)$, $(100, 80)$.

D) Löschen Sie in der Abbildung 4.4 alle eingetragenen Zahlen und lassen Sie nur das Netz der Teilbarkeitsrelation stehen. Bestimmen Sie alle Zahlenpaare $(n, p) \in \mathbb{N}^2$ mit $n, p \leq 200$ so, dass für die Teilerverbände $g\mathbb{T}(n, p) \subseteq \mathbb{T}(n), \mathbb{T}(p)$ das gleiche Netz verwendet werden kann wie in Abbildung 4.4.

E) Bestimmen Sie mit dem Algorithmus aus 4.8 die beiden Zahlen ggT(513, 10701) und ggT(1716, 299).

F) Skizzieren Sie ein Flussdiagramm für den Algorithmus aus 4.8.

G) Ein rechteckiges Grundstück von 52 m Länge und 36 m Breite soll eingezäunt werden, wobei die Zaunpfähle in gleichmässigem Abstand eingepflockt werden sollen. Welches ist der grösste Abstand zwischen den Pfählen, den man wählen kann? Wie viele Pfähle werden mindestens gebraucht?

H) 1000 quadratische Platten gleicher Grösse werden zu einem rechteckigen Platz zusammengefügt.

a) Bei welchem „Format“ ist der Umfang des Platzes am kleinsten?

b) Der Platz soll eingezäunt werden, wobei der Abstand zwischen aufeinanderfolgenden Pfählen immer gleich sein soll. Mit wie vielen Pfählen kann man auskommen? (*Hinweis:* Für jedes „Format“ des Platzes die Frage beantworten.)

I) Ein kleines Zahnrad mit 13 Zähnen wirkt auf ein grosses Zahnrad mit 78 Zähnen. Ein Zahn des kleinen Rades ist beschädigt und zerkratzt beim Eingriff jeweils eine Zahnflanke des grossen Rades.

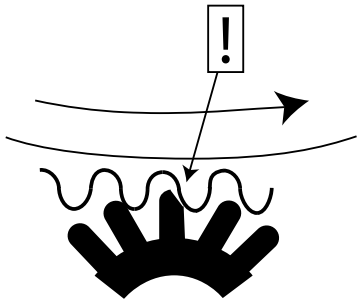


Abbildung 4.6: Zahnräder

Wie viele Zähne des grossen Rades werden zerkratzt? Wie viele Umdrehungen muss jedes der Räder mindestens machen, damit so viele Zähne zerkratzt werden?

J) Wie lauten die Antworten auf die Fragen aus I) allgemein, wenn das „kleine“ Zahnrad m und das „grosse“ n Zähne hat. •

Teilerfremdheit

Nun wollen wir uns mit dem wichtigen Begriff der Teilerfremdheit befassen.

Definition 4.11. Zwei Zahlen $m, n \in \mathbb{Z}$ heissen *teilerfremd*, wenn sie ausser 1 keinen gemeinsamen Teiler haben, d.h. wenn $\mathrm{ggT}(m, n) = 1$. •

Wir beweisen ein *erstes Kriterium für die Teilerfremdheit.*

Satz 4.12. *Seien $m, n \in \mathbb{Z}$. Dann sind äquivalent:*

(i) *m und n sind teilerfremd;*

(ii) *Es gibt Zahlen $u, v \in \mathbb{Z}$ so, dass $um + vn = 1$.*

Beweis: „(i) $\Rightarrow$ (ii)“ : Sei $\mathrm{ggT}(m, n) = 1$. Zuerst zeigen wir die Existenz von u und v für den Fall, dass $m, n \geq 0$. Ohne Einschränkung können wir annehmen, es sei $m \leq n$. Ist $m = 0$, so ist $n = 1$ und wir können $u = 0$ und $v = 1$ wählen. Es genügt also den Fall $m > 0$ zu betrachten. Wir behandeln diesen Fall durch Induktion nach m.

Ist $m = 1$, so wählen wir $u = 1$ und $v = 0$. Sei also $m > 1$. Wir setzen $r := n \bmod (m)$. Dann gilt $0 \leq r < m$ und mit einem geeigneten $q \in \mathbb{Z}$ besteht die Gleichung $n = mq + r$. Dabei ist $\mathrm{ggT}(r, m) = 1$ (s. 4.7 a), d)). Wegen $m > 1$ folgt auch $r \neq 0$ (vgl. 4.7 c)), d.h. $r > 0$.

Weil $r < m$ gilt, können wir nun die Induktionsvoraussetzung auf das Paar $(r, m) \in \mathbb{N} \times \mathbb{N}$ anwenden und davon ausgehen, dass es Zahlen $a, b \in \mathbb{Z}$ so gibt, dass $ar + bm = 1$. Mit $u := b - aq$ und $v := a$ folgt dann

$$\begin{aligned} um + vn &= (b - aq)m + a(mq + r) \\ &= bm + ar - aqm + amq = bm + ar = 1. \end{aligned}$$

Sind m und n nicht beide grösser oder gleich 0, so betrachtet man die beiden teilerfremden Zahlen $|m|, |n| \in \mathbb{N}_0$ (vgl. 4.7 a), b)). Nach dem soeben Gezeigten gibt es dann Zahlen $\overline{u}, \overline{v} \in \mathbb{Z}$ mit $\overline{u}|m| + \overline{v}|n| = 1$. Durch geeignete Vorzeichenwechsel bei $\overline{u}$ und $\overline{v}$ folgt die Behauptung.

„(ii) $\Rightarrow$ (i)“ : Seien $u, v \in \mathbb{Z}$ mit $um + vn = 1$. Sei $g = \mathrm{ggT}(m, n)$. Wegen $g|m$ und $g|n$ folgt $g|1$ (s. 4.5 B) e), d)), also $g = 1$. ■

Bemerkung und Beispiel 4.13. A) Sind $m, n \in \mathbb{Z}$ teilerfremd und nicht zu gross, so kann man die beiden Zahlen u, v aus der Aussage (ii) von 4.12 meist schnell durch systematisches ausprobieren finden: Man erstellt eine Liste der Zahlen $um - 1$ mit $u = 0, 1, 2, \ldots$ und sucht unter diesen Zahlen ein Vielfaches von n. Schreibt man dieses in der Form $(-v)n$, so folgt $um + vn = 1$.

u	0	1	2	3	4	5	6	7	8	9	...
8u-1	-1	7	15	23	31	39	47	55	63 = 7·9	71	···

B) Wir betrachten als Beispiel die Zahlen $m = 8$ und $n = 9$ und erstellen die obenstehende Tabelle. Wir können also $u = 8$ und $v = 7$ wählen. In der Tat ist $8 \cdot 8 + (-7) \cdot 9 = 64 - 63 = 1$. Natürlich sind noch andere Wahlen von u und v möglich, zum Beispiel $u = -1, v = 1$. •

Als Konsequenz von 4.12 ergibt sich ein *zweites Kriterium für die Teilerfremdheit.*

Korollar 4.14. *Seien $m, n \in \mathbb{N}$. Dann sind äquivalent:*

(i) *m und n sind teilerfremd;*

(ii) *Für jede Zahl $k \in \mathbb{Z}$ mit $m|k$ und $n|k$ gilt $mn|k$.*

Beweis: „(i) $\Rightarrow$ (ii)“ : Seien m und n teilerfremd. Sei $k \in \mathbb{Z}$ mit $m|k$ und $n|k$. Mit geeigneten Zahlen $h, l \in \mathbb{Z}$ folgt also $k = mh = nl$. Nach 4.12 gibt es Zahlen $u, v \in \mathbb{Z}$ mit $um+vn = 1$. Es folgt $k = k \cdot 1 = k(um+vn) = kum+kvn = nlum+mhvn = mn(lu+hv)$, also $mn|k$.

„(ii) $\Rightarrow$ (i)“ : Es gelte die Aussage (ii). Sei $g := \mathrm{ggT}(m, n)$. Wir müssen zeigen, dass $g = 1$. Mit geeigneten Zahlen $a, b \in \mathbb{N}$ gelten $m = ga$ und $n = gb$. Sei $k := gab$. Dann gelten $m = ga|k$ und $n = gb|k$. Gemäss Aussage (ii) folgt daraus $mn|k$. Es gibt also ein $h \in \mathbb{N}$ mit $mnh = k$. Es folgt $gagbh = mnh = k = gab$, d.h. $(gab)gh = gab$. Wegen $gab \neq 0$ ergibt sich $gh = 1$, also $g = 1$. ■

Charakterisierungen des grössten gemeinsamen Teilers

Die beiden Teilerfremdheitskriterien 4.12 und 4.14, insbesondere das erste der beiden, begleiten uns ab jetzt als wichtige Werkzeuge durch die Vorlesung. Wir werden dies schon im Beweis des nachfolgenden Satzes 4.16 sehen, der eine neue *Charakterisierung des* ggT gibt, welche 4.12 auf nichtteilerfremde Zahlenpaare erweitert. Um diesen Satz knapp formulieren zu können, führen wir zunächst geeignete Bezeichnungen ein.

Notationen und Bemerkung 4.15. A) Für $m \in \mathbb{Z}$ haben wir schon öfter die naheliegende Schreibweise

$$\mathbb{Z}m := m\mathbb{Z} := \{wm | w \in \mathbb{Z}\} = \{mw | w \in \mathbb{Z}\}$$

benutzt, die wir ab jetzt kommentarlos verwenden.

B) Sind $\mathbb{M}, \mathbb{L} \subseteq \mathbb{Z}$ mit $\mathbb{M}, \mathbb{L} \neq \emptyset$, so setzen wir:

$$\mathbb{M} + \mathbb{L} := \{m + l | m \in \mathbb{M}, l \in \mathbb{L}\}.$$

C) Sofort sieht man, dass für zwei Zahlen $m, n \in \mathbb{Z}$ gilt:

$$\mathbb{Z}m + \mathbb{Z}n = \{mu + nv | u, v \in \mathbb{Z}\}.$$

•

Nun formulieren und beweisen wir den angekündigten Satz.

Satz 4.16. *Seien $m, n \in \mathbb{Z}$ so, dass $m \neq 0$ oder $n \neq 0$. Dann gelten*

a) $\mathrm{ggT}(m, n) = \min(\mathbb{N} \cap (\mathbb{Z}m + \mathbb{Z}n))$.

b) *Es gibt Zahlen $u, v \in \mathbb{Z}$ mit $mu + nv = \mathrm{ggT}(m, n)$.*

c) $\mathbb{Z}m + \mathbb{Z}n = \mathbb{Z}(\mathrm{ggT}(m, n))$.

Beweis: Sei $g := \mathrm{ggT}(m, n)$.

„a)“ : Nach 4.15 C) gilt

(α) $$\mathbb{Z}m + \mathbb{Z}n = \{mu + nv | u, v \in \mathbb{Z}\}.$$

Diese Menge enthält sicher natürliche Zahlen, denn weil m und n nicht beide 0 sind, ist $mm + nn \in \mathbb{N}$. Also ist $\emptyset \neq \mathbb{N} \cap (\mathbb{Z}m + \mathbb{Z}n) \subseteq \mathbb{N}$. Nach 2.4 existiert deshalb

$$t := \min(\mathbb{N} \cap (\mathbb{Z}m + \mathbb{Z}n)).$$

Wir müssen zeigen, dass $g = t$.

Wegen unserer Wahl von t gibt es Zahlen $\overline{u}, \overline{v} \in \mathbb{Z}$ mit $t = m\overline{u} + n\overline{v}$. Wegen $g|m$ und $g|n$ folgt $g|t$, also $g \leq t$, (s. 4.5 D) d)). Es bleibt demnach zu zeigen, dass $t \leq g$. Wegen $g|m$ und $g|n$ finden wir Zahlen $h, k \in \mathbb{Z}$ mit $m = gh$ und $n = gk$. Wir wollen uns überlegen, dass h und k teilerfremd sind: Wäre dies nicht der Fall, so gäbe es ein $s \in \mathbb{N}\backslash\{1\}$ mit $s|h$ und $s|k$. Daraus würden $sg|m$ und $sg|n$ folgen, aber auch $sg > g$, ein Widerspruch

zur Tatsache dass $g = \mathrm{ggT}(m, n)$ der grösste gemeinsame Teiler von m und n ist. Also sind h und k tatsächlich teilerfremd.

Gemäss 4.12 finden wir nun Zahlen $a, b \in \mathbb{Z}$ mit $ha + kb = 1$. Es folgt

$$g = g \cdot 1 = g(ha + kb) = gha + gkb = ma + nb.$$

Dies zeigt, dass $g \in \mathbb{N} \cap (\mathbb{Z}m + \mathbb{Z}n)$, also, dass $t \leq g$.

„b)“ : Klar aus a) und (α).

„c)“ : „$\subseteq$“ : Folgt leicht aus $g|m$ und $g|n$. „$\supseteq$“ : Folgt leicht aus b). ■

Im Sinne eines kleinen Ausblickes fügen wir noch die folgende Bemerkungen (und Definitionen) an.

Definitionen und Bemerkungen 4.17. A) Eine Menge $\mathbb{I} \subseteq \mathbb{Z}$ heisst ein *Ideal*, wenn sie folgenden Forderungen genügt:

(I_1) $\mathbb{I} \neq \emptyset$;

(I_2) $x, y \in \mathbb{I} \Longrightarrow x + y \in \mathbb{I}$;

(I_3) $z \in \mathbb{Z}, x \in \mathbb{I} \Longrightarrow xz \in \mathbb{I}$.

B) Leicht sieht man:

a) *Ist $m \in \mathbb{Z}$, so ist $\mathbb{Z}m$ ein Ideal.*

Ideale der speziellen Form $\mathbb{Z}m$ (mit $m \in \mathbb{Z}$) nennt man *Hauptideale*. Genauer heisst $\mathbb{Z}m$ das *von m erzeugte Hauptideal*.

Beispiele von Hauptidealen sind die Mengen

$$\mathbb{Z}0 = \{0\},\ \mathbb{Z}1 = \mathbb{Z},\ \mathbb{Z}2 = \{n \in \mathbb{Z} \mid 2|n\}, \ldots$$

C) Man kann auch leicht nachrechnen:

a) *Sind $\mathbb{I}, \mathbb{J} \subseteq \mathbb{Z}$ Ideale, so ist auch $\mathbb{I} \cap \mathbb{J}$ ein Ideal.*

b) *Sind $\mathbb{I}, \mathbb{J} \subseteq \mathbb{Z}$ Ideale, so ist auch $\mathbb{I} + \mathbb{J}$ ein Ideal.*

D) Aus den Aussagen B) a) und C) b) folgt natürlich sofort, dass $\mathbb{Z}m + \mathbb{Z}n$ für beliebige Zahlen $m, n \in \mathbb{Z}$ ein Ideal ist. Nach 4.16 c) lässt sich allerdings mehr sagen: $\mathbb{Z}m + \mathbb{Z}n$ ist immer ein Hauptideal (erzeugt durch $\mathrm{ggT}(m, n)$ falls $m \neq 0$ oder $n \neq 0$; erzeugt durch 0, wenn $m = n = 0$). Ganz unerwartet ist diese Aussage allerdings nicht, denn man kann zeigen:

a) *Jedes Ideal* $\mathbb{I} \subseteq \mathbb{Z}$ *ist ein Hauptideal.* •

Als unmittelbare Anwendung von 4.16 erhalten wir:

Korollar 4.18. *Seien* $m, n \in \mathbb{Z}$ *so, dass* $m \neq 0$ *oder* $n \neq 0$*. Dann sind die gemeinsamen Teiler von* m *und* n *gerade die Teiler von* $\mathrm{ggT}(m,n)$*, d.h. (in den Bezeichnungen von 4.5 C) und 4.6 B)):*

$$\mathrm{g}\mathbb{T}(m,n) = \mathbb{T}\left(\mathrm{ggT}(m,n)\right).$$

Beweis: Wir schreiben $g = \mathrm{ggT}(m,n)$. „$\subseteq$“ : Sei $t \in \mathrm{g}\mathbb{T}(m,n)$. Nach 4.16 b) finden wir Zahlen $u, v \in \mathbb{Z}$ mit $g = mu + nv$. Es folgt $t|g$, also $t \in \mathbb{T}(g)$.

„$\supseteq$“ : Sei $t \in \mathbb{T}(g)$, d.h. $t|g$. Wegen $g|m$ und $g|n$ folgen dann $t|m$ und $t|n$, also $t \in \mathrm{g}\mathbb{T}(m,n)$. ■

Bemerkung 4.19. Korollar 4.18 belegt, dass der „ggT im gemeinsamen Teilerverband maximal“ ist:

> *Der grösste gemeinsame Teiler von* m *und* n *ist sowohl bezüglich der Grösser-kleiner-Relation als auch bezüglich der Teilbarkeitsrelation das (eindeutig bestimmte) maximale Element des gemeinsamen Teilerverbandes von* m *und* n*.* •

Aufgaben 4.20. A) Bestimmen Sie $u, v \in \mathbb{Z}$ mit $mu + nv = \mathrm{ggT}(m,n)$ für die Paare $(m,n) = (2,3), (39,299), (72,162)$.

B) Beweisen Sie die Aussagen 4.17 B) a) und C) a), b).

C) Sei $\mathbb{I} \subseteq \mathbb{Z}$ ein Ideal. Zeigen Sie:

a) $x \in \mathbb{I} \Longrightarrow -x \in \mathbb{I}$.

Schliessen Sie aus a):

b) $\mathbb{I} \neq \{0\} \Longrightarrow \mathbb{N} \cap \mathbb{I} \neq \emptyset$.

Seien $\mathbb{I} \neq \{0\}$ und $t := \min(\mathbb{N} \cap \mathbb{I})$ (vgl. b) und 2.4). Zeigen Sie:

c) $x \in \mathbb{I} \Longrightarrow x \bmod (t) \in \mathbb{I}$.

Schliessen Sie aus c):

d) $x \in \mathbb{I} \Longrightarrow x \in \mathbb{Z}t$.

Schliessen Sie aus d):

e) $\mathbb{I} = \mathbb{Z}t$.

(Bravo, Sie haben die Aussage a) aus 4.17 D) bewiesen.)

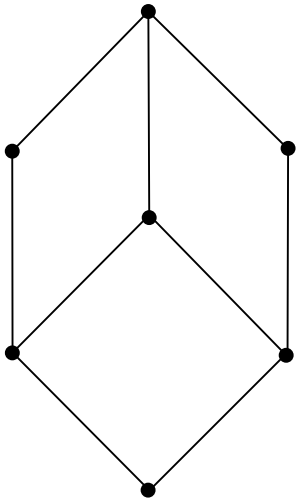


Abbildung 4.7: Netz eines Verbandes

D) Warum kann das dargestellte Netz *nicht* das Netz des gemeinsamen Teilerverbandes zweier natürlicher Zahlen sein? •

Das kleinste gemeinsame Vielfache

Nachdem wir uns nun so ausführlich mit dem grössten gemeinsamen Teiler zweier ganzer Zahlen befasst haben, sollten wir uns doch noch kurz mit seinem „Gegenstück“ befassen, dem kleinsten gemeinsamen Vielfachen.

Definitionen und Bemerkungen 4.21. A) Seien $m, n \in \mathbb{N}$. Ein *gemeinsames Vielfaches* von m und n ist eine Zahl $w \in \mathbb{Z}$, die sowohl von m als auch von n geteilt wird, d.h. eine Zahl $w \in \mathbb{Z}$ mit $m|w$ und $n|w$.

B) Weil $\mathbb{Z}m$ die Menge der Vielfachen von m ist und $\mathbb{Z}n$ die Menge der Vielfachen von n, ist $\mathbb{Z}m \cap \mathbb{Z}n$ die Menge der gemeinsamen Vielfachen von m und n:

$$\mathbb{Z}m \cap \mathbb{Z}n = \{w \in \mathbb{Z} \mid m|w \wedge n|w\}.$$

C) Wegen $mn \in \mathbb{Z}m \cap \mathbb{Z}n$ ist

$$\emptyset \neq \mathbb{N} \cap (\mathbb{Z}m \cap \mathbb{Z}n) \subseteq \mathbb{N}.$$

Nach 2.4 enthält $\mathbb{N} \cap (\mathbb{Z}m \cap \mathbb{Z}n)$ also eine kleinste Zahl. Diese nennen wir das *kleinste gemeinsame Vielfache von m und n* und bezeichnen sie mit $\mathrm{kgV}(m, n)$. Also:

$$\mathrm{kgV}(m, n) := \min\left(\mathbb{N} \cap (\mathbb{Z}m \cap \mathbb{Z}n)\right);\ (m, n \in \mathbb{N}).$$

•

Alles Wesentliche über das kleinste gemeinsame Vielfache wird im folgenden Satz gesagt:

Satz 4.22. *Seien $m, n \in \mathbb{N}$. Dann gilt* $\mathrm{ggT}(m,n)\mathrm{kgV}(m,n) = mn$.

Beweis: Seien $g := \mathrm{ggT}(m,n)$ und $k := \mathrm{kgV}(m,n)$. Wir müssen zeigen, dass $gk = mn$.

Wegen $g|m$ und $g|n$ finden wir Zahlen $h, l \in \mathbb{Z}$ mit $m = gh$ und $n = gl$. Wegen $g, m, n > 0$ sind $h > 0$ und $l > 0$, d.h. es gilt $h, l \in \mathbb{N}$. Nun folgt $mn = ghgl = g(ghl)$, wobei $ghl \in \mathbb{N}$. Natürlich ist ghl ein Vielfaches von $m = gh$ und von $n = gl$. Deshalb ist $k \leq ghl$. Es folgt $gk \leq g(ghl) = mn$. Es bleibt also zu zeigen, dass $gk \geq mn$.

Nach 4.16 b) gibt es Zahlen $u, v \in \mathbb{Z}$ mit $mu + nv = g$. Es gibt wegen $m|k$ und $n|k$ aber auch Zahlen $a, b \in \mathbb{Z}$ mit $ma = k = nb$. Es folgt $gk = (mu + nv)k = muk + nvk = munb + nvma = mn(ub + va)$, also $mn|gk$. Damit ist $mn \leq gk$ (s. 4.5 D) d)). ■

Korollar 4.23. *Seien $m, n \in \mathbb{N}$. Dann sind die gemeinsamen Vielfachen von m und n gerade die Vielfachen von* $\mathrm{kgV}(m,n)$*, d.h.*

$$\mathbb{Z}m \cap \mathbb{Z}n = \mathbb{Z}(\mathrm{kgV}(m,n)).$$

Beweis: Seien $g := \mathrm{ggT}(m,n)$ und $k := \mathrm{kgV}(m,n)$.

„$\supseteq$“ : Sei $x \in \mathbb{Z}k$. Dann gilt $k|x$. Wegen $m|k$ und $n|k$ folgen $m|x$ und $n|x$, also $x \in \mathbb{Z}m \cap \mathbb{Z}n$.

„$\subseteq$“ : Sei $w \in \mathbb{Z}m \cap \mathbb{Z}n$. Wir finden Zahlen $a, b \in \mathbb{Z}$ mit $w = ma = nb$. Nach 4.16 b) gibt es aber auch Zahlen $u, v \in \mathbb{Z}$ mit $g = mu + nv$. Es folgt mit Hilfe von 4.22

$$\begin{aligned} gw &= (mu + nv)w = muw + nvw = \\ &= munb + nvma = mn(ub + va) \\ &= gk(ub + va), \end{aligned}$$

also $w = k(ub + va)$, d.h. $w \in \mathbb{Z}k$. ■

Aufgaben 4.24.

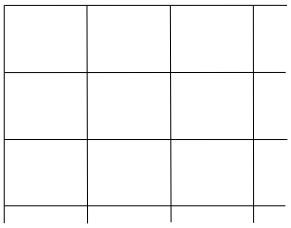


Abbildung 4.8: Bodenplatten

A) Ein quadratischer Gartensitzplatz soll mit rechteckigen Platten vom Format 16 cm × 12 cm belegt werden. Dabei werden nur ganze Platten verwendet. Der Erstellungspreis beträgt Fr. 250.– pro m^2. Die Gesamtkosten dürfen Fr. 3000.– nicht übersteigen. Wie gross darf der Sitzplatz werden?

B) Buslinie A verkehrt ab Zentralplatz alle 10 Minuten.
Buslinie B verkehrt ab Zentralplatz alle 6 Minuten.
Buslinie C verkehrt ab Zentralplatz alle 8 Minuten.

Um 06:00 Uhr verlassen alle drei Busse zum ersten mal den Zentralplatz. Wie oft fahren die Linien AB, AC, BC, ABC gleichzeitig los bis zur Umstellung auf Nachtbetrieb um 20:00 Uhr?

C) Seien $m, n \in \mathbb{Z}$. Zeigen Sie:

a) $\mathbb{Z}mn \subseteq \mathbb{Z}m \cap \mathbb{Z}n$.

b) Für $m \neq 0$ und $n \neq 0$ gilt: $\mathbb{Z}mn = \mathbb{Z}m \cap \mathbb{Z}n \iff \mathrm{ggT}(m, n) = 1$.

D) Die Zeit zwischen zwei aufeinanderfolgenden Vollmonden beträgt (im Mittel)

29 Tage, 12 Stunden und 44 Minuten.

Wann frühestens kann die skizzierte Situation zum nächsten Mal eintreffen?

Abbildung 4.9: Vollmond

(*Hinweis:* In Minuten rechnen; Problem auch für eine Uhr ohne Wochentaganzeige lösen.)

E) Ein Jahr dauert 365 Tage und 6 Stunden. Der Beginn des Jahres x fiel auf einen Mittwoch um 00:00 Uhr. Wann wird diese Situation zum nächsten mal auftreten? (Schaltjahre vernachlässigen.) •

Die Teilervielfachheit

Nun wollen wir uns mit dem Begriff der Teilervielfachheit einer natürlichen Zahl $m > 1$ in einer ganzen Zahl n befassen. Es geht dabei einfach darum, „wie oft“ eine ganze Zahl n durch eine gegebene Zahl $m \in \mathbb{N}\backslash\{1\}$ teilbar ist. Wir gehen aus vom folgenden Satz.

Satz 4.25. *Sei $m \in \mathbb{N}\backslash\{1\}$ und sei $n \in \mathbb{Z}\backslash\{0\}$. Dann gibt es eindeutig bestimmte Zahlen $\nu \in \mathbb{N}_0$ und $l \in \mathbb{Z}$ so, dass*

$$n = m^\nu l \text{ und } m \nmid l.$$

Insbesondere gilt $\nu = \max\{\mu \in \mathbb{N}_0 \mid m^\mu | n\}$.

Beweis: Zuerst zeigen wir die Eindeutigkeit von ν und l. Seien also $\nu, \nu' \in \mathbb{N}_0$ und $l, l' \in \mathbb{Z}$ so, dass $n = m^\nu l = m^{\nu'} l', m \nmid l$ und $m \nmid l'$. Ohne Einschränkung können wir annehmen, es sei $\nu \leq \nu'$. Es folgt nun

$$m^\nu(m^{\nu'-\nu} l') = m^{\nu+\nu'-\nu} l' = m^{\nu'} l' = m^\nu l,$$

also $m^{\nu'-\nu} l' = l$. Wegen $m \nmid l$ muss deshalb $\nu - \nu' = 0$ gelten, d.h. $\nu = \nu'$.

Nun folgt aber auch $m^\nu l = m^\nu l'$, also $l = l'$. Damit ist die Eindeutigkeit von ν und l gezeigt.

Wir beweisen nun die Existenz der Zahlen ν und l und gleichzeitig, dass ν das Maximum der Menge

$$\mathbb{M} := \{\mu \in \mathbb{N}_0 \mid m^\mu | n\}$$

ist.

Zuerst behandeln wir den Fall $n > 0$. Sei zunächst $m \nmid n$. Dann gilt natürlich $\mathbb{M} = \{0\}$ und es genügt, $\nu = 0$ und $l = n$ zu setzen. Es gelte also $m|n$. Dann ist $1 \in \mathbb{M}$ und somit ist $\mathbb{M}\backslash\{0\}$ eine nichtleere Menge natürlicher Zahlen. Ist $\mu \in \mathbb{M}\backslash\{0\}$, so folgt mit 3.3 A) sofort

$$\mu \leq 1 + \mu \leq 1 + \mu(m-1) \leq (1 + (m-1))^\mu = m^\mu.$$

Wegen $m^\mu \in \mathbb{T}(n)$ gilt aber auch $m^\mu \leq n$ (s. 4.5 D) d)), und wir erhalten $\mu \leq n$. Damit ist n eine obere Schranke von $\mathbb{M}\backslash\{0\}$. Nach 2.16 (s. auch 2.15) existiert also die Zahl $\nu := \max(\mathbb{M}\backslash\{0\})$. Dabei ist $\nu > 0$, woraus

$$(\alpha) \qquad \nu = \max(\mathbb{M})$$

folgt. Wegen $\nu \in \mathbb{M}$ gilt $m^\nu | n$. Mit geeignetem $l \in \mathbb{Z}$ können wir also $n = m^\nu l$ schreiben. Um den Fall $n > 0$ abzuschliessen, bleibt nun noch zu zeigen, dass $m \nmid l$. Nehmen wir das Gegenteil an! Dann gibt es eine Zahl $h \in \mathbb{Z}$ mit $l = mh$, und es folgt $m^{\nu+1}h = m^\nu mh = m^\nu l = n$, also $\nu + 1 \in \mathbb{M}$. Dies widerspricht (α). Also gilt $m \nmid l$ und der Fall $n > 0$ ist abgeschlossen.

Sei schliesslich $n < 0$. Dann ist $-n > 0$. Nach dem eben Gezeigten gibt es zwei Zahlen $\nu \in \mathbb{N}_0$ und $l' \in \mathbb{Z}$ mit $-n = m^\nu l'$ und $m \nmid l'$, wobei

$$\nu = \max\{\mu \in \mathbb{N}_0 \mid m^\mu | -n\} = \max\{\mu \in \mathbb{N}_0 \mid m^\mu | n\}.$$

Mit $l := -l'$ folgen $n = m^\nu l$ und $m \nmid l$. ■

Nun können wir die Teilervielfachheit definieren.

Definition und Bemerkungen 4.26. A) Sei $m \in \mathbb{N}\backslash\{1\}$ und sei $n \in \mathbb{Z}\backslash\{0\}$. Nach 4.25 gibt es dann eindeutig bestimmte Zahlen $\nu \in \mathbb{N}_0$ und $l \in \mathbb{Z}$ mit $n = m^\nu l$ und $m \nmid l$. Die Zahl ν nennt man dann die *(Teiler-)Vielfachheit von m in n* und bezeichnet diese mit $\nu_m(n)$.

B) Gemäss 4.25 können wir (für $m \in \mathbb{N}\backslash\{1\}$ und $n \in \mathbb{Z}\backslash\{0\}$) auch schreiben:

a) $$\nu_m(n) = \max\{\mu \in \mathbb{N}_0 \mid m^\mu | n\}.$$

Aus dieser Darstellung sieht man auch:

b) $$\nu_m(n) = 0 \Longleftrightarrow m \nmid n.$$

Das bedeutet, dass $\nu_m(n)$ ein Mass dafür ist, „wie stark m die Zahl n teilt“. Man nennt $\nu_m(n)$ deshalb auch die *Teilerordnung von n bezüglich m.* •

Wir wollen zwei Eigenschaften der Teilerordnung festhalten:

Satz 4.27. *Sei $m \in \mathbb{N}\backslash\{1\}$ und seien $u, v \in \mathbb{Z}\backslash\{0\}$. Dann gelten:*

a) $\nu_m(uv) \geq \nu_m(u) + \nu_m(v)$.

b) $u + v \neq 0 \Longrightarrow \nu_m(u + v) \geq \min\{\nu_m(u), \nu_m(v)\}$.

c) $\nu_m(u) \neq \nu_m(v) \Longrightarrow \nu_m(u + v) = \min\{\nu_m(u), \nu_m(v)\}$.

Beweis: „a)“ : Mit geeigneten Zahlen $h, l \in \mathbb{Z}$ gelten $u = m^{\nu_m(u)}h$ und $v = m^{\nu_m(v)}l$. Es folgt $uv = m^{\nu_m(u)+\nu_m(v)}hl$, also

$$m^{\nu_m(u)+\nu_m(v)} | uv.$$

Gemäss 4.26 B) a) führt dies zu $\nu_m(u) + \nu_m(v) \leq \nu_m(uv)$.

„b)“ : Sei $\nu_m(u) \leq \nu_m(v)$. Dann ist natürlich $\nu_m(u) = \min\{\nu_m(u), \nu_m(v)\}$, und in den obigen Bezeichnungen folgt

$$u + v = m^{\nu_m(u)}h + m^{\nu_m(\nu)}l = m^{\nu_m(u)}(h + m^{\nu_m(\nu)-\nu_m(u)}l),$$

d.h. $m^{\nu_m(u)} | (u + v)$. Mit 4.26 B) a) erhalten wir

$$\min\{\nu_m(u), \nu_m(v)\} = \nu_m(u) \leq \nu_m(u + v).$$

Genauso schliesst man im Fall $\nu_m(u) \geq \nu_m(v)$.

„c)“ : Sei $\nu_m(u) < \nu_m(v)$. Mit den soeben verwendeten Bezeichnungen können wir dann wieder schreiben:

$$u + v = m^{\nu_m(u)}(h + m^{\nu_m(\nu)-\nu_m(u)}l).$$

Dabei gilt $\nu_m(v) - \nu_m(u) > 0$, woraus folgt, dass $m | m^{\nu_m(v)-\nu_m(u)}l$. Wegen $m \nmid h$ folgt nun

$$m \nmid (h + m^{\nu_m(u)-\nu_m(v)}l).$$

Dies zeigt, dass $\nu_m(u + v) = \nu_m(u)$. Entsprechend schliesst man im Fall $\nu_m(u) > \nu_m(v)$. ■

Aufgaben 4.28. A) Erstellen Sie eine Tabelle mit den Werten $\nu_2(n), \nu_3(n), \nu_4(n)$ und $\nu_6(n)$ für $n = 1, 2, \ldots, 36$.

B) Geben Sie möglichst kleine natürliche Zahlen u, v, w an so, dass $\nu_6(uv) > \nu_6(u)+\nu_6(v)$ und $\nu_4(w^2) > 2\nu_4(w)$.

C) Seien $u, v \in \mathbb{Z}\backslash\{0\}$ mit $u + v \neq 0$. Zeigen Sie:

$$\nu_2(u + v) = \min\{\nu_2(u), \nu_2(v)\} \Longleftrightarrow \nu_2(u) \neq \nu_2(v).$$

D) Bestimmen Sie alle Paare $(u, v) \in \mathbb{N} \times \mathbb{N}$ mit der Eigenschaft, dass für jedes $m > 2$ gilt:

$$\nu_m(u) = \nu_m(v) = \nu_m(u + v).$$

E) Zeigen Sie, dass für $m > 2$ die Implikation „$\Leftarrow$“ in Aussage c) von 4.27 nicht gilt. •

Kapitel 5

Primzahlen

Überblick

Die *Primzahlen* sind ein besonders wichtiges und reizvolles Gebiet der Arithmetik. Schon in der Antike haben diese „Atome der Teilbarkeitslehre“ ein starkes Interesse gefunden. Was wir in der Schularithmetik über Primzahlen brauchen und wissen müssen, geht tatsächlich alles auf die vorchristliche Zeit zurück. Da wir hier nur an einzelnen Stellen über die elementare Arithmetik hinausgehen werden, gilt dasselbe auch für das Meiste, das in diesem Kapitel behandelt werden soll.

Im Einzelnen werden wir uns mit den folgenden Themen befassen:

- *Primzahlen und Primteiler,*
- *Teilerordnung bezüglich einer Primzahl,*
- *Bewertungen: ein Ausblick,*
- *Zerlegung in Primfaktoren,*
- *Teilerkriterium und Teilersumme,*
- *Existenz unendlich vieler Primzahlen,*
- *Wurzeln natürlicher Zahlen: ein Rückblick.*

Zentrales Thema dieses Kapitels ist die Zerlegung in Primfaktoren, die wir in strenger Weise herleiten werden. Als wichtigste Konsequenz werden wir ein Teilerkriterium und eine Formel für die Teilersumme einer natürlichen Zahl herleiten.

Primzahlen und Primteiler

Definition 5.1. Eine natürliche Zahl $p > 1$ heisst eine *Primzahl*, wenn sie nur durch 1 und durch sich selbst teilbar ist. Anders gesagt:

$$p \text{ ist eine Primzahl } :\Longleftrightarrow \mathbb{T}(p) = \{1, p\}; (p \in \mathbb{N}\backslash\{1\}).$$

Wir schreiben $\mathbb{P}$ für die Menge der Primzahlen:

$$\begin{aligned}\mathbb{P} :=& \{p \in \mathbb{N} | p \text{ ist Primzahl } \} \\ =& \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots\}.\end{aligned}$$

•

Satz 5.2. *Sei $p \in \mathbb{N}\backslash\{1\}$. Dann sind äquivalent:*

(i) $p \in \mathbb{P}$*;*

(ii) *für jede Zahl $m \in \mathbb{Z}$ folgt aus $p \nmid m$, dass p und m teilerfremd sind;*

(iii) *für je zwei Zahlen $m, n \in \mathbb{Z}$ folgt aus $p \nmid m$ und $p \nmid n$, dass $p \nmid mn$;*

(iv) *für je zwei Zahlen $m, n \in \mathbb{N}_{\leq p-1}$ gilt $p \nmid mn$.*

Beweis: „(i) $\Rightarrow$ (ii)“ : Sei $p \in \mathbb{P}$. Sei $m \in \mathbb{Z}$ mit $p \nmid m$. Sei $g := \mathrm{ggT}(p, m)$. Dann gelten $g|p$ und $g|m$. Wegen $p \in \mathbb{P}$ folgt aus $g|p$, dass $g = 1$ oder $g = p$. Wegen $p \nmid m$ ist $g \neq p$. Also ist $g = 1$.

„(ii) $\Rightarrow$ (iii)“ : Es gelte die Aussage (ii). Seien $m, n \in \mathbb{Z}$ mit $p \nmid m$ und $p \nmid n$. Gemäss Aussage (ii) folgen dann $\mathrm{ggT}(p, m) = 1$ und $\mathrm{ggT}(p, n) = 1$. Nach 4.12 gibt es also Zahlen $u, v, w, t \in \mathbb{Z}$ derart, dass $up + vm = 1$ und $wp + tn = 1$. Es folgt damit aber

$$\begin{aligned}1 = 1 \cdot 1 = (up + vm)(wp + tn) = upwp + uptn + \\ + vmwp + vmtn = (upw + utn + wmw)p + \\ + (vt)mn.\end{aligned}$$

Nach 4.12 heisst dies, dass $\mathrm{ggT}(p, mn) = 1$. Damit ist aber klar, dass $p \nmid mn$.

„(iii) $\Rightarrow$ (iv)“ : Klar, weil aus $m, n \in \mathbb{N}_{\leq p-1}$ folgt, dass $p \nmid m$ und $p \nmid n$ (s. 4.5 B) f)).

„(iv) $\Rightarrow$ (i)“ : Es gelte Aussage (iv). Sei $m \in \mathbb{N}$ mit $m|p$. Wir müssen zeigen, dass $m \in \{1, p\}$. Nehmen wir das Gegenteil an! Zunächst können wir $p = mn$ schreiben, wobei $n \in \mathbb{N}$. Es gilt dann sicher $m, n \in \mathbb{N}_{\leq p}$. Wegen $m \neq p$ gilt $m \in \mathbb{N}_{\leq p-1}$ und wegen $m \neq 1$ gilt $n \neq p$, also $n \in \mathbb{N}_{\leq p-1}$. Nach Aussage (iv) folgt $p \nmid mn = p$, ein Widerspruch!

■

Korollar 5.3. *Sei $p \in \mathbb{P}$, sei $r \in \mathbb{N}$ und seien $n_1, n_2, \ldots, n_r \in \mathbb{Z}$ so, dass $p \nmid n_i$ für $i = 1, \ldots, r$. Dann gilt $p \nmid n_1 n_1 \ldots n_r$. Also: Eine Primzahl teilt ein Produkt genau dann, wenn sie mindestens einen der Faktoren teilt.*

Beweis: (*Induktion bezüglich r*). Im Fall $r = 1$ ist nichts zu zeigen. Sei also $r > 1$. Nach Induktionsvoraussetzung gilt $p \nmid n_1 n_2 \cdots n_{r-1}$. Nach Voraussetzung gilt $p \nmid n_r$. Nach 5.2 folgt $p \nmid (n_1 n_2 \cdots n_{r-1}) n_r = n_1 n_2 \cdots n_r$. ■

Nun wollen wir uns den Primteilern oder Primfaktoren zuwenden, welche in der ganzen Teilbarkeitslehre eine fundamentale Bedeutung haben.

Definition und Bemerkung 5.4. A) Sei $n \in \mathbb{Z}$. Ein *Primfaktor* oder ein *Primteiler von n* ist eine Primzahl p mit $p|n$. Wir schreiben $\mathbb{P}(n)$ für die Menge der Primfaktoren von n, also:

$$\mathbb{P}(n) := \{p \in \mathbb{P} \mid p|n\}.$$

B) Mit den Bezeichnungen von 4.5 C) können wir auch schreiben:

a) $\mathbb{P}(n) = \mathbb{P} \cap \mathbb{T}(n)$.

Im Teilerverband $\mathbb{T}(n)$ von n besteht $\mathbb{P}(n)$ genau aus denjenigen Zahlen, die „unmittelbar über 1 liegen“ :

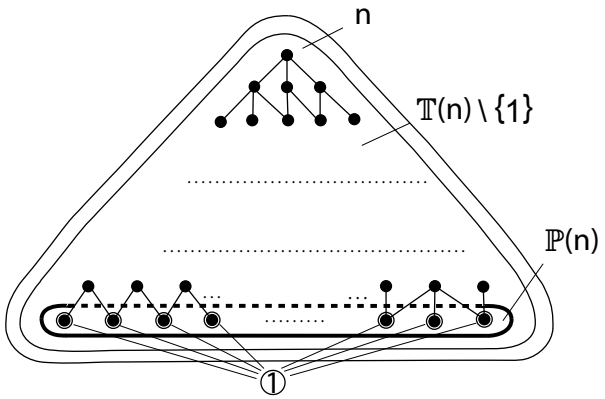


Abbildung 5.1: Primteiler im Teilerverband

•

Wir wollen nun einige grundlegende Eigenschafen der Primteilermengen $\mathbb{P}(n)$ festhalten. Wir beginnen mit einem Hilfsresultat.

Lemma 5.5. *Sei $n \in \mathbb{N}\backslash\{1\}$. Dann gilt*

$$\min\left(\mathbb{T}(n)\backslash\{1\}\right) \in \mathbb{P}(n).$$

Beweis: Wegen $1 \neq n \in \mathbb{T}(n)$ ist $\mathbb{T}(n)\backslash\{1\}$ eine nichtleere Menge natürlicher Zahlen. Also existiert $p := \min(\mathbb{T}(n)\backslash\{1\})$. Es bleibt zu zeigen, dass p eine Primzahl ist.

Nehmen wir das Gegenteil an! Dann gibt es ein $q \in \mathbb{T}(p)\backslash\{1, p\}$. Gemäss 4.5 D) d) folgt $q < p$. Gemäss 4.5 D) c) gilt auch $q \in \mathbb{T}(n)\backslash\{1\}$. Dies widerspricht der Minimalität von p in $\mathbb{T}(n)\backslash\{1\}$. ■

Satz 5.6. *Sei $n \in \mathbb{Z}$. Dann gelten:*

a) $\mathbb{P}(n) = \mathbb{P}(-n)$.

b) $\mathbb{P}(0) = \mathbb{P}$.

c) $n \in \{-1, 1\} \Longleftrightarrow \mathbb{P}(n) = \emptyset$.

d) $n \neq 0 \Longrightarrow \sharp\mathbb{P}(n) < \infty$.

e) $\forall m \in \mathbb{N} : m|n \Longrightarrow \mathbb{P}(m) \subseteq \mathbb{P}(n)$.

Beweis: „a)“ : Klar aus 5.4 B) a) und 4.5 D) b).

„b)“ : Klar aus 5.4 B) a) und 4.5 D) a).

„c)“ : „$\Rightarrow$“ : Klar (vgl. 5.4 B) a) und 4.5 D) a), b)).

„$\Leftarrow$“ : Sei $n \notin \{-1, 1\}$. Wir müssen zeigen, dass $\mathbb{P}(n) \neq \emptyset$. Ist $n = 0$, folgt dies mit Aussage b). Ist $n > 0$, so ist $n \in \mathbb{N}\backslash\{1\}$ und 5.5 liefert $\mathbb{P}(n) \neq \emptyset$. Ist $n < 0$, so kann man jetzt mit Aussage a) schliessen.

„d)“ : Klar nach 5.4 B) a) und 4.5 D) e).

„e)“ : Klar nach 5.4 B) a) und 4.5 D) c). ■

Aufgaben 5.7. A) Geben Sie einige Zahlen $n \in \mathbb{N}$ an so, dass $2^n - 1 \in \mathbb{P}$. Falls Sie mehr darüber zu sagen wissen, äussern Sie sich in Stichworten (bei Informationen aus dem Internet bitte „Link“ angeben).

B) Geben Sie einige Zahlen $p \in \mathbb{N}$ so an, dass $p, p + 2 \in \mathbb{P}$. (Für weitere Anregungen s. Teil A).)

C) Geben Sie Paare $(p, q) \in \mathbb{P}\times\mathbb{P}$ an, für welche $p^q - q^p = 1$ gilt. (Für weitere Anregungen s. Teil A).)

D) Geben Sie für einige Zahlen $n \in \mathbb{N}$ ein Paar $(p_n, q_n) \in \mathbb{P} \times \mathbb{P}$ so an, dass $p_n + q_n = 2n$. (Für weitere Anregungen s. Teil A).)

E) Geben Sie eine Primzahl $p > 10^{12}$ an. Machen Sie eine möglichst grosse Primzahl ausfindig. Geben Sie die Länge der Dezimaldarstellung dieser Zahl an, wenn für eine Ziffer 2 mm gebraucht werden. (Für weitere Anregungen s. Teil A).)

F) Formulieren Sie Fragen, welche zu den obigen Aufgaben A)–E) passen. (Den Hinweis in Teil A) beachten.)

G) Sei $p \in \mathbb{N}\backslash\{1\}$ und sei $n \nmid p$ für alle $n \in \mathbb{N}$ mit $2 \leq n \leq \sqrt{p}$. Zeigen Sie, dass $p \in \mathbb{P}$.

H) Bestimmen Sie $\mathbb{M}_n := \mathbb{N}_{\leq n^2}\backslash\{uv | u, v \in \mathbb{N}_{\leq n}\}$ und $\mathbb{P}_n := \mathbb{P} \cap \mathbb{N}_{\leq n^2}$ für $n = 10$ und $n = 20$.

I) Ergänzen Sie den nachfolgenden Baum zum kleinstmöglichen Netz eines Teilerverbandes. Geben Sie mindestens zwei Zahlen $n \in \mathbb{N}$ so an, dass das erhaltene Netz zum Teilerverband $\mathbb{T}(n)$ gehört.

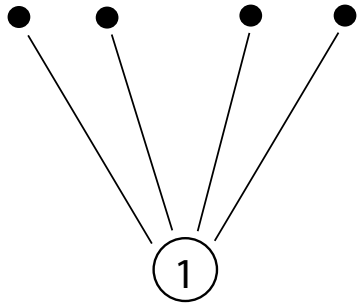


Abbildung 5.2: Atome im Teilerverband

J) Seien $h, p \in \mathbb{N}\backslash\{1\}$. Zeigen Sie, dass gilt:

$$h^p - 1 \in \mathbb{P} \Longrightarrow p \in \mathbb{P}.$$

(*Hinweis:* $p = rs$ schreiben und 3.3 B) mit $q = h^r$ anwenden.)

K) Aufgabe J) steht in Beziehung zu einer der Aufgaben A)–E). Zu welcher und in welcher Weise? •

Teilerordnung bezüglich einer Primzahl

In 4.26 haben wir den Begriff der Teilerordnung bezüglich einer Zahl $m \in \mathbb{N}\backslash\{1\}$ definiert. Wir befassen uns nun mit dem besonders interessanten Spezialfall in dem m eine Primzahl ist. Wir beginnen mit dem folgenden Primalitätskriterium, das stark an 5.2 erinnert.

Satz 5.8. *Sei $p \in \mathbb{N}\backslash\{1\}$. Dann sind äquivalent:*

(i) $p \in \mathbb{P}$;

(ii) *für je zwei Zahlen $m, n \in \mathbb{Z}\backslash\{0\}$ gilt*

$$\nu_p(mn) = \nu_p(m) + \nu_p(n);$$

(iii) *für je zwei Zahlen $m, n \in \mathbb{Z}\backslash\{0\}$ folgt aus $\nu_p(m) = \nu_p(n) = 0$, dass $\nu_p(mn) = 0$*

(iv) *für je zwei Zahlen $m, n \in \mathbb{N}_{\leq p-1}$ gilt $\nu_p(mn) = 0$.*

Beweis: Nach 4.26 B) b) ist die obige Aussage (iii) äquivalent zur Aussage 5.2 (iii). Genauso ist die Aussage (iv) äquivalent zur Aussage 5.2 (iv). Nach 5.2 bestehen also bereits die Äquivalenzen „(i) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (iv)“. Die Implikation „(ii) $\Rightarrow$(iii)“ liegt auf der Hand. Es bleibt also die Implikation „(i) $\Rightarrow$ (ii)“ zu beweisen.

Seien $m, n \in \mathbb{Z}\backslash\{0\}$ und sei $p \in \mathbb{P}$. Wir können $m = p^{\nu_p(m)}l$ und $n = p^{\nu_p(n)}h$ schreiben, wobei $h, l \in \mathbb{Z}$ mit $p \nmid h, l$. Es folgt

$$mn = p^{\nu_p(m)}lp^{\nu_p(n)}h = p^{\nu_p(m)+\nu_p(n)}lh.$$

Nach 5.2 (iii) gilt dabei aber $p \nmid lh$. Daraus folgt $\nu_p(mn) = \nu_p(m) + \nu_p(n)$. ■

Korollar 5.9. *Sei $p \in \mathbb{P}$ und seien $m, n \in \mathbb{Z}\backslash\{0\}$. Dann gelten:*

a) $\nu_p(mn) = \nu_p(m) + \nu_p(n)$.

b) $m + n \neq 0 \Longrightarrow \nu_p(m + n) \geq \min\{\nu_p(m), \nu_p(n)\}$.

c) $\nu_p(m) \neq \nu_p(n) \Longrightarrow \nu_p(m + n) = \min\{\nu_p(m), \nu_p(n)\}$.

Beweis: Klar nach 5.8 und 4.27. ■

Bewertungen: ein Ausblick

Wir wollen jetzt einen ersten Ausblick riskieren, der etwas über den Rahmen dieser Vorlesung hinausgeht.

Bemerkung und Beispiel 5.10. A) Eine Abbildung $\nu : \mathbb{Z}\backslash\{0\} \to \mathbb{N}_0; (n \mapsto \nu(n))$ nennt man eine *Bewertung*, wenn folgende Aussagen gelten:

a) $\exists p \in \mathbb{Z}\backslash\{0\} : \nu(p) = 1$;

b) $\forall m, n \in \mathbb{Z}\backslash\{0\} : \nu(mn) = \nu(m) + (n)$;

c) $\forall m, n \in \mathbb{Z}\backslash\{0\} : m + n \neq 0 \Longrightarrow \nu(m+n) \geq \min\{\nu(m), \nu(n)\}$.

Nun können wir eine Primzahl $p \in \mathbb{P}$ wählen und die Abbildung

d) $\nu_p : \mathbb{Z}\backslash\{0\} \to \mathbb{N}_0; (n \mapsto \nu_p(n))$

betrachten, welche jeder ganzen Zahl $n \neq 0$ die Teilerordnung $\nu_p(n)$ von n bezüglich p zuordnet. Dann gilt $\nu_p(p) = 1$, d.h. das obige Axiom a) ist erfüllt. Gemäss 5.9 a), b) sind aber auch die Axiome b) und c) erfüllt. Damit können wir sagen:

e) Die Abbildung $\nu_p : \mathbb{Z}\backslash\{0\} \to \mathbb{N}_0$ (s. (d)) ist eine Bewertung.

Man nennt diese Abbildung die *zur Primzahl p gehörige Bewertung.*

B) Bewertungen treten in der Mathematik sehr oft auf, wobei man dann meist $\mathbb{Z}$ durch andere Rechenbereiche ersetzt.

Dazu ein Beispiel: Wir schreiben $\mathbb{R}[x]$ für die Menge aller Polynome $f(x) = a_0 + a_1 x + \cdots + a_d x^d$ mit Koeffizienten $a_0, \ldots, a_d \in \mathbb{R}, (d \in \mathbb{N}_0)$:

$$\mathbb{R}[x] := \{a_0 + a_1 x + \cdots + a_d x^d | d \in \mathbb{N}_0; a_0, \ldots, a_d \in \mathbb{R}\}.$$

Es gelten also etwa:

$$0 \in \mathbb{R}[x], 4 \in \mathbb{R}[x], 2 + 3x \in \mathbb{R}[x], 12 - 3x + x^2 \in \mathbb{R}[x], 7 - x^2 + 2x^3 \in \mathbb{R}[x], \ldots$$

Polynome kann man zueinander addieren und miteinander multiplizieren, und in diesem Sinne wird $\mathbb{R}[x]$ zu einem Rechenbereich.

Nun wählen wir eine Zahl $p \in \mathbb{R}$. Ist $f = f(x) \in \mathbb{R}[x]\backslash\{0\}$, so schreiben wir $\mu_p(f)$ für die *Vielfachheit von p als Nullstelle von f*. Es gilt also

a) $f(x) = (x-p)^{\mu_p(f)} g(x)$, *wobei* $g(x) \in \mathbb{R}[x]$ *mit* $g(p) \neq 0$.

Man nennt $\mu_p(f)$ auch die *Verschwindungsordnung* oder *Nullstellenordnung von f in p.* Natürlich kann man $\mu_p(f)$ auch mit Hilfe von Ableitungen charakterisieren, denn es gilt:

b) $f^{(0)}(p) = f^{(1)}(p) = \cdots = f^{(\mu_p(f)-1)}(p) = 0$, *aber* $f^{(\mu_p(f))}(p) \neq 0$,

wobei $f^{(i)}(x) \in \mathbb{R}[x]$ für die i-te Ableitung von $f(x)$ steht.

Am Graphen von f lässt sich die Situation wie folgt veranschaulichen:

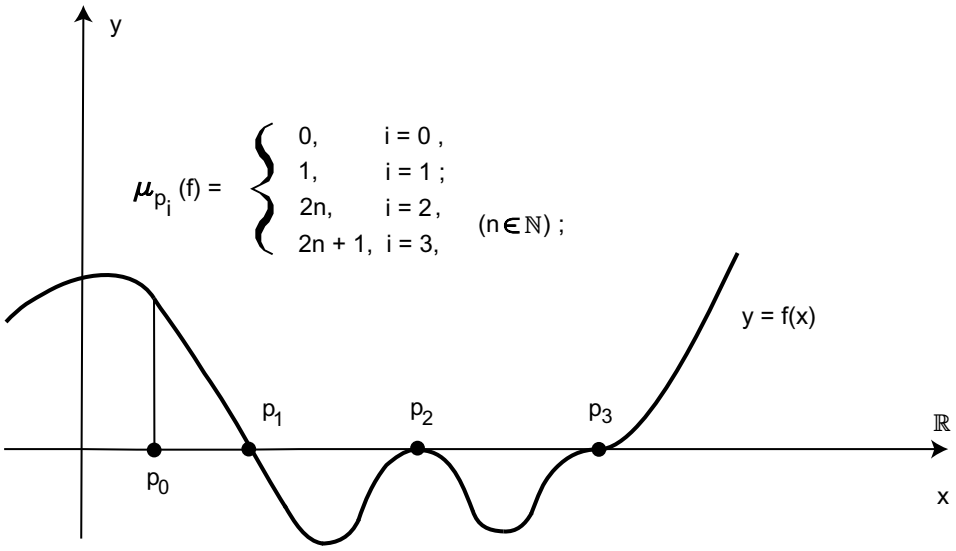


Abbildung 5.3: Nullstellenordnungen eines Polynoms

Es gelten nun für $f, g \in \mathbb{R}[x]\backslash\{0\}$ die folgenden Aussagen:

c) $\mu_p(x-p) = 1$.

d) $\mu_p(fg) = \mu_p(f) + \mu_p(g)$.

e) $f + g \neq 0 \Longrightarrow \mu_p(f+g) \geq \min\{\mu_p(f), \mu_p(g)\}$.

Im Sinne von Teil A) können wir also sagen:

f) *Die Abbildung* $\mu_p : \mathbb{R}[x]\backslash\{0\} \to \mathbb{N}_0$*, welche einem Polynom* $f \in \mathbb{R}[x]\backslash\{0\}$ *die Nullstellenordnung* $\mu_p(f)$ *zuordnet, ist eine Bewertung.*

Es stellt sich hier die Frage, ob hinter der formalen Analogie zwischen den beiden Bewertungen

$$\nu_p : \mathbb{Z}\backslash\{0\} \to \mathbb{N}_0;\ (n \mapsto \nu_p(n));\ (p \in \mathbb{P})$$
$$\mu_p : \mathbb{R}[x]\backslash\{0\} \to \mathbb{N}_0;\ (f \mapsto \mu_p(f));\ (p \in \mathbb{R})$$

vielleicht eine echte Verwandtschaft steckt. Auf diese Frage werden wir nochmals zurückkommen (s. (7.34)). •

Aufgaben 5.11. A) Bestimmen Sie $\nu_p(n)$ für alle $p \in \mathbb{P}$ und für $n = 120, 1024, 9999$.

B) Sei $\nu : \mathbb{Z}\backslash\{0\} \to \mathbb{N}_0$ eine Bewertung (s. 5.10 A)).

a) Zeigen Sie, dass $\nu(1) = 0$.

b) Seien $m, n \in \mathbb{Z}\backslash\{0\}$ und $m', n' \in \mathbb{Z}\backslash\{0\}$ mit $\frac{m}{n} = \frac{m'}{n'}$. Zeigen Sie, dass $\nu(m) - \nu(n) = \nu(m') - \nu(n')$.

c) Begründen Sie mit a) und b), dass man definieren darf:

$$\tilde{\nu}\left(\frac{m}{n}\right) := \nu(m) - \nu(n) \in \mathbb{Z}; (m, n \in \mathbb{Z}\backslash\{0\}).$$

C) Es gelten die Voraussetzungen und Bezeichnungen von Aufgabe B).

a) Zeigen Sie, dass folgende Aussagen gelten:

(α) $n \in \mathbb{Z}\backslash\{0\} \Longrightarrow \tilde{\nu}(n) = \nu(n)$.

(β) $q, r \in \mathbb{Q}\backslash\{0\} \Longrightarrow \tilde{\nu}(qr) = \tilde{\nu}(q) + \tilde{\nu}(r)$.

b) Zeigen Sie, dass $\tilde{\nu} : \mathbb{Q}\backslash\{0\} \to \mathbb{Z},\ (q \mapsto \tilde{\nu}(q))$ die einzige Abbildung ist, für welche (α) und (β) gelten.

c) Zeigen Sie: Sind $q, r \in \mathbb{Q}\backslash\{0\}$ mit $q + r \neq 0$, so gilt $\tilde{\nu}(q + r) \geq \min\{\tilde{\nu}(q), \tilde{\nu}(r)\}$.

D) Berechnen Sie $\mu_p(x^3 - 2x^2)$ für alle $p \in \mathbb{R}$.

E) Zeigen Sie, dass aus der Darstellung $f(x) = (x - p)^{\mu_p(f)} g(x)$ mit $g(p) \neq 0$ in 5.10 B) a) die Aussage 5.10 B) b) folgt. (*Hinweis:* Induktion bezüglich $\mu := \mu_p(f)$).

F) Beweisen Sie die Aussagen c), d) und e) aus 5.10 B). •

Zerlegung in Primfaktoren

Nun wollen wir uns dem wichtigsten Resultat dieses Kapitels zuwenden, dem Satz von der eindeutigen Zerlegung in Primfaktoren. Dieser Satz besagt zwei Dinge, nämlich:

- *Jede natürliche Zahl $n > 1$ „lässt sich aus Atomen aufbauen“, d.h. als Produkt von Primzahlen schreiben.*
- *Der „atomare Aufbau“ einer natürlichen Zahl $n > 1$ ist eindeutig, d.h. die Darstellung von n als Produkt von Primzahlen ist (bis auf die Reihenfolge dieser Primzahlen) eindeutig.*

Ist man noch bereit, die Multiplikation mit „dem Atom“ -1 zuzulassen, so gelten die obigen Aussagen sinngemäss für alle Zahlen $n \in \mathbb{Z}\backslash\{0, 1, -1\}$. Aus Erfahrung (und als Folge von „Indoktrination“ im Arithmetikunterricht) ist uns die eindeutige Zerlegung

in Primfaktoren so selbstverständlich geworden, dass wir zur Ansicht neigen, dass diese Tatsache keines Beweises bedarf. Etwas zurückhaltender wird man in diesem Punkt, wenn man erfährt, dass bereits im 19. Jahrhundert Zahlbereiche entdeckt wurden, in welchen die eindeutige Zerlegung in Primfaktoren nicht richtig ist.

Auch die präzise Formulierung des angestrebten Satzes ist bereits eine Herausforderung, besonders wenn der Satz alle wesentlichen Informationen enthalten soll.

Satz 5.12. *(Satz von der eindeutigen Zerlegung in Primfaktoren) Sei $n \in \mathbb{N}\backslash\{1\}$. Dann gibt es eine eindeutig bestimmte Zahl $r \in \mathbb{N}$, eindeutig bestimmte Primzahlen $p_1, p_2, \ldots, p_r$ und eindeutig bestimmte natürliche Zahlen $\alpha_1, \ldots, \alpha_r$ so, dass*

$$p_1 < p_2 < \cdots < p_r \text{ und } n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Dabei gelten:

a) $\mathbb{P}(n) = \{p_1, \cdots, p_r\}$;

b) $\alpha_i = \nu_{p_i}(n)$ *für* $i = 1, \ldots, r$.

Beweis: Zuerst zeigen wir, dass n überhaupt eine Produktdarstellung der angegebenen Art hat, d.h. dass es ein $r \in \mathbb{N}$, Zahlen $p_1, \ldots, p_r \in \mathbb{P}$ und Zahlen $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$ so gibt, dass $p_1 < \cdots < p_r$ und $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

Nehmen wir das Gegenteil an. Dann besitzt n keine Produktdarstellung der obigen Art. Nach dem Prinzip der kleinsten Zahl können wir dann annehmen, n sei minimal in $\mathbb{N}\backslash\{1\}$ mit der Eigenschaft, keine solche Produktdarstellung zu haben. Nach 5.6 c) und d) gibt es dann eine grösste Zahl $p \in \mathbb{P}(n)$. Wir können nun $n = p^{\nu_p(n)} m$ mit $p \nmid m$ und $m \in \mathbb{N}_{\leq n}$ schreiben. Wegen $p \in \mathbb{P}(n)$ gilt $\nu_p(n) > 0$ (s. 4.26 B) b)), also $m \neq n$, d.h. $m < n$. Es gilt aber auch $m \neq 1$, denn sonst hätte n ja die Produktdarstellung $n = p^{\nu_p(n)}$. Also gelten $m \in \mathbb{N}\backslash\{1\}$ und $m < n$. Wegen der Minimalität von n gibt es also eine Produktdarstellung $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ mit $s \in \mathbb{N}$, $p_1, \ldots, p_s \in \mathbb{P}$, $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$ und $p_1 < \cdots < p_s$. Wegen $m|n$ folgt $p_s \in \mathbb{P}(n)$. Wegen $p_s|m$ und $p \nmid m$ gilt $p_s \neq p$. Weil p so gewählt wurde, dass $p = \max(\mathbb{P}(n))$, folgt $p_s < p$. Setzen wir $r := s+1, p_r := p$ und $\alpha_r := \nu_p(n)$, so folgen $p_1 < \cdots < p_{r-1} < p_r$ und $n = p_r^{\alpha_r} m = m p_r^{\alpha_r} = p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}} p_r^{\alpha_r}$. Also hat n doch eine Produktdarstellung der gesuchten Art; ein Widerspruch. Damit ist die Existenz unserer Produktdarstellung gezeigt.

Wir gehen nun aus von einer Produktdarstellung, wie sie nach dem eben Gezeigten existiert:

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r},\ (r \in \mathbb{N}; p_1, \ldots, p_r \in \mathbb{P};\ \alpha_1, \ldots, \alpha_r \in \mathbb{N};\ p_1 < \cdots < p_r).$$

Als erstes beweisen wir

(α) $\{p_1, \cdots, p_r\} = \mathbb{P}(n)$.

Die Inklusion „$\subseteq$“ ist klar. Gilt umgekehrt $p \in \mathbb{P}(n)$, so folgt $p | p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Nach 5.3 gibt es dann ein $i \in \{1, \cdots, r\}$ mit $p | p_i$. Wegen $p_i \in \mathbb{P}$ und $p \neq 1$ folgt $p = p_i$. Dies beweist die Inklusion „$\supseteq$“. Schliesslich zeigen wir

(β) $\alpha_i = \nu_{p_i}(n)$ für $i = 1, \ldots, r$.

Wir halten dazu i fest und schreiben $l := p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_r^{\alpha_r}$. Dann gilt $n = p_i^{\alpha_i} l$. Weil $p_i \nmid p_j$ für alle $j \neq i$, folgt aus 5.3 aber auch $p_i \nmid l$. Damit gilt aber $\alpha_i = \nu_{p_i}(n)$, und (β) ist bewiesen. Aus (α) und (β) folgt die Eindeutigkeit unserer Produktdarstellung. ■

Definition und Bemerkungen 5.13. A) Sei $n \in \mathbb{N}\backslash\{1\}$. Die (nach 5.12 eindeutig bestimmte) Darstellung

a) $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$; $(r, \alpha_1, \ldots, \alpha_r \in \mathbb{N};\ p_1, \ldots, p_r \in \mathbb{P}$ mit $p_1 < \cdots < p_r)$

heisst die *Zerlegung von n in Primfaktoren*. Entsprechend der Tatsache, dass $\nu_{p_i}(n) = \alpha_i$ für $i = 1, \ldots, r$ ist α_i die *Vielfachheit des Primfaktors p_i in n*.

B) Praktisch ist es auch, die obige Produktdarstellung a) in der Form

a) $n = \prod_{i=1}^{r} p_i^{\alpha_i}$.

zu schreiben. Die rechte Seite dieser Gleichung besagt, dass das Produkt aller Zahlen $p_i^{\alpha_i}$ gebildet wird, wobei i die Zahlen $1, 2, \ldots, r$ durchläuft.

C) Sei $\mu : \mathbb{P} \to \mathbb{N}_0$ eine Abbildung, welche jeder Primzahl p eine Zahl $\mu_p \in \mathbb{N}_0$ zuordnet derart, dass die Menge $\{p \in \mathbb{P} | \mu_p \neq 0\}$ endlich ist. Dann schreiben wir $\prod_{p \in \mathbb{P}} p^{\mu_p}$ für das Produkt aller Zahlen p^{μ_p}, wobei wir uns an den unendlich vielen Faktoren $p^0 = 1$ nicht stören, die auftreten, wenn $\mu_p = 0$.

Ist der Wert n dieses Produktes verschieden von 1, so ist $n = \prod_{p \in \mathbb{P}} p^{\mu_p}$ gerade die Zerlegung in Primfaktoren von n. Die Zerlegung in Primfaktoren von n (s. A) a), B) a)) kann nun auch geschrieben werden in der folgenden Form:

a) $n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$. •

Aufgaben 5.14. A) Zerlegen Sie in Primfaktoren: $1024, 8!, \binom{17}{4}, 99, 999, 9999, 99999$.

B) Seien $p \in \mathbb{P}$ und $k \in \{1, \cdots, p-1\}$. Zeigen Sie, dass $\max\left(\mathbb{P}\left(\binom{p}{k}\right)\right) = p$.

C) Zerlegen Sie $2^{15} - 1$ in Primfaktoren (ohne Rechner!). (*Hinweis:* vgl. 5.7 J).)

D) Bestimmen Sie die fünf kleinsten natürlichen Zahlen, welche durch alle Primzahlen $p \leq 11$ teilbar sind.

E) Seien $m, n \in \mathbb{N}\backslash\{1\}$. Zeigen Sie, dass $\mathbb{P}(mn) = \mathbb{P}(m) \cup \mathbb{P}(n)$ und dass $mn = \Pi_{p \in \mathbb{P}}\, p^{\nu_p(n) + \nu_p(m)}$. •

Teilerkriterium und Teilersumme

Mit Hilfe der Primfaktorzerlegung lassen sich die Teilerverbände natürlicher Zahlen beschreiben:

Satz 5.15. *(Teilerkriterium) Sei* $n \in \mathbb{N}\backslash\{1\}$ *mit der Primfaktorzerlegung*

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, (r, \alpha_1, \ldots, \alpha_r \in \mathbb{N}; p_1, \ldots, p_r \in \mathbb{P}; p_1 < p_2 < \ldots < p_r).$$

Dann gelten:

a) Die Teiler von n sind genau die Zahlen $p_1^{\beta_1} \cdots p_r^{\beta_r}$ *mit* $0 \leq \beta_i \leq \alpha_i$, *d.h.*

$$\mathbb{T}(n) = \{p_1^{\beta_1} \cdots p_r^{\beta_r} | 0 \leq \beta_i \leq \alpha_i;\ i = 1, \ldots, r\}.$$

b) Die Anzahl der Teiler von n beträgt $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$, *d.h.*

$$d(n) := \sharp\mathbb{T}(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1).$$

Beweis: „a)“ : „$\subseteq$“ : Sei $m \in \mathbb{T}(n)$. Nach 5.6 e) gilt dann $\mathbb{P}(m) \subseteq \mathbb{P}(n) = \{p_1, \cdots, p_r\}$. Mit geeigneten Zahlen $\beta_i \in \mathbb{N}_0$ gilt deshalb $m = p_1^{\beta_1} \cdots p_r^{\beta_r}$. Für jeden Index $i \in \{1, \cdots, r\}$ folgt $p_i^{\beta_i} | m$, d.h. $p_i^{\beta_i} | n$, also $\beta_i \leq \nu_{p_i}(n) = \alpha_i$, (s. 4.25, 5.12 b)), und wir erhalten $0 \leq \beta_i \leq \alpha_i$ für $i = 1, \ldots, r$.

„$\supseteq$“ : Seien $\beta_1, \cdots, \beta_r \in \mathbb{N}_0$ mit $\beta_i \leq \alpha_i$. Dann gilt

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = (p_1^{\alpha_1 - \beta_1} \cdots p_r^{\alpha_r - \beta_r}) p_1^{\beta_1} \cdots p_r^{\beta_r},$$

also $p_1^{\beta_1} \cdots p_r^{\beta_r} \in \mathbb{T}(n)$.

„b)“ : Sei

$$\mathbb{B} := \{(\beta_1, \ldots, \beta_r) | \beta_i \in \mathbb{N}_0, \beta_i \leq \alpha_i;\ i = 1, \cdots, r\}.$$

Sind $(\beta_1, \ldots, \beta_r), (\beta'_1, \ldots, \beta'_r) \in \mathbb{B}$ voneinander verschieden, d.h. gilt $\beta_i \neq \beta'_i$ für mindestens einen Index $i \in \{1, \cdots, r\}$, so folgt aus der Eindeutigkeit der Primfaktorzerlegung, dass

$$p_1^{\beta_1} \cdots p_r^{\beta_r} \neq p_1^{\beta'_1} \cdots p_r^{\beta'_r}.$$

Es besteht also die bijektive Abbildung

$$\mathbb{B} \to \mathbb{T}(n);\ (\beta_1, \ldots, \beta_r) \mapsto p_1^{\beta_1} \cdots p_r^{\beta_r}.$$

Es genügt somit zu zeigen, dass $\sharp\mathbb{B} = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$. Diese kombinatorische Aufgabe sei dem Leser überlassen. ■

Dieses soeben bewiesene Ergebnis ist wichtig genug, um es auch noch in anderen Formulierungen festzuhalten, wie wir dies nun tun wollen.

Bemerkungen 5.16. A) Seien $\mu : \mathbb{P} \to \mathbb{N}_0$ $(p \mapsto \mu_p)$ und $\nu : \mathbb{P} \to \mathbb{N}_0$ $(p \mapsto \nu_p)$ zwei Abbildungen so, dass die Mengen $\{p \in \mathbb{P} | \mu_p \neq 0\}$ und $\{p \in \mathbb{P} | \nu_p \neq 0\}$ beide endlich sind. Dann kann man 5.15 a) auch in der Form

a) $\quad \prod_{p\in\mathbb{P}} p^{\mu_p} | \prod_{p\in\mathbb{P}} p^{\nu_p} \Longleftrightarrow \forall p \in \mathbb{P} : \mu_p \leq \nu_p$

schreiben. Um diese Äquivalenz einzusehen, schreiben wir $n = \prod_{p\in\mathbb{P}} p^{\nu_p}$ und $m = \prod_{p\in\mathbb{P}} p^{\mu_p}$. Ist $n = 1$, so gilt $m|n$ genau dann, wenn $m = 1$, also genau dann, wenn $\nu_p = 0 = \mu_p$ für alle $p \in \mathbb{P}$. Gilt $n > 1$, so ist $n = \prod_{p\in\mathbb{P}} p^{\nu_p}$ die Primfaktorzerlegung von n (s. 5.13 C)) und die Äquivalenz a) folgt direkt aus 5.15 a).

B) Beachten wir, dass die Darstellung a) aus 5.13 C) auch dann gilt, wenn $n = 1$, so können wir die obige Aussage A) a) (und damit 5.15 a)) auch in der folgenden Form schreiben:

a) $\quad m|n \Longleftrightarrow \forall p \in \mathbb{P} : \nu_p(m) \leq \nu_p(n);\ (m, n \in \mathbb{N}).$ •

Bemerkung 5.17. Sei $n \in \mathbb{N}$. Eine wichtige Grösse ist die sogenannte *Teilersumme von* n, die wir mit $\sigma(n)$ bezeichnen wollen. Wir können also schreiben

$$\sigma(n) := \sum_{m\in\mathbb{T}(n)} m = \sum_{m|n} m,$$

wobei Σ das sogenannte *Summenzeichen* ist. Dieses Zeichen besagt, das die Summe über alle m zu bilden ist, welche der Bedingung unter dem Summenzeichen genügen (in unserem Fall also der Bedingung $m \in \mathbb{T}(n)$ oder – gleichbedeutend – der Bedingung $m|n$). •

Aus dem Teilerkriterium 5.15 ergibt sich nun die folgende Aussage über die Teilersumme.

Satz 5.18. *(Teilersummensatz) Sei* $n \in \mathbb{N}\backslash\{1\}$ *mit der Primfaktorzerlegung*

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad (r, \alpha_1, \ldots, \alpha_r \in \mathbb{N};\ p_1, \ldots, p_r \in \mathbb{P}; p_1 < \cdots < p_r).$$

Dann gilt

$$\sigma(n) = \sum_{m\in\mathbb{T}(n)} m = \frac{(p_1^{\alpha_1+1} - 1)(p_2^{\alpha_2+1} - 1) \cdots (p_r^{\alpha_r+1} - 1)}{(p_1 - 1)(p_2 - 1) \cdots (p_r - 1)}.$$

Beweis: (*Induktion bezüglich* r) Im Fall $r = 1$ gilt gemäss 5.15 a)

$$\mathbb{T}(n) = \mathbb{T}(p_1^{\alpha_1}) = \{1, p_1, p_1^2, \cdots, p_1^{\alpha_1}\}.$$

Unter Beachtung von 3.3 B) erhalten wir also

$$\sigma(n) = 1 + p_1 + p_1^2 + \cdots p_1^{\alpha_1} = \frac{1 - p_1^{\alpha_1+1}}{1 - p_1} = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}.$$

Sei also $r > 1$. Wir setzen $t := p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}}$. Gemäss Induktionsvoraussetzung gilt dann

$$(\alpha) \quad \sigma(t) = \frac{(p_1^{\alpha_1+1}-1)(p_2^{\alpha_2+1}-1)\cdots(p_{r-1}^{\alpha_{r-1}+1}-1)}{(p_1-1)(p_2-1)\cdots(p_{r-1}-1)}.$$

Nach 5.15 a) besteht $\mathbb{T}(n)$ aber genau aus den Zahlen mp_r^β mit $m \in \mathbb{T}(t)$ und $0 \leq \beta \leq \alpha_r$. Dabei sind diese Zahlen alle voneinander verschieden, d.h. aus $m'p_r^{\beta'} = mp_r^\beta$ mit $m', m \in \mathbb{T}(t)$ und $0 \leq \beta', \beta \leq \alpha$ folgen $m' = m$ und $\beta' = \beta$. Man kann deshalb $\sigma(n)$ berechnen, indem man erst alle Zahlen der Form mp_1^0 mit $m \in \mathbb{T}(t)$ addiert, dann alle Zahlen der Form mp_1^1 mit $m \in \mathbb{T}(t)$ etc. und dann die so erhaltenen Teilsummen zusammenzählt. So erhält man

$$\sigma(n) = \Big(\sum_{m\in\mathbb{T}(t)} m\Big)p_r^0 + \Big(\sum_{m\in\mathbb{T}(t)} m\Big)p_r^1 + \cdots + \Big(\sum_{m\in\mathbb{T}(t)} m\Big)p_r^{\alpha_r}.$$

Mit 3.3 B) folgt nun

$$\sigma(n) = \Big(\sum_{m\in\mathbb{T}(t)} m\Big)(1 + p_r + p_r^2 + \cdots + p_r^{\alpha_1}) =$$
$$= \sigma(t)\frac{1 - p_r^{\alpha_r+1}}{1 - p_r} = \sigma(t)\frac{p_r^{\alpha_r+1} - 1}{p_r - 1}.$$

Zusammen mit (α) liefert dies die Behauptung. ■

Aufgaben 5.19. A) Bestimmen Sie $d(n) := \sharp\mathbb{T}(n)$ und $\sigma(n) = \Sigma_{m\in\mathbb{T}(n)}m$ für alle $n \in \mathbb{N}_{\leq 36}$.

B) Für welche $n \in \mathbb{N}_{\leq 1000}$ gilt $\sharp\mathbb{T}(n) = 15$?

C) Sei $n \in \mathbb{N}$ mit $\sharp\mathbb{T}(n) \in \mathbb{P}$. Was lässt sich über n sagen?

D) Welche Form hat $n \in \mathbb{N}$, wenn $\sharp\mathbb{T}(n)$ das Quadrat einer Primzahl ist?

E) Eine Zahl $n \in \mathbb{N}\backslash\{1\}$ heisst *quadratfrei*, wenn $\nu_p(n) \in \{0, 1\}$ für alle $p \in \mathbb{N}$, d.h. wenn jeder Primfaktor von n nur die Vielfachheit eins hat. Zeigen Sie folgendes:

a) $\sharp\mathbb{T}(n) \geq 2^{\sharp\mathbb{P}(n)}$.

b) $\sharp\mathbb{T}(n) = 2^{\sharp\mathbb{P}(n)} \Longleftrightarrow n$ ist quadratfrei.

F) Seien $m, n \in \mathbb{N}$. Zeigen Sie:

a) $\mathrm{ggT}(m,n) = \Pi_{p\in\mathbb{P}}\, p^{\min\{\nu_p(m),\nu_p(n)\}}$.

b) $\mathbb{P}\left(\mathrm{ggT}(m,n)\right) = \mathbb{P}(m) \cap \mathbb{P}(n)$.

c) m, n sind teilerfremd $\Longleftrightarrow \mathbb{P}(m) \cap \mathbb{P}(n) = \emptyset$.

G) Seien $m, n \in \mathbb{N}$. Zeigen Sie:

a) $\mathrm{kgV}(m,n) = \Pi_{p\in\mathbb{P}}\, p^{\max\{\nu_p(m),\nu_p(n)\}}$.

b) $\mathbb{P}\left(\mathrm{kgV}(m,n)\right) = \mathbb{P}(m) \cup \mathbb{P}(n)$.

H) Sei $n \in \mathbb{N}$. Wir setzen $\mathring{\mathbb{T}}(n) := \{m \in \mathbb{T}(n) | \mathrm{ggT}(m, \frac{n}{m}) = 1\}$ und $\mathring{d}(n) := \sharp\mathring{\mathbb{T}}(n)$. Zeigen Sie:

a) $n \in \mathbb{N} \setminus \{1\} \Longrightarrow \mathring{d}(n) = 2^{\sharp\mathbb{P}(n)}$.

b) $(m, n \in \mathbb{N} \setminus \{1\} \wedge \mathrm{ggT}(m,n) = 1) \Longrightarrow \mathring{d}(mn) = \mathring{d}(m)\mathring{d}(n)$.

I) Zeigen Sie, dass für teilerfremde $m, n \in \mathbb{N}$ die Gleichungen $d(mn) = d(m)d(n)$ und $\sigma(mn) = \sigma(m)\sigma(n)$ gelten.

J) Berechnen Sie $\sigma(p^\alpha)$ für alle $p \in \mathbb{P}$ und alle $\alpha \in \mathbb{N}$, für welche $p^\alpha < 1000$. Berechnen sie damit $\sigma(n)$ für alle $n \leq 1000$. •

Existenz unendlich vieler Primzahlen

Wir haben uns bis jetzt nie die Frage gestellt, wie viele Primzahlen es gibt. Dieser Frage wollen wir uns jetzt zuwenden. Wir beginnen mit dem folgenden Hilfsresultat, das es erlaubt, zu endlich vielen gegebenen Primzahlen noch neue zu finden:

Lemma 5.20. *Seien $m, n \in \mathbb{Z}$ teilerfremd. Dann gilt*

$$\mathbb{P}(n+m) \cup \mathbb{P}(n-m) \subseteq \mathbb{P} \setminus \left(\mathbb{P}(m) \cup \mathbb{P}(n)\right).$$

Beweis: Es gilt zu zeigen, dass $p \notin \mathbb{P}(m) \cup \mathbb{P}(n)$ für $p \in \mathbb{P}(n+m) \cup \mathbb{P}(n-m)$. Nehmen wir das Gegenteil an! Dann gibt es eine Primzahl p, die sowohl eine der beiden Zahlen $n+m$ und $n-m$ als auch eine der beiden Zahlen m und n teilt. Dann teilt p aber beide der Zahlen m und n. Dies widerspricht der Teilerfremdheit von m und n. ■

Aufgaben 5.21. A) Seien $m, n \in \mathbb{N}$ teilerfremd und so, dass $n - m > 1$ und $\mathbb{P}(m) \cup \mathbb{P}(n) = \{2, 3, 5, 7\}$. Zeigen Sie, dass $n - m \geq 11$. Kann man m und auch so wählen, dass $n - m = 11$?

B) Lösen Sie Aufgabe A) für $\mathbb{P}(m) \cup \mathbb{P}(n) = \{2, 3, 5, 7, 11\}$ und mit $n - m \geq 13$ (statt $n - m \geq 11$). •

Nun beweisen wir

Satz 5.22. *(Euklid)* $\sharp\mathbb{P} = \infty$.

Beweis: Nehmen wir an, es sei $\sharp\mathbb{P} < \infty$. Dann gibt es ein $r \in \mathbb{N}$ so, dass $\mathbb{P} = \{p_1, p_2, \cdots, p_r\}$. Nach 5.18 ist dann $\mathbb{P}(p_1 p_2 \cdots p_r + 1) \subseteq \mathbb{P} \setminus (\mathbb{P}(p_1 p_2 \cdots p_r) \cup \mathbb{P}(1)) = \mathbb{P} \setminus \{p_1, \cdots, p_r\} = \emptyset$. Dies widerspricht 5.6 c). ■

Aufgaben 5.23. A) Sei $\Pi(n) := \sharp(\mathbb{P} \cap \mathbb{N}_{\leq n})$ für $n \in \mathbb{N}$. Bestimmen Sie den Wert

$$\frac{\Pi(n)}{n} \ln(n) \text{ für } 2 \leq n \leq 100 \text{ und für } n = 5000.$$

B) Seien $a, b \in \mathbb{N}$ teilerfremd. Wir definieren die Folge $(a_n)_{n \in \mathbb{N}}$ durch $a_1 = a, a_2 = a_1 + b$, $a_3 = a_1 a_2 + b, a_4 = a_1 a_2 a_3 + b, \ldots, a_n = a_1 a_2 \cdots a_{n-1} + b, \ldots$. Zeigen Sie:

a) $\forall n \in \mathbb{N} : \mathrm{ggT}(a_n, b) = 1$.

b) $\forall n, m : (n \neq m \Longrightarrow \mathrm{ggT}(a_n, a_m) = 1)$.

c) Die Vereinigungsmenge $\bigcup_{n \in \mathbb{N}} \mathbb{P}(a_n)$ ist unendlich.

C) Wählen Sie in Aufgabe B) $a = 1$ und $b = 2$. Berechnen Sie a_n für $n = 1, 2, 3, 4$. Stellen Sie eine Vermutung über die Gestalt von a_n auf und beweisen Sie diese durch Induktion.

D) Suchen Sie auf dem Internet Informationen über die Funktion $n \mapsto \frac{\Pi(n)}{n} \ln(n)$ aus Aufgabe A) und vergleichen Sie sie mit dem Ergebnis zu jener Aufgabe. •

Wurzeln natürlicher Zahlen: ein Rückblick

Im Sinne eines Rückblicks wollen wir demonstrieren, dass sich die „Investition“ in die Primfaktorzerlegung gelohnt hat. Wir werden nämlich eine Verallgemeinerung des Satzes 2.8 herleiten – mit einem Beweis, der auf der Zerlegung in Primfaktoren beruht.

Satz 5.24. *Seien $r, n \in \mathbb{N}\backslash\{1\}$. Dann gilt $\sqrt[r]{n} \in \mathbb{N}$ oder $\sqrt[r]{n} \in \mathbb{R}\backslash\mathbb{Q}$.*

Beweis: Nehmen wir das Gegenteil an! Dann gilt $\sqrt[r]{n} \notin \mathbb{N}$ und $\sqrt[r]{n} \in \mathbb{Q}$. Wir können also $\sqrt[r]{n} = \frac{u}{v}$ mit geeigneten natürlichen Zahlen u und v schreiben. Wir zerlegen u und v in Primfaktoren. Nach allfälligem Wegkürzen von gemeinsamen Primfaktoren können wir annehmen, es gelte $\mathbb{P}(u) \cap \mathbb{P}(v) = \emptyset$.

Es gilt $\frac{u^r}{v^r} = \left(\frac{u}{v}\right)^r = (\sqrt[r]{n})^r = n$, also $v^r n = u^r$. Wegen $\sqrt[r]{n} \notin \mathbb{N}$ gilt $v \neq 1$, also $\mathbb{P}(v) \neq \emptyset$. Gilt $p \in \mathbb{P}(v)$, so folgt nun $p|v^r n$,also $p|u^r$. Nach 5.3 folgt $p|u$, also der Widerspruch $p \in \mathbb{P}(u)$. ■

Aufgaben 5.25. A) Geben Sie alle Zahlenpaare $(n, r) \in \mathbb{N}_{\leq 500} \times \mathbb{N}$ an, für welche $\sqrt[r]{n} \in \mathbb{Q}$.

B) Seien $n, r \in \mathbb{N}\backslash\{1\}$ mit $n < 2^r$. Zeigen Sie, dass $\sqrt[r]{n} \notin \mathbb{Q}$. •

Teil C
Von der Arithmetik zur Algebra: Restklassen

ZUSAMMENFASSUNG

In diesem Teil der Vorlesung werden die folgenden beiden Kapitel behandelt:

- Restgleichheit und Restklassen
- Rechnen mit Restklassen

Im ersten dieser Kapitel behandeln wir, zunächst noch in seiner „elementaren“ Form, den *Chinesischen Restsatz*. Anschliessend führen wir das Konzept der *Restklassen* ein. Dieses Konzept geht über das hinaus, was üblicherweise in der Schularithmetik behandelt wird. Um uns daran zu gewöhnen, dass wir anstatt über einzelne Zahlen auch über Restklassen reden können, kehren wir dann wieder zum Chinesischen Restsatz zurück. Dabei formulieren und beweisen wir diesen Satz nochmals in neuer Form, nämlich mit Hilfe von Restklassen. Wir werden sehen, dass das zunächst abstrakt anmutende Konzept der Restklassen einen Zugang zur Veranschaulichung des Chinesischen Restsatzes liefert. Wir wollen so an einem Beispiel demonstrieren, dass der Schritt ins Abstrakte durchaus grössere Klarheit und Übersichtlichkeit in einen Gegenstand bringen und ihn so einem konkreteren Verständnis zugänglich machen kann.

Im anschliessenden Kapitel 7 gehen wir noch einen Schritt weiter und betreiben mit den Restklassen selbst Arithmetik, ähnlich wie wir dies bis jetzt von den Zahlen her kennen. Dieser Abstraktionsschritt wird uns von der elementaren Arithmetik in die Anfänge der Algebra führen. Wir werden nämlich algebraische Strukturen wie *Gruppen*, *Ringe* und *Körper* kennenlernen und im Umgang mit diesen Begriffen eine gewisse Vertrautheit erwerben. Dabei werden wir uns allerdings nur wenig von den algebraischen Objekten entfernen, auf die wir durch die Arithmetik geführt werden: die *Restklassenringe* und *Restklassenkörper*. Besonderes Augenmerk richten wir auf die sogenannten *primen Restklassen*. Deren Anzahl werden wir durch die sogenannte *Eulersche φ-Funktion* berechnen. Ausgiebig werden wir uns auch mit der *Ordnung primer Restklassen* befassen.

Insgesamt möchten wir mit diesem Kapitel auch etwas den Standpunkt der höheren Arithmetik durchscheinen lassen: die Reichhaltigkeit der Phänomene der elementaren Arithmetik umzusetzen in eine Fülle unter sich zwar gleichartiger aber gegenseitig doch verschiedener arithmetisch-algebraischer Strukturen. Ein nächster Schritt wäre die klassifizierende Untersuchung dieser Strukturen – ein Schritt, der in dieser Vorlesung nicht mehr getan wird...

TIPPS FÜR DAS SELBSTSTUDIUM

- *Kapitel 6:* Dieses kurze Kapitel ist sehr wichtig, da es die Treppe zu einer neuen Abstraktionsebene darstellt. Wir empfehlen das Studium der Beweise von 6.2, 6.12 und 6.15. Besonders wichtig sind hier die Aufgaben, etwa 6.14 C), D) und 6.17. Damit Ihnen der Spass an der Sache nicht vergeht, sollten Sie 6.18 konsultieren, bevor Sie sich an die Aufgaben 6.17 wagen.

- *Kapitel 7:* Damit Sie in diesem umfangreichen Kapitel nicht den Mut verlieren, sollten Sie zuerst einen kleinen Erkundungsausflug machen, bevor Sie sich der Vertiefung widmen. Dazu ein Vorschlag: 7.1 (ohne Beweis), 7.2 und 7.4 lesen, dann möglichst viele der Aufgaben aus 7.6 lösen; 7.7 A), B) und 7.9 lesen (ohne Beweis), 7.11 A), B) lösen; 7.16 A), B) lösen. Schliesslich könnten Sie 7.19 lesen (ohne Beweis), dann 7.21 A), B) lösen, 7.23 A), B) lesen und die Aufgaben 7.24 A) B) lösen. Zum Schluss 7.28 und 7.29 lösen und dazu die Aufgaben 7.30 A), B) und allenfalls C) lösen. Zur weiteren Vertiefung empfehlen wir das Studium der Beweise von 7.9, 7.12, 7.17–7.19.

Kapitel 6

Restgleichheit und Restklassen

Überblick

In Kapitel 4 haben wir die Grundlagen der aus der Schule bekannten Teilbarkeitslehre in eine strenge Form gefasst. Mit dem Begriff des Divisionsrestes haben wir ein Konzept von ausserordentlicher Tragweite kennengelernt. Das Ziel dieses Kapitels ist es, dieses Konzept weiter zu entwickeln und die Grundlagen für die Behandlung der Restklassenringe (vgl. Kapitel 7) bereitzustellen.

Die Hauptthemen des vorliegenden Kapitels sind:

- *der Chinesische Restsatz,*
- *die Restgleichheit oder Kongruenz,*
- *Restklassen,*
- *nochmals der Chinesische Restsatz,*
- *eine Veranschaulichung des Chinesischen Restsatzes.*

Der erste Teil des Kapitels hat noch Vertiefungscharakter. Mit den Restklassen führen wir aber ein Konzept ein, welches nicht mehr im Bereich der Schularithmetik liegt.

Bereits in Aufgabe 1.4 B) wurden wir mit dem Problem konfrontiert, eine ganze Zahl zu finden, welche bezüglich zweier vorgegebener teilerfremder Zahlen (z. B. 19 und 8) vorgeschriebene Teilerreste (z. B. 4 resp. 5) hat. Der sogenannte *Chinesische Restsatz* besagt, dass dieses Problem allgemein lösbar ist, und diesen Satz wollen wir in diesem Kapitel auch als erstes beweisen. Dann führen wir die Kongruenzrelation und darauf aufbauend den Begriff der Restklasse ein. Von diesem nun etwas abstrakt gewordenen Standpunkt aus werden wir Rückschau halten und den Chinesischen Restsatz nochmals formulieren – jetzt aber im Rahmen der neuen Begriffe. Dank der Formulierung im

abstrakten Kontext werden wir dann zu einer geometrischen Veranschaulichung dieses Satzes gelangen.

Der Chinesische Restsatz

Wir beginnen mit dem folgenden Hilfsresultat.

Lemma 6.1. *Sei $m \in \mathbb{N}$ und seien $x, y \in \mathbb{Z}$. Dann sind äquivalent:*

(i) $x \bmod (m) = y \bmod (m)$;

(ii) $m|(x-y)$.

Beweis: „(i) $\Longrightarrow$ (ii)“ : Sei $r := x \bmod (m) = y \bmod (m)$. Mit geeigneten Zahlen $p, q \in \mathbb{Z}$ gelten dann $x = pm + r$ und $y = qm + r$. Es folgt

$$x - y = pm + r - (qm + r) = (p - q)m, \text{ also } m|(x-y).$$

„(ii) $\Longrightarrow$ (i)“ : Es gelte $m|(x-y)$. Es gibt dann ein $k \in \mathbb{Z}$ mit $x - y = km$.

Wir schreiben $r := x \bmod (m)$. Es gilt dann $0 \leq r < m$ und mit einer geeigneten Zahl $q \in \mathbb{Z}$ können wir schreiben $x = qm + r$. Es folgt

$$y = x - (x - y) = x - km = qm + r - km = (q - k)m + r.$$

Dies zeigt, dass $y \bmod (m) = r$, d.h. $y \bmod (m) = x \bmod (m)$. ■

Nun beweisen wir den angekündigten Satz.

Satz 6.2. *(Chinesischer Restsatz) Seien $m, n \in \mathbb{N}$ teilerfremd und seien $r, s \in \mathbb{N}_0$ mit $r < m$ und $s < n$. Dann gelten:*

a) *Es gibt eine Zahl $x_0 \in \mathbb{Z}$ mit $x_0 \bmod (m) = r$ und $x_0 \bmod (n) = s$.*

b) *Ist x_0 wie in a) und ist $x \in \mathbb{Z}$, so sind die folgenden beiden Aussagen äquivalent:*

(i) $x \bmod (m) = r$ *und* $x \bmod (n) = s$;

(ii) $mn|(x - x_0)$.

Beweis: „a)“ : Nach 4.12 gibt es Zahlen $u, v \in \mathbb{Z}$ derart, dass $um + vn = 1$. Wir setzen $x_0 := sum + rvn$ und wollen zeigen, dass x_0 die in Aussage a) verlangte Eigenschaft hat.

Wegen $vn = 1 - um$ gilt in der Tat

$$\begin{aligned} x_0 &= sum + rvn = sum + r(1 - um) = sum + r - rum \\ &= (su - ru)m + r, \text{ also } x_0 \mod (m) = r. \end{aligned}$$

Wegen $um = 1 - vn$ gilt aber auch

$$\begin{aligned} x_0 &= sum + rvn = s(1 - vn) + rvn = s - svn + rvn \\ &= (rv - sv)n + s, \text{ also } x_0 \mod (n) = s. \end{aligned}$$

„b)“ : „(i) $\Longrightarrow$ (ii)“ : Seien $x \mod (m) = r$ und $y \mod (n) = s$. Dann folgt $x \mod (m) = x_0 \mod (m)$ und $x \mod (n) = x_0 \mod (n)$. Nach 6.1 erhalten wir $m|(x - x_0)$ und $n|(x - x_0)$. Mit 4.14 ergibt sich daraus, dass $mn|(x - x_0)$.

„(ii) $\Longrightarrow$ (i)“ : Es gelte $mn|(x - x_0)$. Dann folgt $m|(x - x_0)$ und $n|(x - x_0)$. Mit 6.1 folgt $x \mod (m) = x_0 \mod (m) = r$ und $x \mod (n) = x_0 \mod (n) = s$. ■

Bemerkung 6.3. Seien $m, n \in \mathbb{N}$ teilerfremd und seien $r, s \in \mathbb{N}_0$ mit $r < m$ und $s < n$. Wie in 1.4 B) kann man nach allen Zahlen $x \in \mathbb{Z}$ fragen, für welche die Gleichheiten $x \mod (m) = r$ und $x \mod (n) = s$ gelten. Anders gesagt: Wir möchten die Menge

$$\mathbb{L} := \{x \in \mathbb{Z} | x \mod (m) = r \wedge x \mod (n) = s\}$$

bestimmen.

Die Aussage a) des chinesischen Restsatzes besagt, dass wir in $\mathbb{L}$ überhaupt eine Zahl x_0 finden. Ist ein solches x_0 gefunden, so lässt sich $\mathbb{L}$ nach Aussage b) leicht beschreiben in der Form

$$\mathbb{L} = \{x_0 + wmn | w \in \mathbb{Z}\}.$$

Die Bestimmung von $\mathbb{L}$ ist also einfach, wenn wir einmal eine Zahl $x_0 \in \mathbb{L}$ gefunden haben. Der Beweis von 6.2 „ist konstruktiv“, d.h. er gibt im Prinzip an, wie eine solche Zahl x_0 gefunden werden kann: Man suche $u, v \in \mathbb{Z}$ so, dass $um + vn = 1$ (was mit dem Euklidischen Algorithmus geschehen kann) und setze dann $x_0 = sum + rvn$. Sind m und n nicht zu gross, findet man eine Zahl x_0 aber meist schneller durch Ausprobieren. Hilfreich ist es dabei,

$$\mathbb{L} = \mathbb{U} \cap \mathbb{V} \text{mit } \mathbb{U} := \{qm + r | q \in \mathbb{Z}\} \text{ und } \mathbb{V} := \{pn + s | p \in \mathbb{Z}\}$$

zu schreiben und zu beachten, dass man sich bei der Suche nach x_0 auf den Bereich $0 \leq x_0 < mn$ beschränken kann.

Anschaulich ist $\mathbb{U}$ ein Zahlengitter der Maschenweite m, welches r enthält und $\mathbb{V}$ ein Zahlengitter der Maschenweite n, welches s enthält. Die gesuchte Lösungsmenge $\mathbb{L}$ ist dann die Menge der Punkte die zu beiden Gittern $\mathbb{U}$ und $\mathbb{V}$ gehören. •

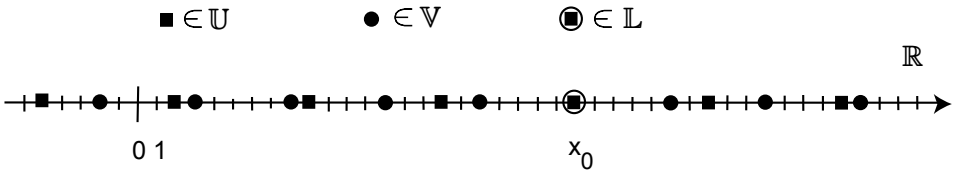


Abbildung 6.1: Zum Chinesischen Restsatz

Aufgaben 6.4. A) Lösen Sie das in 6.3 gestellte Problem für $m = 3$ und $n = 5$ für alle möglichen Reste r und s, indem Sie zu jeder Wahl von r und s eine „Basislösung“ $x_0 \in \{0, 1, \ldots, 14\}$ angeben.

B) Buslinie U verkehrt ab Zentralplatz um $\ldots, 08.00, 08.05, 08.10, \ldots$ und Buslinie V um $\ldots, 08.00, 08.12, 08.24, \ldots$. Zwischen 9 Uhr und 10 Uhr kommt Hans zum Zentralplatz und stellt fest, dass er Bus U um 3 Minuten und Bus V um 7 Minuten verpasst hat. Wie viel Uhr ist es? •

Die Restgleichheit oder Kongruenz

Beim in 6.3 behandelten Problem sind alle Lösungen x gleichberechtigt, welche bezüglich m und n resp. bezüglich mn gleiche Reste haben, d.h. restgleich sind. In der Tat ist es sehr oft so, dass die Restgleichheit zweier Zahlen interessanter ist als deren Gleichheit. Damit sind wir beim zweiten Hauptthema dieses Kapitels angelangt: der Restgleichheit.

Definition 6.5. Sei $m \in \mathbb{N}$. Zwei Zahlen $x, y \in \mathbb{Z}$ heissen *restgleich bezüglich* m oder *kongruent modulo* m, wenn $x \bmod (m) = y \bmod (m)$. Wir schreiben dann $x \equiv y \bmod (m)$, also:

$$x \equiv y \mod (m) :\Longleftrightarrow x \mod (m) = y \mod (m).$$

Gilt diese Beziehung nicht, d.h. gilt $x \bmod (m) \neq y \bmod (m)$, so schreiben wir

$$x \not\equiv y \mod (m).$$

•

Satz 6.6. *(Eigenschaften der Kongruenzrelation) Sei $m \in \mathbb{N}$ und seien $x, y, z, w \in \mathbb{Z}$. Dann gelten:*

a) $x \equiv y \bmod (m) \Longleftrightarrow m|(x - y)$.

b) $x = y \Longrightarrow x \equiv y \bmod (m)$.

c) $x \equiv y \bmod (m) \Longrightarrow y \equiv x \bmod (m)$.

d) $x \equiv y \bmod (m) \wedge y \equiv z \bmod (m) \Longrightarrow x \equiv z \bmod (m)$.

e) $x \equiv 0 \bmod (m) \Longleftrightarrow m|x$.

f) $x \equiv y \bmod (m) \wedge z \equiv w \bmod (m) \Longrightarrow x + z \equiv y + w \bmod (m)$.

g) $x \equiv y \bmod (m) \wedge z \equiv w \bmod (m) \Longrightarrow xz \equiv yw \bmod (m)$.

Beweis: „a)“ : Klar aus 6.1.

„b), c), d)“ : Klar aus der Definition der Kongruenzrelation (s. 6.5).

„e)“ : Klar aus Aussage a).

„f)“ : Gelten $x \equiv y \bmod (m)$ und $z \equiv w \bmod (m)$, so folgt aus Aussage a), dass $m|(x-y)$ und $m|(z-w)$. Damit ergibt sich $m|(x-y)+(z-w) = (x+z)-(y+w)$. Nach Aussage a) folgt $x + z \equiv y + w \bmod (m)$. ■

Aufgaben 6.7. A) Beweisen Sie Aussage 6.6 g).

B) Seien $m \in \mathbb{N}$ und $x, y, z, w \in \mathbb{Z}$. Beweisen Sie: $x \equiv y \bmod (m) \wedge z \equiv w \bmod (m) \Longrightarrow x - z \equiv y - w \bmod (m)$. •

Wir beginnen nun mit den Vorbereitungen für das nächste Hauptthema dieses Kapitel, die Restklassen.

Notation und Bemerkungen 6.8. A) Seien $m, x \in \mathbb{Z}$. Wir verwenden die Bezeichnungen von 4.15 A), B) und definieren

$$x + \mathbb{Z}m := \{x\} + \mathbb{Z}m.$$

Es gilt also

$$x + \mathbb{Z}m = \{x + qm | q \in \mathbb{Z}\}.$$

B) Sofort sieht man:

a) $x + \mathbb{Z}m = x + \mathbb{Z}(-m)$.

b) $0 + \mathbb{Z}m = \mathbb{Z}m$.

c) $x \in x + \mathbb{Z}m$.

C) Sei $m \in \mathbb{N}$. Dann entspricht $\mathbb{Z}m$ dem „0-zentrierten Zahlengitter mit Maschenweite m“ (wobei „0-zentriert“ besagen soll, dass 0 zum Gitter gehört). Die Menge $x + \mathbb{Z}m$ entspricht dann ebenfalls einem Zahlengitter mit Maschenweite m. Es entsteht, indem man das erste Gitter „um x Einheiten nach rechts verschiebt“ :

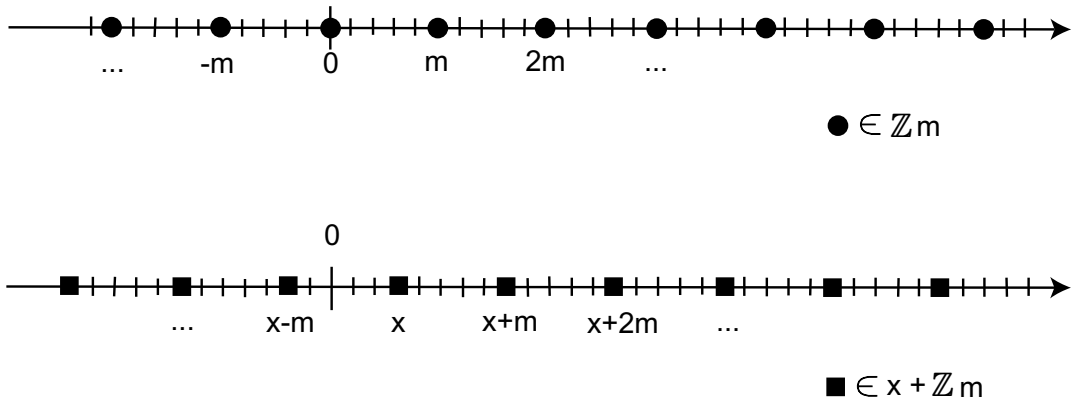


Abbildung 6.2: Zahlengitter $\mathbb{Z}m$ und $x + \mathbb{Z}m$

•

Wir beweisen zuerst das folgende Hilfsresultat, in dem auf verschiedene Weisen zum Ausdruck gebracht wird, wann „die Gitter“ $x + \mathbb{Z}m$ und $y + \mathbb{Z}m$ übereinstimmen.

Lemma 6.9. *Seien $m, x, y \in \mathbb{Z}$. Dann sind äquivalent:*

(i) $x + \mathbb{Z}m = y + \mathbb{Z}m$;

(ii) $x \in y + \mathbb{Z}m$;

(iii) $y \in x + \mathbb{Z}m$;

(iv) $x - y \in \mathbb{Z}m$;

(v) $y - x \in \mathbb{Z}m$;

(vi) $(x + \mathbb{Z}m) \cap (y + \mathbb{Z}m) \neq \emptyset$.

Beweis: „(i) $\Longrightarrow$ (ii)“ : Es gelte $x + \mathbb{Z}m = y + \mathbb{Z}m$. Dann folgt $x = x + 0 \cdot m \in x + \mathbb{Z}m = y + \mathbb{Z}m$, d.h. $x \in y + \mathbb{Z}m$.

„(ii) $\Longrightarrow$ (iii)“ : Es gelte $x \in y + \mathbb{Z}m$. Mit geeignetem $q \in \mathbb{Z}$ ist dann $x = y + qm$. Es folgt $y = x + (-q)m \in x + \mathbb{Z}m$.

„(iii) $\Longrightarrow$ (iv)“ : Es gelte $y \in x + \mathbb{Z}m$. Mit geeignetem $q \in \mathbb{Z}$ gilt dann $y = x + qm$. Es folgt $x - y = (-q)m \in \mathbb{Z}m$.

„(iv) $\Longrightarrow$ (v)“ : Sei $x - y \in \mathbb{Z}m$. Mit geeignetem $q \in \mathbb{Z}$ gilt dann $x - y = qm$, also $y - x = (-q)m \in \mathbb{Z}m$.

„(v) $\Longrightarrow$ (vi)“ Sei $y - x \in \mathbb{Z}m$. Mit geeignetem $q \in \mathbb{Z}$ gilt dann $y - x = qm$. Es folgt $y = x + qm \in x + \mathbb{Z}m$. Es ist aber auch $y = y + 0 \cdot m \in y + \mathbb{Z}m$. Es folgt $y \in (x + \mathbb{Z}m) \cap (y + \mathbb{Z}m)$.

„(vi) $\Longrightarrow$ (i)“ : Sei $(x+\mathbb{Z}m)\cap(y+\mathbb{Z}m) \neq \emptyset$. Wir finden also ein $z \in (x+\mathbb{Z}m)\cap(y+\mathbb{Z}m)$. Mit geeigneten $u, v \in \mathbb{Z}$ gilt also $z = x+um$ und $z = y+vm$. Es folgt $x+um = y+vm$, d.h. $x = y+(v-u)m$. Für jedes $q \in \mathbb{Z}$ erhalten wir somit $x+qm = y+(v-u)m+qm = y+(v-u+q)m \in y+\mathbb{Z}m$. Dies beweist $x + \mathbb{Z}m \subseteq y + \mathbb{Z}m$. Aus Symmetriegründen folgt auch $y + \mathbb{Z}m \subseteq x + \mathbb{Z}m$. ■

Als Quintessenz erhalten wir nun:

Satz 6.10. *Sei $m \in \mathbb{N}$ und seien $x, y \in \mathbb{Z}$. Dann sind äquivalent:*

(i) $x + \mathbb{Z}m = y + \mathbb{Z}m$;

(ii) $x \equiv y \bmod (m)$;

(iii) $x \bmod (m) = y \bmod (m)$;

(iv) $m|(x - y)$.

Beweis: „(i) $\Longrightarrow$ (ii)“ : Es gelte $x + \mathbb{Z}m = y + \mathbb{Z}m$. Nach 6.9 folgt $x - y \in \mathbb{Z}m$, d.h. $x - y = qm$ für ein geeignetes $q \in \mathbb{Z}$. Damit gilt $m|(x - y)$. Nach 6.6 a) folgt $x \equiv y \bmod (m)$.

„(ii) $\Longrightarrow$ (i)“ : Die obigen Schlüsse sind umkehrbar.

„(ii) $\Longleftrightarrow$ (iii)“ : Klar aus der Definition 6.5.

„(ii) $\Longleftrightarrow$ (iv)“ : Klar aus 6.6. ■

Nun sind wir bereit, die Begriffe der *Restklasse*, der *Restklassenmenge* und der *Restklassenabbildung* einzuführen.

Restklassen

Bemerkung und Definitionen 6.11. A) Sei $m \in \mathbb{N}$ und sei $x \in \mathbb{Z}$. Nach 6.10 gilt dann

$$\begin{aligned} x + \mathbb{Z}m &= \{y \in \mathbb{Z} | y \equiv x \mod (m)\} = \\ &= \{y \in \mathbb{Z} | y \mod (m) = x \mod (m)\}. \end{aligned}$$

Also ist $x + \mathbb{Z}m$ gerade die Menge aller ganzen Zahlen y, welche zu x bezüglich m („modulo m“) restgleich sind. Wir nennen $x + \mathbb{Z}m$ deshalb die *Restklasse von x modulo m.*

B) Die Menge aller Restklassen modulo m nennen wir die *Restklassenmenge* $\mathbb{Z}$ *modulo* m und bezeichnen diese mit $\mathbb{Z}/m$, also:

$$\mathbb{Z}/m := \{x + \mathbb{Z}m | x \in \mathbb{Z}\}.$$

C) Die (offenbar surjektive) Abbildung

$$\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/m; (x \mapsto \overline{x} := x + \mathbb{Z}m),$$

welche jeder Zahl $x \in \mathbb{Z}$ ihre Restklasse $x + \mathbb{Z}m$ modulo m zuordnet, nennen wir die *Restklassenabbildung* (*modulo* m). Nach 6.10 gilt insbesondere

a) $$\overline{x} = \overline{y} \Longleftrightarrow x \equiv y \mod (m) \Longleftrightarrow m|(x-y);\ (x, y \in \mathbb{Z}).$$

•

Satz 6.12. *Sei* $m \in \mathbb{N}$ *und sei* $\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/m$ *die Restklassenabbildung. Dann gelten:*

a) Durch $x \mapsto \overline{x}$ *wird eine bijektive Abbildung* $\{0, 1, \ldots, m-1\} \to \mathbb{Z}/m$ *definiert.*

b) Es gibt genau m *verschiedene Restklassen modulo* m*, d.h.* $\sharp(\mathbb{Z}/m) = m$.

Beweis: „a)“ : Sei $\Phi : \{0, 1, \ldots, m-1\} \to \mathbb{Z}/m$ die durch $x \mapsto \overline{x}$ definierte Abbildung. Wir zeigen zuerst, dass Φ injektiv ist. Seien also $x, y \in \{0, 1, \ldots, m-1\}$ mit $x \neq y$. Wir müssen zeigen, dass $\Phi(x) \neq \Phi(y)$. In der Tat gilt $x \bmod (m) = x \neq y = y \bmod (m)$, d.h. $x \not\equiv y \bmod (m)$. Nach 6.11 C) a) folgt $\overline{x} \neq \overline{y}$, also $\Phi(x) \neq \Phi(y)$.

Es bleibt zu zeigen, dass Φ surjektiv ist. Sei also $c \in \mathbb{Z}/m$. Wir müssen ein $x \in \{0, 1, \ldots, m-1\}$ so finden, dass $\Phi(x) = c$. Wir finden ein $z \in \mathbb{Z}$ mit $\overline{z} = c$. Sei $x := z \bmod (m)$. Wegen $0 \leq z \bmod (m) < m$ gilt dann $0 \leq x < m$, d.h. $x \in \{0, 1, \ldots, m-1\}$. Wegen $x \bmod (m) = x = z \bmod (m)$ gilt $x \equiv z \bmod (m)$, also $\overline{x} = \overline{z}$ (s. 6.11 C) a)). Damit gilt $\Phi(x) = c$.

„b)“ : Natürlich gilt $\sharp\{0, 1, \ldots, m-1\} = m$ (z. B. wegen der durch $n \mapsto n-1$ definierten Bijektion $\mathbb{N}_{\leq m} \to \{0, 1, \ldots, m-1\}$ (vgl. 3.19, 3.26 G)). Aus der Aussage a) folgt nun die Behauptung (vgl. 3.20 a)). ■

Bemerkung 6.13. Sei $m \in \mathbb{N}$. Sei $\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/m$ die Restklassenabbildung. Die Aussage 6.12 a) besagt, dass $\mathbb{Z}/m$ gerade aus den m verschiedenen Klassen $\overline{0}, \overline{1}, \ldots, \overline{m-1}$ besteht. Wir können diese m Klassen als die Ecken eines regulären m-Ecks auffassen. Dann „wickelt die Restklassenabbildung $\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/m$ das Zahlengitter $\mathbb{Z}$ ab auf das reguläre m-Eck $\mathbb{Z}/m$“. Diese Idee wurde schon in Aufgabe 4.4 A) vorweggenommen.

Wir wollen diesen Ansatz noch etwas präzisieren. Wir wählen dazu eine Zahl $R > 0$ und betrachten den Kreis $S_R^1 := \{(x, y) \in \mathbb{R}^2 | x^2 + y^2 = R^2\}$ in der Ebene $\mathbb{R}^2$. Auf S_R^1 betrachten wir das reguläre m-Eck mit den Punkten

$$Q_i = \left(R\cos\left(\frac{i}{m}360^\circ\right), R\sin\left(\frac{i}{m}360^\circ\right)\right), (i = 0, \ldots, m-1)$$

und stellen die Restklasse $\overline{i}$ durch den Punkt Q_i dar. Jetzt betrachten wir die Abbildung

$$\varrho_R : \mathbb{R} \to S_R^1; \left(t \mapsto \varrho_R(t) := \left(R\cos\left(\frac{t}{m}360^\circ\right), R\sin\left(\frac{t}{m}360^\circ\right)\right)\right),$$

welche die Zahlengerade $\mathbb{R}$ (streckt und) auf den Trägerkreis S_R^1 des „m-Ecks“ $\mathbb{Z}/m = \{Q_0, \ldots, Q_{m-1}\}$ abwickelt, wobei $\varrho_R(x) = \overline{x}$ für jedes $x \in \mathbb{Z}$ gilt. •

Aufgaben 6.14. A) Skizzieren Sie die in 6.13 beschriebene Situation, z. B. für $m = 5$.

B) Wie muss der Radius R gewählt werden, damit die Abbildung ϱ_R wirklich eine längentreue Abbildung ist?

C) Seien $m, n \in \mathbb{N}$ und sei $\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/m$ die Restklassenabbildung. Zeigen Sie, dass folgende Aussagen äquivalent sind:

(i) $\mathrm{ggT}(m, n) = 1$;

(ii) $\exists u \in \mathbb{Z} : \overline{un} = \overline{1}$;

(iii) $\overline{\mathbb{Z}n} = \mathbb{Z}/m$.

D) Wählen Sie $m = 12$ und verbinden Sie im „12-Eck“ $\mathbb{Z}/12$ die Punkte $\overline{0 \cdot 5}, \overline{1 \cdot 5}$, $\overline{2 \cdot 5}, \ldots \in \mathbb{Z}/12$ durch einen Streckenzug. •

Nochmals der Chinesische Restsatz

Wir wollen jetzt den Chinesischen Restsatz neu formulieren – in der Sprache der Restklassenmengen.

Satz 6.15. *(Neue Version des Chinesischen Restsatzes) Seien $m, n \in \mathbb{N}$ teilerfremd. Dann besteht eine bijektive Abbildung*

$$\varepsilon : \mathbb{Z}/mn \to (\mathbb{Z}/m) \times (\mathbb{Z}/n)$$

zwischen der Restklassenmenge $\mathbb{Z}/mn$ und dem kartesischen Produkt der Restklassenmengen $\mathbb{Z}/m$ und $\mathbb{Z}/n$ so, dass für jede Zahl $x \in \mathbb{Z}$ gilt:

$$\varepsilon(x + \mathbb{Z}mn) = (x + \mathbb{Z}m, x + \mathbb{Z}n).$$

Beweis: Zuerst zeigen wir, dass überhaupt eine Abbildung

$$\varepsilon : \mathbb{Z}/mn \to (\mathbb{Z}/m) \times (\mathbb{Z}/n)$$

besteht derart, dass für jedes $x \in \mathbb{Z}$ gilt:

$$(\alpha) \qquad \varepsilon(x + \mathbb{Z}mn) = (x + \mathbb{Z}m, x + \mathbb{Z}n).$$

Wir wollen also zeigen, dass die Abbildung ε „wohldefiniert“ ist, also, dass (α) wirklich eine Abbildungsvorschrift ist. Genauer müssen wir zeigen, dass die rechte Seite von (α) nur von der Restklasse $x + \mathbb{Z}mn \in \mathbb{Z}/mn$ abhängt und nicht vom gewählten Repräsentanten x dieser Klasse.

Wir wählen dazu $x, y \in \mathbb{Z}$ so, dass $x + \mathbb{Z}mn = y + \mathbb{Z}mn$. Wir müssen zeigen, dass $x + \mathbb{Z}m = y + \mathbb{Z}m$ und $x + \mathbb{Z}n = y + \mathbb{Z}n$. Dies wollen wir nun tun.

Nach 6.9 gilt $x - y \in \mathbb{Z}mn$. Wegen $\mathbb{Z}mn \subseteq \mathbb{Z}m$ und $\mathbb{Z}mn \subseteq \mathbb{Z}n$ folgen $x - y \in \mathbb{Z}m$ und $x - y \in \mathbb{Z}n$. Gemäss 6.9 erhalten wir $x + \mathbb{Z}m = y + \mathbb{Z}m$ und $x + \mathbb{Z}n = y + \mathbb{Z}n$. Damit ist bewiesen, dass die beiden Klassen $x + \mathbb{Z}m$ und $x + \mathbb{Z}n$ (also die rechte Seite in (α)) tatsächlich nur von der Klasse $x + \mathbb{Z}mn$ abhängen und nicht „vom gewählten Repräsentanten x der Klasse“.

Deshalb lässt sich durch die Vorschrift (α) in der Tat eine Abbildung $\varepsilon : \mathbb{Z}/mn \to (\mathbb{Z}/m) \times (\mathbb{Z}/n)$ definieren.

Als nächstes zeigen wir, dass ε injektiv ist. Wir wählen dazu zwei Zahlen $x, y \in \mathbb{Z}$ so, dass $\varepsilon(x + \mathbb{Z}mn) = \varepsilon(y + \mathbb{Z}mn)$. Zu zeigen ist, dass $x + \mathbb{Z}mn = y + \mathbb{Z}mn$.

Wir setzen dazu

$$r := x \mod (m), \; s := x \mod (n).$$

Wegen $\varepsilon(x + \mathbb{Z}mn) = \varepsilon(y + \mathbb{Z}mn)$ gelten

$$(\beta) \qquad x + \mathbb{Z}m = y + \mathbb{Z}m;$$

$$(\beta') \qquad x + \mathbb{Z}n = y + \mathbb{Z}n;$$

Mit 6.10 folgt aus (β), dass $x \equiv y \mod (m)$, also

$$(\gamma) \qquad r = x \mod (m) = y \mod (m).$$

Entsprechend folgt aus (β'), dass

$$(\gamma') \qquad r = x \mod (n) = y \mod (n).$$

Aus (γ) und (γ') folgt mit 6.2 b), dass $mn|(x - y)$. Gemäss 6.6 a) heisst dies, dass $x \equiv y \mod (mn)$. Mit 6.10 folgt nun $x + \mathbb{Z}mn = y + \mathbb{Z}mn$. Dies zeigt, dass ε injektiv ist.

Es bleibt zu zeigen, dass ε surjektiv ist. Wir wählen dazu ein Element $c \in \mathbb{Z}/m \times \mathbb{Z}/n$. Wir müssen ein $x \in \mathbb{Z}$ so finden, dass $\varepsilon(x + \mathbb{Z}mn) = c$. Mit geeigneten Zahlen $u, v \in \mathbb{Z}$ gilt

$$c = (u + \mathbb{Z}m, v + \mathbb{Z}n).$$

Wir schreiben nun

$$a := u \mod (m),\ b := v \mod (n).$$

Nach 6.2 gibt es dann ein $x \in \mathbb{Z}$ so, dass $x \mod (m) = a$ und $x \mod (n) = b$. Es folgt $x \mod (m) = u \mod (m)$ und $x \mod (n) = v \mod (n)$, also $x \equiv u \mod (m)$ und $x \equiv v \mod (n)$. Mit 6.10 erhalten wir daraus $x + \mathbb{Z}m = u + \mathbb{Z}m$ und $x + \mathbb{Z}n = v + \mathbb{Z}n$. Es folgt

$$\varepsilon(x + \mathbb{Z}mn) = (x + \mathbb{Z}m, x + \mathbb{Z}n) = (u + \mathbb{Z}m, v + \mathbb{Z}n) = c.$$

Also ist ε in der Tat surjektiv. ■

Seien (in den Bezeichnungen von 6.15) $r, s \in \mathbb{N}_0$ mit $r < m$ und $s < n$. Weil ε surjektiv ist, gibt es ein $x_0 \in \mathbb{Z}$ so, dass $\varepsilon(x_0 + \mathbb{Z}mn) = (r + \mathbb{Z}m, s + \mathbb{Z}n)$. Es gilt also $x_0 + \mathbb{Z}m = r + \mathbb{Z}m, x_0 + \mathbb{Z}n = s + \mathbb{Z}n$, d.h. $x_0 \mod (m) = r$ und $x_0 \mod (n) = s$. Wir können also sagen:

- *Die Surjektivität der Abbildung $\varepsilon : \mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n$ entspricht der Existenzaussage a) des Chinesischen Restsatzes 6.2.*

Wir können aber auch sagen:

- *Die Injektivität der Abbildung $\varepsilon : \mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n$ entspricht der Eindeutigkeitsaussage b) des Chinesischen Restsatzes 6.2.*

Aufgaben 6.16. A) Beweisen Sie die soeben gemachte Aussage.

B) Wie kann man den Beweis von 6.15 abkürzen, wenn man 6.12 verwendet? (*Hinweis:* Zwei Varianten sind möglich.)

C) Seien $m, n \in \mathbb{N}\backslash\{1\}$ und sei $\varphi : \mathbb{Z}/m \to \mathbb{Z}/n$ eine Abbildung so, dass $\varphi(x + \mathbb{Z}m) = x + \mathbb{Z}n$ für alle $x \in \mathbb{Z}$. Zeigen Sie, dass $n|m$. (*Hinweis:* Es geht um die Wohldefiniertheit von φ.) •

Eine Veranschaulichung des Chinesischen Restsatzes

Es ist natürlich legitim zu fragen, „was es bringt“, den Chinesischen Restsatz in einer neuen Version zu formulieren. Die lakonische Antwort des Mathematikers auf diese Frage lautet: „Einiges“. Im Moment können wir die Antwort noch nicht begründen, da wir bei unserer Behandlung der Restklassenmengen $\mathbb{Z}/m$ noch nicht genügend weit vorgestossen sind: Wie viel „Arithmetik in diesen Restklassenmengen steckt“ werden wir erst in Kapitel 7 sehen. Dann werden wir auch nochmals auf die obige Frage zurückkommen und sie im „algebraischen Sinne“ beantworten (s. 7.32). Was wir aber jetzt schon tun können, ist zu einer tieferen Einsicht über das Wesen des Chinesischen Restsatzes zu gelangen, wobei wir den Ausdruck „Einsicht“ wörtlich verstehen. Da selbst erworbene Einsichten die besten sind, wollen wir in einer Reihe von Aufgaben an die genannte Einsicht führen. Wenn Sie die nachfolgenden Aufgaben direkt nach dem Durchlesen und ohne weitere Hilfe lösen können, sollten Sie sich vielleicht der Frage aus 1.8 nochmals stellen. Andernfalls sollten Sie das Beispiel 6.18 durcharbeiten und dann mit den Aufgaben 6.17 beginnen.

Aufgaben 6.17. Seien $m, n \in \mathbb{N}$ teilerfremd. Wir betrachten das Rechteckgitter

$$(\mathbb{Z} \times \mathbb{Z}) \cap \mathbb{F}, \text{ wo } \mathbb{F} \text{ für das Rechteck } \{(x, y) \in \mathbb{R}^2 | 0 \leq x < m;\ 0 \leq y < n\}$$

steht. Das Element $(r + \mathbb{Z}m, s + \mathbb{Z}n) \in \mathbb{Z}/m \times \mathbb{Z}/n$ (mit $0 \leq r < m,\ 0 \leq s < n$) werde dargestellt durch den Punkt $(r, s) \in (\mathbb{Z} \times \mathbb{Z}) \cap \mathbb{F}$. In $(\mathbb{Z} \times \mathbb{Z}) \cap \mathbb{F}$ soll der „Weg“ $\varepsilon(0 + \mathbb{Z}mn) \rightsquigarrow \varepsilon(1 + \mathbb{Z}mn) \rightsquigarrow \varepsilon(2 + \mathbb{Z}mn) \rightsquigarrow \cdots$ dargestellt werden, die „Abwicklung“ von $\mathbb{Z}/mn$ auf $\mathbb{Z}/m \times \mathbb{Z}/n$.

A) Skizzieren Sie die Situation für $m = 19$ und $n = 7$.

B) Durch verkleben gegenüberliegender Seitenpaare soll $\mathbb{F}$ zu einer Torusfläche $\mathbb{T}$ geschlossen werden. $(\mathbb{Z} \times \mathbb{Z}) \cap \mathbb{F}$ geht dabei über in ein „Torusgitter“ $\mathbb{G} \subseteq \mathbb{T}$. Beschreiben Sie, wie $\mathbb{Z}/mn$ durch ε auf $\mathbb{T}$ abgewickelt wird.

C) Wählen Sie $m = 3$ und $n = 2$ und skizzieren Sie die in B) beschriebene Situation und den oben beschriebenen Weg. •

Beispiel 6.18. (*Lösungshinweise zu 6.17*) Ziel ist die Veranschaulichung der Bijektion

$$\varepsilon : \mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n.$$

aus 6.15, wobei $m, n \in \mathbb{N}$ teilerfremd sind. Wir wissen bereits, dass wir $\mathbb{Z}/mn$ durch ein reguläres mn-Eck veranschaulichen können (s. 6.13, 6.14). Doch wie „sieht $\mathbb{Z}/m \times \mathbb{Z}/n$ aus“ und wie wird die „Perlenkette“ $\mathbb{Z}/mn$ auf das „gesuchte Objekt“ $\mathbb{Z}/m \times \mathbb{Z}/n$ durch ε „abgewickelt“?

A) Wir wählen $m = 7, n = 4$. Es ist also $mn = 28$. Weiter sei $\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/28$ die Restklassenabbildung. Bildlich dargestellt sind wir vorerst in der Situation

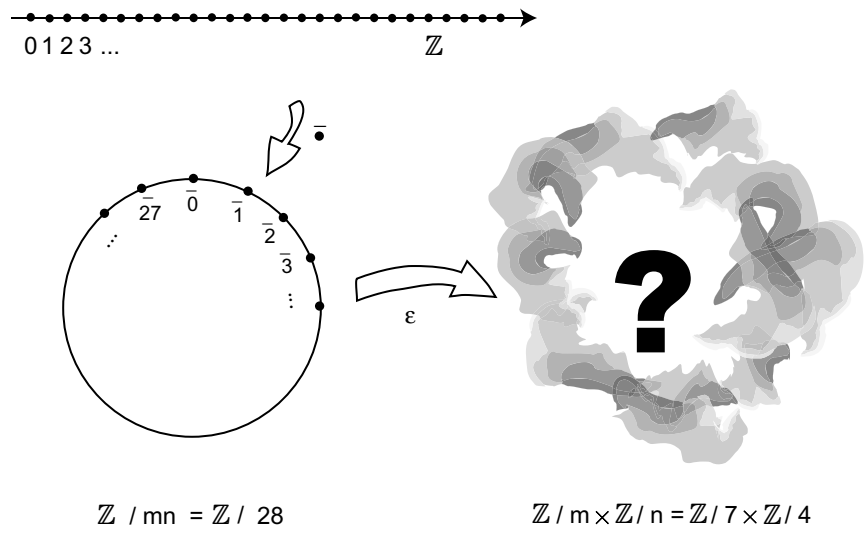


Abbildung 6.3: $\mathbb{Z}/mn \to ?$

Um ε und $\mathbb{Z}/7 \times \mathbb{Z}/4$ sichtbar in Erscheinung treten zu lassen, gehen wir vor wie in 6.17 vorgeschlagen:

Wir betrachten das Rechteck

$$\mathbb{F} = \{(x, y) \in \mathbb{R}^2 | 0 \leq x < m;\ 0 \leq y < n\},$$

sowie das zugehörige Rechteckgitter

$$(\mathbb{Z} \times \mathbb{Z}) \cap \mathbb{F} = \{(r, s) | r, s \in \mathbb{N}_0,\ 0 \leq r < m,\ 0 \leq r < n\}$$

für $m = 7$ und $n = 4$.

Der Punkt (r, s) aus diesem Rechteckgitter soll dann dem Punkt $(r + \mathbb{Z}m, s + \mathbb{Z}n)$ entsprechen, d.h.

$$(r, s) \widehat{=} (r + \mathbb{Z}m, s + \mathbb{Z}n);\ ((r, s) \in (\mathbb{Z} \times \mathbb{Z}) \cap \mathbb{F})\,.$$

Es besteht also die Situation

a)
$$\begin{cases} (r, s) \widehat{=} (r + \mathbb{Z}7, s + \mathbb{Z}4) \in \mathbb{Z}/7 \times \mathbb{Z}/4 \\ \qquad (0 \leq r < 7;\ 0 \leq s < 4). \end{cases}$$

b)
$$\begin{cases} (r, 4) \widehat{=} (r + \mathbb{Z}7, 0 + \mathbb{Z}4) \widehat{=} (r, 0);\ (0 \leq r < 7); \\ (7, s) \widehat{=} (0 + \mathbb{Z}7, s + \mathbb{Z}4) \widehat{=} (0, s);\ (0 \leq s < 4); \\ (7, 4) \widehat{=} (0 + \mathbb{Z}7, 0 + \mathbb{Z}4) \widehat{=} (0, 0). \end{cases}$$

Im Rechteckgitter $(\mathbb{Z} \times \mathbb{Z}) \cap \mathbb{F}$ geben wir nun den gesuchten Verbindungsweg

$$\begin{aligned} \varepsilon(\overline{0}) = (0 + \mathbb{Z}m, 0 + \mathbb{Z}n) &\mathrel{\widehat{=}} (0,0) \;\rightsquigarrow\; \varepsilon(\overline{1}) = (1 + \mathbb{Z}m, 1 + \mathbb{Z}n) \\ &\mathrel{\widehat{=}} (1,1) \;\rightsquigarrow\; \varepsilon(\overline{2}) = (2 + \mathbb{Z}m, 2 + \mathbb{Z}n) \mathrel{\widehat{=}} \cdots \end{aligned}$$

an, also den Verbindungsweg

$$\begin{aligned} \varepsilon(\overline{0}) = (0 + \mathbb{Z}7, 0 + \mathbb{Z}4) &\mathrel{\widehat{=}} (0,0) \;\rightsquigarrow\; \varepsilon(\overline{1}) = (1 + \mathbb{Z}7, 1 + 4\mathbb{Z}) \mathrel{\widehat{=}} (1,1) \\ \rightsquigarrow\; \varepsilon(\overline{2}) = (2 + \mathbb{Z}7, 2 + \mathbb{Z}4) &\mathrel{\widehat{=}} (2,2) \;\rightsquigarrow\; \varepsilon(\overline{3}) = (3 + \mathbb{Z}7, 3 + 4\mathbb{Z}) \mathrel{\widehat{=}} (3,3) \\ \rightsquigarrow\; \varepsilon(\overline{4}) = (4 + \mathbb{Z}7, 4 + \mathbb{Z}4) &\mathrel{\widehat{=}} (4,4) \;\rightsquigarrow\; \cdots \end{aligned}$$

Wir erhalten das folgende Bild:

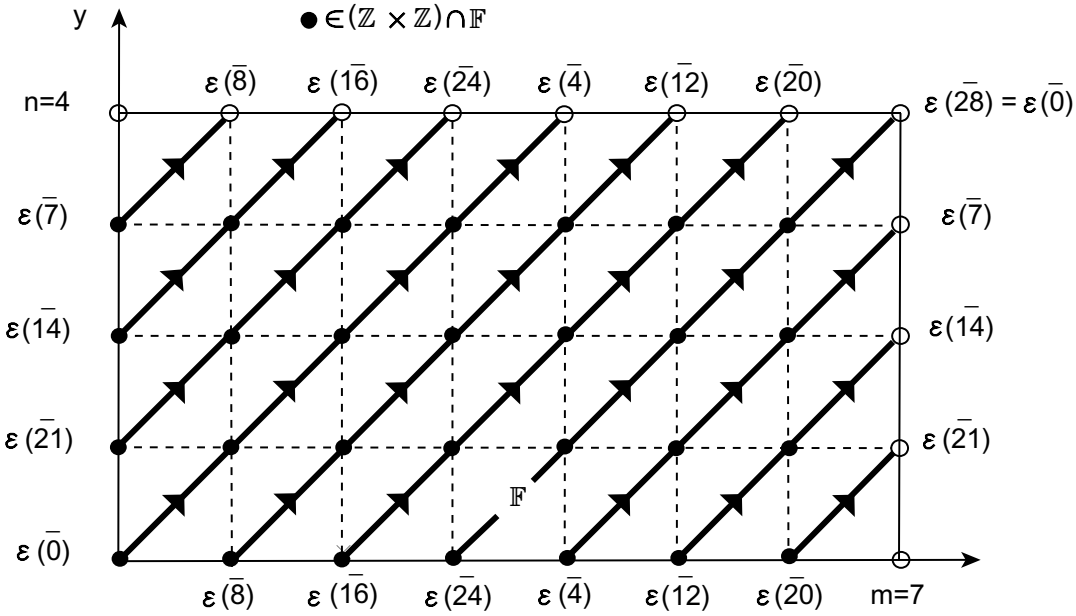


Abbildung 6.4: Rechteckgitter mit Verbindungsweg

B) Das Gitter $(\mathbb{Z} \times \mathbb{Z}) \cap \mathbb{F} = \{(r,s) | 0 \leq r < 7, 0 \leq s < 4\}$ ist wohl noch keine ganz befriedigende Darstellung von $\mathbb{Z}/7 \times \mathbb{Z}/4$: Jede „Zeile“ dieses Gitters sollte ja „aussehen“ wie das „7-Eck“ $\mathbb{Z}/7$ und jede Spalte wie das „4-Eck“ $\mathbb{Z}/4$.

Anders gesagt: Wir müssen eine Veranschaulichung finden, welche den Identifikationen b) aus Teil A) Rechnung trägt. Dazu muss man gegenüberliegende Seiten des Rechtecks $\mathbb{F}$ „verkleben“, wie nachfolgend schematisch dargestellt.

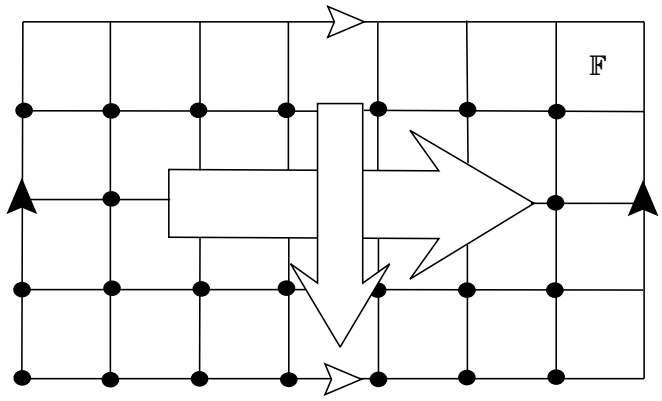


Abbildung 6.5: Verklebungsvorschrift für $\mathbb{F}$

Durch den nachfolgend in 4 Teilschritten symbolisch dargestellten Prozess wird das gewünschte Ziel erreicht.

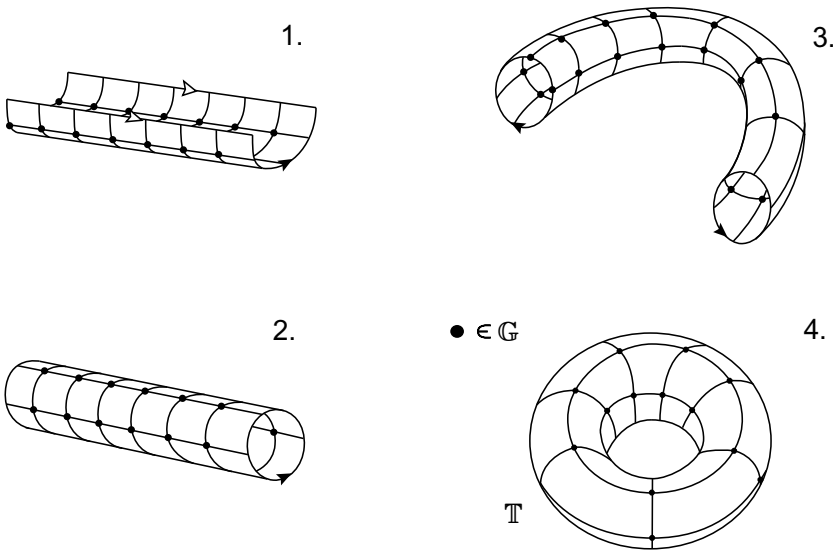


Abbildung 6.6: Vom Rechteck zum Torus

Die Fläche $\mathbb{F}$ schliesst sich bei Schritt 4 zu einem *Torus* $\mathbb{T}$. Das Rechteckgitter $(\mathbb{Z}\times\mathbb{Z})\cap\mathbb{F}$ geht beim durchgeführten Verklebungsprozess über in ein *Torusgitter* $\mathbb{G} \subseteq \mathbb{T}$.

Die „Perlenkette“ $\mathbb{Z}/mn = \mathbb{Z}/7 \cdot 4 = \mathbb{Z}/28$ wird nun durch $\varepsilon : \mathbb{Z}/28 \to (\mathbb{Z}/7 \times \mathbb{Z}/4)\widehat{=}\mathbb{G}$ auf den Torus „aufgewickelt“. Dabei erscheinen die „Perlen“ $i + \mathbb{Z}28 = \overline{i}$ als die Punkte von $\mathbb{G}$. Der Weg $\varepsilon(\overline{0}) \rightsquigarrow \varepsilon(\overline{1}) \rightsquigarrow \cdots$ erscheint als geschlossene Kurve $\mathcal{C}$ auf $\mathbb{T}$, welche „diagonal“ durch das Torusgitter $\mathbb{G}$ verläuft.

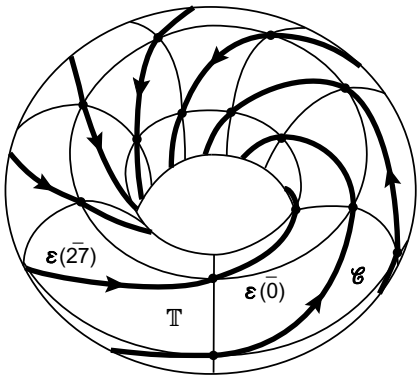


Abbildung 6.7: Verbindungsweg auf Torus

C) In der Aufsicht auf den Torus $\mathbb{T}$ erhalten wir die folgende Situation ($\underline{\varepsilon} \mathrel{\widehat{=}}$ „unten“, d.h. Punkt verdeckt, $\varepsilon \mathrel{\widehat{=}}$ „oben“, d.h. Punkt sichtbar):

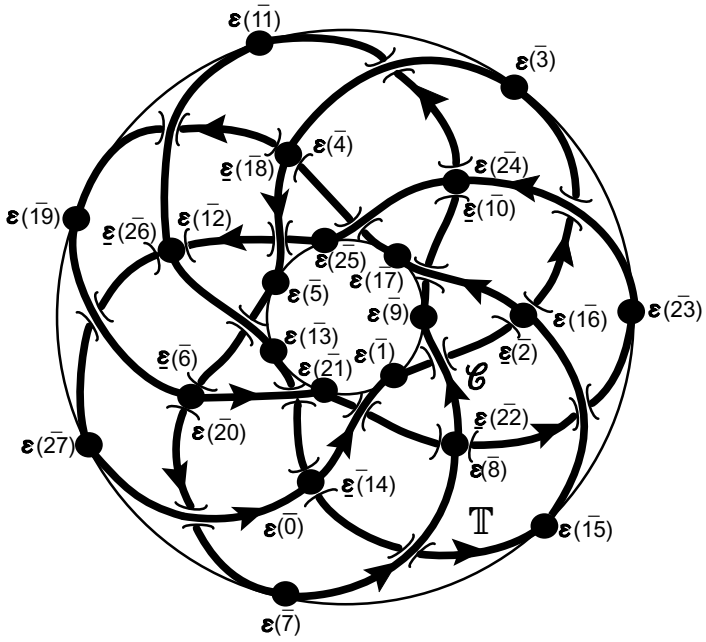


Abbildung 6.8: Verbindungsweg als Torusknoten

Die Verbindungskurve $\mathcal{C} \subseteq \mathbb{T}$ tritt als sogenannter $7/4$-*Torusknoten* in Erscheinung.

D) Um den oben anschaulich beschriebenen Übergang von $\mathbb{F}$ nach $\mathbb{T}$ analytisch streng zu fassen, wählen wir $r, R \in \mathbb{R}$ mit $0 < r < R$. Dann betrachten wir die Abbildung

$$\begin{aligned}
&\tau : \mathbb{R}^2 \to \mathbb{R}^3, \text{ gegeben durch} \\
&\tau(s,t) = (u(s,t), v(s,t), w(s,t)) \text{ mit} \\
&u(s,t) := \left(R - r\sin\left(\frac{t}{n}360^\circ\right)\right)\cos\left(\frac{s}{m}360^\circ\right), \\
&v(s,t) := \left(R - r\sin\left(\frac{t}{n}360^\circ\right)\right)\sin\left(\frac{s}{m}360^\circ\right), \\
&w(s,t) := r\cos\left(\frac{t}{n}360^\circ\right);
\end{aligned}$$

Dann sind $\mathbb{T} := \tau(\mathbb{F}) \subseteq \mathbb{R}^3$ ein Torus und $\mathbb{G} := \tau\left((\mathbb{Z}\times\mathbb{Z}) \cap \mathbb{F}\right) \subseteq \mathbb{T}$ unser Torusgitter, und $\mathcal{C}$ ist parametrisiert durch $t \mapsto \tau(t,t)$.

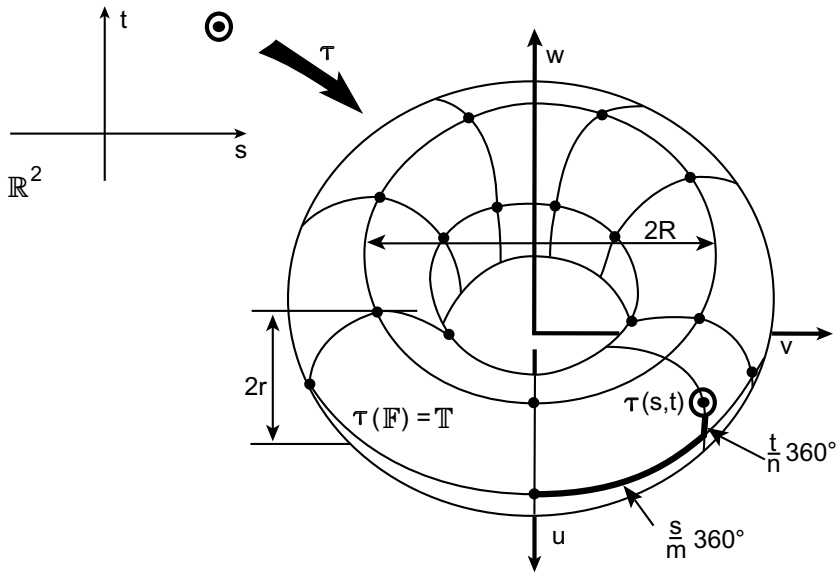


Abbildung 6.9: Parameterdarstellung des Torus

•

Aufgaben 6.19. A) Verwenden Sie die Parameterdarstellung aus 6.18 D) um die Koordinaten der Punkte auf dem Torusgitter $\mathbb{G}$ anzugeben.

B) Es gelten die Bezeichnungen von 6.18 D). Seien $s, t, s', t' \in \mathbb{R}$. Zeigen Sie

a) $\tau(s,t) = \tau(s',t') \iff (s - s' \in \mathbb{Z}m \wedge t - t' \in \mathbb{Z}n)$.

Seien $u, v \in \mathbb{R}$. Zeigen Sie:

b) $\tau(s,t) = \tau(s',t') \Longleftrightarrow \tau(s+u,t+v) = \tau(s'+u,t'+v)$.

C) Es gelten die Bezeichnungen von Teil B). Zeigen Sie mit Hilfe von B) b), dass auf $\mathbb{T}$ durch

$$\tau(s,t) \boxplus \tau(u,v) := \tau(s+u,t+v), (u,v,s,t \in \mathbb{R})$$

eine Verknüpfung „$\boxplus$“ definiert wird und zeigen Sie, dass mit $0 := \tau(0,0)$ für alle $P, Q, R \in \mathbb{T}$ gelten:

a) $P \boxplus (Q \boxplus R) = (P \boxplus Q) \boxplus R$.

b) $P \boxplus Q = Q \boxplus P$.

c) $P \boxplus 0 = P$.

d) $\exists P' \in \mathbb{T} : P \boxplus P' = 0$.

Zeigen Sie mit Hilfe von Teil A):

e) $P, Q \in \mathbb{G} \Longrightarrow P \boxplus Q \in \mathbb{G}$.

D) Auf wie viele verschiedene Weisen lässt sich die „Perlenkette“ $\mathbb{Z}/k$ gemäss 6.18 B) und C) auf einen Torus aufwickeln, falls $k = 28, 30, 120, 210, \ldots$? (*Hinweis:* r, R festhalten und alle in 6.18 D) angegebenen Parameterdarstellungen τ suchen, welche für k in Frage kommen.)

E) Lösen Sie Aufgabe D), wenn $1 < \mu := \sharp\mathbb{P}(k)$. •

Kapitel 7

Rechnen mit Restklassen

Überblick

In Kapitel 6 haben wir Restklassen eingeführt. Die Einführung der Restklassenmengen $\mathbb{Z}/m$ war sicher ein Schritt ins Abstrakte. Andererseits hat gerade dieser Schritt dabei geholfen, den Chinesischen Restsatz neu zu verstehen und ihn schliesslich auf diese Weise der Anschauung zugänglich zu machen (s. 6.17, 6.18).

Bei der Behandlung der Restklassenmengen $\mathbb{Z}/m$ sind wir allerdings auf halbem Wege stehen geblieben: $\mathbb{Z}/m$ ist nämlich nicht nur eine Menge, sondern ein „Rechenbereich“ mit ähnlichen Eigenschaften wie der Rechenbereich $\mathbb{Z}$. Wir wollen jetzt $\mathbb{Z}/m$ mit seiner „arithmetischen Struktur“ versehen und dann als neuen Rechenbereich untersuchen.

Dies mag vielleicht als reine Gedankenspielerei erscheinen. Aber gerade die „Restklassenarithmetik“ erweist sich als eine der wichtigsten Entdeckungen der Mathematik. Dazu kommt, dass diese Art von Arithmetik in neuester Zeit zahlreiche Anwendungen gefunden hat, so etwa im Bereich der Computeralgebra, der Codierungstheorie oder der Kryptographie.

Mit der Restklassenarithmetik werden wir den Schritt von der Arithmetik zur Algebra vollziehen. Dieser Schritt drängt sich hier geradezu auf, da wir dazu algebraische Strukturen wie Ringe und Körper einführen müssen.

Wir werden im Einzelnen die folgenden Themen zur Sprache bringen:

- *Addition und Multiplikation von Restklassen,*
- *Restklassenringe,*
- *Prime Restklassen,*
- *Restklassenkörper,*

- *Die Anzahl primer Restklassen und die φ-Funktion,*
- *Potenzieren in einem Ring,*
- *Ordnung einer primen Restklasse,*
- *Ordnung und Anzahl der Einheiten,*
- *die algebraische Form des Chinesischen Restsatzes: ein Rückblick,*
- *Zahlen als Funktionen: ein Ausblick.*

Wir hoffen, mit dem in diesem Kapitel vollzogenen Schritt in die Algebra die Neugierde zu wecken und zu einem tieferen Vordringen in dieses Gebiet zu ermutigen.

Addition und Multiplikation von Restklassen

Wir wollen nun als erstes die Addition und die Multiplikation von Restklassen einführen. Dazu beweisen wir das folgende Hilfsresultat.

Lemma 7.1. *Sei $m \in \mathbb{N}$ und sei $\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/m$ die Restklassenabbildung. Seien $x, y, z, w \in \mathbb{Z}$ so, dass $\overline{x} = \overline{y}$ und $\overline{z} = \overline{w}$. Dann gelten:*

a) $\overline{x + z} = \overline{y + w}$.

b) $\overline{xz} = \overline{zw}$.

Beweis: „a)“ : Gemäss Voraussetzung gilt (s. 6.11 C) a)) $x \equiv y \bmod (m)$ und $z \equiv w \bmod (m)$. Mit Hilfe von 6.6 f) folgt daraus $(x+z) \equiv (y+w) \bmod (m)$, also $\overline{x + z} = \overline{y + w}$ (s. 6.11 C) a)).

„b)“ : Gleich wie der Beweis von a), mit 6.6 g) anstelle von 6.6 f). ■

Jetzt können wir die angekündigten Rechenoperationen für Restklassen definieren.

Definitionen und Bemerkungen 7.2. A) Sei $m \in \mathbb{N}$ und sei $\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/m$ die Restklassenabbildung. Ist $x \in \mathbb{Z}$, so heisst x ein *Repräsentant* der Restklasse $\overline{x} = x + \mathbb{Z}m \in \mathbb{Z}/m$. Die Klasse $\overline{x}$ hat noch andere Repräsentanten als x, denn wegen $\overline{x + qm} = x + qm + \mathbb{Z}m = x + \mathbb{Z}m = \overline{x}$ ist jede Zahl $x + qm$ mit $q \in \mathbb{Z}$ ebenfalls ein Repräsentant von $\overline{x}$.

B) Lemma 7.1 besagt nun, dass die Restklassen $\overline{x + z} \in \mathbb{Z}/m$ und $\overline{xz} \in \mathbb{Z}/m$ nur von den beiden Klassen $\overline{x}, \overline{z} \in \mathbb{Z}/m$ abhängen, nicht aber von deren Repräsentanten. Damit

können wir aber auf $\mathbb{Z}/m$ eine *Addition* und eine *Multiplikation* definieren, indem wir die *Summe* $\overline{x}+\overline{z}$ und das *Produkt* $\overline{x}\ \overline{z}$ zweier Restklassen $\overline{x},\overline{z}\in\mathbb{Z}/m, (x,z\in\mathbb{Z})$ definieren durch

$$\overline{x}+\overline{z}:=\overline{x+z}\ ;\quad \overline{x}\ \overline{z}:=\overline{xz}.$$

C) Die beiden Klassen

$$0_{\mathbb{Z}/m}:=\overline{0}\ ,\quad 1_{\mathbb{Z}/m}:=\overline{1}$$

nennen wir die *Nullklasse* resp. die *Einsklasse in* $\mathbb{Z}/m$. •

Durch die soeben eingeführte Addition und Multiplikation haben wir die Restklassenmenge $\mathbb{Z}/m$ zu einem „Rechenbereich“ gemacht. Wir haben die Rechenoperationen auf $\mathbb{Z}/m$ mit Hilfe der üblichen Addition und Multiplikation in $\mathbb{Z}$ definiert. Deshalb ist es nicht weiter erstaunlich, dass in $\mathbb{Z}/m$ viele Rechenregeln gelten, die uns schon von den ganzen Zahlen her bekannt sind. Im nachfolgenden Satz soll dies detailliert festgehalten werden.

Satz 7.3. *(Rechenregeln für Restklassen) Sei* $m\in\mathbb{N}$. *Für alle* $a,b,c\in\mathbb{Z}/m$ *gelten dann:*

a) (Assoziativität der Addition)

$$a+(b+c)=(a+b)+c.$$

b) (Neutralität von $0_{\mathbb{Z}/m}$ *bezüglich der Addition)*

$$a+0_{\mathbb{Z}/m}=a.$$

c) (Existenz des Entgegengesetzten bezüglich der Addition)

$$\exists(-a)\in\mathbb{Z}/m : a+(-a)=0_{\mathbb{Z}/m}.$$

d) (Kommutativität der Addition)

$$a+b=b+a.$$

e) (Assoziativität der Multiplikation)

$$a(bc)=(ab)c.$$

f) (Neutralität von $1_{\mathbb{Z}/m}$ *bezüglich der Multiplikation)*

$$a1_{\mathbb{Z}/m}=a.$$

g) (Distributivität)

$$(a+b)c = ac + bc.$$

h) (Kommutativität der Multiplikation)

$$ab = ba.$$

i) (Trivialitätsbedingung)

$$0_{\mathbb{Z}/m} = 1_{\mathbb{Z}/m} \Longleftrightarrow m = 1.$$

Beweis: Sei $\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/m$ die Restklassenabbildung und seien $x, y, z \in \mathbb{Z}$ mit $a = \overline{x}, b = \overline{y}$ und $c = \overline{z}$.

„a)“ : $a+(b+c) = \overline{x}+(\overline{y}+\overline{z}) = \overline{x}+\overline{(y+z)} = \overline{x+(y+z)} = \overline{(x+y)+z} = \overline{(x+y)}+\overline{z} = (\overline{x}+\overline{y})+\overline{z} = (a+b)+c.$

„b)“ : $a + 0_{\mathbb{Z}/m} = \overline{x} + \overline{0} = \overline{x+0} = \overline{x} = a.$

„c)“ : Mit $-a := \overline{(-x)}$ folgt $a + (-a) = \overline{x} + \overline{(-x)} = \overline{x+(-x)} = \overline{0} = 0_{\mathbb{Z}/m}.$

„d)“ : $a + b = \overline{x} + \overline{y} = \overline{x+y} = \overline{y+x} = \overline{y} + \overline{x} = b + a.$

„e)“ : $a(bc) = \overline{x}(\overline{y}\ \overline{z}) = \overline{x}(\overline{yz}) = \overline{x(yz)} = \overline{(xy)z} = \overline{(xy)}\overline{z} = (\overline{x}\ \overline{y})\overline{z} = (ab)c.$

„f)“ : $a1_{\mathbb{Z}/m} = \overline{x}\overline{1} = \overline{x1} = \overline{x} = a.$

„g)“ : $(a+b)c = (\overline{x}+\overline{y})\overline{z} = \overline{(x+y)}\overline{z} = \overline{(x+y)z} = \overline{xz+yz} = \overline{xz} + \overline{yz} = ac + bc.$

„h)“ : $ab = \overline{x}\ \overline{y} = \overline{xy} = \overline{yx} = \overline{y}\ \overline{x} = ba.$

„i)“ : $0_{\mathbb{Z}/m} = 1_{\mathbb{Z}/m}$ ist gleichbedeutend zu $\overline{0} = \overline{1}$, also zu $m|1-0$ (s. 6.11 C) a)) und damit zu $m = 1$. ■

Restklassenringe

Es ist angebracht, allgemein über Rechenbereiche zu reden, welche den obigen Rechengesetzen genügen. Solche Rechenbereiche treten nämlich in der Mathematik an ganz verschiedenen Orten auf.

Definition und Bemerkungen 7.4. A) Eine Menge R zusammen mit zwei (nicht notwendigerweise verschiedenen) Elementen $0_R, 1_R \in R$ und zwei Verknüpfungen (geschrieben $a+b$ und ab für alle $a, b \in R$) heisst ein *Ring* mit *Nullelement* 0_R, *Einselement* 1_R, *Addition* „+“ und *Multiplikation* „$\cdot$“, wenn die Rechengesetze 7.3 a), b), c), d), e), f), g) erfüllt sind. Gilt auch noch das Rechengesetz 7.3 h), so sprechen wir von einem *kommutativen Ring*.

Wir sagen in dieser Situation einfach kurz,

$$(R; 0_R, 1_R; +, \cdot)$$

sei ein (kommutativer) Ring, oder sogar nur, R sei ein (kommutativer) Ring.

B) Natürlich ist $\mathbb{Z}$, versehen mit der üblichen Addition und Multiplikation ein kommutativer Ring mit Nullelement 0 und Einselement 1. Anders gesagt, ist

$$(\mathbb{Z}; 0, 1; +, \cdot)$$

ein kommutativer Ring.

C) Sei $m \in \mathbb{N}$. Nach 7.3 ist dann

$$(\mathbb{Z}/m; 0_{\mathbb{Z}/m}, 1_{\mathbb{Z}/m}; +, \cdot)$$

ein kommutativer Ring, der sogenannte *Restklassenring von* $\mathbb{Z}$ *modulo* m. Insbesondere ist also die Restklassenmenge $\mathbb{Z}/m$ mit der arithmetischen Struktur eines kommutativen Ringes versehen. Wir können deshalb in $\mathbb{Z}/m$ ähnlich rechnen wie in $\mathbb{Z}$.

D) Natürlich sind auch

$$(\mathbb{Q}; 0, 1; +, \cdot) \text{ und } (\mathbb{R}; 0, 1; +, \cdot)$$

kommutative Ringe. Dabei sind $0, 1$ und die Operationen „$+$“ und „$\cdot$“ wie üblich zu verstehen. Es handelt sich sogar um spezielle Ringe, auf die wir später noch zu sprechen kommen, nämlich um sogenannte *Körper*. •

In jedem Ring kann man leicht eine Subtraktion einführen. Insbesondere kann man also auch Restklassen voneinander subtrahieren. Im folgenden wollen wir dies allgemein ausführen.

Bemerkungen und Notation 7.5. A) Sei zunächst $(R; 0, 1; +, \cdot)$ ein Ring. Ist $a \in R$, so existiert ein a *entgegengesetztes Element* $(-a) \in R$, d.h. ein Element $(-a) \in R$ so, dass $a + (-a) = 0$. Dieses Element $(-a)$ ist durch a eindeutig festgelegt:

Ist nämlich $b \in R$ ein weiteres Element mit $a+b = 0$, so folgt $b = b+0 = b+(a+(-a)) = (b+a)+(-a) = (a+b)+(-a) = 0+(-a) = (-a)+0 = (-a)$, also in der Tat $b = (-a)$.

Wir nennen $(-a)$ deshalb *das* a *entgegengesetzte Element*. Oft schreiben wir $-a$ anstelle von $(-a)$. Nun können wir im Ring R eine *Subtraktion* einführen, indem wir die *Differenz* $a - b$ von a und b definieren durch

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

B) Sei $m \in \mathbb{N}$ und sei $\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/m$ die Restklassenabbildung. Dann gilt für jedes $x \in \mathbb{Z}$ die Beziehung $\overline{x} + \overline{(-x)} = \overline{x + (-x)} = \overline{0}_{\mathbb{Z}/m}$. Dies zeigt, dass

$$-\overline{x} = \overline{-x}; \quad (x \in \mathbb{Z}).$$

Entsprechend erhalten wir für die Subtraktion zweier Restklassen $\overline{x}, \overline{y}$ $(x, y \in \mathbb{Z})$ die Gleichheiten $\overline{x} - \overline{y} = \overline{x} + (-\overline{y}) = \overline{x} + \overline{(-y)} = \overline{x + (-y)} = \overline{x - y}$. Es gilt also:

$$\overline{x} - \overline{y} = \overline{x - y}; \quad (x, y \in \mathbb{Z}). \qquad \bullet$$

Aufgaben 7.6. Sei $m \in \mathbb{N}$ und sei $\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/m$ die Restklassenabbildung.

A) Es gelte $\overline{2} = \overline{7}$. Wie gross ist m?

B) Es gelte $\overline{9} = \overline{5}$ und $\overline{26} \neq \overline{0}$. Wie gross ist m?

C) Es gelte $\overline{2} + \overline{2} = \overline{1}$. Wie gross ist m?

D) Es gelte $\overline{6} \cdot \overline{8} = \overline{11}$. Wie gross ist m?

E) Bestimmen Sie alle Restklassen $\overline{x} \in \mathbb{Z}/7$ für welche gilt $\overline{2}\overline{x} = \overline{5}$.

F) Sei $\overline{x} \in \mathbb{Z}/5$ mit $\overline{x} \neq \overline{0}$. Berechnen Sie $\overline{x}^4$ $(:= \overline{x}\ \overline{x}\ \overline{x}\ \overline{x})$.

G) Geben Sie alle Restklassen $\overline{x} \in \mathbb{Z}/11$ an, für welche gilt: $\overline{x}^2 (:= \overline{x}\ \overline{x}) = -\overline{2}$.

H) Bestimmen Sie alle Restklassen $\overline{x} \in \mathbb{Z}/16$ mit $\overline{x} \cdot \overline{2} = \overline{0}$. $\bullet$

Wie das Beispiel $\mathbb{Z}$ zeigt, lässt sich in einem Ring die Division nicht allgemein durchführen. Der Grund ist einfach: Zu einem von 0 verschiedenen Element a eines Ringes R lässt sich nicht immer ein Inverses finden, d.h. ein Element a^{-1} mit $a\ a^{-1} = 1$. Das Bilden von Inversen ist aber gerade in Restklassenringen sehr wichtig. Wir machen dazu eine allgemeine Vorbetrachtung für beliebige kommutive Ringe.

Definitionen und Bemerkungen 7.7. A) Sei $(R; 0, 1; +, \cdot)$ ein kommutativer Ring. Ein Element $a \in R$ heisst *invertierbar* oder eine *Einheit in* R, wenn es ein Element $a^{-1} \in R$ so gibt, dass $a\ a^{-1} = 1$.

In diesem Fall ist a^{-1} durch a eindeutig festgelegt:

Ist nämlich $b \in R$ ein weiteres Element mit $ab = 1$, so folgt $b = b1 = b(aa^{-1}) = (ba)a^{-1} = (ab)a^{-1} = 1a^{-1} = a^{-1}1 = a^{-1}$, also in der Tat $b = a^{-1}$. Wir nennen a^{-1} *das zu* a *inverse Element* oder das *Inverse zu* a.

B) Die Menge aller invertierbaren Elemente von R bezeichnen wir mit R^*, also

$$R^* := \{a \in R | \exists b \in R : ab = 1\}.$$

Jedes Element $a \in R^*$ hat also ein eindeutiges Inverses a^{-1}.

C) Wegen $1 \cdot 1 = 1$ ist klar:

a) $$1 \in R^*;\ 1^{-1} = 1.$$

Aus der Definition des Inversen folgt sofort

b) $$a \in R^* \Longrightarrow (a^{-1} \in R^* \wedge (a^{-1})^{-1} = a).$$

Sind $a, b \in R^*$, so folgt $(ab)(a^{-1}b^{-1}) = (ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = (a1)a^{-1} = aa^{-1} = 1$. Dies zeigt:

c) *Sind* $a, b \in R^*$ *so folgen* $ab \in R^*$ *und* $(ab)^{-1} = a^{-1}b^{-1}$.

D) Insbesondere können wir sagen: Das Produkt zweier invertierbarer Elemente $a, b \in R^*$ ist wieder invertierbar. Dabei ist die Multiplikation assoziativ (und kommutativ) und hat das Neutralelement 1. Zu jedem $a \in R^*$ gibt aber auch ein $b \in R^*$ mit $ab = 1$ nämlich $b = a^{-1}$. In der Sprechweise der Algebra heisst dies, dass R^* bezüglich der Multiplikation eine (kommutative) Gruppe mit Einselement 1 ist. Man nennt deshalb R^* auch die *Einheitengruppe von* R.

E) Sind $a \in R$ und $b \in R^*$, so kann man den Quotienten

$$\frac{a}{b} := ab^{-1} \in R$$

definieren. Diese Bruchbildung genügt den erwarteten Rechenregeln. Nur die Wahl der Nenner ist das Neue. •

Beispiele 7.8. Sofort sieht man:

$$\mathbb{Z}^* = \{1, -1\};\ \mathbb{Q}^* = \mathbb{Q}\backslash\{0\};\ \mathbb{R}^* = \mathbb{R}\backslash\{0\}.$$ •

Prime Restklassen

Prime Restklassen sind nichts anderes als Einheiten in einem Restklassenring. Der Ausdruck „prime Restklasse“ nimmt Bezug auf die spezielle Natur der Einheiten in einem Restklassenring.

Im Falle der Restklassenringe gilt nämlich die folgende Charakterisierung der invertierbaren Elemente.

Satz 7.9. *Sei $m \in \mathbb{N}\backslash\{1\}$. Sei $\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/m$ die Restklassenabbildung und sei $x \in \mathbb{Z}$. Dann sind äquivalent:*

(i) $\overline{x} \in (\mathbb{Z}/m)^*$;

(ii) *x und m sind teilerfremd.*

Beweis: „(i) $\Longrightarrow$ (ii)“ : Sei $\overline{x} \in (\mathbb{Z}/m)^*$. Mit einem geeigneten $b \in \mathbb{Z}/m$ gilt dann $\overline{x}b = 1_{\mathbb{Z}/m} = \overline{1}$. Wir finden ein $y \in \mathbb{Z}$ mit $b = \overline{y}$. Es folgt $\overline{xy} = \overline{x}\,\overline{y} = \overline{x}b = \overline{1}$, also $\overline{xy} = \overline{1}$, d.h. $m|(xy-1)$ (s. 6.11 C) a)). Also sind x und m teilerfremd.

„(ii) $\Longrightarrow$ (i)“ : Seien x und m teilerfremd. Mit geeigneten Zahlen $y, z \in \mathbb{Z}$ gilt dann $xy + mz = 1$. Daraus folgt wegen $\overline{mz} = \overline{0}$ sofort $\overline{x}\,\overline{y} = \overline{xy} + \overline{0} = \overline{xy} + \overline{mz} = \overline{xy + mz} = \overline{1} = 1_{\mathbb{Z}/m}$, also $\overline{x}\,\overline{y} = 1_{\mathbb{Z}/m}$, d.h. $\overline{x} \in (\mathbb{Z}/m)^*$. ■

Bemerkungen und Definition 7.10. A) Sei $m \in \mathbb{N}\backslash\{1\}$ und sei $\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/m$ die Restklassenabbildung. Um die Menge $(\mathbb{Z}/m)^*$ zu bestimmen genügt es, die Menge

$$\mathbb{M}_m := \{x \in \mathbb{N} | x < m \text{ und } \mathrm{ggT}(x, m) = 1\}$$

der zu m teilerfremden natürlichen Zahlen $x < m$ zu bestimmen. Nach 7.9 gilt dann ja (vgl. 6.14):

$$(\mathbb{Z}/m)^* = \{\overline{x} | x \in \mathbb{M}_m\}.$$

B) Der Beweis von 7.9 zeigt aber auch, wie wir zu jedem Element $\overline{x} \in (\mathbb{Z}/m)^*$ mit $x \in \mathbb{M}_m$ das Inverse bestimmen:

Wir suchen ganze Zahlen $y, z \in \mathbb{Z}$ mit $xy + mz = 1$. Dann gilt

$$\overline{y} = \overline{x}^{-1}.$$

C) Anstatt zu sagen, x sei teilerfremd zu m, sagt man auch, x sei *(relativ) prim zu m*. Wegen Satz 7.9 nennt man deshalb die Restklassen $\overline{x} \in (\mathbb{Z}/m)^*$ auch *prime Restklassen modulo m*. Entsprechend nennt man die Einheitengruppe $(\mathbb{Z}/m)^*$ von $\mathbb{Z}/m$ (vgl. 7.7 D)) auch die *prime Restklassengruppe modulo m*. •

Aufgaben 7.11. A) Bestimmen Sie $\mathbb{M}_m, (\mathbb{Z}/m)^*$ und bestimmen Sie $\overline{x}^{-1}$ für alle $x \in \mathbb{M}_m$ im Fall $m = 12$.

B) Lösen Sie Aufgabe A) mit $m = 36$ statt 12.

C) Sei $m \in \mathbb{N}\backslash\{1\}$ und sei $a \in \mathbb{Z}/m$. Zeigen Sie, dass folgende Aussagen äquivalent sind:

(i) $a \notin (\mathbb{Z}/m)^*$;

(ii) $\exists b \in (\mathbb{Z}/m)\backslash\{\overline{0}\} : ab = \overline{0}$;

(iii) die Abbildung $\mu : \mathbb{Z}/m \to \mathbb{Z}/m, (b \mapsto ab)$ ist nicht injektiv;

(iv) die Abbildung μ aus (iii) ist nicht bijektiv.

D) Sei $\mathbb{R}[x]$ wie in 5.10 B). Dann ist $(\mathbb{R}[x]; 0, 1; +, \cdot)$ (mit der üblichen Addition und Multiplikation) ein Ring. Bestimmen Sie $(\mathbb{R}[x])^*$. •

Restklassenkörper

Besonders interessant sind die Restklassenringe modulo Primzahlen. Sie geben uns den Anlass, eine neue algebraische Struktur einzuführen: den Körper. Wir beweisen dazu als erstes:

Satz 7.12. *Sei $p \in \mathbb{N}\backslash\{1\}$. Dann sind äquivalent:*

(i) $p \in \mathbb{P}$;

(ii) $(\mathbb{Z}/p)^* = (\mathbb{Z}/p)\backslash\{0_{\mathbb{Z}/p}\}$.

Beweis: „(i) $\Longrightarrow$ (ii)“ : Sei $p \in \mathbb{P}$. Wir schreiben $\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/p$ für die Restklassenabbildung. Sei $a \in \mathbb{Z}/p$. Wir finden ein $x \in \mathbb{Z}$ mit $\overline{x} = a$. Unter Beachtung von 6.11 C) a) folgt

$$a = 0_{\mathbb{Z}/p} \Longleftrightarrow \overline{x} = \overline{0} \Longleftrightarrow x \equiv 0 \mod (p) \Longleftrightarrow p|x.$$

Mit 5.2 (ii) und 7.9 folgt daraus

$$a \neq 0_{\mathbb{Z}/p} \Longleftrightarrow p \nmid x \Longleftrightarrow \mathrm{ggT}(p, x) = 1 \Longleftrightarrow a = \overline{x} \in (\mathbb{Z}/p)^*.$$

Dies bedeutet, dass $\mathbb{Z}/p\backslash\{0_{\mathbb{Z}/p}\} = (\mathbb{Z}/p)^*$.

„(ii) $\Longrightarrow$ (i)“ Sei $\mathbb{Z}/p\backslash\{0_{\mathbb{Z}/p}\} = (\mathbb{Z}/p)^*$. Sei $x \in \mathbb{Z}$ beliebig gewählt mit der Eigenschaft, dass $p \nmid x$. Dann ist $\overline{x} \neq \overline{0}$ (s. 6.11 C) a)), d.h. $\overline{x} \neq 0_{\mathbb{Z}/p}$, also $\overline{x} \in \mathbb{Z}/p\backslash\{0_{\mathbb{Z}/p}\} = (\mathbb{Z}/p)^*$.

Nach 7.9 folgt $\mathrm{ggT}(p,x)=1$. Damit ist gezeigt, dass für jede Zahl $x\in\mathbb{Z}$ aus $p\nmid x$ folgt, dass $\mathrm{ggT}(p,x)=1$. Nach 5.2 muss p also eine Primzahl sein. ■

Im Restklassenring modulo einer Primzahl sind also alle von 0 verschiedenen Elemente invertierbar. Zu dieser wichtigen Eigenschaft eines Ringes möchten wir nun einiges bemerken.

Bemerkungen und Definition 7.13. A) Sei $(R;0,1;+,\cdot)$ ein kommutativer Ring mit $1\neq 0$. Für jedes Element $a\in R$ gilt dann $0a=0a+0=0a+(a+(-a))=(0a+a)+(-a)=(0a+1a)+(-a)=(0+1)a+(-a)=1a+(-a)=a+(-a)=0\neq 1$. Dies zeigt, dass $0\notin R^*$ also, dass

$$R^*\subseteq R\backslash\{0\}.$$

B) Enthält R so viele Einheiten wie möglich, d.h. gilt $R^*=R\backslash\{0\}$, so sagt man R (oder $(R;0,1;+,\cdot)$) sei ein *Körper*. Anders gesagt:

> *Ein kommutativer Ring heisst ein Körper, wenn in ihm alle Elemente ausser dem Nullelement invertierbar sind.*

C) Typische Beispiele von Körpern sind (vgl. 7.4)

> der *Körper* $\mathbb{Q}$ *der rationalen Zahlen* oder der *Körper* $\mathbb{R}$ *der reellen Zahlen.*

D) Ist $(K;0,1;+,\cdot)$ ein Körper, so kann man in K „durch jedes von 0 verschiedene Element dividieren“, genauer: Sind $a,b\in K$ mit $b\neq 0$, so kann man den *Quotienten* $\frac{a}{b}:=ab^{-1}$ definieren, und zwar für alle Nenner $b\neq 0$ (vgl. 7.7 E)). Die Division von a durch b ist einfach die Bildung des Quotienten $\frac{a}{b}=ab^{-1}$. •

Den Satz 7.12 können wir nun auch wie folgt aussprechen:

Korollar 7.14. *Sei $p\in\mathbb{N}\backslash\{1\}$. Dann sind äquivalent:*

(i) $p\in\mathbb{P}$*;*

(ii) Der Restklassenring $\mathbb{Z}/p$ ist ein Körper.

Beweis: Klar aus 7.12. ■

Entsprechend setzen wir fest:

Definition 7.15. Ist $p\in\mathbb{P}$, so nennen wir $\mathbb{Z}/p$ den *Restklassenkörper von $\mathbb{Z}$ modulo p.* •

Aufgaben 7.16. A) Sei $p \in \mathbb{P}$ und sei $\overline{\bullet} : \mathbb{Z} \to \mathbb{Z}/p$ die Restklassenabbildung. Erstellen Sie Verknüpfungstabellen für die Addition, die Subtraktion, die Multiplikation und die Division im Restklassenkörper $\mathbb{Z}/p = \{\overline{0}, \overline{1}, \ldots, \overline{p-2}, \overline{p-1}\}$ falls $p = 3$.

B) Lösen Sie Aufgabe A) mit $p = 5$, aber nur für die Addition und die Multiplikation.

C) Sei $(K; 0, 1; +, \cdot)$ ein endlicher Körper (d.h. es gelte $\sharp K < \infty$). Beschreiben Sie, wie man aus einer Verknüpfungstabelle für die Multiplikation eine für die Division gewinnen kann.

D) Verwenden Sie Aufgabe C), um Aufgabe B) auch für die Division zu lösen.

E) Sei $(R; 0, 1; +, \cdot)$ ein Ring. Zeigen Sie, dass gilt:

$$1 = 0 \Longleftrightarrow R = \{0\}.$$

(*Hinweis:* $0a = 0$ verwenden.) •

Die Anzahl primer Restklassen und die φ-Funktion

Ist $p \in \mathbb{P}$, so folgt aus 7.12 und 6.12, dass $\sharp(\mathbb{Z}/p)^* = p - 1$. Nun wollen wir $\sharp(\mathbb{Z}/m)^*$ für beliebige Zahlen $m \in \mathbb{N}\backslash\{1\}$ bestimmen. Wir beginnen mit zwei Hilfsresultaten:

Lemma 7.17. *Sei $p \in \mathbb{P}$ und sei $\alpha \in \mathbb{N}$. Dann gilt $\sharp(\mathbb{Z}/p^\alpha)^* = (p-1)p^{\alpha-1}$.*

Beweis: Wie in 7.10 betrachten wir die Menge

$$\mathbb{M} := \mathbb{M}_{p^\alpha} := \{x \in \mathbb{N} | x < p^\alpha \text{ und } \mathrm{ggT}(x, p^\alpha) = 1\}$$

der zu p^α teilerfremden natürlichen Zahlen $x < p^\alpha$. Wegen der eindeutigen Zerlegung in Primfaktoren sind x und p^α genau dann teilerfremd, wenn $p \not| \, x$. Damit gilt

$$(\alpha) \qquad \mathbb{M} = \{x \in \mathbb{N} | x < p^\alpha \text{ und } p \not| \, x\} = \{1, 2, \ldots, p^\alpha\} \backslash \mathbb{U},$$

wobei $\mathbb{U}$ aus allen Zahlen $x \in \{1, 2, \cdots, p^\alpha\}$ besteht, welche durch p geteilt werden. Damit können wir schreiben

$$\begin{aligned} \mathbb{U} &= \{py | y \in \mathbb{N} \text{ und } py \leq p^\alpha\} = \{py | y \in \mathbb{N} \text{ und } y \leq p^{\alpha-1}\} \\ &= \{py | y \in \{1, \ldots, p^{\alpha-1}\}\}. \end{aligned}$$

Dies zeigt, dass $\mathbb{U}$ aus $p^{\alpha-1}$ Elementen besteht, d.h. $\sharp\mathbb{U} = p^{\alpha-1}$. Wegen $\sharp\{1, 2, \ldots, p^\alpha\} = p^\alpha$ folgt aus der Aussage (α), dass $\sharp\mathbb{M} = p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$.

Weil durch $x \mapsto \overline{x} := x + \mathbb{Z}/p^\alpha$ eine Bijektion $\mathbb{M} \to (\mathbb{Z}/p^\alpha)^*$ definiert wird (vgl. 7.10), folgt $\sharp(\mathbb{Z}/p^\alpha)^* = (p-1)p^{\alpha-1}$. ■

Lemma 7.18. *Seien $m, n \in \mathbb{N}\backslash\{1\}$ teilerfremd. Durch Einschränkung der Abbildung*

$$\varepsilon : \mathbb{Z}/mn \to (\mathbb{Z}/m) \times (\mathbb{Z}/n)$$

(s. 6.15) erhält man eine bijektive Abbildung

$$\varepsilon\restriction: (\mathbb{Z}/mn)^* \to (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*.$$

Beweis: Zunächst machen wir eine Vorbetrachtung. Wir wählen nämlich $x \in \mathbb{Z}$ und wollen zeigen, dass gilt:

$$(\alpha) \qquad \text{ggT}(x, mn) = 1 \Longleftrightarrow (\text{ggT}(x, m) = 1 \wedge \ \text{ggT}\ (x, n) = 1)$$

„$\Rightarrow$“ : Ist x teilerfremd zu mn, dann ist x natürlich erst recht teilerfremd zu m und n.

„$\Leftarrow$“ : Ist x teilerfremd zu m und zu n, so hat x weder mit m noch mit n einen gemeinsamen Primfaktor. Dann hat x gemäss 5.2 keinen gemeinsamen Primfaktor mit mn. Also ist x teilerfremd zu mn. Damit ist (α) bewiesen.

Gemäss 7.9 können wir die Aussage (α) auch aussprechen in der Form:

$$(\alpha') \qquad x + \mathbb{Z}mn \in (\mathbb{Z}/mn)^* \Longleftrightarrow \begin{cases} x + \mathbb{Z}m \in (\mathbb{Z}/m)^* \\ \text{und} \\ x + \mathbb{Z}n \in (\mathbb{Z}/n)^*. \end{cases}$$

Schreiben wir $a := x + \mathbb{Z}mn$, so gilt gemäss 6.15

$$\varepsilon(a) = (x + \mathbb{Z}m, x + \mathbb{Z}n) \in \mathbb{Z}/m \times \mathbb{Z}/n.$$

Damit können wir aber (α') auch formulieren als

$$a \in (\mathbb{Z}/mn)^* \Longleftrightarrow \varepsilon(a) \in (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*.$$

Da wir bereits wissen, dass ε bijektiv ist, folgt unsere Behauptung. ■

Nun können wir die Anzahl der primen Restklassen modulo m berechnen:

Satz 7.19. *Sei $m \in \mathbb{N}\backslash\{1\}$ mit der Primfaktorzerlegung $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ (mit $n \in \mathbb{N}$, $p_1, \ldots, p_r \in \mathbb{P}$, $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$ und $p_1 < \cdots < p_r$). Dann gilt:*

$$\varphi(m) := (p_1 - 1) \cdots (p_n - 1) p_1^{\alpha_1 - 1} \cdots p_n^{\alpha_n - 1} = \sharp(\mathbb{Z}/m)^*.$$

Beweis: (Induktion nach n) Ist $n = 1$, so schliesst man mit 7.17.

Sei also $n > 1$. Wir schreiben $m = uv$ mit $u = p_1^{\alpha_1} \cdots p_{n-1}^{\alpha_{n-1}}$ und $v = p_n^{\alpha_n}$. Dann sind u und v teilerfremd. Nach Induktionsvoraussetzung gilt

$$(\alpha) \qquad \sharp(\mathbb{Z}/u)^* = (p_1 - 1) \cdots (p_{n-1} - 1) p_1^{\alpha_1 - 1} \cdots p_{n-1}^{\alpha_{n-1} - 1}.$$

Nach 7.17 gilt aber auch

$$(\beta) \qquad \sharp(\mathbb{Z}/v)^* = (p_n - 1) p_n^{\alpha_n - 1}.$$

Aus 7.18 folgt

$$(\gamma) \qquad \sharp(\mathbb{Z}/m)^* = \sharp(\mathbb{Z}/uv)^* = \sharp(\mathbb{Z}/u)^* \cdot \sharp(\mathbb{Z}/v)^*.$$

Aus $(\alpha), (\beta), (\gamma)$ ergibt sich die Behauptung. ■

Definition und Bemerkung 7.20. A) Ist $m \in \mathbb{N}\backslash\{1\}$ mit der Primfaktorzerlegung

$$m = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \ (n, \alpha_1, \ldots, \alpha_n \in \mathbb{N}; p_1, \ldots, p_n \in \mathbb{P}; p_1 < p_2 < \cdots < p_n),$$

so schreiben wir wie in 7.19

$$\varphi(m) := (p_1 - 1) \cdots (p_n - 1) p_1^{\alpha_1 - 1} \cdots p_n^{\alpha_n - 1} = \Pi_{p \in \mathbb{P}(m)} \ (p - 1) p^{\nu_p(m) - 1}.$$

Wir setzen zudem $\varphi(1) := 1$. So erhalten wir eine Funktion $\varphi : \mathbb{N} \to \mathbb{N}$, die sogenannte *Eulersche φ-Funktion.*

B) Gemäss 7.19 können wir sagen:

> *Ist $m \in \mathbb{N}\backslash\{1\}$, so gilt $\varphi(m) = \sharp(\mathbb{Z}/m)^*$, d.h. der Wert $\varphi(m)$ der Eulerschen φ-Funktion ist die Anzahl der primen Restklassen modulo m.* •

Aufgaben 7.21. A) Bestimmen Sie $\sharp(\mathbb{Z}/m)^*$ für alle $m \in \mathbb{N}\backslash\{1\}$ mit $m \leq 30$.

B) Berechnen Sie $a^2 = a \cdot a$ für alle $a \in (\mathbb{Z}/m)^*$ in den Fällen $m = 5$ und $m = 8$. Begründen Sie damit, dass $(\mathbb{Z}/5)^*$ und $(\mathbb{Z}/8)^*$ sich „arithmetisch unterscheiden“, obwohl beide Mengen gleich viele Elemente enthalten.

C) Sei $\varphi : \mathbb{N} \to \mathbb{N}$ die Eulersche φ-Funktion. Zeigen Sie:

a) φ ist weder injektiv noch surjektiv.

b) $\mathrm{ggT}(m, n) = 1 \Longrightarrow \varphi(mn) = \varphi(m)\varphi(n)$.

D) Bestimmen Sie alle Zahlen $m \in \mathbb{N}\backslash\{1\}$ mit $\frac{\varphi(m)}{m} = \frac{4}{15}$ und alle Zahlen $n \in \mathbb{N}\backslash\{1\}$ mit $\frac{\varphi(n)}{n} = \frac{8}{35}$.

E) Sei $\mathbb{U} := \{m \in \mathbb{N}\backslash\{1\} | \sharp\mathbb{P}(m) = 4\}$ die Menge aller natürlichen Zahlen mit genau 4 verschiedenen Primfaktoren. Zeigen Sie, dass für alle $m \in \mathbb{U}$ und alle $n \in \mathbb{N}$ gelten:

a) $\frac{\varphi(m)}{m} \geq \frac{8}{35}$.

b) $\mathbb{P}(m) \cap \mathbb{N}_{\leq n} = \emptyset \Longrightarrow \frac{\varphi(m)}{m} > (1 - \frac{1}{n})^4$.

F) Es gelten die Bezeichnungen von Aufgabe E). Zeigen Sie, dass es eine Zahlenfolge $(m_n)_{n\in\mathbb{N}} \subseteq \mathbb{U}$ so gibt, dass $\lim_{n\to\infty} \frac{\varphi(m_n)}{m_n} = 1$.

G) Es gelten die Bezeichnungen von Aufgabe F). Sei $p \in \mathbb{P}$. Zeigen Sie, dass es eine Zahlenfolge $(m_n)_{n\in\mathbb{N}} \subseteq \mathbb{U}$ so gibt, dass $\lim_{n\to\infty} \frac{\varphi(m_n)}{m_n} = 1 - \frac{1}{p}$. •

Potenzieren in einem Ring

Genau wie in $\mathbb{Z}, \mathbb{Q}$ oder $\mathbb{R}$ kann man in einem beliebigen Ring die Operation des Potenzierens einführen, z. B. in Restklassenringen. Das Potenzieren in Restklassenringen ist für die Zahlentheorie von besonderer Bedeutung, insbesondere das Potenzieren von primen Restklassen. Wir werden das Thema „Potenzieren“ allerdings nicht im rein „arithmetischen“ Rahmen behandeln, sondern im erweiterten „algebraischen“ Kontext. Wir werden also unser Augenmerk nicht bloss auf das Potenzieren primer Restklassen richten, sondern allgemein auf das Potenzieren von Einheiten in einem kommutativen Ring.

Definition und Bemerkungen 7.22. A) Sei $(R; 0, 1; +, \cdot)$ ein kommutativer Ring, sei $a \in R$ und sei $n \in \mathbb{N}_0$. Wie üblich kann man nun die *n-te Potenz von a* definieren durch

$$a^n := \begin{cases} 1, & \text{falls } n = 0 \\ a^{n-1} \cdot a, & \text{falls } n > 0. \end{cases}$$

B) Durch Induktion über n prüft man leicht nach, dass die folgenden vertrauten Rechenregeln gelten $(a, b \in R; m, n \in \mathbb{N}_0)$:

a) $1^n = 1$.

b) $a^m a^n = a^{m+n}$.

c) $(a^m)^n = a^{mn}$.

d) $(ab)^n = a^n b^n$.

C) Mit Hilfe der Aussage 7.7 C) a) beweist man leicht durch Induktion bezüglich n:

a) *Ist* $a \in R^*$, *so gelten* $a^n \in R^*$ *und* $(a^n)^{-1} = (a^{-1})^n$, $(n \in \mathbb{N})$.

Für Einheiten in R kann man nun auch Potenzen mit negativen Exponenten definieren, indem man setzt:

$$a^n := (a^{-1})^{-n};\ (a \in R^*; n \in \mathbb{Z}, n < 0).$$

Mit Hilfe von a) kann man dann sehr leicht nachprüfen, dass die Rechenregeln b), c) und d) aus B) auch für beliebige Exponenten $m, n \in \mathbb{Z}$ gelten, solange die Elemente a und b Einheiten sind in R.

Damit haben wir das Rechnen mit negativen, ganzzahligen Exponenten, das uns von $\mathbb{Q}$ und $\mathbb{R}$ her vertraut ist, auf beliebige kommutative Ringe verallgemeinert. •

Die Ordnung einer primen Restklasse

Die Menge $(\mathbb{Z}/m)^*$ der primen Restklassen ist endlich. Deshalb wollen wir uns im folgenden auf Ringe R mit endlicher Einheitengruppe R^* konzentrieren. In dieser Situation lässt sich zu jeder Einheit $a \in R^*$ eine natürliche Zahl definieren: die *Ordnung von* a.

Bemerkungen und Definition 7.23. A) Sei $(R; 0, 1; +, \cdot)$ ein kommutativer Ring so, dass die Menge R^* endlich ist. Wir wählen $a \in R^*$ und betrachten die Menge

$$\langle a \rangle := \{a^n | n \in \mathbb{N}_0\}.$$

Nach 7.22 C) a) gilt

a) $\langle a \rangle \subseteq R^*$.

Insbesondere ist $\langle a \rangle$ eine endliche Menge.

B) Wir wollen uns überlegen, dass folgendes gilt:

a) *Sind* $m, n \in \mathbb{N}_0$ *mit* $m \leq n$ *und* $a^m = a^n$, *so gilt* $a^{n-m} = 1$.

In der Tat gilt $a^{n-m} = (a^{n-m})1 = a^{n-m}(a^m(a^m)^{-1}) = (a^{n-m}a^m)(a^m)^{-1} = a^{(n-m)+m}(a^m)^{-1} = a^n(a^m)^{-1} = a^m(a^m)^{-1} = 1$.

Weil die Menge $\langle a \rangle$ endlich ist, gibt es Zahlen $m, n \in \mathbb{N}_0$ so, dass $m \neq n$ und $a^m = a^n$. Ohne Einschränkung können wir annehmen, es gelte $m < n$. Setzen wir $t = n - m$, so folgt $t \in \mathbb{N}$, und gemäss Aussage a) gilt $a^t = 1$. Damit ist gezeigt:

b) $\exists t \in \mathbb{N} : a^t = 1.$

Die kleinste natürliche Zahl t mit dieser Eigenschaft nennen wir die *Ordnung von* a und bezeichnen diese mit $\mathrm{ord}(a)$, also:

c) $\mathrm{ord}(a) := \min\{t \in \mathbb{N} | a^t = 1\},\ (a \in R^*)$.

C) Die soeben eingeführte Ordnung einer Einheit lässt sich auch noch etwas anders charakterisieren. Seien nämlich $a \in R^*$ und $t \in \mathbb{N}$. Dann gilt die folgende Äquivalenz:

a) $a^t = 1 \Longleftrightarrow \mathrm{ord}(a)|t.$

Wir überlegen uns die Richtigkeit dieser Aussage.

„$\Longrightarrow$“ : Sei $a^t = 1$. Wir schreiben $t = q\ \mathrm{ord}(a) + r$ mit $q \in \mathbb{N}_0$ und $0 \leq r < \mathrm{ord}(a)$. Dann folgt $1 = a^t = a^{q\ \mathrm{ord}(a)+r} = (a^{\mathrm{ord}(a)})^q a^r = 1^q a^r = a^r$. Wegen $r < \mathrm{ord}(a)$ erhalten wir $r \notin \mathbb{N}$, also $r = 0$. Deshalb gilt $\mathrm{ord}(a)|t$.

„$\Longleftarrow$“ : Ist $\mathrm{ord}(a)|t$, so gibt es ein $q \in \mathbb{N}_0$ mit $t = \mathrm{ord}(a)q$. Es folgt $a^t = a^{\mathrm{ord}(a)q} = (a^{\mathrm{ord}(a)})^q = 1^q = 1$. •

Aufgaben 7.24. A) Bestimmen Sie $\mathrm{ord}(a)$ und $\langle a \rangle$ für alle $a \in (\mathbb{Z}/m)^*$ und alle $m \in \{2, \cdots, 5\}$.

B) Bestimmen Sie alle primen Restklassen $a \in (\mathbb{Z}/m)^*$ der Ordnung 2 und der Ordnung 4 für $m = 5$ und $m = 8$.

C) Sei $(R; 0, 1; +, \cdot)$ ein kommutativer Ring so, dass $\sharp R^* < \infty$. Zeigen Sie, dass für je zwei Elemente $a, b \in R^*$ gelten $(ab)^{kgV(\mathrm{ord}(a),\mathrm{ord}(b))} = 1$ und $\mathrm{ord}(ab) \leq kgV(\mathrm{ord}(a), \mathrm{ord}(b))$.

D) Es gelten die Bezeichnungen von Aufgabe C). Zeigen Sie, dass für jedes $a \in R^*$ gilt $\mathrm{ord}(a) = \mathrm{ord}(a^{-1})$. •

Ordnung und Anzahl der Einheiten

Nun möchten wir einen wichtigen Zusammenhang zwischen der Ordnung $\mathrm{ord}(a)$ einer Einheit $a \in R^*$ eines kommutativen Ringes R und der Anzahl $\sharp R^*$ aller Einheiten herleiten. Wir beginnen mit zwei Hilfsresultaten.

Lemma 7.25. *Sei $(R; 0, 1; +, \cdot)$ ein kommutativer Ring so, dass R^* eine endliche Menge ist. Dann gelten für jedes Element $a \in R^*$:*

a) *Durch $n \mapsto a^n$ wird eine bijektive Abbildung*

$$\lambda_a : \{1, \ldots, \ ord(a)\} \to \langle a \rangle$$

definiert.

b) $\sharp\langle a \rangle = ord(a)$.

Beweis: Es genügt, die Aussage „a)“ zu zeigen.

„λ_a ist injektiv“ : Seien $m, n \in \{1, \ldots, \mathrm{ord}(a)\}$ mit $\lambda_a(m) = \lambda_a(n)$, d.h. mit $a^m = a^n$. Wir müssen zeigen, dass $m = n$. Nehmen wir das Gegenteil an! Dann gilt $m \neq n$. Ohne Einschränkung können wir annehmen, es gelte $m < n$. Dann gilt $n - m \in \mathbb{N}$, und aus 7.23 B) a) folgt $a^{n-m} = 1$. Damit gilt $\mathrm{ord}(a) \leq n - m < n \leq \mathrm{ord}(a)$, d.h. wir erhalten einen Widerspruch.

„λ_a ist surjektiv“ : Sei $u \in \langle a \rangle$. Wir müssen ein $m \in \{1, \ldots, \mathrm{ord}(a)\}$ so finden, dass $\lambda_a(m) = u$. Wir können $u = a^n$ für ein $n \in \mathbb{N}$ schreiben. Mit geeigneten Zahlen $q, r \in \mathbb{N}_0$ gelten dann:

$$n = q \ \mathrm{ord}(a) + r, \ r < \ \mathrm{ord}(a).$$

Es folgt $u = a^n = a^{q \ \mathrm{ord}(a) + r} = a^{q \ \mathrm{ord}(a)} a^r = (a^{\mathrm{ord}(a)})^q a^r = 1^q a^r = 1a^r = a^r$. Setzen wir nun

$$m := \begin{cases} \mathrm{ord}(a), & \text{falls } r = 0; \\ r, & \text{falls } r \neq 0, \end{cases}$$

so folgen $m \in \{1, \ldots, \mathrm{ord}(a)\}$ und $u = a^m = \lambda_a(m)$. ■

Lemma 7.26. *Sei $(R; 0, 1; +, \cdot)$ ein kommutativer Ring so, dass R^* eine endliche Menge ist. Sei $a \in R^*$. Dann gelten:*

a) *Für jedes $u \in R^*$ wird durch $x \mapsto ux$ eine Bijektion $\mu_u : R^* \to R^*$ definiert.*

b) *Sind $u, v \in R^*$ mit $\mu_u(\langle a \rangle) \cap \mu_v(\langle a \rangle) \neq \emptyset$, so folgt $\mu_u(\langle a \rangle) = \mu_v(\langle a \rangle)$.*

c) *Für alle $u \in R^*$ gilt $u \in \mu_u(\langle a \rangle)$.*

Beweis: „a)“ : Sei $u \in R^*$.

„μ_u ist injektiv“ : Seien $x, y \in R^*$ mit $\mu_u(x) = \mu_u(y)$. Dann folgt $ux = uy$, also $x = 1x = (u^{-1}u)x = u^{-1}(ux) = u^{-1}(uy) = (u^{-1}u)y = 1y = y$.

„μ_u ist surjektiv“ : Sei $z \in R^*$. Dann folgt $z = 1z = (uu^{-1})z = u(u^{-1}z) = \mu_u(u^{-1}z)$.

„b)“ : Sei $\mu_u(\langle a \rangle) \cap \mu_v(\langle a \rangle) \neq \emptyset$. Dann gibt es Elemente $x, y \in \langle a \rangle$ mit $\mu_u(x) = \mu_v(y)$ also mit $nx = uy$. Wir finden natürliche Zahlen s, t mit $x = a^s$ und $y = a^t$. Es folgt

$$(\alpha) \qquad ua^s = va^t.$$

Sei nun $z \in \mu_u(\langle a\rangle)$ beliebig gewählt. Es gibt dann ein $m \in \mathbb{N}$ so, dass $z = \mu_u(a^m) = ua^m$. Wir setzen $o = \mathrm{ord}(a)$. Dann folgt wegen $a^{so} = 1$ (s. 7.23 C) a)) sofort $z = ua^m = (ua^m)(a^{so}) = u(a^m a^{so}) = ua^{m+so}$. Wir schreiben $p = m + so$. Dann gilt $p \geq s$ und wir erhalten mit Hilfe von (α)

$$\begin{aligned} z &= ua^p = ua^{(p-s)+s} = u(a^{p-s}a^s) = u(a^s a^{p-s}) = (ua^s)a^{p-s} = (va^t)a^{p-s} \\ &= v(a^t a^{p-s}) = v(a^{t+p-s}) = \mu_v(a^{t+p-s}) \in \mu_v(\langle a\rangle). \end{aligned}$$

Damit ist gezeigt, dass $\mu_u(\langle a\rangle) \subseteq \mu_v(\langle a\rangle)$. Genauso folgt aber auch, dass $\mu_v(\langle a\rangle) \subseteq \mu_u(\langle a\rangle)$. Also gilt $\mu_u(\langle a\rangle) = \mu_v(\langle a\rangle)$.

„c)“ : Wegen $1 \in \langle a\rangle$ ist $u = u1 = \mu_u(1) \in \mu_u(\langle a\rangle)$. ■

Jetzt sind wir so weit, dass wir unser Hauptresultat über die Ordnung von Einheiten formulieren und beweisen können.

Satz 7.27. *Sei $(R; 0, 1; +, \cdot)$ ein kommutativer Ring so, dass R^* eine endliche Menge ist. Dann gelten für jede Einheit $a \in R^*$:*

a) $ord(a) | \sharp R^*$.

b) $a^{\sharp R^*} = 1$.

Beweis: „a)“ : Weil $\mu_u : R^* \to R^*$ für jedes $u \in R^*$ eine Bijektion ist (vgl. 7.26 a)) gilt (vgl. 7.25 b)):

(α) $$\sharp\mu_u(\langle a\rangle) = \sharp\langle a\rangle = \mathrm{ord}(a), \ (u \in R^*).$$

Nach 7.26 b), c) ist auch sofort klar:

(β) Jedes $x \in R^*$ liegt in genau einer der Mengen $\mu_u(\langle a\rangle)$.

(Dabei kann es natürlich vorkommen, dass $\mu_u(\langle a\rangle) = \mu_v(\langle a\rangle)$, obwohl $u \neq v$).

Ist r die Anzahl der verschiedenen Mengen $\mu_u(\langle a\rangle)$, d.h.

$$r := \sharp\{\mu_u(\langle a\rangle) | u \in R^*\},$$

so folgt aus (α) und (β) sofort $\sharp R^* = r \ \mathrm{ord}(a)$ (vgl. 3.26 B)), d.h. $\mathrm{ord}(a) | \sharp R^*$.

„b)“ : Klar aus Aussage a) und aus 7.23 C) a). ■

Nun möchten wir „von der Algebra wieder zur Zahlentheorie zurückkehren“. Wir tun dies, indem wir das eben Gezeigte auf Restklassenringe anwenden. Wir erhalten dann das folgende Ergebnis.

Korollar 7.28. *Sei $m \in \mathbb{N}\backslash\{1\}$ und sei $\varphi(m)$ definiert gemäss 7.20 A). Sei $a \in (\mathbb{Z}/m)^*$. Dann gelten:*

a) $ord(a)|\varphi(m)$.

b) $a^{\varphi(m)} = 1$.

Beweis: Klar aus 7.27 und 7.20 B). ■

Besonders wichtig ist der folgende Spezialfall des obigen Resultates.

Korollar 7.29. *Sei $p \in \mathbb{P}$ und sei $a \in (\mathbb{Z}/p)^*$. Dann gelten:*

a) $ord(a)|p-1$.

b) $a^{p-1} = 1$.

Beweis: Klar aus 7.28 weil $\varphi(p) = p - 1$. ■

Aufgaben 7.30. A) Bestimmen Sie ord(a) für alle $a \in (\mathbb{Z}/7)^*$.

B) Stellen Sie im „Siebzehneck“ $\mathbb{Z}/17$ die Mengen $\langle\overline{3}\rangle$ und $\langle\overline{7}\rangle$ durch Streckenzüge dar.

C) (*Kleiner Satz von Fermat*) Seien $p \in \mathbb{P}$ und $n \in \mathbb{Z}$ so, dass $p \nmid n$. Zeigen Sie, dass

$$n^{p-1} \equiv 1 \mod (p).$$

D) Seien $p \in \mathbb{P}$ und $n \in \mathbb{Z}$ so, dass $p \nmid n, n-1$. Zeigen Sie, dass $p|n^{p-2} + n^{p-3} + \cdots + 1$.

E) Bestimmen Sie für jede prime Restklasse $\overline{x} = a \in (\mathbb{Z}/11)^*$ die kleinste Zahl $n(a) \in \mathbb{N}_0$ so, dass $\overline{3}^{n(a)} = a$. •

Die algebraische Form des Chinesischen Restsatzes: ein Rückblick

Am Schluss von Kapitel 6 haben wir die „Restklassenversion“ des Chinesischen Restsatzes (6.15) anschaulich geometrisch interpretiert (siehe 6.17, 6.18). Im Sinne eines ergänzenden Rückblickes wollen wir nun auch zu einem vertieften algebraischen Verständnis des Chinesischen Restsatzes gelangen. Wir sind nämlich mittlerweile genügend weit in die Algebra vorgedrungen, dass dies ohne grossen Zusatzaufwand möglich ist. Zunächst einige Vorbereitungen:

Definitionen und Bemerkungen 7.31. A) Seien $(R; 0_R, 1_R; +, \cdot)$ und $(S; 0_S, 1_S; +, \cdot)$ zwei (kommutative) Ringe. Unter einem *Homomorphismus von R nach S* versteht man eine Abbildung $h : R \to S$ so, dass Folgendes gilt:

a) $h(1_R) = 1_s$;

b) $\forall x, y \in R : h(x + y) = h(x) + h(y);\ h(xy) = h(x)h(y)$.

Ist h zusätzlich bijektiv, so spricht man von einem *Isomorphismus von R nach S*.

B) Wir betrachten das kartesische Produkt

$$R \times S = \{(x, x') | x \in R, x' \in S\}$$

der Mengen R und S, welche den Ringen aus A) zugrunde liegen.

Wir führen folgende Elemente ein

a) $0 = 0_{R\times S} := (0_R, 0_S) \in R \times S$;

b) $1 = 1_{R\times S} := (1_R, 1_S) \in R \times S$.

Weiter definieren wir auf $R \times S$ „komponentenweise“ eine Addition und eine Multiplikation durch

c) $(x, x') + (y, y') := (x + y, x' + y')$; $\qquad (x, y \in R; x', y' \in S)$.

d) $(x, x')(y, y') := (xy, x'y')$.

Mit etwas Fleiss kann man nun leicht nachprüfen:

e) $(R \times S; 0_{R\times S}; 1_{R\times S}; +, \cdot)$ *ist ein kommutativer Ring.*

Man nennt diesen Ring das *Produkt der Ringe R und S* und schreibt dafür meist kurz $R \times S$. •

Nun kommen wir zur angekündigten algebraischen Vertiefung des Chinesischen Restsatzes. Es handelt sich um die nachfolgende Verschärfung von 6.15:

Satz 7.32. *(Algebraische Form des Chinesischen Restsatzes). Seien $m, n \in \mathbb{N}\backslash\{1\}$ teilerfremd. Dann ist die Abbildung*

$$\varepsilon : \mathbb{Z}/mn \to (\mathbb{Z}/m) \times (\mathbb{Z}/n)$$

aus 6.15 ein Isomorphismus (vom Ring $\mathbb{Z}/mn$ nach dem Produkt $(\mathbb{Z}/m) \times (\mathbb{Z}/n)$ der Ringe $\mathbb{Z}/m$ und $\mathbb{Z}/n$). ■

Damit haben wir den Chinesischen Restsatz in seine optimale Form gebracht: Aus einer Aussage über das Auffinden von Zahlen mit vorgegebenen Teilerresten ist nun ein Vergleichssatz für algebraische Strukturen geworden. Damit dürfte auch klar sein, dass es „Einiges gebracht hat“, den Chinesischen Restsatz für Restklassen zu formulieren ...

Aufgaben 7.33. A) Beweisen Sie Satz 7.32.

B) Seien R und S kommutative Ringe und sei $h : R \to S$ ein Isomorphismus. Zeigen Sie, dass auch die Umkehrabbildung $h^{-1} : S \to R$ ein Isomorphismus ist.

C) Seien R und S wie in Aufgabe B). Sei $h : R \to S$ ein Homomorphismus. Zeigen Sie:

a) $h(R^*) \subseteq S^*$.

b) Ist h ein Isomorphismus, so gilt $h(R^*) = S^*$. (*Hinweis:* B) verwenden.)

D) Seien R und S wie in Aufgabe B). Zeigen Sie, dass für den Ring $R \times S$ gilt:

$$(R \times S)^* = R^* \times S^*.$$

E) Zeigen Sie nochmals auf „algebraischem Wege“, dass man durch einschränken der Abbildung ε aus 6.15 eine bijektive Abbildung

$$\varepsilon\restriction: (\mathbb{Z}/mn)^* \to (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*$$

erhält. (*Hinweis:* Verwenden Sie 7.32 und die Aufgaben C) und D).) •

Zahlen als Funktionen: ein Ausblick

Nach dem vorangehenden Rückblick wollen wir aber auch einen Ausblick wagen.

Der Begriff des Restklassenkörpers modulo einer Primzahl, den wir in diesem Kapitel kennen gelernt haben, ist von grosser Bedeutung in der Zahlentheorie. Im Sinne eines Ausblickes wollen wir diesen Begriff deshalb nochmals von einer andern Seite beleuchten. Die Leitidee unserer Betrachtung ist, eine „ganze Zahl als Funktion“ zu verstehen.

Bemerkung 7.34. A) Sei $n \in \mathbb{Z}$. Niemand hindert uns daran, jeder Primzahl $p \in \mathbb{P}$ die Restklasse

$$n(p) := n + \mathbb{Z}p \in \mathbb{Z}/p\mathbb{Z}$$

zuzuordnen. Auf diese Weise erhalten wir eine „Funktion“ $n(\bullet)$, welche jedem „Punkt“ $p \in \mathbb{P}$ einen Wert $n(p)$ im Restklassenkörper $\mathbb{Z}/p$ zuordnet.

Um eine gewisse intuitive Idee der Situation zu erhalten, riskieren wir die folgende geometrische Veranschaulichung:

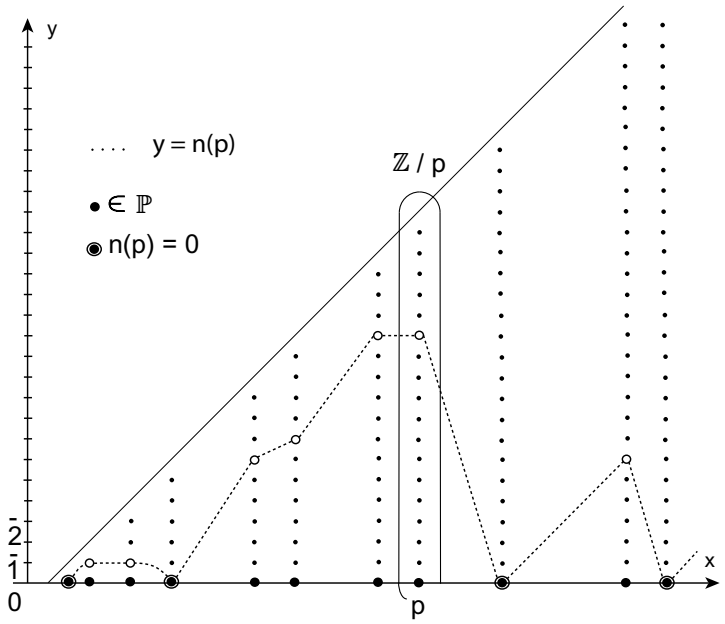


Abbildung 7.1: Graph von $p \mapsto n + \mathbb{Z}/p = n(p)$

B) Wir können natürlich auch beliebige Funktionen f betrachten, welche jeden Punkt $p \in \mathbb{P}$ eine Restklasse $f(p) \in \mathbb{Z}/p\mathbb{Z}$ zuordnen. Die Menge aller dieser Funktionen f bezeichnet man mit

$$\prod_{p\in\mathbb{P}} (\mathbb{Z}/p)$$

und nennt sie das *(direkte) Produkt* der Restklassenkörper $\mathbb{Z}/p$.

Natürlich gilt nun

$$n(\bullet) \in \prod_{p\in\mathbb{P}} (\mathbb{Z}/p),\ (n \in \mathbb{Z}).$$

Sind $f, g \in \prod_{p\in\mathbb{P}} \mathbb{Z}/p$, so können wir die *Summe* resp. das *Produkt von f und g* definieren durch

$$f + g,\ f \cdot g \in \prod_{p\in\mathbb{P}} (\mathbb{Z}/p) :$$
$$(f + g)(p) := f(p) + g(p);\ (f \cdot g)(p) := f(p)g(p), \quad (p \in \mathbb{P}).$$

Wir können also mit den Funktionen aus $\prod_{p\in\mathbb{P}}(\mathbb{Z}/p)$ in ähnlicher Weise rechnen, wie wir dies mit Funktionen im üblichen Sinn tun.

Nun prüft man leicht nach, dass für je zwei ganze Zahlen m, n gelten:

a) $\quad (m + n)(\bullet) = m(\bullet) + n(\bullet).$

b) $(mn)(\bullet) = m(\bullet)n(\bullet)$.

C) Wir definieren nun eine Abbildung

$$\iota : \mathbb{Z} \to \prod_{p\in\mathbb{P}} (\mathbb{Z}/p);\ (n \mapsto n(\bullet)).$$

Wir wollen uns überlegen, dass diese Abbildung injektiv ist.

Dazu wählen wir zwei Zahlen $m, n \in \mathbb{Z}$ so, dass $\iota(m) = \iota(n)$. Zu zeigen ist, dass $m = n$. Ohne Einschränkung können wir $m \leq n$ voraussetzen. Wegen $\sharp\mathbb{P} = \infty$ (s. 5.22) gibt es eine Primzahl p mit $n - m < p$. Wegen $\iota(m) = \iota(n)$ ist $m(\bullet) = n(\bullet)$. Insbesondere gilt $m(p) = n(p)$, also $m + \mathbb{Z}p = n + \mathbb{Z}p$. Dies bedeutet aber, dass $p|n - m$. Wegen $0 \leq n - m < p$ folgt daraus $n - m = 0$, also $n = m$.

Damit ist gezeigt, dass die Abbildung ι injektiv ist. Insbesondere können wir $\mathbb{Z}$ vermöge der Abbildung ι „einbetten in die Menge $\prod_{p\in\mathbb{P}}(\mathbb{Z}/p)$“. Anders gesagt, wir könne jeweils n und $\iota(n) = n(\bullet)$ identifizieren und so $\mathbb{Z}$ als Teilmenge von $\prod_{p\in\mathbb{P}}(\mathbb{Z}/p)$ auffassen. In diesem Sinn wird dann jede ganze Zahl zu einer Funktion in $\prod_{p\in\mathbb{P}}(\mathbb{Z}/p)$.

D) Sind $n \in \mathbb{Z}$ und $p \in \mathbb{P}$, so gilt für die Teilervielfachheit $\nu_p(n)$ von p in n (s. 4.26 A) b)):

$$\nu_p(n) > 0 \Longleftrightarrow p|n \Longleftrightarrow n(p) = \overline{0}.$$

Anders gesagt: $\nu_p(n)$ ist genau dann positiv, wenn die Funktion $n(\bullet)$ an der Stelle $p \in \mathbb{P}$ „verschwindet“ (d.h. den Wert $0 = \overline{0} = 0_{\mathbb{Z}/p}$ annimmt). Deshalb liegt es nahe, die *Verschwindungsordnung* $\mu_p(n(\bullet))$ *der Funktion* $n(\bullet)$ *an der Stelle* p zu definieren durch

$$\nu_p(n(\bullet)) := \nu_p(n).$$

Bei näherem Hinsehen ergibt sich eine auffällige Ähnlichkeit zum Beispiel aus 5.10:

- Die Menge $\mathbb{P}$ der Primzahlen hat die Rolle der Zahlengeraden $\mathbb{R}$ übernommen.
- Der Ring $\mathbb{Z}$ hat die Rolle des Polynomrings $\mathbb{R}[x]$ übernommen.
- Die Teilervielfachheit einer ganzen Zahl $n \neq 0$ an einer Stelle $p \in \mathbb{P}$ entspricht der Nullstellenvielfachheit eines Polynoms $f \in \mathbb{R}[x]\backslash\{0\}$ an einer Stelle $p \in \mathbb{R}$.

Die schon in 5.10 B) festgestellte Analogie zwischen den Bewertungen

$$\nu_p : \mathbb{Z}\backslash\{0\} \to \mathbb{N}_0,\ (n \mapsto \nu_p(n) = \nu_p(n(\bullet)));\ (p \in \mathbb{P})$$
$$\mu_p : \mathbb{R}[x]\backslash\{0\} \to \mathbb{N}_0,\ (f \mapsto \mu_p(f));\ (p \in \mathbb{R})$$

ist damit eingespannt in eine weitergehende Ähnlichkeit. Diese erweiterte Ähnlichkeit beruht darauf, dass wir die Menge $\mathbb{P}$ der Primzahlen als geometrisches Objekt aufgefasst haben – vergleichbar mit der Zahlengeraden $\mathbb{R}$. Ganze Zahlen entsprechen dann Polynomen und Teilervielfachheiten ensprechen Nullstellenordnungen.

E) Mit der soeben skizzierten „Geometrisierungsidee“ versuchten wir, zwei recht verschiedenartige Beispiele unter einen Hut zu bringen. Es stellt sich die Frage, ob es tatsächlich eine mathematische Theorie gibt, in der so unterschiedliche Objekte in einheitlicher Form behandelt werden können. Das Bestehen einer solchen Theorie würde die oben beobachtete Ähnlichkeit streng erklären.

Eine solche Theorie existiert in der Tat: die Theorie der *Schemata*, welche um 1960 von J. Dieudonné und A. Grothendieck entwickelt wurde. Schon unsere Beispiele legen nahe, dass in dieser Theorie die Grenze zwischen der Algebra/Arithmetik einerseits und der Geometrie andererseits weitgehend verschwindet. Bemerkenswert ist, dass einige der wichtigsten und tiefsten Resultate der neueren Zahlentheorie im Rahmen der Theorie der Schemata gewonnen wurden. Wir erwähnen als Beispiel den Beweis der sogenannten Mordellvermutung (eine Vermutung aus dem Jahre 1922), welcher 1983 durch G. Faltings erbracht wurde. •

Aufgaben 7.35. A) Zeigen Sie, dass die Menge $\prod_{p\in\mathbb{P}}(\mathbb{Z}/p)$ bezüglich der in 7.31 B) eingeführten Addition und Multiplikation ein kommutativer Ring mit Nullelement $0 = 0(\bullet)$ und Einselement $1 = 1(\bullet)$ ist.

B) Zeigen Sie, dass die Abbildung $\iota : \mathbb{Z} \to \prod_{p\in\mathbb{Z}}(\mathbb{Z}/p)$ ein Homomorphismus von Ringen ist.

C) Bestimmen Sie $\prod_{p\in\mathbb{P}}(\mathbb{Z}/p)^*$ und schliessen Sie, dass $\prod_{p\in\mathbb{P}}(\mathbb{Z}/p)$ kein Körper ist.

D) Sei $f \in \prod_{p\in\mathbb{P}}(\mathbb{Z}/p)$ und sei $r \in \mathbb{N}$. Zeigen Sie:

$$f^r = 0 \Longleftrightarrow f = 0.$$

E) Skizzieren Sie den Graphen der Funktion $30(\bullet) \in \prod_{p\in\mathbb{P}}(\mathbb{Z}/p)$ entsprechend der Abbildung 7.1.

F) Seien $m, n \in \mathbb{Z}$ so, dass $\sharp\{p \in \mathbb{P} | m(p) = n(p)\} = \infty$. Zeigen Sie, dass $m = n$. •

Teil D
Von der Arithmetik zur Geometrie: diophantische Gleichungen und rationale Punkte auf Kurven

ZUSAMMENFASSUNG

In diesem letzten Teil der Vorlesung behandeln wir die folgenden Kapitel:

- Diophantische Gleichungen
- Homogene quadratische diophantische Gleichungen
- Rationale Punkte auf Quadriken

Im ersten dieser Kapitel behandeln wir einige Typen diophantischer Gleichungen, ohne Anspruch auf Systematik und Vollständigkeit zu erheben. Zunächst geht es uns um *lineare diophantische Gleichungen in zwei Unbekannten*. Von diesen speziellen Gleichungen gelangen wir dann zu den diophantischen Gleichungen der Form $ax + by = f(z)$, wo a und b ganze Zahlen und $f(z)$ ein ganzzahliges Polynom in z ist. In diesen einfachen Fällen lässt sich in unserem Rahmen eine systematische Behandlung realisieren. Danach befassen wir uns mit den diophantischen Gleichungen $x^n + y^n = z^n$ ($n \in \mathbb{Z}_{\geq 2}$), wobei wir naturgemäss die Fälle $n = 2$ und $n > 2$ getrennt besprechen... Im Sinne der interdisziplinären Zielsetzung dieses letzten Teils der Vorlesung wollen wir das Lösen dieser diophantischen Gleichungen auch geometrisch als Suche nach Gitterpunkten auf einer Fläche verstehen.

Im Fall der Gleichungen $x^n+y^n = z^n$ werden wir einen Gedanken vorwegnehmen, welcher später die Motivation für das letzte Kapitel der Vorlesung liefert: den Zusammenhang zwischen den Lösungen einer solchen Gleichung – also den Gitterpunkten auf dem durch die Gleichung definierten Kegel – und den rationalen Punkten auf einem horizontalen

Schnitt durch diesen Kegel. Als horizontale Schnitte werden wir so die *Fermatkurven* finden und bereits die Frage nach rationalen Punkten auf einer Kurve als zahlentheoretisch relevant erkennen können.

Schliesslich streifen wir – im Sinne einer Schnupperlehre und nicht einer systematischen Behandlung – die *Gleichungen vom Pell'schen Typ*. Eine systematische Behandlung dieses Themas müsste sinnvollerweise die Kettenbruchentwicklung einbeziehen. Doch die Kettenbrüche ihrerseits ordnen sich dem Thema „Zahlen darstellen“ unter, das sich in dieser Vorlesung nicht mehr einbringen liess...

Kapitel 9 behandelt eine Klasse diophantischer Gleichungen, an der sich der Dualismus zwischen Arithmetik und Geometrie gut demonstrieren lässt: die *homogenen quadratischen diophantischen Gleichungen*. Um die Thematik einzuführen, werfen wir zuerst einen Blick auf die *pythagoräischen Tripel*, welche wir unter Zuhilfenahme einer rationalen Parametrisierung des Kreises bestimmen. Der Rückgriff auf eine solche Parametrisierung wäre an sich nicht notwendig; wir nehmen ihn aber vor, um an einem expliziten Beispiel nochmals die arithmetische Relevanz der Frage nach den rationalen Punkten auf einer Kurve vor Augen zu führen. Dann wenden wir uns den allgemeinen homogenen quadratischen diophantischen Gleichungen zu. Auch für diese diskutieren wir kurz den Zusammenhang zwischen den Lösungen und Punkten auf einer geeigneten ebenen Kurve. Im Anschluss daran befassen wir uns kurz mit der Frage, wann eine rationale Quadrik überhaupt rationale Punkte besitzt. Das sogenannte *Hasseprinzip*, das diese Frage allgemein beantwortet, übersteigt allerdings den Rahmen dieser Vorlesung. Wir werden uns also mit der Behandlung von Einzelfällen begnügen.

Was uns im Falle des Einheitskreises gelungen ist – nämlich die Parametrisierung aller rationalen Punkte – soll in Kapitel 10 auf beliebige (nichtausgeartete) *Quadriken* übertragen werden. Wir befassen uns dazu als erstes eingehend mit den ebenen Quadriken und deren Verhalten beim Schneiden mit Geraden. Im Sinne eines „Vertiefungsangebots“ sind wir hier bewusst ausführlicher als dies in der zur Verfügung stehenden Vorlesungszeit möglich ist. Wir hoffen aber, dass mindestens einige Studierende dies als Einladung verstehen, sich etwas eingehender mit der ebenen „analytischen“ (genauer algebraischen) Geometrie zu befassen.

Nach diesen allgemeinen Vorbereitungen werden wir dann Quadriken rational parametrisieren und so die in Kapitel 9 für den Einheitskreis angewandte Parametrisierungsmethode verallgemeinern. Insesondere werden wir mit dieser Methode aus einem einzigen rationalen Punkt auf einer rationalen Quadrik alle rationalen Punkte dieser Quadrik bestimmen können.

Zur Abrundung des Bildes werden wir auch kurz über *Parallelprojektionen* aus sogenannten „kritischen“ Richtungen sprechen und diese im Falle der Parabeln etwas genauer studieren.

TIPPS FÜR DAS SELBSTSTUDIUM

- *Kapitel 8:* Wichtig und grundlegend sind hier die Ausführungen über die linearen diophantischen Gleichungen (8.2–8.4). Zum Verständnis des Stoffes aus Kapitel 9 – und um eine erste Einsicht in den Zusammenhang zwischen Arithmetik und Geometrie zu gewinnen – sollten Sie sich relativ eingehend mit 8.7 und 8.8 befassen, aber auch die zugehörigen Aufgaben 8.9 mindestens zum Teil lösen. Das Thema der Pell'schen Gleichungen wird nicht umfassend behandelt, sondern eher als eine Einladung zum Ausprobieren und Knobeln. Hier sollten Sie (nach einem „Einlesen" bei 8.10) vor allem den Übungsaufgaben 8.11 Ihre Aufmerksamkeit schenken.

- *Kapitel 9:* Als Weg durch dieses Kapitel bietet sich etwa an: 9.1, mindestens ein Teil der Aufgabe 9.2, die rationale Parametrisierung des Einheitskreises (9.3) und die Bestimmung der pythagoräischen Tripel mit Hilfe des Satzes von Diophantos (9.6). Einige der Aufgaben aus 9.7 zu lösen wird ebenfalls empfohlen. Nicht schaden kann es auch, nochmals die in 9.8 rekapitulierte Idee durchzugehen. Zum Thema der homogenen quadratischen diophantischen Gleichungen im allgemeinen (9.11) empfehlen wir vor allem auch die Aufgaben 9.12 und 9.14. Dem Beispiel 9.15 und den Aufgaben 9.17 sollen Sie ebenfalls Bedeutung beimessen.

- *Kapitel 10:* Lassen Sie sich vom Umfang dieses stark auf „freiwillige Vertiefung" ausgerichteten Kapitels nicht entmutigen. Auch „Eilige" sollten die Vorbetrachtung in 10.1–10.3 mindestens intensiv durchlesen und die zugehörigen Aufgaben 10.4 nicht ganz verschmähen. Was hier zur Sprache gebracht wird ist „klassische mathematische Kultur". Wer mehr Zeit investieren kann und sich von etwas anspruchsvolleren Gedankengängen nicht abschrecken lässt, ist eingeladen weiter vorzudringen – etwa bis zum Hauptsatz 10.24. Der Weg bis zu diesem Meilenstein ist sicher nicht mit lockerem Schlendern zu schaffen – aber er ist so angelegt, dass er sich mit den Kenntnissen der Mittelschulmathematik, einem klaren Kopf und etwas Hartnäckigkeit begehen lässt. Wer „blindlings" der Algebra vertraut und auf die geometrische Anschauung verzichten will kann auf diesem Weg auch 10.6, 10.16, 10.17, 10.18 D) und 10.19 überspringen. Wenn Sie bis zum Etappenziel 10.24 gelangt sind, haben Sie sich vermutlich genügend „Fitness" erworben, um auch den verbleibenden kleinen Rest des Kapitels mit Leichtigkeit zu bezwingen...

Kapitel 8

Diophantische Gleichungen

Überblick

Diophantische Gleichungen sind (algebraische) Gleichungen mit ganzzahligen Koeffizienten in zwei oder mehr Unbekannten, bei welchen man nur nach den ganzzahligen Lösungen fragt. Diese Gleichungen werden so benannt nach Diophantos von Alexandria (3. Jh.).

Beispiele von diophantischen Gleichungen sind etwa

(8.0) a) $2x - 3y = 5$;

b) $x^2 + y^2 = z^2$;

c) $x^n + y^n = z^n$ $(n = 3, 4, \ldots)$;

d) $x^2 - 7y^2 = 1$;

d') $x^2 - 410286423278424y^2 = 1$.

Die Gleichung a) ist eine sogenannte *lineare diophantische Gleichung*. Vielleicht haben Sie diese Art Gleichung schon in der Schule kennen und lösen gelernt. Es handelt sich um Gleichungen, die schon in der früheren Antike und im alten China ausgiebig studiert wurden.

Die unter b) genannte diophantische Gleichung haben wir schon in 1.7 F) angetroffen und werden sie im nächsten Kapitel noch eingehender diskutieren. Die in c) aufgeführten diophantischen Gleichungen haben wir ebenfalls schon angetroffen (s. 1.9, 1.10). Vielleicht handelt es sich dabei um die „berühmtesten“ diophantischen Gleichungen überhaupt. Auch auf diese Gleichungen werden wir nochmals zurückkommen.

Die unter d) und d') genannten diophantischen Gleichungen sind sogenannte *Pell'sche Gleichungen*. Dieser Typ von Gleichungen wurde schon in der griechischen Antike, aber

auch von den indischen und arabischen Mathematikern des 7. bis 12. Jahrhunderts studiert und hat bis heute immer wieder das Interesse von Forschern und Tüftlern gefunden.

Mit diesem kleinen „Bouquet berühmter Gleichungen“ soll angetönt werden, dass wir uns mit den diophantischen Gleichungen in einem Kerngebiet der Zahlentheorie bewegen.

Zunächst ist das Lösen solcher diophantischer Gleichungen ein rein arithmetisches Problem. Doch ist es ein wichtiges Anliegen dieses Kapitels, auch die geometrische Natur dieses arithmetischen Problems aufzuzeigen. Mindestens andeutungsweise wagen wir damit den Blick in eine Richtung zu wenden, die sich in den letzten Jahrzehnten als besonders fruchtbar für die Zahlentheorie erwiesen hat: die *diophantische Geometrie*. Allerdings werden wir auch hier auf dem Boden der elementaren Arithmetik bleiben müssen, denn für Höhenflüge reicht unser „mathematischer Treibstoff“ nicht aus.

Folgende Themen werden wir behandeln:

- *Lineare diophantische Gleichungen mit zwei Unbekannten,*
- *Gleichungen der Form* $ax + by = f(z)$,
- *Die Gleichungen* $x^n + y^n = z^n$,
- *Pell'sche Gleichungen.*

Vom Stil her gesehen handelt es sich bei diesem Kapitel um eine „Schnupperlehre in Diophantik“ : Wir werden, ausser bei der Behandlung der linearen diophantischen Gleichungen, keine allgemeinen Sätze beweisen. Vielmehr wollen wir Einzelfälle und Beispiele betrachten, um so an das Gebiet der diophantischen Gleichungen heranzuführen.

Lineare diophantische Gleichungen mit zwei Unbekannten

Zuerst befassen wir uns mit diophantischen Gleichungen des in 8.0 a) genannten Typs, d.h. mit diophantischen Gleichungen der Form

$$ax + by = c \ (a, b, c \in \mathbb{Z}).$$

Dabei interessieren wir uns für *ganzzahlige Lösungen* dieser Gleichung, also für Lösungspaare $(x, y) \in \mathbb{Z}^2$. Wir werden ein Kriterium dafür angeben, dass die lineare diophantische Gleichung $ax + by = c$ überhaupt ganzzahlige Lösungen hat und eine Methode entwickeln, um diese Lösungen zu finden.

Wir beginnen mit dem folgenden Hilfsresultat.

Lemma 8.1. *Seien* $a, b \in \mathbb{Z}\backslash\{0\}$. *Seien* $w, z \in \mathbb{Z}$ *mit* $aw + bz = 0$. *Dann gibt es ein* $t \in \mathbb{Z}$ *so, dass* $w = \frac{tb}{\mathrm{ggT}(a,b)}$ *und* $z = \frac{-ta}{\mathrm{ggT}(a,b)}$.

Beweis: Sei $g = \mathrm{ggT}(a,b)$. Dann sind $\frac{a}{g}$ und $\frac{b}{g} \in \mathbb{Z}$ und es gilt $\frac{a}{g}w + \frac{b}{g}z = 0$, also

$$(\alpha) \qquad \frac{a}{g}w = -\frac{b}{g}z.$$

Nach 4.16 b) gibt es Zahlen $s, r \in \mathbb{Z}$ mit $as + br = g$. Es folgt $\frac{a}{g}s + \frac{b}{g}r = 1$, also mit Hilfe von (α)

$$\begin{aligned} w = 1 \cdot w &= \left(\frac{a}{g}s + \frac{b}{g}r\right) w = \\ &= s\frac{a}{g}w + rw\frac{b}{g} = -s\frac{b}{g}z + rw\frac{b}{g} = \\ &= (-sz + rw)\frac{b}{g}. \end{aligned}$$

Mit $t := -sz + rw$ folgt also $w = t\frac{b}{g}$. Mit (α) folgt $-\frac{b}{g}z = \frac{a}{g}w = \frac{b}{g}\frac{a}{g}t$, d.h. in der Tat auch $z = -\frac{a}{g}t$. ■

Im folgenden Satz werden die linearen diophantischen Gleichungen abschliessend behandelt.

Satz 8.2. *Seien $a, b \in \mathbb{Z}\backslash\{0\}$ und $c \in \mathbb{Z}$. Dann gelten:*

a) *Die Gleichung*

$$ax + by = c$$

besitzt genau dann eine ganzzahlige Lösung $(x_0, y_0) \in \mathbb{Z}^2$, wenn $\mathrm{ggT}(a,b)|c$.

b) *Ist $(x_0, y_0) \in \mathbb{Z}^2$ eine Lösung der obigen Gleichung und ist $(x, y) \in \mathbb{Z}^2$ ein weiteres Paar ganzer Zahlen, so gilt*

$$ax + by = c$$

genau dann, wenn es eine Zahl $t \in \mathbb{Z}$ gibt mit

$$x = x_0 + t\frac{b}{\mathrm{ggT}(a,b)} \text{ und } y = y_0 - t\frac{a}{\mathrm{ggT}(a,b)}.$$

Beweis: Sei $g := \mathrm{ggT}(a,b)$. „a)“ : Nehmen wir zunächst an, unsere Gleichung habe eine ganzzahlige Lösung $(x_0, y_0) \in \mathbb{Z}^2$, sodass $ax_0 + by_0 = c$. Wegen $g|a$ und $g|b$ folgt dann $g|c$.

Es gelte umgekehrt $g|c$. Mit einer geeigneten Zahl $d \in \mathbb{Z}$ gilt dann $c = dg$. Nach 4.16 b) gibt es Zahlen $u, v \in \mathbb{Z}$ mit $au + bv = g$. Mit $x_0 := ud$ und $y_0 := vd$ folgt dann $ax_0 + by_0 = c$. Also ist (x_0, y_0) eine ganzzahlige Lösung unserer Gleichung.

„b)“ : Sei $t \in \mathbb{Z}$ und seien $x = x_0 + t\frac{b}{g}$ und $y = y_0 - t\frac{a}{g}$. Dann folgt $ax + by = a(x_0 + t\frac{b}{g}) + b(y_0 - t\frac{a}{g}) = ax_0 + by_0 + t(a\frac{b}{g} - b\frac{a}{g}) = ax_0 + by_0 + t \cdot 0 = c$.

Sei umgekehrt $(x, y) \in \mathbb{Z}^2$ mit $ax + by = c$. Es folgt $a(x - x_0) + b(y - y_0) = ax + by - ax_0 - by_0 = c - c = 0$, also $\frac{a}{g}(x - x_0) + \frac{b}{g}(y - y_0) = 0$. Nach 8.1 gibt es ein $t \in \mathbb{Z}$ mit $x - x_0 = \frac{b}{g}t$ und $y - y_0 = -\frac{a}{g}t$. Es folgen $x = x_0 + \frac{b}{g}t$ und $y = y_0 - \frac{a}{g}t$. ■

Bemerkungen 8.3. A) Leicht prüft man nach, dass die Aussagen a) und b) im Satz 8.2 auch richtig sind, wenn eine der beiden Zahlen a oder b Null ist.

B) Satz 8.2 und sein Beweis belehren uns darüber, wie wir die Lösungsmenge

a) $$\mathbb{L} := \left\{(x, y) \in \mathbb{Z}^2 | ax + by = c\right\}$$

der diophantischen Gleichung $ax + by = c$ (mit $(a, b) \neq (0, 0)$) bestimmen:

Sei $g := \mathrm{ggT}(a, b)$ und seien $u, v \in \mathbb{Z}$ mit $au + bv = g$. Ist $g \nmid c$, so ist $\mathbb{L} = \emptyset$. Sei also $g|c$. Dann sieht man aus dem Beweis von 8.2, dass das Zahlenpaar

$$(x_0, y_0) := \left(\frac{c}{g}u, \frac{c}{g}v\right)$$

eine Lösung unserer diophantischen Gleichung ist. Nach 8.2 b) folgt deshalb

b) $$\mathbb{L} = \left\{ \left(\frac{c}{g}u + t\frac{b}{g}, \frac{c}{g}v - t\frac{a}{g}\right) \middle| t \in \mathbb{Z} \right\}.$$

C) Geometrisch können wir das Lösen unserer diophantischen Gleichung leicht verstehen:

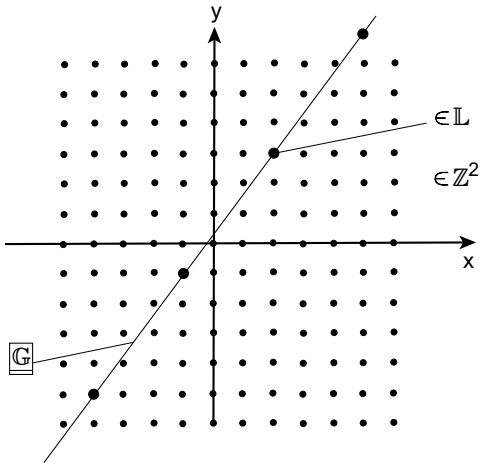


Abbildung 8.1: Lösungen der diophantischen Gleichung $4x - 3y = -1$

Die *reelle Lösungsmenge*

$$\mathbb{G} := \{(x, y) \in \mathbb{R}^2 | ax + by = c\}$$

entspricht einer *Geraden* in der Ebene $\mathbb{R}^2$. Die ganzzahlige Lösungsmenge $\mathbb{L}$ ist die Menge $\mathbb{G} \cap \mathbb{Z}^2$ der *Gitterpunkte* auf der Geraden $\mathbb{G}$, d.h. der Geradenpunkte mit ganzzahligen Koordinaten. •

Aufgaben 8.4. A) Lösen Sie die diophantische Gleichung $-x + 2y = 3$ und skizzieren Sie die Situation.

B) Geben Sie alle möglichen diophantischen Gleichungen $ax + by = c$ an, welche im Rechteck $\{(x, y)|0 \leq x \leq 2, 0 \leq y \leq 1\}$ mindestens 2 verschiedene Lösungen haben.

C) Geben Sie alle möglichen diophantischen Gleichungen $ax + by = 1$ an, welche zwei verschiedene Lösungen mit einem Abstand echt kleiner als 4 besitzen (nur Fälle mit $ab \neq 0$).

D) Seien $a, b, c \in \mathbb{Z}$ mit $a, b \neq 0$ und $\text{ggT}(a, b)|c$. Geben Sie den kleinstmöglichen Abstand d zweier verschiedener Lösungen der diophantischen Gleichung $ax + by = c$ in der Ebene $\mathbb{R}^2$ an.

E) Seien $a, b, c \in \mathbb{Z}$ und $d \in \mathbb{R}$ definiert wie in Aufgabe D). Sei $\delta := \frac{c}{\sqrt{a^2+b^2}}$. Zeigen Sie:

a) Der Nullpunkt hat von der durch $ax + by = c$ definierten Geraden den Abstand $|\delta|$.

b) Die diophantische Gleichung $ax + by = c$ hat mindestens eine und höchstens zwei ganzzahlige Lösungen $(x, y) \in \mathbb{Z}^2$ mit einem Abstand kleiner oder gleich $\sqrt{\delta^2 + \frac{d^2}{4}}$ vom Nullpunkt.

F) Bestimmen Sie alle ganzzahligen Lösungen $(x, y) \in \mathbb{Z}^2$ der Gleichung $2x^2 - 3y^2 - 5xy + x + 11y = 6$. (*Hinweis:* Zerlegung in Linearfaktoren.) •

Gleichungen der Form $ax + by = f(z)$

Gewisse einfache diophantische Gleichungen mit drei Unbekannten lassen sich mit dem in 8.3 beschriebenen Verfahren ebenfalls lösen. Wir führen dazu die nachfolgenden Gedanken an:

Bemerkungen 8.5. A) Sei $f(z)$ ein ganzzahliges Polynom. Seien $a, b \in \mathbb{Z}\backslash\{0\}$. Wir möchten die diophantische Gleichung

a) $$ax + by = f(z)$$

lösen, d.h. alle ganzzahligen Lösungstripel $(x, y, z) \in \mathbb{Z}^3$ der Gleichung a) finden. Dazu kann man wie folgt vorgehen:

Zuerst sucht man wieder zwei Zahlen $u, v \in \mathbb{Z}$ mit $au + bv = \mathrm{ggT}(a, b) =: g$. Nach 8.3 B) ist dann klar, dass die Lösungen der diophantischen Gleichung a) gerade die Zahlentripel der Form

b) $$\left(\frac{f(z)}{g}u + t \cdot \frac{b}{g}, \frac{f(z)}{g}v - t\frac{a}{g}, z\right);\ (t, z \in \mathbb{Z}, g|f(z))$$

sind. Für beliebiges f ist die Bedingung $g|f(z)$ nicht leicht zu kontrollieren. Deshalb führt diese Methode eigentlich nur im Fall wo a und b teilerfremd sind, d.h. wo $g = 1$ gilt, sicher zu Ziel.

B) Geometrisch kann man die soeben gelöste Aufgabe so verstehen: Die Menge aller reellen Lösungen (x, y, z) der Gleichung a) bildet eine Fläche $\mathbb{F}$ im Raum $\mathbb{R}^3$. Die ganzzahligen Lösungen b) sind die Gitterpunkte dieser Fläche, d.h. die Punkte der Menge $\mathbb{F} \cap \mathbb{Z}^3$.

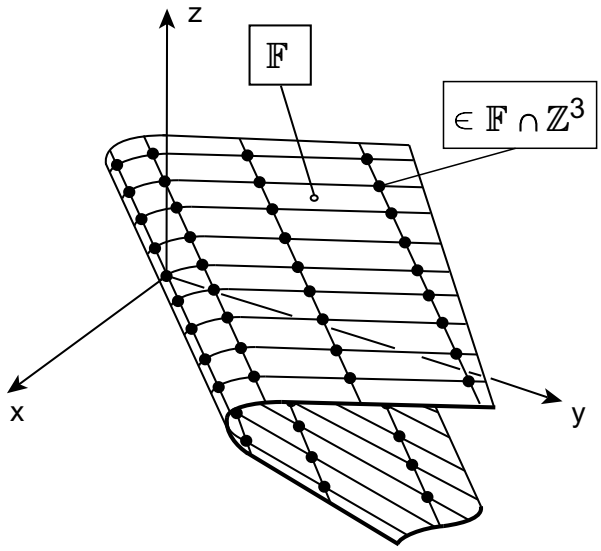


Abbildung 8.2: Lösungen von $ax + by = f(z)$

•

Aufgaben 8.6. A) Lösen Sie die diophantische Gleichung

$$x + y = z$$

gemäss 8.5 und skizzieren Sie den geometrischen Sachverhalt.

B) Lösen Sie Aufgabe A) mit der diophantischen Gleichung

$$-x + y = z^2.$$

C) Beschreiben Sie die Menge aller ganzzahligen Lösungstripel (x, y, z) der Gleichung

$$2x - 6y = z^2 + 1.$$

D) Wie muss $b \in \mathbb{Z}$ gewählt werden, damit die diophantische Gleichung

$$5x - by = 10z^4 - 11$$

keine Lösung hat. Welches sind andernfalls ihre Lösungen, falls zudem noch $b \in \{0, 1, 2, 3, 4, 5\}$ gilt? •

Die Gleichungen $x^n + y^n = z^n$

Vielleicht etwas provokativ wollen wir nun die in 8.0 b) und c) genannten Gleichungen zum Anlass einer weiteren Überlegung nehmen. Wir können dabei nämlich wieder etwas Neues über die geometrisch-arithmetische Doppelnatur der diophantischen Gleichungen lernen. Dass die betrachteten Gleichungen für $n \geq 3$ (angeblich) keine interessanten ganzzahligen Lösungen haben (vgl. 1.10 A)), stört uns dabei wenig.

Beispiel 8.7. A) Wir wählen $n \in \mathbb{N}$ und betrachten die diophantische Gleichung

a) $$x^n + y^n = z^n.$$

Anders gesagt, wir interessieren uns für die Menge aller Tripel $(x, y, z) \in \mathbb{Z}^3$, welche der obigen Gleichung genügen. Für $n = 1$ sollte uns diese Gleichung keine Schwierigkeiten bieten (s. 8.5). Wir nehmen also an, es sei $n \geq 2$. Natürlich hat die Gleichung a) einfach zu findende Lösungen $(x, y, z) \in \mathbb{Z}^3$, wenn eine der drei Zahlen x, y und z gleich 0 ist. Diese sogenannten *trivialen Lösungen* wollen wir nicht mehr ins Auge fassen. Wir wollen also insbesondere annehmen, es sei $z \neq 0$.

B) Wir missachten alles, was wir im Fall $n \geq 3$ über die Gleichung A) a) schon gelesen und gehört haben und im Fall $n = 2$ vielleicht schon wissen (vgl. 1.6, 1.7, 1.10). Wir fragen also nach Lösungen (x, y, z) der Gleichung A) a) in $\mathbb{Z}^3$ mit $z \neq 0$. Die Ausführungen aus 8.5 legen es nahe, die Anzahl der Unbekannten von 3 auf 2 zu reduzieren. Dies lässt sich in der Tat tun, allerdings auf neuartige Weise:

Ist $(x, y, z) \in \mathbb{Z}^3$ eine Lösung der Gleichung A) a) so, dass $z \neq 0$, dann gilt mit

$$u := \frac{x}{z},\ v := \frac{y}{z} \in \mathbb{Q}$$

die Gleichung

a) $$u^n + v^n = 1.$$

Sind umgekehrt $u, v \in \mathbb{Q}$ mit $u^n + v^n = 1$, so können wir einen gemeinsamen Nenner $z \in \mathbb{Z}\backslash\{0\}$ von u und v suchen. Dann gilt mit

$$x := uz,\ y := vz \in \mathbb{Z}$$

die Beziehung $x^n+y^n = u^n z^n+v^n z^n = (u^n+v^n)z^n = z^n$. Also ist (x, y, z) eine ganzzahlige Lösung der Gleichung A) a). Damit ist gezeigt:

b)
$$\left\{\begin{array}{l} \textit{Sind } u, v \in \mathbb{Q} \textit{ mit } u^n + v^n = 1 \textit{ und ist } z \in \mathbb{Z}\backslash\{0\} \textit{ so, dass} \\ uz, vz \in \mathbb{Z}, \textit{ dann ist das Zahlentripel} \\ \qquad\qquad (uz, vz, z) \in \mathbb{Z}^3 \\ \textit{eine ganzzahlige Lösung der Gleichung } x^n + y^n = z^n. \end{array}\right.$$

Zudem ist *jede* Lösung der diophantischen Gleichung $x^n + y^n = z^n$ nach dem Verfahren b) zu finden.

Insgesamt kommt es also auf dasselbe heraus, ob wir ganzzahlige Lösungen der Gleichung A) a) oder rationale Lösungen der Gleichung B) a) suchen.

C) Wir wollen uns nun auch Klarheit verschaffen über die Geometrie, die sich hinter dem soeben beschriebenen Konzept verbirgt. Wir betrachten die Menge

a) $$\mathbb{K} := \{(x, y, z) \in \mathbb{R}^3 | x^n + y^n = z^n\}$$

aller *reellen Lösungstripel* $(x, y, z) \in \mathbb{R}^3$ der Gleichung A) a). Dabei fällt uns folgendes auf:

Sind $(x, y, z) \in \mathbb{K}$ und $\lambda \in \mathbb{R}$, so folgt $(\lambda x)^n + (\lambda y)^n = \lambda^n x^n + \lambda^n y^n = \lambda^n(x^n + y^n) = \lambda^n z^n = (\lambda z)^n$, also $(\lambda x)^n + (\lambda y)^n = (\lambda z)^n$, d.h. $(\lambda x, \lambda y, \lambda z) \in \mathbb{K}$. Schreiben wir

$$\mathbb{R}(x, y, z) := \{(\lambda x, \lambda y, \lambda z) | \lambda \in \mathbb{R}\},$$

so gilt also:

b) $$(x, y, z) \in \mathbb{K} \Longrightarrow \mathbb{R}(x, y, z) \subseteq \mathbb{K}.$$

Ist $(x, y, z) \in \mathbb{K}\backslash\{(0, 0, 0)\}$, so ist $\mathbb{R}(x, y, z)$ die durch $(0, 0, 0)$ und (x, y, z) laufende Gerade. Wie wir eben festgestellt haben, liegt diese Gerade ganz in $\mathbb{K}$. Anders gesagt: $\mathbb{K}$ enthält mit jedem Punkt $(x, y, z) \in \mathbb{K}\backslash\{(0, 0, 0)\}$ auch die ganze Gerade durch $(0, 0, 0)$ und den Punkt (x, y, z). Damit ist $\mathbb{K}$ ein sogenannter *Kegel mit Spitze* $(0, 0, 0)$.

Wir halten die Situation in der nachfolgenden Skizze fest, für welche wir $n = 2$ gewählt haben.

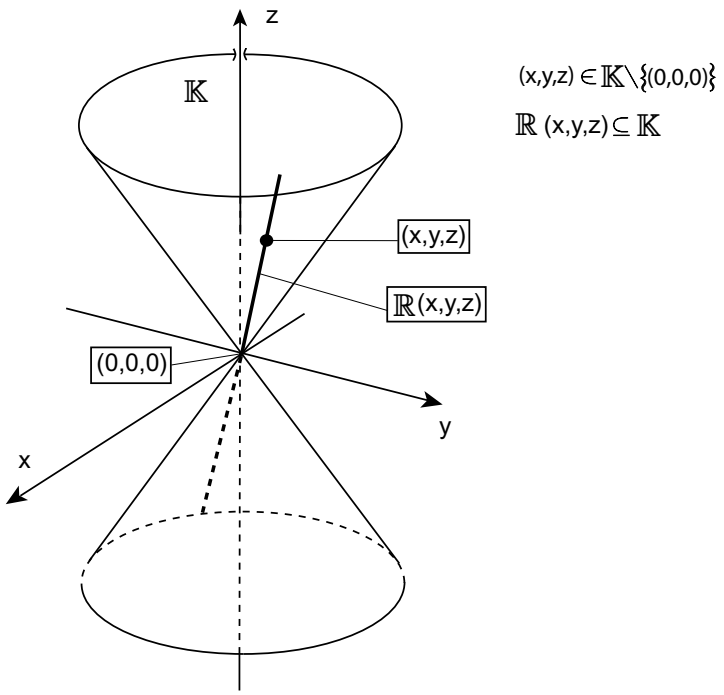


Abbildung 8.3: Kegel zur Gleichung $x^2 + y^2 = z^2$

D) Wir sind allerdings nicht an allen reellen Lösungstripeln der Gleichung A) a) interessiert, sondern nur an der Menge

$$\mathbb{K} \cap \mathbb{Z}^3 = \{(x, y, z) \in \mathbb{Z}^3 | x^n + y^n = z^n\}$$

der ganzzahligen Lösungstripel der Gleichung A) a). Anders gesagt: Uns interessieren *Gitterpunkte auf* $\mathbb{K}$. In B) b) haben wir bereits angegeben, wie man diese Gitterpunkte erhält, wenn man die rationalen Lösungspaare $(u, v) \in \mathbb{Q}^2$ der Gleichung B) a) kennt. Die Gleichung B) a) erhält man aber aus der Gleichung A) a), indem man $z = 1$ setzt und u resp. v für x resp. y schreibt. Das Lösen der Gleichung B) a) entspricht also dem

Schneiden des Kegels $\mathbb{K}$ mit der durch $z = 1$ definierten Ebene $\mathbb{E}$. Das Aufsuchen der rationalen Lösungen von B) a) entspricht deshalb dem Aufsuchen aller Punkte $(u, v, 1)$ auf der Schnittkurve $\mathcal{C} := \mathbb{E} \cap \mathbb{K}$ mit $(u, v) \in \mathbb{Q}^2$. Hat man einen solchen Punkt $(u, v, 1)$ gefunden, so sucht man einen gemeinsamen Nenner z von u und v und erhält so den Gitterpunkt $(uz, vz, z) \in \mathbb{K} \cap \mathbb{Z}^3$. Dieser Gitterpunkt liegt dann auf der Geraden

$$m := \mathbb{R}(u, v, 1) \subseteq \mathbb{K},$$

also auf der *Kegelmantellinie* durch $(u, v, 1)$. So lassen sich leicht alle Gitterpunkte von $\mathbb{K}$ finden, welche auf dieser Mantellinie liegen. Lässt man schliesslich (u, v) alle rationalen Lösungspaare von B) a) durchlaufen, so findet man alle Gitterpunkte $(x, y, z) \in \mathbb{Z}^3 \cap \mathbb{K}$ mit $z \neq 0$.

Geometrisch lässt sich die Situation wie folgt veranschaulichen (auch hier wurde $n = 2$ gewählt):

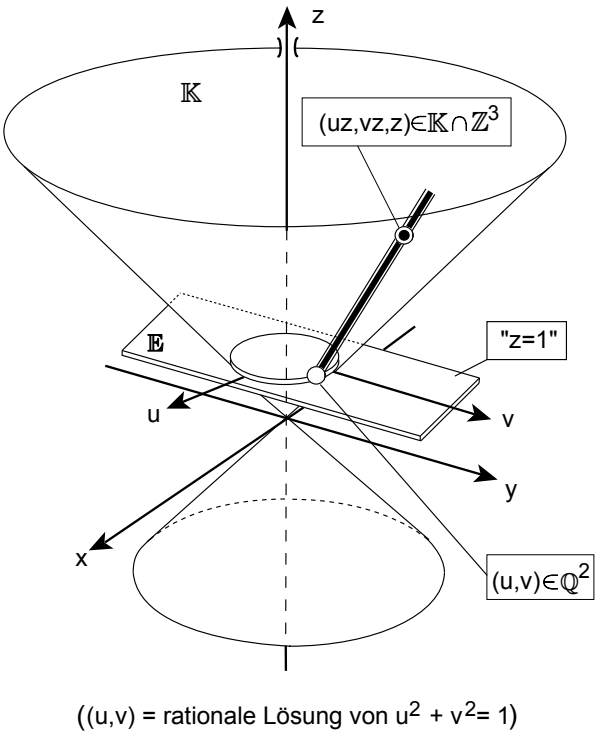


Abbildung 8.4: Lösungen von $x^2 + y^2 = z^2$ und $u^2 + v^2 = 1$

E) Nachdem wir nun den Zusammenhang zwischen den ganzzahligen Lösungen der Gleichung A) a) und den rationalen Lösungen B) a) geometrisch interpretiert haben, wollen wir die Gleichung B) a) selbst geometrisch betrachten.

Die Menge

$$\mathbb{M} := \{(u, v) \in \mathbb{R}^2 | u^n + v^n = 1\}$$

aller *reellen Lösungspaare* $(u, v) \in \mathbb{R}^2$ von B) a) bildet eine Kurve in der Ebene $\mathbb{R}^2$.

Wir betrachten diese Kurven $\mathbb{M}$ für $n = 1, 2, 3, 4$. Die Schnittpunkte von $\mathbb{M}$ mit den Koordinatenachsen nennen wir *triviale Punkte*. Sie werden mit $\circ$ markiert.

Für $n = 1$ ist $\mathbb{M}$ eine Gerade. Für $n = 2$ ist $\mathbb{M}$ ein Kreis. Ist $n \geq 3$, so nennt man $\mathbb{M}$ die *n-te Fermatkurve*. Allgemein nennt man die Lösungsmenge $\mathbb{M} \subseteq \mathbb{R}^2$ einer algebraischen Gleichung vom Grad n in zwei Unbekannten eine *Kurve vom Grad n*.
Man sagt, eine solche Kurve sei eine Quadrik, eine Kubik, eine Quartik, eine Quintik, eine Sextik, ... je nachdem, ob es sich um eine Kurve vom Grad $2, 3, 4, 5, 6, \ldots$ handelt. Entsprechend redet man von der Fermatkubik, -quartik, -quintik, -sextik, ...

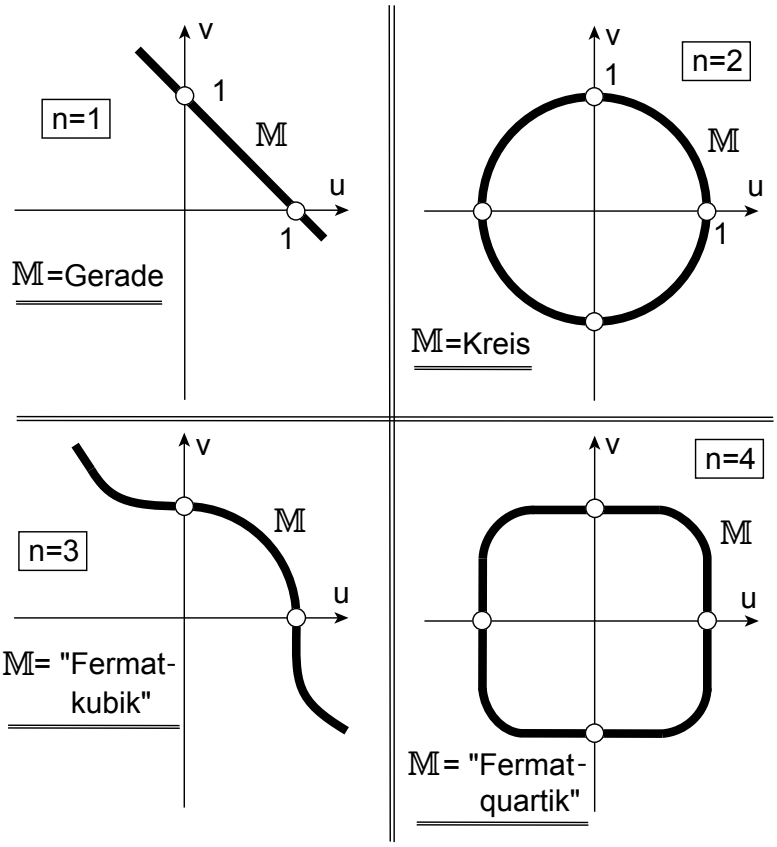


Abbildung 8.5: Lösungskurven der Gleichung $u^n + v^n = 1$

F) Sie hatten in 1.10 A) bereits die Möglichkeit, sich zur diophantischen Gleichung A) a) zu äussern und dabei wohl richtig festgestellt:

a) *Ist $n \geq 3$, so hat die Gleichung $x^n + y^n = z^n$ nur triviale ganzzahlige Lösungstripel (x, y, z), d.h. solche mit $xyz = 0$.*

Die Frage, ob dies wirklich so sei, geht auf Pierre de Fermat (1601–1665) zurück und hat als *grosses Fermatproblem* die Mathematik 350 Jahre lang beschäftigt. Für den Exponenten $n = 4$ wurde diese Vermutung bereits von Fermat selbst bewiesen. Im Jahre 1753 lieferte L. Euler (1707–1783) einen Beweis für den Exponenten $n = 3$. Nach immer wieder neuen Teilresultaten wurde das grosse Fermatproblem schliesslich im Jahre 1994 durch R. Taylor und A. Wiles vollständig gelöst, indem sie zeigten, dass die Aussage F) a) für jeden Exponenten $n \geq 3$ gilt. •

Bemerkung 8.8. A) Die Aussage a) aus 8.7 F) besagt, dass wir in 8.7 ausführlich über das Lösen diophantischer Gleichungen gesprochen haben, für die es in den meisten Fällen gar keine Lösung gibt. Dies erweckt den Eindruck, wir hätten in 8.7 viel Lärm um (fast) nichts gemacht.

Dieser Eindruck ist allerdings nicht richtig, denn die in 8.7 B) entwickelte Idee und die in 8.7 C), D) gezogenen geometrischen Schlussfolgerungen lassen sich auf eine grosse Klasse diophantischer Gleichungen übertragen, nämlich auf die sogenannten *homogenen diophantischen Gleichungen*. Bei diesen Gleichungen haben alle auftretenden Potenzprodukte der Unbekannten den gleichen Grad. Diesen Grad nennt man den *Grad der homogenen diophantischen Gleichung*. So ist etwa

a) $$x^3 + 3xy^2 - xyz + 7z^3 = 4yz^2$$

eine homogene Gleichung vom Grad 3 und

b) $$x^4 - xyz^2 + 11z^4 = 0$$

eine homogene Gleichung vom Grad 4.

B) Die Aussage b) aus 8.7 B) gilt nun sinngemäss für jede homogene diophantische Gleichung. Um die entsprechende Aussage zu formulieren, denken wir uns eine homogene diophantische Gleichung der Form

a) $$F(x, y, z) = 0$$

gegeben. Dazu betrachten wir auch die Gleichung

b) $$f(u, v) := F(u, v, 1) = 0,$$

welche aus a) durch umbenennen der Unbekannten und einsetzen von $z = 1$ entsteht. Dann gilt in Verallgemeinerung von 8.7 B) b) Folgendes:

c) $$\begin{cases} \textit{Sind } u, v \in \mathbb{Q} \textit{ mit } f(u, v) = 0 \textit{ und ist } z \in \mathbb{Z}\backslash\{0\} \textit{ derart, dass} \\ uz, vz \in \mathbb{Z}\textit{, so ist das Tripel } (uz, vz, z) \in \mathbb{Z}^3 \textit{ eine Lösung der} \\ \textit{homogenen diophantischen Gleichung } F(x, y, z) = 0\ . \end{cases}$$

Umgekehrt lässt sich auch hier jedes ganzzahliges Lösungstripel $(x, y, z) \in \mathbb{Z}^3$ der Gleichung a) mit $z \neq 0$ durch die in c) beschriebenen Methode finden.

C) Weil $F(x, y, z) = 0$ eine homogene Gleichung ist, gilt in den Bezeichnungen von 8.7 C) für die Menge

a) $$\mathbb{K} := \{(x, y, z) \in \mathbb{R}^3 | F(x, y, z) = 0\}$$

wieder die Aussage (vgl. 8.7 C) b)):

b) $$(x, y, z) \in \mathbb{K} \Longrightarrow \mathbb{R}(x, y, z) \subseteq \mathbb{K}.$$

Damit ist $\mathbb{K}$ auch hier wieder ein Kegel mit Spitze $(0, 0, 0)$, und die ganzzahligen Lösungen der homogenen diophantischen Gleichung B) a) sind die Gitterpunkte auf dem Kegel $\mathbb{K}$. Geometrisch besteht also auch hier eine Situation, die genau dem entspricht, was wir in 8.7 D) angetroffen haben. •

Aufgaben 8.9. A) Formulieren Sie den Satz von Taylor-Wiles als eine Aussage über die in 8.7 eingeführten Fermatkurven.

B) Zeigen Sie: Sind $a \in \mathbb{Q}\backslash\{0, 1, -1\}$ und $n \geq 3$, so ist $\sqrt[n]{1 - a^n}$ kein Bruch (*Hinweis:* A) verwenden).

C) Zeigen Sie, dass die Aussage aus B) nicht gilt, wenn $n = 2$.

D) Sei $\mathbb{M}_n$ die n-te Fermatkurve. Bestimmen Sie $a_n > 0$ so, dass $(a_n, a_n) \in \mathbb{M}_n$, und bestimmen Sie $\lim_{n\to\infty} a_n$.

E) Sei $\mathbb{M}_n$ wie in Aufgabe D). Sei $u \in]-1, 1[$. Bestimmen Sie $v_n > 0$ so, dass $(u, v_n) \in \mathbb{M}_n$. Berechnen Sie $\lim_{n\to\infty} v_n$.

F) Sei $u \in \mathbb{R}$ mit $|u| > 1$. Bestimmen Sie $w_k \in \mathbb{R}$ so, dass $(u, w_k) \in \mathbb{M}_{2k+1}$. Berechnen Sie $\lim_{k\to\infty} w_k$.

G) Skizzieren Sie den Kegel $\mathbb{K}$ aus 8.7 C) für $n = 3$ und $n = 4$ und stellen Sie die Situation entsprechend der Abbildung 8.4 dar.

H) Zeigen Sie, dass die Aussage b) aus 8.8 C) für die beiden Gleichungen 8.8 A) a), b) gilt. •

Pell'sche Gleichungen

Die diophantischen Gleichungen der Form

$$x^2 - dy^2 = 1;\ (d \in \mathbb{N}, \sqrt{d} \notin \mathbb{N})$$

heissen *Pell'sche Gleichungen*. Diese Gleichungen sind nach dem englischen Mathematiker John Pell (1610–1685) benannt, wohl fälschlicherweise: Alles deutet darauf hin, dass Pell selbst sich nicht mit diesen Gleichungen befasst hat. Die unter 8.0 d) und d') aufgeführten Gleichungen sind von diesem Typ (zumindest für die Gleichung d) besteht darüber kein Zweifel).

Bemerkungen 8.10. A) Bereits im 12. Jahrhundert beschrieb Bhaskara d. J. (1114–1191) eine allgemeine Lösungsmethode für Pell'sche Gleichungen ohne zu beweisen, dass die Methode wirklich immer zu einem Ergebnis führt. J. L. Lagrange (1736–1813) bewies im Jahre 1768, dass jede Pell'sche Gleichung unendlich viele Lösungen hat.

B) Schon Brahmagupta (598–670) kannte eine Methode, um aus einer nichttrivialen Lösung einer Pell'schen Gleichung neue Lösungen zu finden:

a) *Ist* $d \in \mathbb{N}$ *mit* $\sqrt{d} \notin \mathbb{N}$, *ist* $(x, y) \in \mathbb{N}^2$ *mit* $x^2 - dy^2 = 1$ *und ist* $n \in \mathbb{N}$, *so gibt es eindeutig bestimmte Zahlen* $x_n, y_n \in \mathbb{N}$ *mit* $x_n + y_n\sqrt{d} = (x + y\sqrt{d})^n$. *Für diese Zahlen gilt dann*

$$x_n^2 + dy_n^2 = 1;$$

d.h. (x_n, y_n) *ist wieder eine Lösung der gegebenen Pell'schen Gleichung.*

Wählt man etwa $n = 2$, so gilt $(x + y\sqrt{d})^2 = x^2 + 2xy\sqrt{d} + y^2d = (x^2 + y^2d) + (2xy)\sqrt{d}$, also $x_2 = x^2 + dy^2$ und $y_2 = 2xy$.

Gilt $x^2 - dy^2 = 1$, so folgt in der Tat

$$\begin{aligned} & x_2^2 - dy_2^2 \\ &= (x^2 + dy^2)^2 - 4dx^2y^2 \\ &= x^4 + 2dx^2y^2 + d^2y^4 - 4dx^2y^2 \\ &= x^4 - 2dx^2y^2 + d^2y^4 = (x^2 - dy^2)^2 = 1^2 = 1, \end{aligned}$$

d.h.

$$x_2^2 - dy_2^2 = 1.$$

Von Brahmagupta stammt auch die folgende Aussage:

b) *Wer innerhalb eines Jahres ein Lösungspaar* $(x, y) \in \mathbb{N}^2$ *der Gleichung*

$$x^2 - 92y^2 = 1$$

findet, ist ein(e) Mathematiker(in).

C) Ist d nicht zu gross, so lässt sich manchmal durch ausprobieren leicht die *kleinste nichttriviale Lösung* einer Pell'schen Gleichung finden (d.h. die Lösung $(x, y) \in \mathbb{N}^2$ mit kleinstem y):

Man berechnet dazu der Reihe nach die Zahlen

$$1^2, d2^2, d3^2, \ldots, dy^2, \ldots$$

und prüft jedesmal nach, ob $dy^2 + 1$ das Quadrat einer natürlichen Zahl x ist.

Ist dies der Fall, so ist $(x, y) \in \mathbb{N}^2$ eine Lösung der Gleichung $x^2 - dy^2 = 1$.

Im Fall $d = 5$ ergibt sich etwa

y	1	2	3	4	$\cdots$
$dy^2 + 1$	6	21	46	$81 = 9^2$	$\cdots$

$$\underline{\underline{9^2 - 5 \cdot 4^2 = 1}}.$$

Also ist $(9, 4)$ die kleinste nichttriviale Lösung der Pell'schen Gleichung $x^2 - 5y^2 = 1$.

D) Die Menge

a) $$\mathbb{H} := \{(x, y) \in \mathbb{R}^2 | x^2 - dy^2 = 1\}$$

aller *reellen Lösungspaare* (x, y) der Pell'schen Gleichung $x^2 - dy^2 = 1$ bildet eine Hyperbel mit den Scheitelpunkten $(1, 0)$ und $(-1, 0)$ und den Asymptoten $y = \pm\sqrt{d}^{-1}x$. Die ganzzahligen Lösungen dieser Gleichung sind also gerade die Gitterpunkte auf der Hyperbel $\mathbb{H}$:

b) $$\{(x, y) \in \mathbb{Z}^2 | x^2 - dy^2 = 1\} = \mathbb{Z}^2 \cap \mathbb{H}.$$

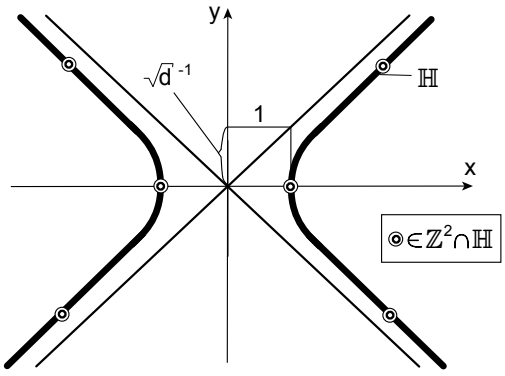


Abbildung 8.6: Lösungskurve einer Pell'schen Gleichung

•

Aufgaben 8.11. A) Bestimmen Sie die minimalen Lösungen der folgenden Pell'schen Gleichungen:

$$x^2 - 2y^2 = 1,\ x^2 - 3y^2 = 1,\ x^2 - \ 7y^2 = 1,$$
$$x^2 - 6y^2 = 1,\ x^2 - 8y^2 = 1,\ x^2 - 10y^2 = 1.$$

B) Sei $d \in \mathbb{N}$ mit $\sqrt{d} \notin \mathbb{N}$. Seien $x, y, x', y' \in \mathbb{N}$ so, dass $x + y\sqrt{d} = x' + y'\sqrt{d}$. Zeigen Sie, dass $x = x'$ und $y = y'$ (*Hinweis:* 2.8 beachten).

C) Sei $d \in \mathbb{N}$ mit $\sqrt{d} \notin \mathbb{N}$ und sei $(x, y) \in \mathbb{N}^2$ mit $x^2 - dy^2 = 1$. Wir definieren die Paare $(x_n, y_n) \in \mathbb{N}^2$ $(n = 1, 2, 3, \ldots)$ durch

$$x_n = \begin{cases} x, & \text{falls } n = 1; \\ xx_{n-1} + dyy_{n-1}, & \text{falls } n > 1, \end{cases};$$
$$y_n = \begin{cases} y, & \text{falls } n = 1; \\ xy_{n-1} + x_{n-1}y, & \text{falls } n > 1. \end{cases}$$

Zeigen Sie durch Induktion über n:

a) $x_n^2 - dy_n^2 = 1.$

b) $x_n + y_n\sqrt{d} = (x + y\sqrt{d})^n.$

c) $x_n - y_n\sqrt{d} = (x - y\sqrt{d})^n.$

D) Sei $d \in \mathbb{N}$ so, dass $d + 2$ das Quadrat einer natürlichen Zahl ist. Zeigen Sie, dass das Paar $\left(d + 1, \sqrt{d + 2}\right)$ eine Lösung der Pell'schen Gleichung $x^2 - dy^2 = 1$ ist.

E) Wenden Sie D) mit $d = 23$ und dann C) mit $n = 2$ an um zu zeigen, dass Sie ein(e) Mathematiker(in) sind.

F) Sei $d \in \mathbb{N}$ mit $\sqrt{d} \notin \mathbb{N}$. Zeigen Sie:

Ist $(x, y) \in \mathbb{N}^2$ eine Lösung der Pell'schen Gleichung $x^2 - dy^2 = 1$, so gilt

$$x = \min\left\{n \in \mathbb{N} \,\middle|\, n > \sqrt{d}y\right\}.$$

G) Versuchen Sie (z. B. im Internet) ausfindig zu machen, worin der Ruhm der Gleichung 8.0 d') bestehen könnte und berichten Sie kurz über das Gefundene.

H) Beweisen Sie ohne Rechner und nur unter Verwendung der letzten drei Ziffern im Zahlkoeffizienten der Gleichung 8.0 d'), dass diese Gleichung wirklich eine Pell'sche Gleichung ist (*Hinweis:* Durch 8 teilen!).

I) Geben Sie jeweils 3 verschiedene nichttriviale Lösungspaare $(x, y) \in \mathbb{N}^2$ der Pell'schen Gleichungen

$$x^2 - 14y^2 = 1, \; x^2 - 34y^2 = 1$$

an. (*Hinweis:* Aufgaben C), E).)

J) (*Square-Town*) Ein quadratisches Wohnquartier besteht aus lauter gleich grossen quadratischen Parzellen. Zwei Parzellen werden als Spielplatz genutzt. Auf jeder anderen Parzelle steht ein Einfamilienhaus, von denen jedes einen quadratischen Sitzplatz hat. Dabei sind alle Sitzplätze gleich gross. Zwischen dem Wohnquartier und dem in ca. 45 m Entfernung vorbeifliessenden Fluss befindet sich ein quadratischer Parkplatz, der eine unwesentlich grössere Fläche hat als alle Sitzplätze zusammen (Unterschied weniger als 0.2m^2. Alle Plätze sind mit ganzen quadratischen Platten der Grösse $40\text{cm} \times 40\text{cm}$ belegt. Auf jedem Sitzplatz liegen gleichviele Platten wie es im Quartier Parzellen hat.

Wie viele Häuser stehen höchstens im Quartier?

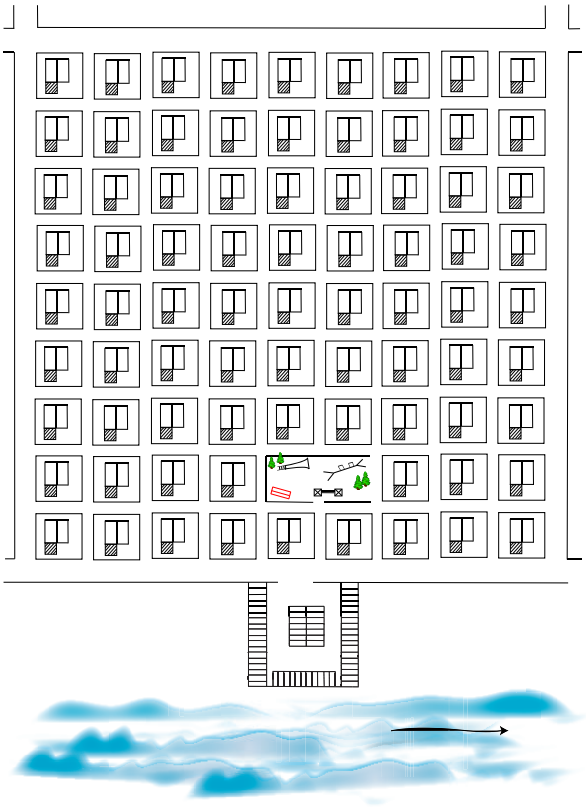


Abbildung 8.7: Square-Town

•

Kapitel 9

Homogene quadratische diophantische Gleichungen

Überblick

Wir beginnen dieses Kapitel mit der Bestimmung der sogenannten *pythagoräischen Tripel*. Wir greifen dazu auf die in 8.7 gemachte Beobachtung zurück, dass es dazu genügt, die rationalen Punkte auf dem Einheitskreis „zu bestimmen“. Zur Bestimmung dieser rationalen Punkte verwenden wir die schon in Aufgabe 1.7 ins Spiel gebrachte Idee der „*rationalen Parametrisierung des Einheitskreises*“. In Tat und Wahrheit könnten wir die pythagoräischen Tripel auch ohne dieses geometrische Hilfsmittel bestimmen. Doch dann würde uns der schöne Zusammenhang zwischen der Arithmetik und der Geometrie entgehen, der für eine grössere Klasse von diophantischen Gleichungen besteht: Alle Lösungen einer sogenannten *(nichtausgearteten) homogenen quadratischen diophantischen Gleichung* lassen sich mit Hilfe einer geometrischen Methode aus einer einzigen nichttrivialen Lösung berechnen.

Das Lösen (nichtausgearteter) homogener quadratischer diophantischer Gleichungen zerfällt also in zwei Teilschritte:

- Entscheiden, ob eine nichttriviale Lösung existiert und bestimmen einer solchen;
- Explizite Beschreibung aller Lösungen mit Hilfe der im ersten Schritt bestimmen Einzellösung.

Der erste Teilschritt ist rein arithmetischer Art und beruht auf einer Methode, die wir im Rahmen dieser Vorlesung nicht behandeln können – dem sogenannten *Hasseprinzip*.

Der zweite Teilschritt beruht auf der geometrischen Idee der *rationalen Parametrisierung von Quadriken*. Eine detaillierte Behandlung dieser Methode würde den Rahmen dieses Kapitels allerdings sprengen. Wir verlegen dieses Thema deshalb ins nächste Kapitel.

Trotzdem wollen wir uns unentwegt daran machen, die im Titel genannten Gleichungen zu behandeln. Im einzelnen kommen folgende Themen zur Sprache:

- *Pythagoräische Tripel,*
- *Rationale Parametrisierung des Einheitskreises,*
- *Bestimmung der phythagoräischen Tripel,*
- *Von der Geometrie zur Arithmetik: ein Rückblick,*
- *Homogene quadratische diophantische Gleichungen,*
- *Zur Existenz nichttrivialer Lösungen.*

Pythagoräische Tripel

Wir befassen uns als erstes mit den sogenannten *pythagoräischen Tripeln*, d.h. mit den nichttrivialen Lösungen der diophantischen Gleichung $x^2+y^2=z^2$. Das Ziel ist schliesslich die Bestimmung aller dieser Tripel und zwar auf dem Weg, der schon in den Aufgaben 1.6 und 1.7 nahe gelegt wurde. Zunächst machen wir allerdings eine allgemeine Vorbetrachtung über pythagoräische Tripel.

Definition und Bemerkung 9.1. A) Ein *pythagoräisches Tripel* ist ein Tripel $(x, y, z) \in \mathbb{N}^3$ natürlicher Zahlen so, dass $x^2 + y^2 = z^2$.

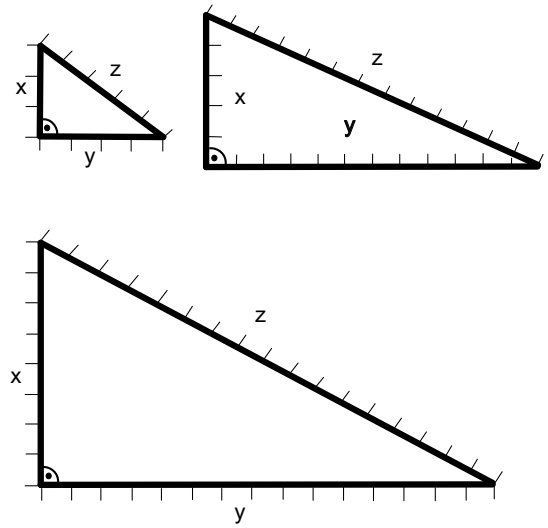


Abbildung 9.1: Pythagoräische Tripel

B) Schon in der Antike hat man nach der Menge aller pythagoräischen Tripel gesucht, und Diophantos hat zu diesem Problem die Lösung gefunden. Wir wollen dieses Problem nochmals im Lichte der Bemerkung 8.7 betrachten, wie wir das im Prinzip schon in 1.6 und 1.7 gemacht haben.

Es geht also darum, alle Lösungstripel $(x, y, z) \in \mathbb{Z}^3$ der diophantischen Gleichung $x^2 + y^2 = z^2$ (d.h. der Gleichung a) aus 8.7 A) mit $n = 2$) zu finden, die zudem noch der Nebenbedingung $0 < x \leq y \leq z$ genügen sollen. Ist $(x, y, z) \in \mathbb{Z}^3$ ein Lösungstripel mit $x, y, z \neq 0$, so lässt sich durch Vorzeichenwechsel und allfälliges Vertauschen von x und y ein Lösungstripel gewinnen, das unserer Nebenbedingung genügt. Wenn wir im Moment die Nebenbedingung ausser acht lassen, geht es somit genau um das Lösen der diophantischen Gleichung $x^2 + y^2 = z^2$. Nach 8.7 B) sind wir also mit dem Problem konfrontiert, die *rationalen Punkte auf dem Einheitskreis*

$$\mathbb{M} = \{(u, v) \in \mathbb{R}^2 | u^2 + v^2 = 1\}$$

„zu bestimmen“. •

Aufgaben 9.2. A) Interpretieren Sie diese antike Werbeanzeige (*Hinweis:* vgl. 1.6).

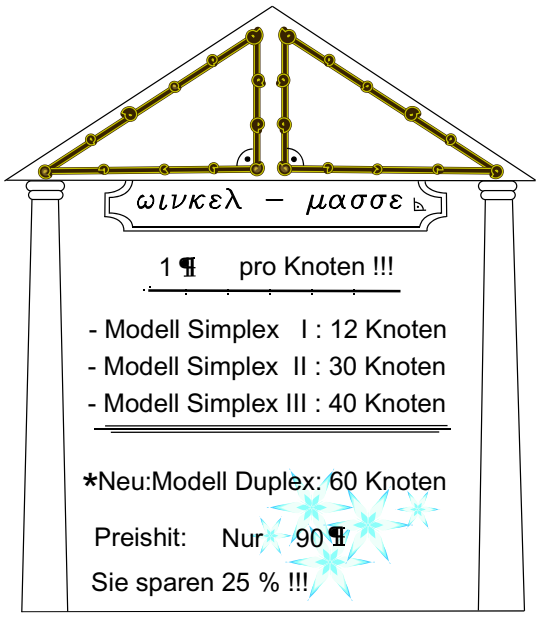


Abbildung 9.2: Antike Werbeanzeige

B) Sei $(x, y, z) \in \mathbb{N}^3$ ein pythagoräisches Tripel. Zeigen Sie die folgende Implikation: $x \in \mathbb{P} \Longrightarrow y = \frac{x^2-1}{2} \wedge z = \frac{x^2+1}{2}$. (*Hinweis:* Schreiben Sie $x^2 = \ldots$).

C) Sei $(x, y, z) \in \mathbb{N}^3$ ein pythagoräisches Tripel mit $x \leq y$. Zeigen Sie, dass $x < y$ und $y \notin \mathbb{P}$.

D) Zeigen Sie, dass es zu jedem ungeraden $x \in \mathbb{N}_{\geq 3}$ genau ein pythagoräisches Tripel (x, y, z) gibt, für welches $z = y + 1$ gilt. Drücken Sie y und z durch x aus.

E) Zeigen Sie, dass es unendlich viele pythagoräische Tripel (x, y, z) so gibt, dass $z = y+1$ gilt und dass z eine Quadratzahl ist (*Hinweis:* z durch x ausdrücken, 8.10 A) oder – noch besser – 8.10 B) a) resp. 8.11 C), D) verwenden). •

Rationale Parametrisierung des Einheitskreises

Bereits in Aufgabe 1.7 haben wir ein geometrisches Verfahren vorgeschlagen, welches erlaubt, die rationalen Punkte auf dem Einheitskreis „zu bestimmen“, d.h. in befriedigender Weise zu beschreiben. Es handelt sich dabei um eine sogenannte *rationale Parametrisierung des Einheitskreises*. Wir wollen nun die in Aufgabe 1.7 vorgeschlagene rationale Parametrisierung nochmals eingehend diskutieren.

Konstruktion 9.3. (vgl. 1.7 A)) A) Wir betrachten den Einheitskreis

$$\mathbb{M} = \{(u, v) \in \mathbb{R}^2 | u^2 + v^2 - 1 = 0\}.$$

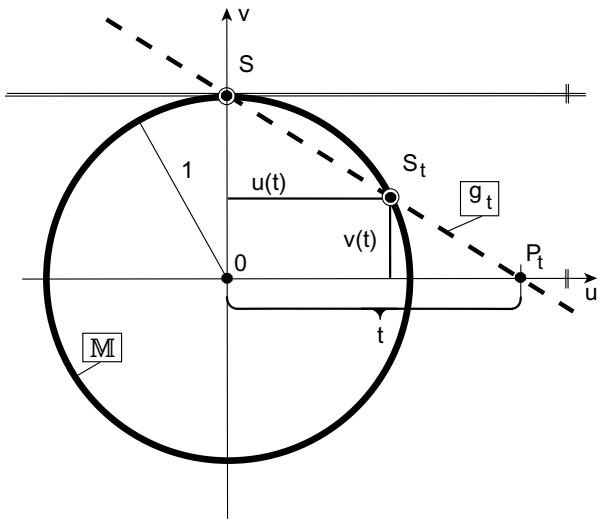


Abbildung 9.3: Parametrisierung des Einheitskreises

Dann wählen wir einen „Parameterwert“ $t \in \mathbb{R}$ und betrachten die Gerade g_t, welche die beiden Punkte

$$P_t := (t, 0) \text{ und } S := (0, 1)$$

verbindet. Die Gerade g_t schneidet $\mathbb{M}$ in S und einem weiteren Punkt S_t. Die Koordinaten von S_t bezeichnen wir mit $u(t)$ und $v(t)$, also

$$S_t = (u(t), v(t)) \,;\, \mathbb{M} \cap g_t = \{S, S_t\}.$$

Die Gerade g_t hat die Parameterdarstellung

$$s \mapsto \overrightarrow{0S} + s\overrightarrow{SP_t} = (0,1) + s(t,-1) = (st, 1-s).$$

Um S_t zu suchen, muss man s so wählen, dass $(st, 1-s) \in \mathbb{M}$. Dies führt zur Gleichung

$$(st)^2 + (1-s)^2 - 1 = 0.$$

Die linke Seite dieser Gleichung lässt sich schreiben als

$$s^2t^2 + 1 - 2s + s^2 - 1 = s^2t^2 + s^2 - 2s = s\left(s(t^2+1) - 2\right).$$

So erhalten wir die Gleichung

$$s\left(s(t^2+1) - 2\right) = 0.$$

Diese Gleichung hat die beiden Lösungen

$$s = 0 \text{ und } s = \frac{2}{t^2+1}.$$

Für $s = 0$ erhalten wir den Schnittpunkt S. Für $s = \frac{2}{t^2+1}$ erhalten wir also den Schnittpunkt $S_t = (u(t), v(t))$. Einsetzen von $s = \frac{2}{t^2+1}$ in die Parameterdarstellung a) liefert demnach

$$(u(t), v(t)) = S_t = \left(\frac{2t}{t^2+1}, 1 - \frac{2}{t^2+1}\right) = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right),$$

d.h.

$$u(t) = \frac{2t}{t^2+1} \text{ und } v(t) = \frac{t^2-1}{t^2+1}.$$

(Die geometrische Überlegung aus der Musterlösung zu 1.7 hat mit andern Bezeichnungen das Gleiche geliefert.)

B) Insbesondere besteht nun eine Abbildung

$$\varepsilon : \mathbb{R} \to \mathbb{M}\backslash\{S\},\ t \mapsto \varepsilon(t) := (u(t), v(t)) = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right).$$

Schon aus der geometrischen Situation ist klar, dass ε bijektiv ist. Um diese Bijektivität rein algebraisch zu zeigen, kann man aber auch die Abbildung

$$\iota : \mathbb{M}\backslash\{S\} \to \mathbb{R},\ (u,v) \mapsto \iota(u,v) := \frac{u}{1-v}$$

einführen und nachrechnen, dass ι die Umkehrabbildung von ε ist, d.h. dass

a) $$\iota(\varepsilon(t)) = t \text{ für alle } t \in \mathbb{R} \text{ und}$$

b) $$\varepsilon(\iota(u,v)) = (u,v) \text{ für alle } (u,v) \in \mathbb{M}\backslash\{S\}.$$

Die Abbildung ε ist eine sogenannte *rationale Parametrisierung von* $\mathbb{M}$ (genauer von $\mathbb{M}\backslash\{S\}$), da ihre Komponentenfunktionen $u(t)$ und $v(t)$ rationale Funktionen sind.

C) Schliesslich wollen wir uns überlegen, dass für eine reelle Zahl $t \in \mathbb{R}$ die folgende Äquivalenz besteht:

$$t \in \mathbb{Q} \Longleftrightarrow \varepsilon(t) \in \mathbb{Q}^2.$$

Wegen $\varepsilon(t) = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right)$ ist die Implikation „$\Longrightarrow$“ sofort klar. Ist umgekehrt $\varepsilon(t) = (u,v) \in \mathbb{Q}^2$, so gilt $t = \iota(\varepsilon(t)) = \iota(u,v) = \frac{u}{1-v} \in \mathbb{Q}$.

Damit ist aber gezeigt:

- *Durch Einschränken von ε erhält man eine bijektive Abbildung*

$$\varepsilon\restriction\colon \mathbb{Q} \to \mathbb{Q}^2 \cap (\mathbb{M}\backslash\{S\}),\ t \mapsto \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right).$$

Die Abbildung $\varepsilon\restriction$ liefert also eine *Parametrisierung von* $\mathbb{Q}^2 \cap (\mathbb{M}\backslash\{S\})$ *durch die Menge* $\mathbb{Q}$ *der rationalen Zahlen.* Wir sprechen auch von einer *Parametrisierung der rationalen Punkte auf* $\mathbb{M}$ oder einer *Parametrisierung der rationalen Lösungen der Gleichung* $u^2 + v^2 - 1 = 0$.

Insbesondere lässt sich die *Menge* $\mathbb{Q}^2 \cap \mathbb{M}$ *der rationalen Punkte auf* $\mathbb{M}$ einfach beschreiben:

a) $$\mathbb{Q}^2 \cap \mathbb{M} = \varepsilon(\mathbb{Q}) \cup \{S\} = \left\{ \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right) \middle| t \in \mathbb{Q} \right\} \cup \{(0,1)\}.$$

•

Aufgaben 9.4. A) Wir betrachten den Einheitskreis

$$\mathbb{M} = \{(u,v) \in \mathbb{R}^2 | u^2 + v^2 - 1 = 0\}$$

und die Abbildung (d.h. die Parametrisierung von $\mathbb{M}$)

$$\varphi : \mathbb{R} \to \mathbb{M},\ \alpha \mapsto (\cos(\alpha), \sin(\alpha)).$$

Bestimmen Sie $\varphi^{-1}(u,v)$ für einen beliebigen Punkt $(u,v) \in \mathbb{M}$.

B) Es gelten die Bezeichnungen von A). Zeigen Sie, dass die Menge $\mathbb{S} := \varphi^{-1}(\mathbb{Q}^2 \cap \mathbb{M})$ folgende Eigenschaften hat:

a) $0 \in \mathbb{S}$;

b) $\alpha \in \mathbb{S} \Rightarrow -\alpha \in \mathbb{S}$;

c) $\alpha, \beta \in \mathbb{S} \Rightarrow \alpha + \beta \in \mathbb{S}$, (*Hinweis:* Additionstheoreme);

d) $\alpha \in \mathbb{S}, n \in \mathbb{Z} \Rightarrow \alpha + 2n\pi \in \mathbb{S}$.

C) Rechnen Sie nach, dass die Aussagen c) und d) aus 9.3 B) tatsächlich gelten.

D) Skizzieren Sie auf dem Einheitskreis die Punkte $\varepsilon(0), \varepsilon(1), \varepsilon(2), \varepsilon(3), \ldots$ und bestimmen Sie $\lim_{n\to\infty} \varepsilon(n)$ (vgl. 9.3).

E) Zeigen Sie, dass $(2n, n^2 - 1, n^2 + 1)$ für jedes $n \in \mathbb{N}_{\geq 2}$ ein pythagoräisches Tripel ist.

F) Lösen Sie nochmals die Aufgabe 1.7 B)–E), falls Sie es damals nicht schafften. •

Bestimmung der pythagoräischen Tripel

Mit Hilfe der oben beschriebenen *Parametrisierung der rationalen Lösungen der Gleichung* $u^2 + v^2 - 1 = 0$ wollen wir nun pythagoräische Tripel $(x, y, z) \in \mathbb{N}^3$ bestimmen.

Bemerkungen und Definition 9.5. A) Seien $m, n \in \mathbb{N}$. Wir wollen uns überlegen:

a) *Sind* m *und* n *ungerade, so gelten* $m^2+n^2 \equiv 2 \mod (4)$ *und* $m^2-n^2 \equiv 0 \mod (4)$.

In der Tat gelten mit geeigneten Zahlen $k, l \in \mathbb{Z}$ die Gleichungen $m = 2k + 1$ und $n = 2l + 1$, und es folgen

$$m^2 + n^2 = (2k + 1)^2 + (2l + 1)^2 = 4(k^2 + l^2 + k + l) + 2,$$
$$m^2 - n^2 = (2k + 1)^2 - (2l + 1)^2 = 4(k^2 + l^2 + k - l).$$

B) Sei $z \in \mathbb{N}$. Dann gilt $z^2 \not\equiv 2 \bmod(4)$, was man sich wie folgt überlegt: Falls z ungerade ist, so ist es auch z^2, und es folgt $z^2 \not\equiv 2 \bmod(4)$. Ist z gerade, so gilt $z = 2n$ für ein geeignetes $n \in \mathbb{N}$. Damit erhalten wir aber $z^2 = 4n^2 \equiv 0 \bmod(4) \not\equiv 2 \bmod(4)$. Aus der ersten Kongruenz in A) a) folgt damit sofort:

a) *Ist* (x, y, z) *ein pythagoräisches Tripel, so ist mindestens eine der Zahlen* x *oder* y *gerade.*

C) Ein *primitives pythagoräisches Tripel* ist ein pythagoräisches Tripel (x, y, z) so, dass

$$\mathrm{ggT}(x, y) = 1 \text{ und } 2|x.$$

Für ein solches Tripel (x, y, z) gelten offenbar

a) $$2 \nmid y \text{ und } \mathrm{ggT}(x, z) = \mathrm{ggT}(y, z) = 1.$$

D) Ein beliebiges pythagoräisches Tripel (x, y, z) entsteht immer, indem in einem geeigneten primitiven pythagoräischen Tripel (x_0, y_0, z_0) alle Komponenten mit einer geeigneten Zahl $k \in \mathbb{N}$ multipliziert und dann allenfalls noch die ersten beiden Komponenten vertauscht werden:

Ist nämlich $k = \mathrm{ggT}(x, y)$, so folgt $k^2|(x^2 + y^2) = z^2$, also $k|z$. Mit geeigneten Zahlen $x_0, y_0, z_0 \in \mathbb{N}$ gelten also $x = kx_0, y = ky_0$ und $z = kz_0$, und wegen $k^2(x_0^2+y_0^2) = x^2+y^2 = z^2 = k^2z_0^2$ ist (x_0, y_0, z_0) wieder ein pythagoräisches Tripel. Dabei ist $\mathrm{ggT}(x_0, y_0) = 1$. Gemäss Aussage B) a) können wir nach allfälligem Vertauschen von x_0 und y_0 annehmen, es gelte $2|x_0$. •

Nun können wir die angekündigte Charakterisierung der pythagoräischen Tripel vornehmen.

Satz 9.6. *(Satz von Diophantos) Die primitiven pythagoräischen Tripel sind genau die Tripel der Form*

$$(2mn, m^2 - n^2, m^2 + n^2) \in \mathbb{N}^3$$

mit $m, n \in \mathbb{N}$ *so, dass*

$$n < m,\ \mathrm{ggT}(m, n) = 1,\ m \not\equiv n \bmod(2).$$

Beweis: Sind $x = 2mn$, $y = m^2-n^2$ und $z = m^2+n^2$ mit $m, n \in \mathbb{N}$ wie im Satz verlangt, so haben x, y, z sicher keinen gemeinsamen Teiler. Denn ein gemeinsamer Primfaktor von $x = 2mn$ und $y = m^2 - n^2$ müsste ein gemeinsamer Faktor von m und n oder aber 2 sein. Beides ist nach Voraussetzung ausgeschlossen.

Zudem gilt $x^2 + y^2 = (2mn)^2 + (m^2 - n^2)^2 = m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2 = z^2$. Also ist (x, y, z) ein primitives pythagoräisches Tripel.

Sei nun umgekehrt $(x, y, z) \in \mathbb{N}^3$ ein primitives pythagoräisches Tripel. Seien $u = \frac{x}{z}$ und $v = \frac{y}{z}$. Dann ist (u, v) ein rationaler Punkt auf dem Einheitskreis $\mathbb{M}$. Wegen $x \neq 0$ ist $u \neq 0$, also $(u, v) \neq (0, 1)$. Nach 9.3 C) a) gibt es also ein $t \in \mathbb{Q}$ mit

$$u = \frac{2t}{t^2 + 1}, \quad v = \frac{t^2 - 1}{t^2 + 1}.$$

Wegen $u > 0$ und $v > 0$ ist klar, dass $t > 1$. Wir können also schreiben:

$$t = \frac{m}{n} \text{ mit } m, n \in \mathbb{N},\ n < m,\ \text{ggT}(m, n) = 1.$$

Es folgen:

$$u = \frac{2\frac{m}{n}}{\frac{m^2}{n^2} + 1} = \frac{2mn}{m^2 + n^2}; \quad v = \frac{\frac{m^2}{n^2} - 1}{\frac{m^2}{n^2} + 1} = \frac{m^2 - n^2}{m^2 + n^2}.$$

Wegen $u = \frac{x}{z}$ und $v = \frac{y}{z}$ erhalten wir

$$(\alpha) \qquad x(m^2 + n^2) = 2mnz;$$

$$(\beta) \qquad y(m^2 + n^2) = (m^2 - n^2)z.$$

Wir wollen als nächstes zeigen, dass $m \not\equiv n \mod (2)$. Nehmen wir an, es sei $m \equiv n \mod (2)$, also $2|(m - n)$. Weil m und n teilerfremd sind, müssen dann beide ungerade sein. Nach 9.5 A) a) folgen $4|(m^2 - n^2)$ und $4 \nmid (m^2 + n^2)$. Mit (β) ergibt sich daraus $2|y$, also ein Widerspruch zu 9.5 C) a). Deshalb ist $m \not\equiv n \mod(2)$.

Insbesodere ist eine der beiden Zahlen m oder n ungerade, die andere aber gerade. Deshalb gilt $2 \nmid (m^2 + n^2)$. Dies zieht aber nach sich, dass

$$(\gamma) \qquad \text{ggT}(m^2 + n^2, 2mn) = 1,$$

denn ein gemeinsamer Primfaktor von $m^2 + n^2$ und $2mn$ wäre ja ein Primfaktor von $m^2 + n^2$ und mn, was der Teilerfremdheit von m und n widerspräche.

Aus den Gleichungen (α) und (γ) ergibt sich $(m^2 + n^2)|z$.

Weil x und z teilerfremd sind (s. 9.5 C) a)), folgt aus Gleichung (α) auch $z|(m^2 + n^2)$. Damit wird $z = m^2 + n^2$ und die Gleichungen (α) und (β) liefern $x = 2mn, y = m^2 - n^2$. ■

Aufgaben 9.7. A) Ist (x, y, z) ein pythagoräisches Tripel, so nennen wir $x + y + z$ den *Umfang* dieses Tripels. Zeigen Sie, dass eine Zahl $u \in \mathbb{N}$ genau dann der Umfang eines primitiven pythagoräischen Tripels ist, wenn gilt:

$$u = 2mk,\ \text{mit } m, k \in \mathbb{N}, m < k < 2m,\ k \text{ ungerade und } \text{ggT}(m, k) = 1.$$

B) Sei $v \in \mathbb{N} \setminus \{1\}$ und sei $\mathring{\mathbb{T}}(v) := \{w \in \mathbb{T}(v) | \text{ggT}(w, \frac{v}{w}) = 1\}$ (vgl. 5.19 H)). Zeigen Sie, dass die Anzahl primitiver pythagoräischer Tripel vom Umfang $u := 2v$ gegeben ist durch

$$\lambda(u) := \sharp \left\{ m \in \mathring{\mathbb{T}}(v) \setminus \{1, v\} \,\middle|\, \frac{v}{2} < m^2 < v \wedge 2^{\nu_2(v)} | m \right\}.$$

C) Zeigen Sie, dass eine Zahl $u \in \mathbb{N}$ genau dann der Umfang eines pythagoräischen Tripels ist, wenn $u = 2mkl$, wobei $m, k, l \in \mathbb{N}$ und m und k den Bedingungen aus Teil A) genügen. Schliessen Sie, dass die Anzahl pythagoräischer Tripel vom Umfang u gegeben ist durch $\lambda(u) := \sum_{2|w|u} \lambda(w)$.

D) Sei u das Produkt der ersten 8 Primzahlen. Wie viele pythagoräische Tripel mit Umfang u gibt es?

E) Für jedes $n \in \mathbb{N}_{\geq 2}$ sei (x_n, y_n, z_n) ein primitives pythagoräisches Tripel mit Umfang $2^n(2^{n-1}+1)$. Bestimmen Sie dieses Tripel und berechnen Sie

$$\lim_{n\to\infty} \frac{y_n}{x_n}, \ \lim_{n\to\infty} \frac{z_n}{x_n} \text{ und } \lim_{n\to\infty} \frac{z_n}{y_n}.$$

F) Sei $\mathbb{H} := \{(x, y, z) \in \mathbb{Z}^3 \backslash \{(0, 0, 0)\} | x^2 + y^2 = z^2\}$. Zeigen Sie:

$$(x, y, z), (x', y', z') \in \mathbb{H} \Longrightarrow (xx' - yy', xy' + x'y, zz') \in \mathbb{H}.$$

G) Gemäss F) können wir auf $\mathbb{H}$ eine Verknüpfung „$\oplus$“ definieren durch

$$(x, y, z) \oplus (x', y', z') := (xx' - yy', xy' + x'y, zz').$$

Zeigen Sie, dass diese Verknüpfung assoziativ und kommutativ ist und das Neutralelement $(1, 0, 1)$ hat. •

Von der Geometrie zur Arithmetik: ein Rückblick

Mit 9.6 haben wir ein klassisches Problem der Arithmetik gelöst: die Bestimmung aller (primitiven) pythagoräischen Tripel, d.h. die Bestimmung aller (nichttrivialen) Lösungen der diophantischen Gleichung $x^2 + y^2 - z^2 = 0$.

Als wesentliches Hilfsmittel haben wir gebraucht, dass die Parametrisierung ε aus 9.3 zu jeder rationalen Zahl t ein Lösungstripel $(x(t), y(t), z(t)) \in \mathbb{Z}^3 \backslash \{(0, 0, 0)\}$ unserer Gleichung liefert. Diese Idee, mit Hilfe der Geometrie ein arithmetisches Problem zu lösen, wurde natürlich schon in der Aufgabe 1.7 vorweggenommen. Diese Idee ist aber so wichtig, dass wir sie im folgenden nochmals rekapitulieren.

Bemerkung 9.8. A) Wir setzen

$$F(x, y, z) := x^2 + y^2 - z^2$$

und interessieren uns für die Tripel $(x, y, z) \in \mathbb{Z}^3 \backslash \{(0, 0, 0)\}$ mit $F(x, y, z) = 0$, also für die Menge

$$\mathbb{L}(F) := \left\{ (x, y, z) \in \mathbb{Z}^3 \backslash \{(0, 0, 0)\} \,\middle|\, F(x, y, z) = 0 \right\}.$$

Für jedes Tripel $(x, y, z) \in \mathbb{L}(F)$ muss natürlich $z \neq 0$ gelten. Wir können also

$$\mathbb{L}_z(F) := \{(x, y, z) \in \mathbb{L}(F) | z \neq 0\}$$

schreiben und haben dann $\mathbb{L}_z(F) = \mathbb{L}(F)$. Es genügt deshalb, dass wir $\mathbb{L}_z(F)$ bestimmen. Offensichtlich gilt

$$(x_0, y_0, z_0) := (0, 1, 1) \in \mathbb{L}_z(F).$$

Aus diesem einen Tripel in $\mathbb{L}_z(F)$ lassen sich nun alle andern wie folgt finden:

B) Wir betrachten das quadratische Polynom in u und v, das gegeben ist durch (vgl. 9.3)

$$f(u, v) := F(u, v, 1) = u^2 + v^2 - 1,$$

sowie die Menge

$$\mathbb{M}(f) := \left\{(u, v) \in \mathbb{R}^2 | f(u, v) = 0\right\} = \mathbb{M}$$

und den Punkt

$$S = (u_0, v_0) := \left(\frac{x_0}{z_0}, \frac{y_0}{z_0}\right) = (0, 1) \in \mathbb{Q}^2 \cap \mathbb{M}.$$

Dann betrachten wir die rationale Parametrisierung

$$\varepsilon : \mathbb{R} \longrightarrow \mathbb{M}\backslash\{S\};\ t \mapsto \varepsilon(t) := (u(t), v(t))$$

aus 9.3 B) und die aus dieser resultierende Beziehung (vgl. 9.3 C))

a) $$\mathbb{Q}^2 \cap \mathbb{M} = \varepsilon(\mathbb{Q}) \cup \{S\} = \{(u(t), v(t)) \,|t \in \mathbb{Q}\} \cup \{(u_0, v_0)\}\,.$$

C) Nun haben wir alle rationalen Punkte von $\mathbb{M}$ in geschlossener Form dargestellt und können jetzt 8.7 anwenden um alle ganzzahligen Lösungen der Gleichung $F(x, y, z) = 0$ (mit $z \neq 0$) zu bestimmen. Wir wollen auch diesen letzten Schritt nochmals rekapitulieren. Dazu führen wir zunächst eine geeignete Bezeichnungsweise ein.

Sind $u, v \in \mathbb{Q}$, so stehe $\eta(u, v)$ für den *kleinsten gemeinsamen Nenner von u und v*, also

$$\eta(u, v) := \min\{n \in \mathbb{N} | nu, nv \in \mathbb{Z}\}$$

oder, in der Bezeichnungsweise von 2.6:

a) $$\eta(u, v) = \mathrm{kgV}\,(\eta(u), \eta(v))\,.$$

Ist $z \in \mathbb{Z}\backslash\{0\}$, so kann man sagen:

$$zu, zv \in \mathbb{Z} \Longleftrightarrow \eta(u, v) | z.$$

Nun liefert die Aussage 8.7 B) b) sofort

$$\mathbb{L}_z(F) = \left\{(zu, zv, z) \,\middle|\, (u, v) \in \mathbb{Q}^2 \cap \mathbb{M}, z \in \mathbb{Z}\eta(u, v)\backslash\{0\}\right\},$$

und mit der obigen Aussage B) a) folgt

$$\mathbb{L}_z(F) = \{(zu(t), zv(t), z) | t \in \mathbb{Q}, z \in \mathbb{Z}\eta(u(t), v(t))\backslash\{0\}\}$$
$$\cup \{(\lambda x_0, \lambda y_0, \lambda z_0) | \lambda \in \mathbb{Z}\backslash\{0\}\}.$$

Da man zu jedem $t \in \mathbb{Q}$ leicht die rationalen Zahlen $u(t), v(t)$ und deren gemeinsamen Nenner $\eta(u(t), v(t))$ bestimmen kann, liefert diese Aussage eine gute Beschreibung der Lösunsmenge $\mathbb{L}_z(F)$. •

Aufgaben 9.9. A) Seien $u(t)$ und $v(t)$ wie in 9.3. Bestimmen Sie zu jedem pythagoräischen Tripel (x, y, z) vom Umfang kleiner oder gleich 60 einen positiven Bruch t so, dass $(x, y, z) = (zu(t), zv(t), z)$.

B) Es gelten die Bezeichnungen von A). Bestimmen Sie vier positive Brüche t_1, t_2, t_3, t_4 so, dass $\eta(u(t_1), v(t_1)) < \eta(u(t_2), v(t_2)) < \eta(u(t_3), v(t_3)) < \eta(u(t_4), v(t_4))$ und dass die Zahl $\eta(u(t_4), v(t_4))$ möglichst klein wird.

C) Sei $t \in \mathbb{Q}_{\geq 0}\backslash\{1\}$. Bestimmen Sie eine Zahl $s \in \mathbb{Q}_{\geq 0}\backslash\{t\}$ so, dass $\eta(u(s), v(s)) = \eta(u(t), v(t))$. Begründen oder interpretieren Sie das Ergebnis geometrisch. •

Homogene quadratische diophantische Gleichungen

Die in 9.8 beschriebene Lösungsidee für die diophantische Gleichung $x^2 + y^2 - z^2 = 0$ lässt sich auf eine grössere Klasse diophantischer Gleichungen $F(x, y, z) = 0$ übertragen: auf die sogenannten (nichtausgearteten) *homogenen quadratischen diophantischen Gleichungen*. Zu dieser Klasse diophantischer Gleichungen gehören etwa

Beispiele 9.10.

a) $x^2 + y^2 - z^2 = 0$;

b) $x^2 - y^2 - z^2 = 0$;

c) $xz - y^2 = 0$;

d) $2x^2 - 7y^2 - z^2 = 0$;

e) $x^2 - 29y^2 - z^2 = 0$;

f) $x^2 - 2xy + y^2 + 2z^2 - xz - yz = 0$.

•

Wir wollen nun diese Klasse von Gleichungen definieren und eingehender betrachten. Die Basis der in 9.8 beschriebenen Lösungsidee – die Bestimmung der rationalen Punkte der Kurve $F(u, v, 1) = 0$ – werden wir allerdings erst im nächsten Kapitel systematisch behandeln.

Definitionen 9.11. A) Eine *homogene diophantische Quadrik* in den Unbestimmten x, y, z ist ein Polynom $Q = Q(x, y, z)$ der Form

$$Q(x, y, z) = Ax^2 + Cy^2 + Fz^2 + Bxy + Dxz + Eyz$$

mit $A, B, C, D, E, F \in \mathbb{Z}$.

B) Es gelten die obigen Bezeichnungen. Die Zahl

$$\Delta_Q := 4ACF + BDE - AE^2 - CD^2 - FB^2$$

heisst die *Diskriminante von* Q. Ist $\Delta_Q \neq 0$, so sagt man, die Quadrik Q sei *nichtausgeartet*. Ist $\Delta_Q = 0$, so heisst Q *ausgeartet*.

C) Eine *homogene quadratische diophantische Gleichung* in den Unbekannten x, y, z ist eine Gleichung der Form

$$Q(x, y, z) = 0,$$

in welcher $Q(x, y, z)$ eine homogene diophantische Quadrik ist. Ist zudem $\Delta_Q \neq 0$, so spricht man von einer *nichtausgearteten homogenen quadratischen diophantischen Gleichung*. •

Aufgaben 9.12. A) Bestimmen Sie für jede der Gleichungen aus 9.10 die 6 Koeffizienten A, B, C, D, E, F aus 9.11 A).

B) Zeigen Sie, dass alle Gleichungen aus 9.10 nichtausgeartet sind.

C) Bestimmen Sie zu jeder der diophantischen Gleichungen 9.10 a), b), c), d), f) ein (möglichst einfaches) Lösungstripel $(x, y, z) \in \mathbb{Z}^3$ mit $z = 1$.

D) Lösen Sie Aufgabe C) auch für die Gleichung 9.10 e), wobei ein Lösungstripel (x, y, z) mit $y \neq 1$ anzugeben ist. •

Sofort lässt sich ein Teil dessen, was wir in 9.8 über die Gleichung 9.10 a) gesagt haben auf beliebige homogene quadratische diophantische Gleichungen übertragen:

Bemerkung 9.13. A) Wir betrachten die homogene diophantische Quadrik (vgl. 9.11 A))

$$Q(x,y,z) = Ax^2 + Cy^2 + Fz^2 + Bxy + Dxz + Eyz$$

und interessieren uns für die nichttrivialen Lösungen der diophantischen Gleichung $Q(x,y,z) = 0$, also für die Menge

a) $$\mathbb{L}(Q) := \left\{(x_0,y_0,z_0) \in \mathbb{Z}^3 \setminus \{(0,0,0)\} \,|Q(x_0,y_0,z_0) = 0\right\}.$$

Wir definieren

b) $$\begin{cases} \mathbb{L}_x(Q) := & \{(x_0,y_0,z_0) \in \mathbb{L}(Q) | x_0 \neq 0\}; \\ \mathbb{L}_y(Q) := & \{(x_0,y_0,z_0) \in \mathbb{L}(Q) | y_0 \neq 0\}; \\ \mathbb{L}_z(Q) := & \{(x_0,y_0,z_0) \in \mathbb{L}(Q) | z_0 \neq 0\}. \end{cases}$$

Dann gilt natürlich

$$\mathbb{L}(Q) = \mathbb{L}_x(Q) \cup \mathbb{L}_y(Q) \cup \mathbb{L}_z(Q).$$

Um $\mathbb{L}(Q)$ zu bestimmen genügt es also, die drei Mengen $\mathbb{L}_x(Q), \mathbb{L}_y(Q)$ und $\mathbb{L}_z(Q)$ zu bestimmen.

B) Will man ein allgemeines Lösungsprinzip für die diophantische Gleichung $Q(x,y,z) = 0$ angeben, so kann man sich ohne Einschränkung der Allgemeinheit auf die Bestimmung der Menge $\mathbb{L}_z(Q)$ beschränken. In den folgenden Bemerkungen wollen wir dies so halten und einiges, was wir in 9.8 für die Gleichung $x^2 + y^2 - z^2 = 0$ gesagt haben auf beliebige homogene quadratische diophantische Gleichungen übertragen. Wir halten dazu die obigen Bezeichnungen fest und setzen

$$f(u,v) := Q(u,v,1),$$

sodass gilt

$$f(u,v) = Au^2 + Buv + Cv^2 + Du + Ev + F.$$

Man nennt $f = f(u,v)$ eine *Quadrik in u und v*. Nun setzen wir:

$$\mathbb{M}(f) := \{(u,v) \in \mathbb{R}^2 | f(u,v) = 0\}.$$

Im allgemeinen wird $\mathbb{M}(f)$ eine Kurve in der Ebene sein. Sofort sieht man:

$$(x_0,y_0,z_0) \in \mathbb{L}_z(Q) \Longrightarrow (u_0,v_0) := \left(\frac{x_0}{z_0}, \frac{y_0}{z_0}\right) \in \mathbb{Q}^2 \cap \mathbb{M}(f).$$

C) Die Aussage 9.8 C) a) lässt sich nun leicht auf unsere homogene quadratische Gleichung übertragen (vgl. 8.8 B) c)):

a) $$\mathbb{L}_z(Q) = \{(zu, zv, z) | (u,v) \in \mathbb{Q}^2 \cap \mathbb{M}(f), z \in \mathbb{Z}\eta(u,v) \setminus \{0\}\}.$$

Insbesondere können wir sagen:

b) $$\mathbb{L}_z(Q) = \emptyset \Longleftrightarrow \mathbb{Q}^2 \cap \mathbb{M}(f) = \emptyset.$$

•

Die Aussage 9.13 C) a) bringt etwas zum Ausdruck, was wir schon aus 8.8 wissen:

- *Um die (Teil-)Lösungsmenge $\mathbb{L}_z(Q)$ der homogenen quadratischen diophantischen Gleichung $Q(x, y, z) = 0$ zu beschreiben genügt es, die Menge $\mathbb{Q}^2 \cap \mathbb{M}(f)$ der rationalen Punkte der Quadrik $f(u, v) = Q(u, v, 1)$ zu beschreiben.*

Aufgaben 9.14. A) Beweisen Sie die Aussage 9.13 C) a).

B) Skizzieren Sie $\mathbb{M}(f)$ (mit $f := f(u, v) = Q(u, v, 1)$) für

a) $Q(x, y, z) = xz - y^2$;

b) $Q(x, y, z) = x^2 - y^2 - z^2$;

c) $Q(x, y, z) = x^2 + y^2 - 7z^2$;

d) $Q(x, y, z) = -x^2 + 2y^2 - 3z^2$.

•

Zur Existenz nichttrivialer Lösungen

Wir werden später lernen, wie man mit Hilfe einer sogenannten *rationalen Parametrisierung der Quadrik $f(u, v) = Q(u, v, 1)$* deren rationale Punkte, also die Menge $\mathbb{Q}^2 \cap \mathbb{M}(f)$ beschreibt. Gemäss dem oben Gesagten lässt sich dann auch die Menge $\mathbb{L}_z(Q)$ beschreiben. Es kann allerdings vorkommen, dass die Menge $\mathbb{L}_z(Q)$ leer ist, also dass die Menge $\mathbb{M}(f)$ keine rationalen Punkte enthält, obwohl $\mathbb{M}(f)$ eine „ganze Kurve“ ist. Wie schon im Überblick zu diesem Kapitel gesagt, übersteigt die systematische Behandlung dieses Phänomens unsere Möglichkeiten. Trotzdem wollen wir zwei Beispiele dazu anführen.

Beispiel 9.15. A) Wir betrachten die homogene quadratische diophantische Gleichung

a) $$x^2 + y^2 - 7z^2 = 0$$

und wollen zeigen, dass diese nur die triviale Lösung hat, also dass (vgl. 9.13 A) a)):

b) $$\mathbb{L}(x^2 + y^2 - 7z^2) = \emptyset.$$

Wir nehmen an, es sei $(x_0, y_0, z_0) \in \mathbb{L}(x^2 + y^2 - 7z^2)$ und leiten daraus eine Widerspruch her. Nach weglassen gemeinsamer Faktoren können wir annehmen x_0, y_0 und z_0 hätten keinen gemeinsamen Teiler, also (vgl. 5.4)

c) $$\mathbb{P}(x_0) \cap \mathbb{P}(y_0) \cap \mathbb{P}(z_0) = \emptyset.$$

Nun können wir schreiben:

$$x_0 = 7m + r \text{ mit } m \in \mathbb{Z} \text{ und } r \in \{0, 1, \cdots, 6\};$$

$$y_0 = 7n + s \text{ mit } n \in \mathbb{Z} \text{ und } s \in \{0, 1, \cdots, 6\}.$$

Aus c) ergibt sich zusätzlich

d) $$(r, s) \neq (0, 0).$$

Einsetzen in die Gleichung a) liefert

$$\begin{aligned} 7z^2 = x^2 + y^2 &= (7m + r)^2 + (7n + s)^2 = 49m^2 + 14mr + r^2 + 49n^2 + 14ns + s^2 \\ &= 7(7m^2 + 2mr + 7n^2 + 2ns) + r^2 + s^2. \end{aligned}$$

Also können wir sagen (vgl. auch d)):

e) $$\exists r, s \in \{0, 1, \cdots, 6\} : 7 | r^2 + s^2 \neq 0.$$

Wir tabellieren die Werte von $r^2 + s^2$ für $r, s \in \{0, 1, \ldots, 6\}$:

s \ r	0	1	2	3	4	5	6
0	0	1	4	9	16	25	36
1	1	2	5	10	17	26	37
2	4	5	8	13	20	29	40
3	9	10	13	18	25	34	45
4	16	17	20	25	32	41	52
5	25	26	29	34	41	50	61
6	36	37	40	45	52	61	72

Die Tabelle zeigt, dass Aussage e) nicht gilt.

B) Insbesondere folgt aus der Aussage A) b):

$$\mathbb{L}_z(x^2 + y^2 - 7z^2) = \emptyset.$$

Gemäss Aussage 9.13 C) b) ergibt sich daraus

$$\mathbb{Q}^2 \cap \mathbb{M}(u^2 + v^2 - 7) = \emptyset.$$

Die Quadrik $\mathbb{M}(u^2 + v^2 - 7)$ enthält also keinen einzigen rationalen Punkt, obwohl $\mathbb{M}(u^2 + v^2 - 7)$ „sehr viele“ Punkte enthält:
Für jedes $u \in [-\sqrt{7}, \sqrt{7}]$ gilt $(u, \pm\sqrt{7 - u^2}) \in \mathbb{M}(u^2 + v^2 - 7)$ (vgl. auch 9.14 B) c)). •

Wir betrachten ein weiteres Beispiel.

Beispiel 9.16. A) Wir wollen zeigen, dass

a) $$\mathbb{L}(-x^2 + 2y^2 - 3z^2) = \emptyset.$$

Wir nehmen im Gegenteil an, es gäbe ein Tripel $(x_0, y_0, z_0) \in \mathbb{L}(-x^2+2y^2-3z^2)$. Wieder können wir annehmen, es sei

$$\mathbb{P}(x_0) \cap \mathbb{P}(y_0) \cap \mathbb{P}(z_0) = \emptyset$$

und schreiben

$$x_0 = 3m + r \text{ mit } m \in \mathbb{Z} \text{ und } r \in \{0, 1, 2\};$$
$$y_0 = 3n + s \text{ mit } n \in \mathbb{Z} \text{ und } s \in \{0, 1, 2\};$$

b) $$(r, s) \neq (0, 0).$$

Es folgt

$$\begin{aligned} 3z_0^2 &= -x_0^2 + 2y_0^2 = 2(3n + s)^2 - (3m + r)^2 = 18n^2 + 12ns + 2s^2 - 9m^2 - 6mr - r^2 \\ &= 3(6n^2 + 4ns - 3m^2 - 2mr) + 2s^2 - r^2, \end{aligned}$$

also

c) $$3|2s^2 - r^2.$$

Wir tabellieren die Werte von $2s^2 - r^2$ für $r, s \in \{0, 1, 2\}$ und sehen, dass die Aussagen b) und c) nicht gleichzeitig gelten können:

r \ s	0	1	2
0	0	2	8
1	-1	1	7
2	-4	-2	4

B) Aus der Aussage A) a) folgt wieder

$$\mathbb{L}_z(-x^2 + 2y^2 - 3z^2) = \emptyset$$

und damit

$$\mathbb{Q}^2 \cap \mathbb{M}(-u^2 + 2v^2 - 3) = \emptyset.$$

Die Quadrik $\mathbb{M}(-u^2 + 2v^2 - 3)$ enthält also wieder keinen rationalen Punkt, obwohl $\left(u, \pm\sqrt{\frac{3+u^2}{2}}\right) \in \mathbb{M}(-u^2 + 2v^2 - 3)$ für jede Zahl $u \in \mathbb{R}$ (vgl. Aufgabe 9.14 B) d)). •

Aufgaben 9.17. A) Bestimmen Sie die Mengen

a) $$\mathbb{L}(x^2 + y^2 - 3z^2);$$

b) $$\mathbb{M}(u^2 + v^2 - 3).$$

B) Bestimmen Sie alle Zahlen $c \in \{1, 2, \cdots, 10\}$ mit

$$\mathbb{L}(x^2 + y^2 - cz^2) = \emptyset.$$

C) Sei $(a_n)_{n\in\mathbb{N}}$ eine Folge positiver rationaler Zahlen mit $\lim_{n\to\infty} a_n = \sqrt{7}$. Sei weiter $f_n = f_n(u, v) = u^2 + v^2 - \frac{a_n^2}{7}$. Zeigen Sie, dass $\mathbb{Q}^2 \cap \mathbb{M}(f_n) = \emptyset$ und beschreiben Sie die Folge der Mengen $\mathbb{M}(f_n)$ geometrisch.

D) Lösen Sie Aufgabe C) mit $f_n = f_n(u, v) = \frac{a_n^2}{7}\, u^2 + \frac{7}{a_n^2}\, v^2 - 1$. •

Kapitel 10

Rationale Punkte auf Quadriken

Überblick

In diesem Kapitel soll die rationale Parametrisierung des Einheitskreises, welche wir in Kapitel 9 erfolgreich für die Bestimmung der pythagoräischen Tripel eingesetzt haben, auf beliebige nichtausgeartete ebene Quadriken übertragen werden. Wir werden also die rationale Parametrisierung nichtausgearteter ebener Quadriken behandlen. Dieses an sich rein geometrische Prinzip ist von grösster Bedeutung für die in Kapitel 9 behandelten nichtausgearteten homogenen quadratischen diophantischen Gleichungen. Es liefert nämlich eine Methode um aus einer einzigen nichttrivialen Lösung einer solchen diophantischen Gleichung alle andern nichttrivialen Lösungen zu finden. Mit dieser Illustration der intensiven Wechselwirkung zwischen Arithmetik und Geometrie schliesst sich der thematische Kreis des letzten Teiles unserer Vorlesung weitgehend: Unbehandelt muss nur die Frage bleiben, wie man denn überhaupt zu einer nichttrivialen Lösung kommt.

Dieses Kapitel kann auch als eine erste Einführung in die ebene algebraische Geometrie verstanden werden. In der Sprache der algebraischen Geometrie ausgedrückt besteht dieses Kapitel im Wesentlichen aus einem konstruktiven Beweis der Tatsache, dass nichtausgeartete ebene Quadriken rationale Kurven sind.

Es werden folgende Themen behandelt:

- *Eine Vorbetrachtung*,
- *Ebene Quadriken*,
- *Partielle Ableitungen und Diskriminanten*,
- *Quadriken und Geraden*,
- *Geometrische Bedeutung der Tangenten und der kritischen Geraden*,

- *Rationale Parametrisierung der Quadriken,*
- *Projektionen aus kritischen Richtungen,*
- *Zur Existenz rationaler Punkte.*

Haben wir beim Kapitel 8 von einer „Schnupperlehre in Diophantik“gesprochen, so könnten wir bei diesem Kapitel von einer „Schnupperlehre in algebraischer Geometrie“reden. Allerdings ist der Stil nun ganz anders als in Kapitel 8. Es wird uns hier um eine systematische und strenge Behandlung eines zentralen Themas gehen und nicht mehr um ein Hüpfen von Einzelfall zu Einzelfall.

Eine Vorbetrachtung

In diesem Abschnitt wollen wir den Inhalt des vorliegenden Kapitles zusammenfassend darstellen.

Bemerkung 10.1. Sei

$$Q(x,y,z) = Ax^2 + Cy^2 + Fz^2 + Bxy + Dxz + Eyz$$

eine homogene diophantische Quadrik (vgl. 9.11 A)). Wie in 9.13 A) a)) stehe $\mathbb{L}(Q)$ wieder für die Menge der nichttrivialen Lösungen der diophantischen Gleichung $Q(x,y,z) = 0$. Wie in 9.13 A) b) schreiben wir wieder $\mathbb{L}_z(Q)$ für die Menge aller Tripel $(x_0,y_0,z_0) \in \mathbb{L}(Q)$ mit $z_0 \neq 0$. Wir sind interessiert an einem Verfahren, das es erlaubt, aus einer einzigen Lösung $(x_0,y_0,z_0) \in \mathbb{L}(Q)$ alle andern Lösungen zu gewinnen.

Wie wir schon in 9.13 B) bemerkt haben, genügt es, ein Verfahren anzugeben, mit dem sich aus einer einzigen Lösung $(x_0,y_0,z_0) \in \mathbb{L}_z(Q)$ alle andern Tripel in $\mathbb{L}_z(Q)$ gewinnen lassen.

Das Verfahren, das wir beschreiben wollen, beruht auf einer geometrischen Idee und macht sich zu Nutzen, was wir bereits in 9.13 B), C) festgestellt haben:

Die Menge $\mathbb{L}_z(Q)$ lässt sich aus der Menge $\mathbb{Q}^2 \cap \mathbb{M}(f)$ der rationalen Punkte der Quadrik

$$f = f(u,v) = Q(u,v,1) = Au^2 + Buv + Cv^2 + Du + Ev + F$$

gewinnen.

Es genügt also, ein Verfahren anzugeben, welches erlaubt, aus einem Punkt $(u_0,v_0) \in \mathbb{Q}^2 \cap \mathbb{M}(f)$ alle Punkte von $\mathbb{Q}^2 \cap \mathbb{M}(f)$ zu gewinnen. •

Wir wollen das oben erwähnte Verfahren im folgenden kurz skizzieren. Es handelt sich um die *rationale Parametrisierung von Quadriken.*

Konstruktion 10.2. A) Wir betrachten wieder die homogene diophantische Quadrik

$$Q(x,y,z) = Ax^2 + Cy^2 + Fz^2 + Bxy + Dxz + Eyz.$$

Zusätzlich wollen wir annehmen, dass $Q = Q(x,y,z)$ nichtausgeartet ist, also dass (vgl. 9.11 B))

$$\Delta_Q := 4ACF + BDE - AE^2 - CD^2 - FB^2 \neq 0.$$

Wir betrachten die zugehörige *ebene Quadrik*

$$f = f(u,v) := Q(u,v,1) = Au^2 + Buv + Cv^2 + Du + Ev + F$$

und deren Nullstellenmenge

$$\mathbb{M}(f) = \{(u,v) \in \mathbb{R}^2 \,\big|\, f(u,v) = 0\}.$$

Wir wollen annehmen, es sei

$$S = (u_0, v_0) \in \mathbb{Q}^2 \cap \mathbb{M}(f).$$

Nun soll also ein Verfahren angegeben werden, welches erlaubt, aus S alle Punkte von $\mathbb{Q}^2 \cap \mathbb{M}(f)$ zu gewinnen.

B) Als erstes legen wir eine Tangente an die Kurve $\mathbb{M}(f)$ im Punkt $S = (u_0, v_0)$ (vgl. 10.13 B)). Dann legen wir eine Hilfsgerade h, welche parallel ist zur gelegten Tangente. Diese Hilfsgerade besitzt dann eine Parameterdarstellung der Form (vgl.10.18 A) b))

$$h : t \mapsto P_t := (u_0 + b + at, v_0 - a + bt);\ (t \in \mathbb{R}),$$

wobei a und b geeignete rationale Zahlen sind, die nicht beide verschwinden. Zu jedem Parameterwert $t \in \mathbb{R}$ legen wir nun die Gerade g_t durch die Punkte P_t und S. Dann schneiden wir die Kurve $\mathbb{M}(f)$ mit der Geraden g_t.

Wir werden später zeigen, dass folgendes gilt: Vermeidet t gewisse „kritische Werte“, so haben $\mathbb{M}(f)$ und g_t nebst S noch genau einen weiteren Schnittpunkt, den wir mit $S_t = (u(t), v(t))$ bezeichnen (vgl. 10.18 C)).

Es treten höchstens zwei der genannten kritischen Werte auf. Für diese kritischen Werte von t ist S der einzige Schnittpunkt von $\mathbb{M}(f)$ mit g_t (vgl. 10.18 C)).

Schreiben wir $\mathcal{C}$ für die Menge der (höchstens zwei) kritischen Parameterwerte, so erhalten wir eine bijektive Abbildung (vgl. 10.20)

$$\varepsilon_S = \varepsilon : \mathbb{R}\backslash\mathcal{C} \xrightarrow{\approx} \mathbb{M}\backslash\{S\};\ t \mapsto \varepsilon(t) := (u(t), v(t)).$$

Dabei gilt, wie wir später beweisen werden (vgl. 10.21):

$$t \in \mathbb{Q} \Longleftrightarrow \varepsilon(t) \in \mathbb{Q}^2;\ (t \in \mathbb{R}\backslash\mathcal{C}).$$

Insbesondere gilt also (vgl. 10.22 b))

$$\mathbb{Q}^2 \cap \mathbb{M}(f) = (u_0, v_0) \cup \{\varepsilon(t) = (u(t), v(t)) \,\big|\, t \in \mathbb{Q}\backslash\mathcal{C}\}.$$

Damit sind alle Punkte von $\mathbb{Q}^2 \cap \mathbb{M}(f)$ vermöge $\varepsilon = \varepsilon_S = \varepsilon_{(u_0,v_0)}$ parametrisiert, und das gewünschte Ziel ist erreicht.

C) Im folgenden ist die soeben beschriebene Methode der rationalen Parametrisierung einer Quadrik f anschaulich illustriert. Wir haben dabei an den Fall gedacht, wo $\mathbb{M}(f)$ eine Parabel ist (vgl. 10.6 C)). In diesem Fall tritt ein kritischer Wert auf (vgl. 10.16 D) (δ')).

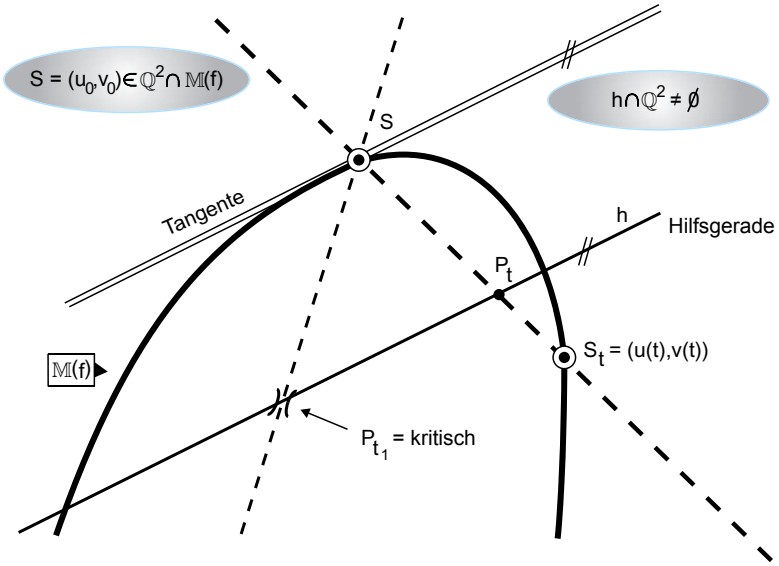


Abbildung 10.1: Rationale Parametrisierung einer Quadrik

•

Bemerkung 10.3. A) Im Spezialfall $A = C = 1, B = D = E = 0$ und $F = 1$ gilt $f(u, v) = u^2 + v^2 - 1$. In diesem Fall ist $\mathbb{M} = \mathbb{M}(f)$ gerade der Einheitskreis. Wählt man $S = (u_0, v_0) = (0, 1)$, ist h die u-Achse und setzt man $a = 1$ und $b = 0$, so liefert das in 10.2 beschriebene Verfahren gerade die in 9.3 vorgenommene rationale Parametrisierung des Einheitskreises.

B) Man könnte im allgemeinen Fall die tangentenparallele Hilfsgerade h ersetzen durch irgendeine Gerade h', welche den Punkt $S = (u_0, v_0)$ vermeidet. Die arithmetische Handhabung der Parametrisierung könnte sich damit sogar vereinfachen. Andererseits wäre dann ein „Schönheitsfehler“in Kauf zu nehmen: Es tritt ein zusätzlicher kritischer Parameterwert auf! Deswegen könnte bei der Parametrisierung ein Punkt in $\mathbb{Q}^2 \cap \mathbb{M}(f)$ „verloren gehen“d.h. nicht erfasst werden. Aus diesem Grund werden wir nur den Fall weiterverfolgen, in dem die Hilfsgerade h parallel zur Tangente zu f in $S = (u_0, v_0)$ ist.•

Aufgaben 10.4. A) Wählen Sie $A = \frac{1}{4}, C = 1, F = -1$ und $B = D = E = 0$. Wählen Sie $S = (0, 1)$ und wählen Sie die Hilfsgerade h so, dass $P_0 := (0, 0) \in h$. Berechnen Sie die beiden Funktionen $u(t)$ und $v(t)$ aus 10.2 B) und bestimmen Sie die Menge $\mathcal{C} \subseteq \mathbb{R}$ aller kritischen Werte. Skizzieren Sie die Situation im Sinne der Abbildung 10.1.

B) Lösen Sie Aufgabe A) für $A = B = E = F = 0, C = 1$ und $D = -1$ mit $S = (0, 0)$, wobei $P_0 := (-1, 0) \in h$.

C) Lösen Sie dieselbe Aufgabe, aber mit $A = 1, C = F = -1, B = D = E = 0, S = (1, 0)$ und $P_0 = (0, 0) \in h$.

D) Wählen Sie in jedem der Beispiele aus A)–C) eine Hilfsgerade $h' \neq h$ durch den jeweils vorgeschlagenen Punkt P_0. Machen Sie damit das in 10.3 B) Gesagte anschaulich an einer Skizze klar. •

Ebene Quadriken

Wir wollen uns nun daran machen, die im vorangehenden Abschnitt beschriebene Konstruktion wirklich durchzuführen und streng zu begründen. Wir beginnen mit dem „Grundmaterial“unserer Konstruktion: Den *ebenen Quadriken*, d.h. den Quadriken in zwei Unbestimmten.

Definition 10.5. A) Eine *Quadrik in den Unbestimmten* u und v ist ein Polynom vom Grad 2 in zwei Unbestimmten u und v mit reellen Koeffizienten, also ein Polynom der Form

$$f(u, v) = Au^2 + Buv + Cv^2 + Du + Ev + F$$

mit

$$A, B, C, D, E, F \in \mathbb{R}.$$

B) Die Zahl

$$\Delta_f := 4ACF + BDE - AE^2 - CD^2 - FB^2$$

heisst die *Diskriminante* der Quadrik $f = f(u, v)$. Man nennt die Quadrik f *ausgeartet*, wenn $\Delta_f = 0$. Man nennt f *nichtausgeartet*, wenn $\Delta_f \neq 0$, also wenn

$$4ACF + BDE - AE^2 - CD^2 - FB^2 \neq 0.$$

C) Ist $f = f(u, v)$ eine Quadrik, so schreiben wir $\mathbb{M}$ oder $\mathbb{M}(f)$ für die Menge aller reellen Lösungspaare (u, v) der Gleichung $f(u, v) = 0$. Also

$$\mathbb{M} = \mathbb{M}(f) := \{(u, v) \in \mathbb{R}^2 \mid f(u, v) = 0\}.$$

D) Die Quadrik

$$f(u, v) = Ax^2 + Bxy + Cy^2 + Dx + Ey + F$$

heisst *rational*, wenn ihre Koeffizienten rationale Zahlen sind, d.h. wenn

$$A, B, C, D, E, F \in \mathbb{Q}.$$

•

Wir wollen nun als Beispiele einige besonders einfache aber wichtige Spezialfälle nichtausgearteter rationaler Quadriken betrachten und geometrisch einordnen.

Spezialfälle und Beispiele 10.6. A) Wir betrachten den Fall der rationalen Quadrik $f(u, v) = u^2 + v^2 - 1$, d.h. den Fall

$$A = C = 1, F = -1, B = D = E = 0.$$

Hier ist $\mathbb{M} = \mathbb{M}(f)$ der Einheitskreis. Die rationalen Punkte auf dieser Menge $\mathbb{M}$ haben wir bereits eingehend studiert.

B) Wir betrachten die rationale Quadrik

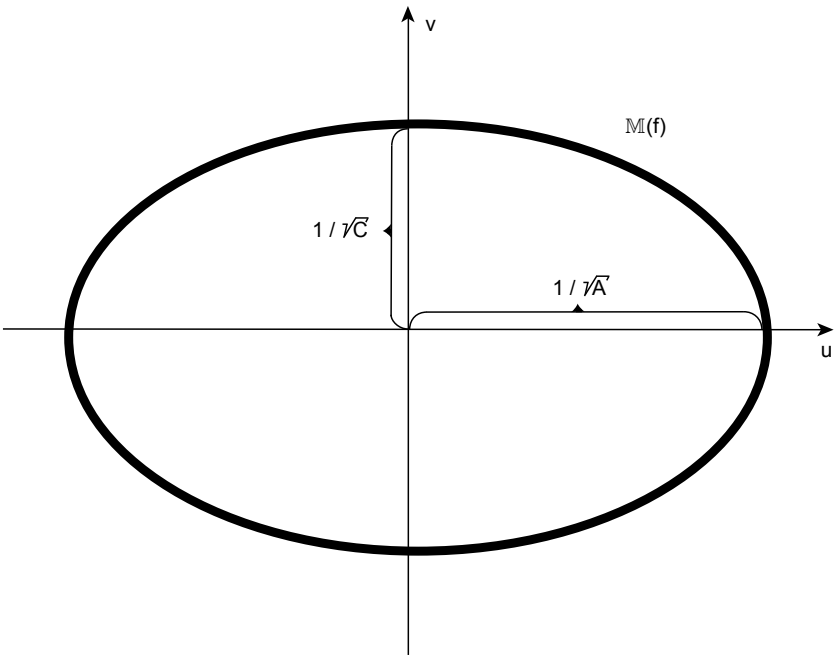


Abbildung 10.2: Ellipse

$$f(u, v) = Au^2 + Cv^2 - 1; \quad (0 < A \leq C),$$

d.h. den Fall

$$0 < A \leq C, F = -1, B = D = E = 0.$$

Hier ist $\mathbb{M} = \mathbb{M}(f)$ eine *Ellipse* mit *grosser Halbachse* $1/\sqrt{A}$ und *kleiner Halbachse* $1/\sqrt{C}$.

C) Wir betrachten die rationale Quadrik

$$f(u,v) = Cv^2 - u - 1; \quad (C > 0),$$

d.h. den Fall

$$A = B = E = 0, C > 0, D = F = -1.$$

Es handelt sich bei $\mathbb{M} = \mathbb{M}(f)$ um eine *Parabel* durch die 3 Punkte $(-1,0), (0, \pm\sqrt{1/C})$.

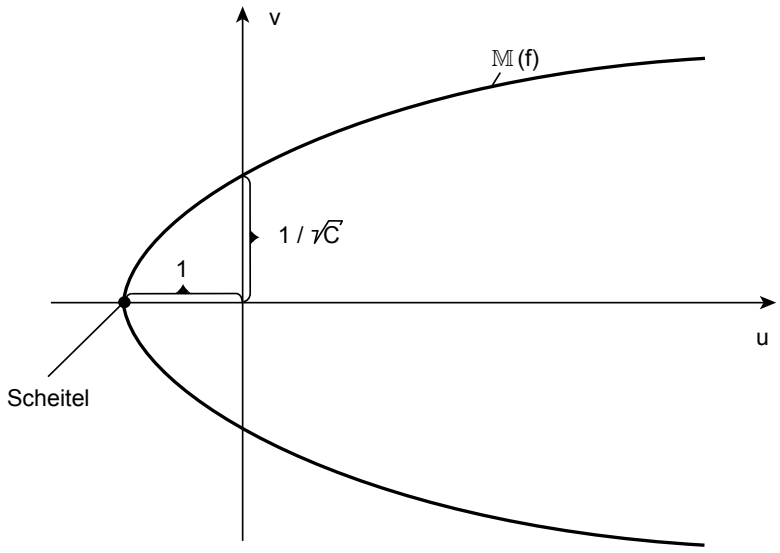


Abbildung 10.3: Parabel

D) Schliesslich betrachten wir noch die rationale Quadrik

$$f(u,v) = Au^2 + Cv^2 - 1; \quad (A < 0 < C),$$

also den Fall

$$B = D = E = 0, \ A < 0 < C, F = -1.$$

Es handelt sich bei $\mathbb{M} = \mathbb{M}(f)$ nun um eine *Hyperbel*. Die Asymptoten der Hyperbel $\mathbb{M}$ sind die beiden Geraden mit den Gleichungen

$$v = \pm\sqrt{-\frac{A}{C}}\, u.$$

Die Scheitelpunkte der Hyperbel sind $(0, \pm\sqrt{\frac{1}{C}})$.

•

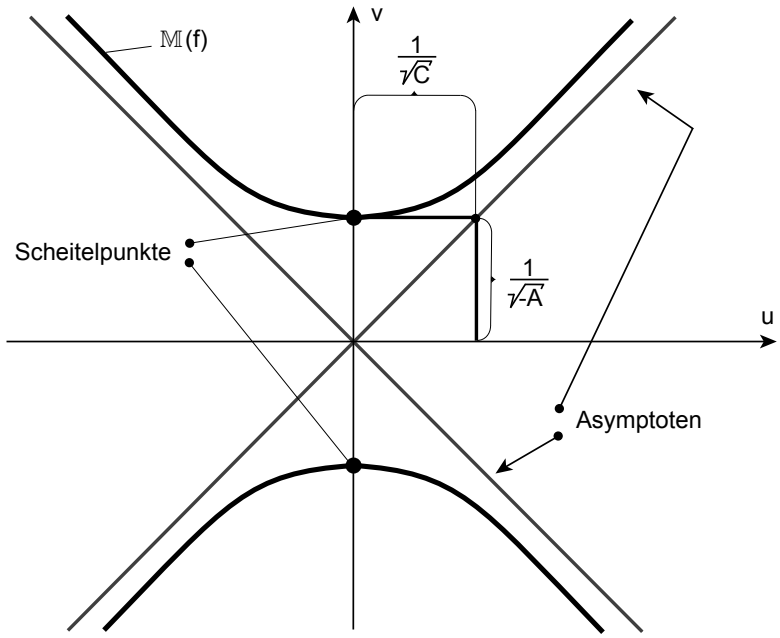


Abbildung 10.4: Hyperbel

Aufgaben 10.7. A) Zeigen Sie, dass die vorangehenden Beispiele aus 10.6 A)–D) nichtausgeartete (rationale) Quadriken sind.

B) Sei $f(u,v) = Au^2+Buv+Cv^2+Du+Ev+F$ eine nichtausgeartete rationale Quadrik. Zeigen Sie, dass folgende Polynome nichtausgeartete rationale Quadriken sind:

a) $f(v,u)$;

b) $\alpha f(u,v), (\alpha \in \mathbb{Q}\backslash\{0\})$;

c) $f(\alpha u,v), (\alpha \in \mathbb{Q}\backslash\{0\})$;

d) $f(u+\gamma,v), (\gamma \in \mathbb{Q})$;

e) $f(u+\gamma v,v), (\gamma \in \mathbb{Q})$.

C) Ellipsen, Parabeln und Hyperbeln sind sogenannte *Kegelschnitte*. Können Sie diesen Begriff erklären?

D) Zeigen Sie, dass die folgenden Quadriken f nichtausgeartet sind und skizzieren Sie jeweils $\mathbb{M}(f)$:

a) $f(v,u) = u^2+v^2+1$;

b) $\alpha f(u,v), (\alpha \in \mathbb{Q}\backslash\{0\})$;

c) $f(u,v) = u^2 + v^2 - 2u$;

d) $f(u+\gamma, v), (\gamma \in \mathbb{Q})$;

e) $f(u,v) = u^2 + uv + v^2 - 1$.

E) Sei f wie in B). Zeigen Sie, dass f durch wiederholtes Anwenden der Transformationen a)–e) aus B) übergeführt werden kann in eine der 4 Quadriken $u^2 + v^2 + 1, u^2 + v^2 - 1, -u^2 + v^2 - 1, v^2 - u - 1$. •

Partielle Ableitungen und Diskriminanten

In diesem Unterabschnitt beweisen wir eine Formel für die Diskriminante einer Quadrik und wenden diese an. Wir benötigen dabei den Begriff der partiellen Ableitung. Wir fixieren eine Quadrik

$$f = f(u,v) = Au^2 + Buv + Cv^2 + Du + Ev + F.$$

Definition und Bemerkung 10.8. A) Die *partielle Ableitung*

$$\frac{\partial f}{\partial u} = \frac{\partial f}{\partial u}(u,v)$$

der Funktion $f = f(u,v)$ *bezüglich* (oder *nach*) u ist die Ableitung der Funktion $f(u,v)$ nach der Variablen u, wenn v als Konstante betrachtet wird.

Entsprechend ist auch die *partielle Ableitung*

$$\frac{\partial f}{\partial v} = \frac{\partial f}{\partial v}(u,v)$$

der Funktion $f = f(u,v)$ *bezüglich* (oder *nach*) v definiert: als die Ableitung der Funtkon $f(u,v)$ nach der Variablen v bei konstantem u.

B) Der Graph

$$\{(u,v,f(u,v)) \,\big|\, u,v \in \mathbb{R}\} \subseteq \mathbb{R}^3$$

der Funktion $f = f(u,v)$ entspricht einer Fläche im Raum. Sind $u_0, v_0 \in \mathbb{R}$, so folgt aus der wohlbekannten Interpretation der gewöhnlichen Ableitung als Steigung (der Tangente) des Graphen:

$\frac{\partial f}{\partial u}(u_0,v_0)$ ist die Steigung des Graphen von f in Richtung u an der Stelle (u_0,v_0),

$\frac{\partial f}{\partial v}(u_0,v_0)$ ist die Steigung des Graphen von f in Richtung v an der Stelle (u_0,v_0).

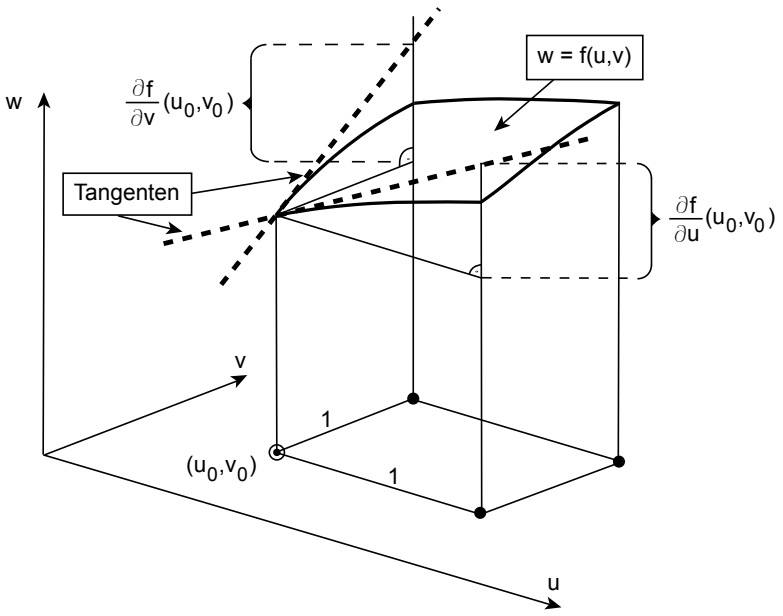


Abbildung 10.5: Partielle Ableitungen

C) Für unsere Quadrik $f = f(u, v)$ erhält man sofort:

a) $\frac{\partial f}{\partial u}(u_0, v_0) = 2Au_0 + Bv_0 + D$;

b) $\frac{\partial f}{\partial v}(u_0, v_0) = 2Cv_0 + Bu_0 + E$.

Satz 10.9. *(Diskriminantenformel) Sind $u_0, v_0 \in \mathbb{R}$ mit $f(u_0, v_0) = 0$, so gilt*

$$-\Delta_f = A\left(\frac{\partial f}{\partial v}(u_0, v_0)\right)^2 - B\frac{\partial f}{\partial u}(u_0, v_0)\frac{\partial f}{\partial v}(u_0, v_0) + C\left(\frac{\partial f}{\partial u}(u_0, v_0)\right)^2.$$

Beweis: 10.8 C) a), b) ergibt für die rechte Seite der behaupteten Gleichung den Term

$A(2Cv_0 + Bu_0 + E)^2 - B(2Au_0 + Bv_0 + D)(2Cv_0 + Bu_0 + E) + C(2Au_0 + Bv_0 + D)^2.$

Durch Ausmultiplizieren der einzelnen Summanden erhält man somit für die rechte Seite unserer Gleichung die Summe

$$\begin{aligned}
&\underline{4AC^2v_0^2} + \underline{AB^2u_0^2} + AE^2 + \underline{4ABCu_0v_0} + \underline{2ABEu_0} + \underline{4ACEv_0} \\
&- \underline{4ABCu_0v_0} - \underline{2AB^2u_0^2} - \underline{2ABEu_0} - \underline{2B^2Cv_0^2} \\
&- \underline{B^3u_0v_0} - \underline{B^2Ev_0} - \underline{2BCDv_0} - \underline{B^2Du_0} - BDE \\
&+ \underline{4A^2Cu_0^2} + \underline{B^2Cv_0^2} + CD^2 + \underline{4ABCu_0v_0} + \underline{4ACDu_0} + \underline{2BCDv_0}.
\end{aligned}$$

Die mit $\underline{\bullet}$ unterstrichenen Summanden ergeben zusammen

$$4AC(Au_0^2 + Bu_0v_0 + Cv_0^2 + Du_0 + Ev_0) = 4AC(f(u_0, v_0) - F) = -4ACF.$$

Die mit $\underset{\sim}{\bullet}$ unterstrichenen Summanden ergeben zusammen

$$-B^2(Au_0^2 + Bu_0v_0 + Cv_0^2 + Du_0 + Ev_0) = -B^2(f(u_0, v_0) - F) = B^2F.$$

Die mit $\underline{\underset{\sim}{\bullet}}$ unterstrichenen Summanden ergeben zusammen 0. Die ganze Summe hat also den Wert

$$-4ACF + B^2F + AE^2 - BDE + CD^2 = -\Delta_f.$$

■

Korollar 10.10. *Sei $f = f(u, v)$ nichtausgeartet und seien $u_0, v_0 \in \mathbb{R}$ mit $f(u_0, v_0) = 0$. Dann gilt:*

a) $\frac{\partial f}{\partial u}(u_0, v_0) \neq 0$ *oder* $\frac{\partial f}{\partial v}(u_0, v_0) \neq 0$*;*

b) Sind $\alpha, \beta \in \mathbb{R}$ mit

$$A\alpha^2 + B\alpha\beta + C\beta^2 = \frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta = 0,$$

so folgt $\alpha = \beta = 0$.

Beweis: „a)“: Klar aus 10.9 wegen $\Delta_f \neq 0$.

„b)“: Wegen $\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta = 0$ folgt $\alpha\frac{\partial f}{\partial u}(u_0, v_0) = -\beta\frac{\partial f}{\partial v}(u_0, v_0)$. Daraus ergeben sich die Gleichungen

$$\begin{aligned}
\alpha^2 \left(\frac{\partial f}{\partial u}(u_0, v_0)\right)^2 &= \beta^2 \left(\frac{\partial f}{\partial v}(u_0, v_0)\right)^2, \\
\alpha^2 \frac{\partial f}{\partial u}(u_0, v_0)\frac{\partial f}{\partial v}(u_0, v_0) &= -\alpha\beta \left(\frac{\partial f}{\partial v}(u_0, v_0)\right)^2, \\
\beta^2 \frac{\partial f}{\partial u}(u_0, v_0)\frac{\partial f}{\partial v}(u_0, v_0) &= -\alpha\beta \left(\frac{\partial f}{\partial u}(u_0, v_0)\right)^2.
\end{aligned}$$

Nun folgt mit 10.9

$$
\begin{aligned}
&-(\alpha^2+\beta^2)\Delta_f = (\alpha^2+\beta^2)A\left(\frac{\partial f}{\partial v}(u_0,v_0)\right)^2\\
&-(\alpha^2+\beta^2)B\frac{\partial f}{\partial u}(u_0,v_0)\frac{\partial f}{\partial v}(u_0,v_0)\\
&+(\alpha^2+\beta^2)C\left(\frac{\partial f}{\partial u}(u_0,v_0)\right)^2 =\\
&A\alpha^2\left(\left(\frac{\partial f}{\partial v}(u_0,v_0)\right)^2+\left(\frac{\partial f}{\partial u}(u_0,v_0)\right)^2\right)\\
&+B\alpha\beta\left(\left(\frac{\partial f}{\partial v}(u_0,v_0)\right)^2+\left(\frac{\partial f}{\partial u}(u_0,v_0)\right)^2\right)\\
&+C\beta^2\left(\left(\frac{\partial f}{\partial v}(u_0,v_0)\right)^2+\left(\frac{\partial f}{\partial u}(u_0,v_0)\right)^2\right) =\\
&(A\alpha^2+B\alpha\beta+C\beta^2)\left(\left(\frac{\partial f}{\partial v}(u_0,v_0)\right)^2+\left(\frac{\partial f}{\partial u}(u_0,v_0)\right)^2\right)=0.
\end{aligned}
$$

Wegen $\Delta_f \neq 0$ folgt $\alpha^2+\beta^2=0$. ■

Quadriken und Geraden

Jetzt wollen wir uns den Beziehungen zwischen Quadriken und Geraden zuwenden. Wieder fixieren wir ein Quadrik

$$f = f(u,v) = Au^2+Buv+Cv^2+Du+Ev+F.$$

Notation und Festsetzung 10.11. A) Wir betrachten einen Punkt $S=(u_0,v_0)\in \mathbb{M}(f)=\mathbb{M}$, d.h. einen Punkt mit $f(u_0,v_0)=0$. Zudem wählen wir eine Gerade g, welche durch den Punkt $S=(u_0,v_0)$ läuft. Wir werden uns später speziell für die Schnittpunkte von $\mathbb{M}(f)$ und g interessieren, d.h. für die Menge $\mathbb{M}(f)\cap g$.
Die Gerade g sei durch die folgende Parameterdarstellung beschrieben

a) $\quad g: s\mapsto (u_0+\alpha s, v_0+\beta s)$, wobei $(\alpha,\beta)\in\mathbb{R}^2\backslash\{(0,0)\}$.

B) Die *Richtung* der Geraden g ist bestimmt durch den „Winkel φ zwischen der positiven u-Achse und g“genauer durch den Winkel (im Bogenmass)

a)
$$\varphi := \begin{cases} \arctan\left(\frac{\beta}{\alpha}\right), & \text{falls } \alpha\neq 0;\\ \frac{\pi}{2}, & \text{falls } \alpha = 0.\end{cases}$$

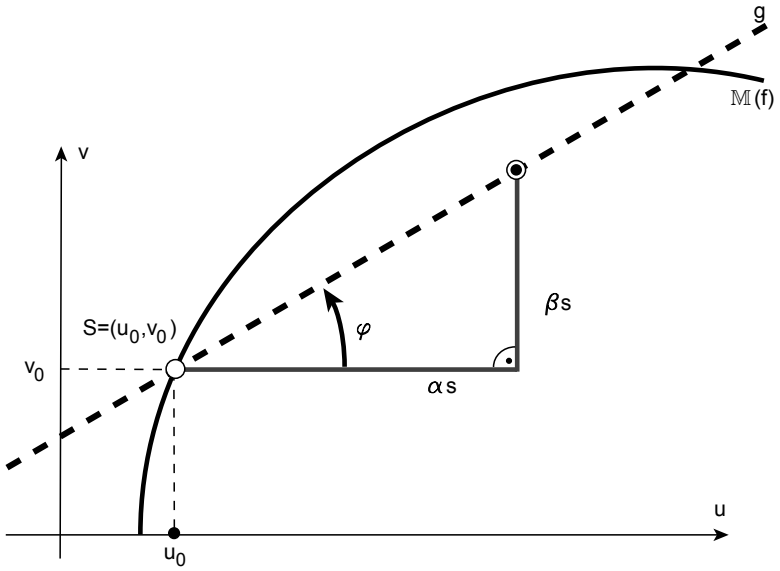


Abbildung 10.6: Quadrik und Gerade

Die *Distanz* des Punktes $\odot = (u_0 + \alpha s, v_0 + \beta s)$ vom Punkt $S = (u_0, v_0)$ ist natürlich gerade gegeben durch

b) $$\operatorname{dist}\left((u_0, v_0), (u_0 + \alpha s, v_0 + \beta s)\right) = |s|\sqrt{\alpha^2 + \beta^2}.$$

•

Für die Schnittpunkte der Quadrik $\mathbb{M} = \mathbb{M}(f)$ und der Geraden g gilt nun der nachfolgende Satz, auf dem alle späteren Ausführungen beruhen werden.

Satz 10.12. *Sei $f = f(u, v)$ nichtausgeartet und sei $S = (u_0, v_0) \in \mathbb{M}(f) = \mathbb{M}$. Sei g definiert wie in 10.11. Dann gilt:*

a) Gilt $A\alpha^2 + B\alpha\beta + C\beta^2 = 0$ oder

$$\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta = 0,$$

so ist S der einzige Schnittpunkt von $\mathbb{M}$ und g.

b) Gelten $A\alpha^2 + B\alpha\beta + C\beta^2 \neq 0$ und

$$\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta \neq 0,$$

so haben $\mathbb{M}$ und g nebst S noch genau einen weiteren Schnittpunkt. Dieser ist gegeben durch $S_g = (u_0 - s_0\alpha, v_0 - s_0\beta)$, wobei

$$s_0 = \frac{\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta}{A\alpha^2 + B\alpha\beta + C\beta^2}.$$

Beweis: Der Punkt $\odot = (u_0 + s\alpha, v_0 + s\beta)$ ist genau dann ein von S verschiedener Schnittpunkt von $\mathbb{M}$ und g, wenn die folgenden beiden Aussagen gelten:

(α) $f(u_0 + \alpha s, v_0 + \beta s) = 0$;

(α') $s \neq 0$.

Es gilt

$$\begin{aligned}
&f(u_0 + \alpha s, v_0 + \beta s)\\
&= A(u_0 + \alpha s)^2 + B(u_0 + \alpha s)(v_0 + \beta s) + C(v_0 + \beta s)^2\\
&+ D(u_0 + \alpha s) + E(v_0 + \beta s) + F\\
&\underline{Au_0^2} + 2Au_0\alpha s + A\alpha^2 s^2 + \underline{Bu_0v_0} + u_0\beta s\\
&+ Bv_0\alpha s + B\alpha\beta s^2 + \underline{Cv_0^2} + 2Cv_0\beta s + C\beta^2 s^2\\
&+ \underline{Du_0} + D\alpha s + \underline{Ev_0} + E\beta s + \underline{F}.
\end{aligned}$$

Die unterstrichenen Terme ergeben zusammen $f(u_0, v_0) = 0$ und können deshalb weggelassen werden. Wir fassen $f(u_0 + \alpha s, v_0 + \beta s)$ als Polynom von einem Grad kleiner oder gleich 2 in s auf und ordnen entsprechend nach Potenzen von s:

$$\begin{aligned}
&f(u_0 + \alpha s, v_0 + \beta s) =\\
&(2Au_0\alpha + Bu_0\beta + Bv_0\alpha + 2Cv_0\beta + D\alpha + E\beta) + s\\
&(A\alpha^2 + B\alpha\beta + C\beta^2)s^2.
\end{aligned}$$

So erhalten wir

$$\begin{aligned}
&f(u_0 + \alpha s, v_0 + \beta s) =\\
&((2Au_0 + Bv_0 + D)\alpha + (2Cv_0 + Bu_0 + E)\beta)\, s +\\
&(A\alpha^2 + B\alpha\beta + C\beta^2)s^2.
\end{aligned}$$

Beachten wir die Formeln 10.8 C) a), b), so ergibt sich schliesslich

$$\begin{aligned}
&f(u_0 + \alpha s, v_0 + \beta s)\\
&= \left(\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta\right) s + (A\alpha^2 + B\alpha\beta + C\beta^2)s^2.
\end{aligned}$$

Die Gleichung (α) ist also äquivalent zur Gleichung

$$s\left(\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta + (A\alpha^2 + B\alpha\beta + C\beta^2)s\right) = 0.$$

Die Aussagen (α) und (α') sind also genau dann beide erfüllt, wenn die folgenden Aussagen gelten:

(β) $\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta + (A\alpha^2 + B\alpha\beta + C\beta^2)s = 0$;

(β') $s \neq 0$.

Ist $\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta = 0$, so ist $A\alpha^2 + B\alpha\beta + C\beta^2 \neq 0$ (s. 10.10 b), 10.11 A) a)). Dann können aber (β) und (β') nicht gleichzeitig gelten. Ist $A\alpha^2 + B\alpha\beta + C\beta^2 = 0$, so ist $\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta \neq 0$ (s. 10.10 b), 10.11 A) a)). Dann kann aber (β) nicht gelten. Ist also eine der beiden Grössen $A\alpha^2 + B\alpha\beta + C\beta^2$ oder $\frac{\partial f}{\partial u}(x_0, y_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta$ gleich 0, so können die Aussagen (α) und (α') nicht gleichzeitig gelten. In diesem Fall muss also S der einzige Schnittpunkt von g und $\mathbb{M}$ sein. Dies beweist die Behauptung a).

Sind $A\alpha^2 + B\alpha\beta + C\beta^2$ und $\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta$ beide verschieden von 0, so sind die beiden Aussagen (β), (β') (und damit auch die beiden Aussagen (α), (α')) genau dann erfüllt, wenn

$$s = -\frac{\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta}{A\alpha^2 + B\alpha\beta + C\beta^2}.$$

Dies beweist die Aussage b). ■

Definition und Bemerkung 10.13. A) Es gelten die Bezeichnungen von 10.11. Ist $A\alpha^2 + B\alpha\beta + C\beta^2 = 0$, so sagen wir, g sei eine (bezüglich f) *kritische Gerade durch* S. Die Bedingung kritische Gerade zu sein hängt offenbar nicht von der Wahl von S ab, sondern nur von der Richtung von g (s. 10.11 B)). Die Richtung einer kritischen Geraden nennt man entsprechend eine kritische Richtung von f.

B) Ist f nichtausgeartet, so gibt es wegen 10.10 a) genau eine Gerade g durch $S = (u_0, v_0)$, für die gilt

$$\frac{\partial f}{\partial u}(u_0, v_0)\alpha + \frac{\partial f}{\partial v}(u_0, v_0)\beta = 0.$$

Diese Gerade nennen wir die *Tangente* zu f in S. Wir wollen uns überlegen, dass die Eigenschaft kritisch und Tangente zu sein sich gegenseitig ausschliessen, also:

a) *Die Gerade g kann nicht zugleich Tangente zu f in S und kritisch bezüglich f sein.*

Wäre dies nämlich der Fall, so hätten wir gemäss 10.10 b) die Gleichheit $\alpha = \beta = 0$, entgegen unserer Annahme, dass $(\alpha, \beta) \neq (0, 0)$. •

Aus der letzten Definition ist zunächst überhaupt nicht direkt ersichtlich, ob die Eigenschaft Tangente zu f zu sein unserer geometrischen Vorstellung einer Tangente entspricht. Ebenso leuchtet die geometrische Bedeutung der kritischen Gerade bezüglich f nicht ein. Auf beide Punkte werden wir später zu sprechen kommen. Als Konsequenz von 10.12 erhalten wir nun in der soeben eingeführten Sprechweise:

Korollar 10.14. *Seien $f, \mathbb{M}, S$ und g wie in 10.12. Dann gilt: Ist g kritisch bezüglich f oder die Tangente zu f in S, so ist S der einzige Schnittpunkt von $\mathbb{M}$ und g. Andernfalls haben $\mathbb{M}$ und g nebst S genau einen weiteren Schnittpunkt.* ■

Um die Bedeutung des vorangehenden Satzes zu schätzen sollte man wissen, ob es bezüglich einer Quadrik viele kritische Geraden geben kann. In der Tat kann es höchstens zwei solcher Geraden geben. Genauer gilt:

Satz 10.15. *Sei $f = Au^2 + Buv + Cv^2 + Du + Ev + F$ eine nichtausgeartete Quadrik, sei $S = (u_0, v_0) \in \mathbb{M}(f)$ und sei $\delta := B^2 - 4AC$. Dann gilt:*

a) *Ist $\delta < 0$, so gibt es keine bezüglich f kritische Gerade.*

b) *Ist $\delta = 0$, so gibt es genau eine bezüglich f kritische Gerade durch S. Die kritische Richtung ist dann festgelegt durch den gemäss 10.11 B) a) definierten Winkel*

$$\varphi = \begin{cases} \arctan\left(\frac{-B}{2C}\right), & \text{falls } C \neq 0; \\ \frac{\pi}{2}, & \text{falls } C = 0. \end{cases}$$

c) *Ist $\delta > 0$, so gibt es genau zwei bezüglich f kritische Geraden durch S. Die kritischen Richtungen sind dann festgelegt durch die Winkel*

$$\varphi = \begin{cases} \arctan(\frac{-B+\sqrt{\delta}}{2C}), & \text{falls } C \neq 0; \\ \frac{\pi}{2}, & \text{falls } C = 0, \end{cases}$$

$$\varphi' = \begin{cases} \arctan(\frac{-B-\sqrt{\delta}}{2C}), & \text{falls } C \neq 0; \\ \arctan(\frac{-A}{B}), & \text{falls } C = 0. \end{cases}$$

Beweis: Ist g eine kritische Gerade, so besteht in den Bezeichnungen von 10.11 die Gleichung $A\alpha^2 + B\alpha\beta + C\beta^2 = 0$. Aus dieser erhalten wir wegen $(\alpha, \beta) \neq (0, 0)$:

(α) $\alpha \neq 0 \Rightarrow \left(\frac{\beta}{\alpha}\right)^2 C + \left(\frac{\beta}{\alpha}\right) B + A = 0$;

(α') $\alpha = 0 \Rightarrow \beta \neq 0$ und $C = 0$.

Aus der Schule weiss man, dass die Gleichung

$$x^2 C + xB + A = 0$$

(β) keine Lösung hat, wenn $\delta < 0$;

(β') genau die Lösung $x = \frac{-B}{2C}$ hat, wenn $C \neq 0$ und $\delta = 0$;

(β'') genau die zwei Lösungen $x_{1/2} = \frac{-B \pm \sqrt{\delta}}{2C}$ hat, wenn $C \neq 0$ und $\delta > 0$.

„a)“: Ist $\delta < 0$, so ist $C \neq 0$. Mit $(\alpha), (\alpha')$ und (β) folgt sofort, dass es in diesem Fall keine kritische Gerade durch S gibt.

„b)“: Sei $\delta = 0$. Ist $C \neq 0$, so folgt aus $(\alpha), (\alpha')$ und (β'), dass es genau eine kritische Gerade durch S gibt, wobei $\alpha \neq 0$ und $\frac{\beta}{\alpha} = \frac{-B}{2C}$ gelten müssen. Ist $C = 0$, so folgt aus $\delta = 0$ auch $B = 0$. Weil f nichtausgeartet ist, folgt $A \neq 0$, also $\alpha = 0$ und es gibt wieder eine einzige kritische Gerade durch S. Die Aussage über den Winkel φ folgt nun mit 10.11 B) a).

„c)“: Sei $\delta > 0$. Ist $C \neq 0$, so folgt aus $(\alpha), (\alpha')$ und (β''), dass es genau zwei kritische Geraden durch S gibt, wobei für diese gilt $\frac{\beta}{\alpha} = \frac{-B \pm \sqrt{\delta}}{2C}$.

Ist $C = 0$, so gilt wegen $\delta > 0$ sicher $B \neq 0$, und die möglichen kritischen Geraden g durch S sind festgelegt durch die Lösungspaare (α, β) der Gleichung $A\alpha^2 + B\alpha\beta = 0$. Dies führt wieder zu genau zwei kritischen Geraden g durch den Punkt S. Für die eine dieser Geraden ist $\alpha = 0$, für die andere ist $\alpha \neq 0$ und $\frac{\beta}{\alpha} = -\frac{A}{B}$. ■

Geometrische Bedeutung der Tangenten und der kritischen Geraden

Wie schon früher angekündigt, möchten wir uns nun auch mit der anschaulich-geometrischen Seite des Begriffs der kritischen Geraden und der Tangenten auseinandersetzen.

Bemerkung 10.16. A) Sei $f(u, v) = Au^2 + Buv + Cv^2 + Du + Ev + F$ eine nichtausgeartete Quadrik und sei $S = (u_0, v_0) \in \mathbb{M}(f)$. Wir wählen $\tau \in \mathbb{R}$, setzen $\alpha = \cos(\tau)$ und $\beta = \sin(\tau)$ und betrachten die zugehörige Gerade g, definiert durch die Parameterdarstellung $s \mapsto (u_0 + \cos(\tau)s, v_0 + \sin(\tau)s)$ (s. 10.11 A) a)). Wir bezeichnen diese Gerade mit g_τ. Durchläuft τ das Intervall $\left]-\frac{\pi}{2}, \frac{\pi}{2}\right]$ (oder sogar ganz $\mathbb{R}$), so durchläuft g_τ alle möglichen Geraden durch S.

Sei zunächst τ so gewählt, dass g_τ weder Tangente zu f noch kritische Gerade bezüglich f ist. Gemäss 10.14 hat dann $\mathbb{M} = \mathbb{M}(f)$ mit g_τ nebst S genau einen weiteren Schnittpunkt, den wir mit $S_{[\tau]}$ bezeichnen wollen. Wegen $\sqrt{\cos(\tau)^2 + \sin(\tau)^2} = 1$ erhalten wir aus 10.12 und 10.11 B) b) (mit $\alpha = \cos(\tau)$ und $\beta = \sin(\tau)$) für die Distanz der beiden Punkte S und $S_{[\tau]}$ den Wert

$$\text{a)} \qquad \operatorname{dist}(S, S_{[\tau]}) = \left| \frac{\frac{\partial f}{\partial u}(u_0,v_0)\cos(\tau) + \frac{\partial f}{\partial v}(u_0,v_0)\sin(\tau)}{A\cos(\tau)^2 + B\cos(\tau)\sin(\tau) + C\sin(\tau)^2} \right|$$

B) Sei nun $\psi \in \left]-\frac{\pi}{2}, \frac{\pi}{2}\right]$ der Richtungswinkel der Tangente zu f in S, d.h. g_ψ ist die Tangente zu f in S. Dann ist ψ sicher keine kritische Richtung bezüglich f (s. 10.13 B) a)). Also ist

$$N := A\cos(\psi)^2 + B\cos(\psi)\sin(\psi) + C\sin(\psi)^2 \neq 0.$$

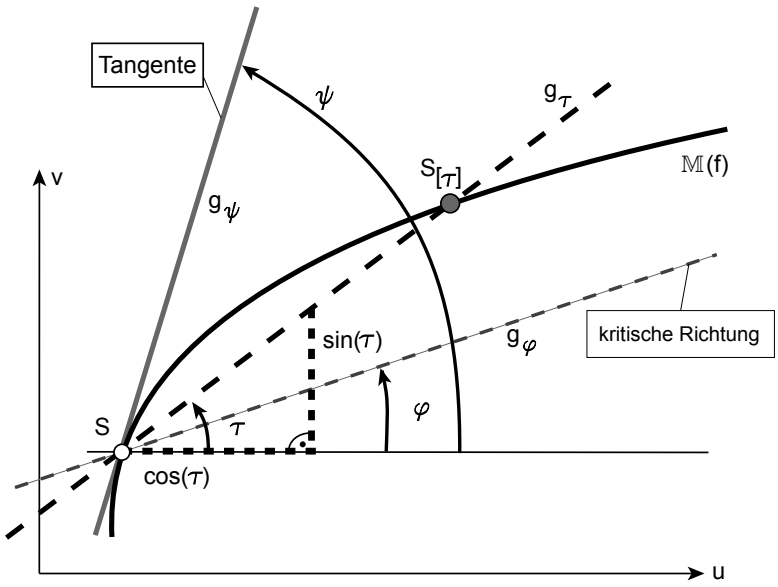


Abbildung 10.7: Tangente und kritische Gerade

Andererseits ist

$$\frac{\partial f}{\partial u}(u_0, v_0)\cos(\psi) + \frac{\partial f}{\partial v}(u_0, v_0)\sin(\psi) = 0.$$

Lassen wir τ (in $\mathbb{R}\backslash\{\psi + n\pi | n \in \mathbb{Z}\}$) nach ψ streben, so strebt der Zähler des in A) a) rechts stehenden Bruches nach 0, während der Nenner nach $N \neq 0$ strebt, denn sowohl der Zähler als auch der Nenner sind stetige Fuktionen in τ. Es gilt deshalb

$$\lim_{\tau \to \psi} \operatorname{dist}(S, S_{[\tau]}) = 0.$$

In Worten ausgedrückt: Dreht die Gerade g_τ zur Tangente g_ψ ein, so strebt der Schnittpunkt $S_{[\tau]}$ von g_τ mit $\mathbb{M}$ gegen den Punkt S : g_τ wird im anschaulichen Sinne zur Tangente, wenn „g_τ zu g_ψ eindreht“.

C) Wir wählen nun $\varphi \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ so, dass g_φ eine kritische Gerade ist. Solche kritische Werte gibt es nach 10.15 höchstens zwei.

Nun ist aber (weil g_φ eine kritische Gerade ist)

$$A\cos(\varphi)^2 + B\cos(\varphi)\sin(\varphi) + C\sin(\varphi) = 0$$

und (weil g_φ gemäss 10.13 B) a) keine Tangente ist)

$$Z := \frac{\partial f}{\partial u}(u_0, v_0)\cos(\varphi) + \frac{\partial f}{\partial v}(u_0, v_0)\sin(\varphi) \neq 0.$$

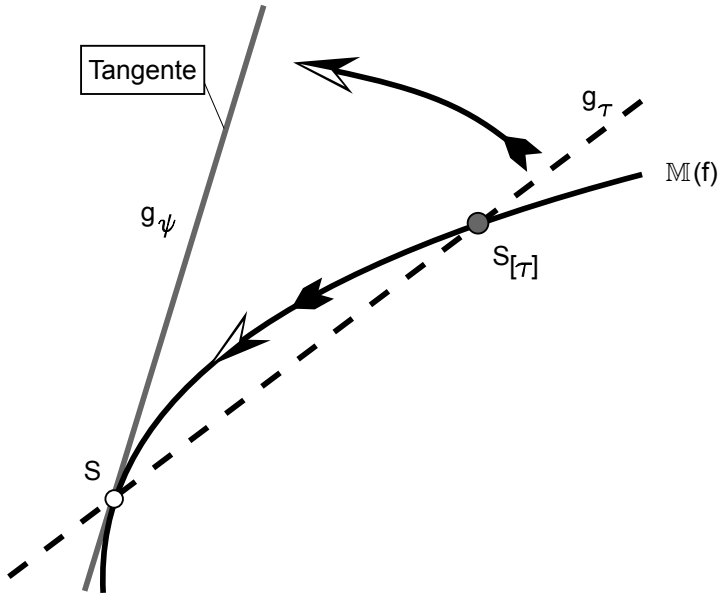


Abbildung 10.8: Grenzverhalten in Tangentenrichtung

Lässt man τ nach φ streben (unter Vermeidung der Werte $\varphi + n\pi$ und $\varphi' + n\pi$ ($n \in \mathbb{Z}$), wo $\varphi' \in \left]-\frac{\pi}{2}, \frac{\pi}{2}\right]$ die allfällige zweite kritische Richtung von f festlegt), so strebt der Zähler des in A) a) rechts stehenden Bruches nach Z, der Nenner aber nach 0. Es folgt

$$\lim_{\tau \to \varphi} \operatorname{dist}(S, S_{[\tau]}) = \infty.$$

In Worten ausgedrückt: Dreht die Gerade g_τ in eine kritische Richtung ein, so wandert der Schnittpunkt $S_{[\tau]}$ ins Unendliche ab. Die Kurve $\mathbb{M}(f)$ verschwindet also in der kritischen Richtung im Unendlichen.

D) Ohne weiteren Kommentar wollen wir festhalten, was die vorangehenden Überlegungen im Fall $\mathbb{M}(f) \neq \emptyset$ nahelegen:

a) *Ist $B^2 - 4AC < 0$, d.h. gibt es keine bezüglich f kritische Gerade, so ist $\mathbb{M}(f)$ eine Ellipse.*

b) *Ist $B^2 - 4AC = 0$, d.h. gibt es genau eine bezüglich f kritische Richtung, so ist $\mathbb{M}(f)$ eine Parabel, und die kritische Richtung ist die Achsenrichtung dieser Parabel.*

c) *Ist $B - 4AC > 0$, d.h. gibt es genau zwei bezüglich f kritische Richtungen, so ist $\mathbb{M}(f)$ eine Hyperbel und, die kritischen Richtungen sind die Asymptotenrichtungen dieser Hyperbel.*

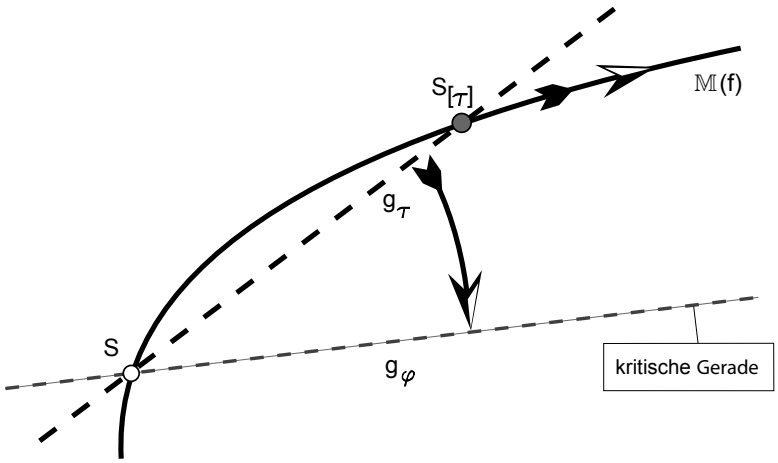


Abbildung 10.9: Grenzverhalten in kritischer Richtung

Wenn Sie finden, dass die Überlegungen aus A)–C) diese Aussagen nahelegen, so wissen Sie bereits, was Ellipsen, Parabeln und Hyperbeln sind. In diesem Fall fühlen Sie sich vielleicht herausgefordert, die Aussagen a), b) und c) zu beweisen. Sollte letzteres zutreffen, wäre ein Blick auf die Frage 1.8 (sinngemäss abgewandelt) vielleicht angezeigt. Sind für Sie Ellipsen, Parabeln, Hyperbeln und deren Eigenschaften hingegen Neuland, so können Sie die Aussagen a), b) und c) als Definition der neuen Begriffe verstehen. •

Aufgaben 10.17. A) Bestimmen Sie eine Parameterdarstellung und den Richtungswinkel der Tangente g zur Quadrik $f(u,v) = u^2 + 4v^2 - 4$ im Punkt $(u_0, v_0) = (u_0, ?)$ mit $v_0 > 0$.

B) Bestimmen Sie die kritischen Richtungen der Quadrik $-4u^2 + v^2 - 4 = f(u,v)$. Skizzieren Sie die Situation.

C) Sei $f(u,v) = u^2 - 2uv + v^2 + u - 1$. Zeigen Sie, dass f nichtausgeartet ist und bestimmen Sie die kritischen Richtungen von $f = f(u,v)$. Bestimmen Sie $(u_0, v_0) = S \in \mathbb{M} = \mathbb{M}(f)$ so, dass die Tangente zu f in S senkrecht zu einer kritischen Richtung verläuft.

D) Sei $f = f(u,v)$ eine nichtausgeartete Quadrik. Sei $h \subseteq \mathbb{R}^2$ eine Gerade. Zeigen Sie:

a) $\sharp \mathbb{M}(f) \cap h \leq 2$;

b) $\sharp \mathbb{M}(f) \cap h = 1$ gilt genau dann, wenn h kritisch oder eine Tangente zu f ist;

c) h kann nicht gleichzeitig Tangente und kritisch sein.

E) Sei $f = f(u,v)$ wie in C). Skizzieren Sie für $c \in \{0, \pm 1, \pm 2\}$ die Niveaulinien von $f(u,v) = c$. •

Rationale Parametrisierung der Quadriken

Nun führen wir die in 10.2 skizzierte Konstruktion auch wirklich aus.

Konstruktion 10.18. A) Sei $f(u,v) = Au^2 + Buv + Cv^2 + Du + Ev + F$ eine nichtausgeartete Quadrik. Sei $S = (u_0, v_0) \in \mathbb{M} = \mathbb{M}(f)$. Nach 10.10 a) sind dann die beiden partiellen Ableitungen $\frac{\partial f}{\partial u}(u_0, v_0)$ und $\frac{\partial f}{\partial v}(u_0, v_0)$ nicht beide 0. Wir wählen nun zwei Zahlen $a, b \in \mathbb{R}$ mit

$$\tfrac{\partial f}{\partial u}(u_0, v_0)a + \tfrac{\partial f}{\partial v}(u_0, v_0, v_0)b = 0 \text{ und } (a,b) \neq (0,0).$$

Eine Wahl, die sich aufdrängt, ist natürlich etwa (s. auch 10.8 C) a), b)):

a) $a := \frac{\partial f}{\partial v}(u_0, v_0) + 2Cv_0 + Bu_0 + E;$

$b := -\frac{\partial f}{\partial u}(u_0, v_0, v_0) = -(2Au_0 + Bv_0 + D).$

Nun betrachten wir die Hilfsgerade h, gegeben durch die Parameterdarstellung

b) $h : t \mapsto P_t := (u_0 + b + at, v_0 - a + bt).$

Gemäss 10.13 B) wird die Tangente zu f in S parametrisiert durch $t \mapsto (u_0 + at, v_0 + bt)$ und hat damit den gleichen Richtungsvektor wie die Gerade h, nämlich (a, b). Damit ist h parallel zur Tangente oder fällt mit dieser zusammen. Für jede Wahl von t gilt aber auch

$$\begin{aligned}\operatorname{dist}(S, P_t) &= \sqrt{(b+at)^2 + (-a+bt)^2} \\ &= \sqrt{a^2 + a^2t^2 + b^2 + b^2t^2} = \sqrt{a^2(1+t^2) + b^2(1+t^2)} \\ &= \sqrt{1+t^2}\sqrt{a^2+b^2} \geq \sqrt{a^2+b^2} > 0,\end{aligned}$$

also $S \neq P_t$. Dies bedeutet aber, dass $S \notin h$. Deshalb ist h nicht die Tangente zu f in S.

B) Wegen $S \neq P_t$ für alle $t \in \mathbb{R}$ gibt es zu jeder Zahl $t \in \mathbb{R}$ eine eindeutig bestimmte Gerade durch die Punkte S und P_t, die wir mit g_t bezeichnen. Die Gerade g_t parametrisieren wir nun gemäss 10.11 A) a) durch

$$g_t : s \mapsto (u_0 + \alpha(t)s, v_0 + \beta(t)s),$$

wobei

a) $\alpha(t) := b + at; s\beta(t) := -a + bt.$

Wegen $S, P_t \in g_t, S \notin h$ und $P_t \in h$ ist g_t sicher nicht parallel zu h, also auch nicht parallel zur Tangente zu f in S.

C) Ist g_t eine bezüglich f kritische Gerade, d.h. gilt (s. 10.13 A))

$$A\alpha(t)^2 + B\alpha(t)\beta(t) + C\beta(t)^2 = 0,$$

so nennen wir t einen *kritischen Parameterwert*. Da es höchstens zwei kritische Geraden gibt, kann es höchstens zwei kritische Parameterwerte geben. Wir schreiben $\mathcal{C}$ für die Menge dieser kritischen Parameterwerte, also

$$\mathcal{C} := \{t \in \mathbb{R} \,\big|\, A\alpha(t)^2 + B\alpha(t)\beta(t) + C\beta(t)^2 = 0\},$$

und vergessen nicht, dass $\sharp\mathcal{C} \leq 2$.

Nun wählen wir $t \in \mathbb{R}\backslash\mathcal{C}$. Dann ist g_t bezüglich f nicht kritisch und hat deshalb mit $\mathbb{M}$ nebst S noch genau einen weiteren Schnittpunkt $S_t := S_{g_t}$, der gemäss 10.12 b) gegeben ist durch

a) $$S_t = (u_0 - s(t)\alpha(t),\ v_0 - s(t)\beta(t)),$$

wobei

b) $$s(t) = \frac{\frac{\partial f}{\partial u}(u_0,v_0)\alpha(t) + \frac{\partial f}{\partial v}(u_0,v_0)\beta(t)}{A\alpha(t)^2 + B\alpha(t)\beta(t) + C\beta(t)^2}.$$

Anschaulich präsentiert sich die Situation (im Fall wo $\mathbb{M}$ eine Hyperbel ist) wie in Abbildung 10.10 dargestellt.

D) Um zu einer „parameterfreien“Beschreibung unserer Konstruktion zu gelangen, beachten wir, dass die Parametrisierung $t \mapsto P_t$ von h (vgl. A) b)) eine bijektive Abbildung ist. Zu jedem Punkt $P \in h$ gibt es also genau einen Parameterwert $t \in \mathbb{R}$ mit $P_t = P$. Diesen Parameterwert bezeichnen wir mit $t(P)$. Es gilt also

$$P_{t(P)} = P.$$

Wir schreiben auch

$$g(P) := g_{t(P)}.$$

Ist $g(P)$ eine bezüglich f kritische Gerade, d.h. ist $t(P) \in \mathcal{C}$, so nennen wir $P \in h$ einen bezüglich f kritischen Punkt. Wegen $\sharp\mathcal{C} \leq 2$ gibt es höchstens 2 kritische Punkte auf h. Die Menge der nichtkritischen Punkte auf h bezeichnen wir mit h^0, also:

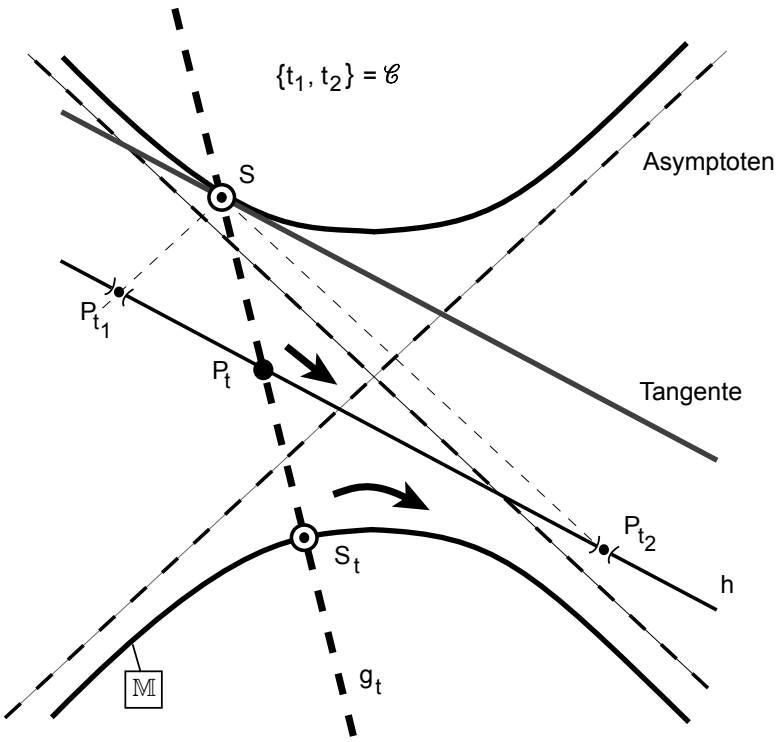


Abbildung 10.10: Konstruktion einer Parametrisierung

a) $h^0 := \{P \in h \,|\, t(P) \notin \mathcal{C}\}$.

Für $P \in h^0$ ist also $t(P)$ kein kritischer Parameterwert und wir können deshalb setzen:

b) $S(P) := S_{t(P)}, (P \in h^0)$.

Veranschaulicht an unserer Hyperbel $\mathbb{M}$ besteht nun also die Situation, die in Abbildung 10.11 dargestellt ist. •

Nun gelangen wir zum eigentlichen Hauptsatz dieses ganzen Kapitels, den wir zunächst wie folgt formulieren wollen:

Satz 10.19. *Es gelten die Voraussetzungen und Bezeichnungen aus 10.18. Dann besteht die bijektive Abbildung*

$$\sigma : h^0 \xrightarrow{\approx} \mathbb{M}\backslash\{S\};\ P \overset{\sigma}{\mapsto} S(P).$$

Beweis: Nach den Ausführungen in 10.18 ist $S(P) \in \mathbb{M}$ für alle $P \in h^0$ definiert, und von S verschieden. Also ist die angegebene Abbildung $\sigma : h^0 \to \mathbb{M}\backslash\{S\}$ überhaupt definiert.

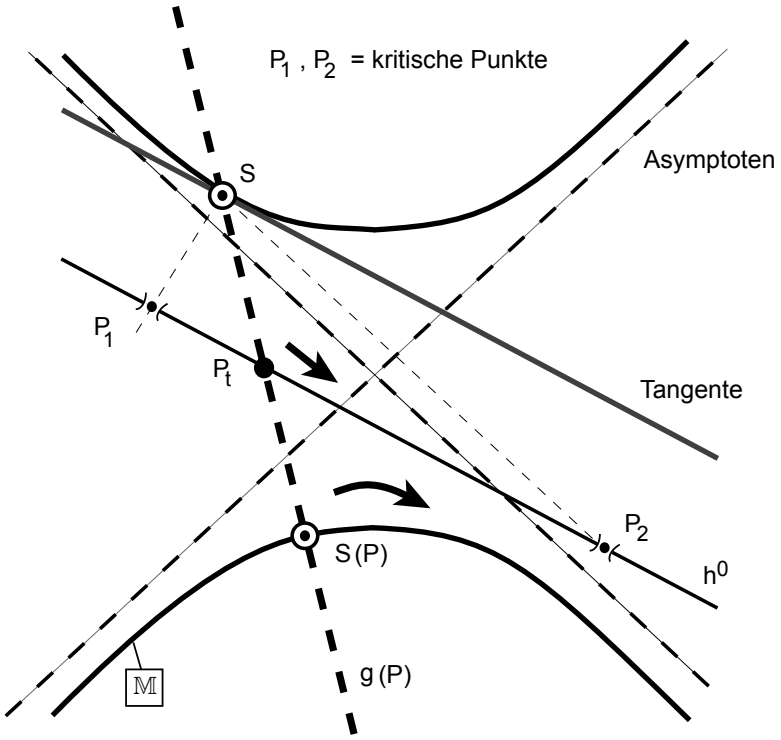


Abbildung 10.11: Parameterfreie Beschreibung der Konstruktion

Zuerst zeigen wir, dass σ injektiv ist. Seien also $P, Q \in h^0$ mit $\sigma(P) = \sigma(Q)$. Dann ist $S(P) = S(Q)$. Nun läuft aber $g(P)$ durch die Punkte S und $S(P)$, während $g(Q)$ durch die Punkte S und $S(Q)$ verläuft. Wegen $S(P) = S(Q) \neq S$ folgt $g(P) = g(Q)$. Nun sind aber P der Schnittpunkt von $g(P)$ mit h und Q der Schnittpunkt von $g(Q)$ mit h. Wegen $g(P) = g(Q)$ folgt $P = Q$. Damit ist gezeigt, dass σ injektiv ist.

Es bleibt zu zeigen, dass σ surjektiv ist. Sei also $T \in \mathbb{M}\backslash\{S\}$. Sei g die Gerade durch S und T. Weil g mit $\mathbb{M}$ mindestens die zwei verschiedenen Punkte S und T gemeinsam hat, kann g gemäss 10.16 weder kritisch bezüglich f noch die Tangente zu f in S sein. Weil h zu dieser Tangente parallel ist, folgt aus $S \in g$, dass h und g nicht parallel sind. Insbesondere schneidet g die Hilfsgerade h in einem einzigen Punkt P. Weil g bezüglich f nicht kritisch ist, gilt $P \in h^0$. Nun ist aber g die Gerade durch S und P, also $g = g(P)$. Weiter ist T der (nach 10.18 einzige) Schnittpunkt von $\mathbb{M}$ mit $g(P)$, der von S verschieden ist, also $T = S(P) = \sigma(P)$. Dies beweist, dass σ surjektiv ist. ■

Nun wollen wir den vorangehenden Satz in eine Form bringen, welche tatsächlich eine Parametrisierung der Menge $\mathbb{M}\backslash\{S\}$ ergibt.

Satz 10.20. *(Rationale Parametrisierung einer nichtausgearteten Quadrik) Sei* $f(u, v) = Au^2 + Buv + Cv^2 + Du + Ev + F$ *eine nichtausgeartete Quadrik und sei* $S = (u_0, v_0) \in$

$\mathbb{M} = \mathbb{M}(f)$. *Wir setzen*

$$\begin{aligned}
&a := 2Cv_0 + Bu_0 + E;\ b := 2Au_0 + Bv_0 + D;\\
&N(t) := -\Delta_f t^2 - (B(a^2 - b^2) - 2(A - C)ab)t + Ab^2 - Bab + ca^2;\\
&\mathcal{C} := \{t \in \mathbb{R} \,\big|\, N(t) = 0\};\\
&u(t) := u_0 + (a^2 + b^2)\frac{b + at}{N(t)}, (t \in \mathbb{R} \setminus \mathcal{C});\\
&v(t) := v_0 - (a^2 + b^2)\frac{a - bt}{N(t)}, (t \in \mathbb{R} \setminus \mathcal{C}).
\end{aligned}$$

Dann besteht die bijektive Abbildung

$$\varepsilon_S = \varepsilon : \mathbb{R}\backslash\mathcal{C} \xrightarrow{\approx} \mathbb{M}\backslash\{S\};\ t \mapsto \varepsilon(t) := (u(t), v(t)).$$

Beweis: In den Bezeichnungen von 10.18 A) a) und 10.18 B) a) gilt

$$\begin{aligned}
&A\alpha(t)^2 + B\alpha(t)\beta(t) + C\beta(t)^2\\
&= A(b + at)^2 + B(b + at)(-a + bt) + C(-a + bt)^2\\
&= (Aa^2 + Bab + Cb^2)t^2 + (2Aab - Ba^2 + Bb^2 - 2Cab)t\\
&+ Ab^2 - Bab + Ca^2.
\end{aligned}$$

Nach 10.18 A) a) und der Diskriminantenformel 10.9 gilt aber $Aa^2 + Bab + Cb^2 = -\Delta_f$ und es folgt

$$A\alpha(t)^2 + B\alpha(t)\beta(t) + C\beta(t)^2 = N(t).$$

Es gilt also tatsächlich

$$\mathcal{C} = \{t \in \mathbb{R} \,\big|\, t \text{ ist ein kritischer Parameterwert}\}.$$

Ist $t \in \mathbb{R}\backslash\mathcal{C}$, so gilt nun in den Bezeichnungen von 10.18 C) b) wegen 10.18 A) a) und 10.18 B) a) auch

$$s(t) = \frac{-b(b + at) + a(-a + bt)}{N(t)} = \frac{-b^2 - a^2}{N(t)},$$

also

$$s(t) = -\frac{a^2 + b^2}{N(t)}.$$

Vermöge 10.18 C) a) und 10.18 B) a) folgt also

$$S_t = \left(u_0 + \frac{a^2 + b^2}{N(t)}(b + at), v_0 + \frac{a^2 + b^2}{N(t)}(-a + bt)\right),$$

und damit

$$(\alpha) \qquad S_t = (u(t), v(t)),\ (t \in \mathbb{R}\backslash\mathcal{C}).$$

In den Bezeichnungen von 10.18 D) ist die Abbildung $t(\bullet) : h \to \mathbb{R}, (P \mapsto (t(P))$ bijektiv. Weiter gilt $t(h^0) = \mathbb{R}\backslash\mathcal{C}$, (s. 10.18 D) a)). Wir erhalten also die bijektive Abbildung

$$\psi : h^0 \xrightarrow{\approx} \mathbb{R}\backslash\mathcal{C};\ (P \mapsto t(P)).$$

Nach 10.18 D) b) und 10.19 gilt für alle $t \in \mathbb{R}\backslash\mathcal{C}$ die Beziehung

$$S_t = S_{\psi(\psi^{-1}(t))} = S_{t(\psi^{-1}(t))} = S(\psi^{-1}(t)) = \sigma(\psi^{-1}(t)).$$

Für die durch $t \mapsto S_t$ definierte Abbildung $\varepsilon : \mathbb{R}\backslash\mathcal{C} \to \mathbb{M}\backslash\{S\}$ gilt also

$$\varepsilon(t) = \sigma(\psi^{-1}(t)) = \sigma \circ \psi^{-1}(t);\ (t \in \mathbb{R}\backslash\mathcal{C}).$$

Damit ist ε die Komposition der bijektiven Abbildung ψ^{-1} mit der nach 10.19 ebenfalls bijektiven Abbildung σ. Also ist ε bijektiv, d.h. es besteht gemäss (α) tatsächlich die bijektive Abbildung

$$\varepsilon : \mathbb{R}\backslash\mathcal{C} \xrightarrow{\approx} \mathbb{M}\backslash\{S\};\ t \mapsto \varepsilon(t) = S(t) = (u(t), v(t)).$$

■

Für nichtausgeartete rationale Quadriken gilt nun die folgende wichtige Ergänzung:

Korollar 10.21. *Es gelten die Voraussetzungen und Bezeichnungen von 10.20. Zudem seien die Quadrik f rational (d.h. $A, B, C, D, E, F \in \mathbb{Q}$) und der Punkt $S \in \mathbb{M}$ rational (d.h. $u_0, v_0 \in \mathbb{Q}$). Weiter sei $t \in \mathbb{R}\backslash\mathcal{C}$. Dann gilt:*

$$t \in \mathbb{Q} \Longleftrightarrow \varepsilon(t) \in \mathbb{Q}^2.$$

Beweis: „$\Longrightarrow$“: Sei $t \in \mathbb{Q}$. Nach Voraussetzung gilt $A, B, C, D, E, F, u_0, v_0 \in \mathbb{Q}$. Es folgt $a, b \in \mathbb{Q}$. Wegen $t \in \mathbb{Q}$ folgt nun aber auch $N(t) \in \mathbb{Q}$ und $b - at, a + bt \in \mathbb{Q}$, d.h. $u(t), v(t) \in \mathbb{Q}$, also $\varepsilon(t) = (u(t), v(t)) \in \mathbb{Q}^2$.

„$\Longleftarrow$“: Sei $\varepsilon(t) \in \mathbb{Q}^2$. Dann gilt $u(t), v(t) \in \mathbb{Q}$. Wegen $u_0, v_0 \in \mathbb{Q}$ folgen $a, b, (a^2 + b^2)\frac{b+at}{N(t)}, (a^2 + b^2)\frac{a-bt}{N(t)} \in \mathbb{Q}$. Nach 10.10 a) ist $a \neq 0$ oder $b \neq 0$. Insbesondere ist $a^2 + b^2 \in \mathbb{Q}\backslash\{0\}$ und es folgt

$$(\alpha) \qquad \frac{b + at}{N(t)}, \quad \frac{a - bt}{N(t)} \in \mathbb{Q}.$$

Ist $a - bt = 0$, so folgt aus $(a, b) \neq (0, 0)$, dass $b \neq 0$, also, dass $t = \frac{a}{b} \in \mathbb{Q}$.

Sei also $a - bt \neq 0$. Durch Division der beiden Brüche aus (α) folgt dann $\frac{b+at}{a-bt} \in \mathbb{Q}$. Mit geeignetem $q \in \mathbb{Q}$ gilt also

$$\frac{b + at}{a - bt} = q,$$

d.h.

$$(\beta) \qquad b - aq = -(a + bq)t.$$

Ist $a + bq \neq 0$, so folgt aus $b - aq, a + bq \in \mathbb{Q}$, dass $t \in \mathbb{Q}$ und wir sind fertig.

Ist $a+bq = 0$, so ist gemäss (β) auch $b-aq = 0$, d.h. $b = aq$ und es folgt der Widerspruch $a^2 + b^2 = a^2 + abq = a(a + bq) = 0$. Also muss immer gelten $a + bq \neq 0$. ■

Als Anwendung ergibt sich:

Korollar 10.22. *Sei $f(u, v) = Au^2 + Buv + Cv^2 + Eu + Dv + F$ eine nichtausgeartete rationale Quadrik und sei $S = (u_0, v_0) \in \mathbb{M} = \mathbb{M}(f)$ mit $u_0, v_0 \in \mathbb{Q}$. Dann gilt in den Bezeichnungen von 10.20:*

a) *Durch Einschränkung der Abbildung $\varepsilon = \varepsilon_S : \mathbb{R}\backslash\mathcal{C} \to \mathbb{M}\backslash\{S\}$ erhält man eine bijektive Abbildung*

$$\varepsilon_S\restriction = \varepsilon\restriction : \mathbb{Q}\backslash\mathcal{C} \xrightarrow{\approx} \mathbb{Q}^2 \cap (\mathbb{M}\backslash\{S\}), \ (t \mapsto (u(t), v(t)).$$

b) $\mathbb{Q}^2 \cap \mathbb{M} = \{S\} \cup \{(u(t), v(t)) \,\big|\, t \in \mathbb{Q}\backslash\mathcal{C}\}$.

Beweis: „a)“: Weil $\varepsilon : \mathbb{R}\backslash\mathcal{C} \to \mathbb{M}\backslash\{S\}$ gemäss 10.20 bijektiv ist, folgt die Behauptung sofort aus 10.21.

„b)“: Klar aus Aussage a). ■

Definition 10.23. A) Sei $f(u, v) = Au^2+Buv+Cv^2+Du+Ev+F$ eine nichtausgeartete Quadrik und sei $S = (u_0, v_0) \in \mathbb{M} = \mathbb{M}(f)$. Die bijektive Abbildung

$$\varepsilon_S = \varepsilon : \mathbb{R}\backslash\mathcal{C} \xrightarrow{\approx} \mathbb{M}\backslash\{S\}; \ (t \mapsto \varepsilon(t) = (u(t), v(t)))$$

aus 10.20 heisst die *zu S gehörige rationale (Standard-)Parametrisierung von f* (oder von $\mathbb{M}$).

B) Sei nun $f(u, v) = Au^2 + Buv + Cv^2 + Du + Ev + F$ eine nichtausgeartete rationale Quadrik und sei $S = (u_0, v_0) \in \mathbb{Q} \cap \mathbb{M}$ ein rationaler Punkt von $\mathbb{M}$. Die bijektive Abbildung

$$\varepsilon_S\restriction = \varepsilon\restriction : \mathbb{Q}\backslash\mathcal{C} \xrightarrow{\approx} \mathbb{Q}^2 \cap (\mathbb{M}\backslash\{S\}); \ (t \mapsto \varepsilon(t) = (u(t), v(t))$$

aus 10.22 heisst dann die *zu S gehörige (Standard-)Parametrisierung der rationalen Punkte von f (oder von $\mathbb{M}$).* •

Unsere bisherigen Ausführungen mögen sehr technisch erscheinen. Ihre Quintessenz lässt sich aber in prägnanter Weise auch ohne viel algebraischen Apparat formulieren:

Hauptsatz 10.24. *Ist $f = f(u, v)$ eine nichtausgeartete rationale Quadrik und ist S ein rationaler Punkt von f, so können mit Hilfe der zu S gehörigen Standardparametrisierung von f alle rationalen Punkte von f beschrieben werden.* ■

Oder noch prägnanter

- *Kennt man einen einzigen rationalen Punkt einer nichtausgearteten rationalen Quadrik, so kennt man alle rationalen Punkte dieser Quadrik.*

Aufgaben 10.25. A) Skizzieren Sie die in Abbildungen 10.10 und 10.11 dargestellte Situation falls f

a) eine Ellipse ist (d.h. $\mathcal{C} = \emptyset$);

b) eine Parabel ist (d.h. $\sharp\mathcal{C} = 1$).

B) Bestimmen Sie die rationale Standard-Parametrisierung von $f(u, v)$ bezüglich $S = (u_0, v_0) \in \mathbb{M} = \mathbb{M}(f)$ falls

a) $f(u, v) = Au^2 + Cv^2 - 1$ mit $0 < A \leq C$ und $S = (0, 1/\sqrt{C})$;

b) $f(u, v) = Cv^2 - u - 1$ mit $C > 0$ und $S = (1-, 0)$;

c) $f(u, v) = Au^2 + Cv^2 - 1$ mit $A < 0 < C$ und $S = (0, 1/\sqrt{-A})$.

C) Sei $f(u, v) = Au^2 + Buv + Cv^2 + Du + Ev$ eine nichtausgeartete Quadrik. Bestimmen Sie die rationale Standard-Parametrisierung von f bezüglich $S = (0, 0)$.

D) Bestimmen Sie die rationale Standard-Parametrisierung der Quadrik $f = f(u, v) = u^2 + v^2 + u + v$ bezüglich $S = (0, 0)$ und beschreiben Sie damit $\mathbb{Q}^2 \cap \mathbb{M}(f)$.

E) Bestimmen Sie die rationale Standard-Parametrisierung der Quadrik $f = f(u, v) = u^2 - dv^2 - 1$ für $d \in \mathbb{N}$ bezüglich $s = (1, 0)$. Bestimmen Sie damit $\mathbb{Q}^2 \cap \mathbb{M}(f)$. Was lässt sich über $\mathbb{Z}^2 \cap \mathbb{M}(f)$ sagen? •

Projektionen aus kritischen Richtungen im parabolischen Fall

Im Fall, wo die nichtausgeartete Quadrik $f = f(u, v)$ eine Parabel oder eine Hyperbel ist, d.h. kritische Richtung hat, bietet sich noch eine weitere Möglichkeit zur Parametrisierung an. Wir machen dazu die folgende geometrische Betrachtung.

Bemerkung 10.26. A) Sei $f = f(u, v) = Au^2 + Buv + Cv^2 + Du + Ev + F$ eine nichtausgeartete Quadrik und sei $S = (u_0, v_0) \in \mathbb{M} = \mathbb{M}(f)$. Geometrisch beruht die zu S gehörige rationale Standard-Parametrisierung von f auf der bijektiven Abbildung $\sigma : h^0 \xrightarrow{\approx} \mathbb{M}\backslash\{S\}$ aus 10.19 oder – gleichbedeutend – auf deren Umkehrabbildung

$$\pi := \sigma^{-1} : \mathbb{M}\backslash\{S\} \xrightarrow{\approx} h^0.$$

Diese Umkehrabbildung kommt aber dadurch zustande, dass man $\mathbb{M}\backslash\{S\}$ aus dem Projektionszentrum S auf die Hilfsgerade h projiziert. Man nennt π auch die *stereographische Projektion der Quadrik f aus dem Zentrum S* auf die Hilfsgerade h.

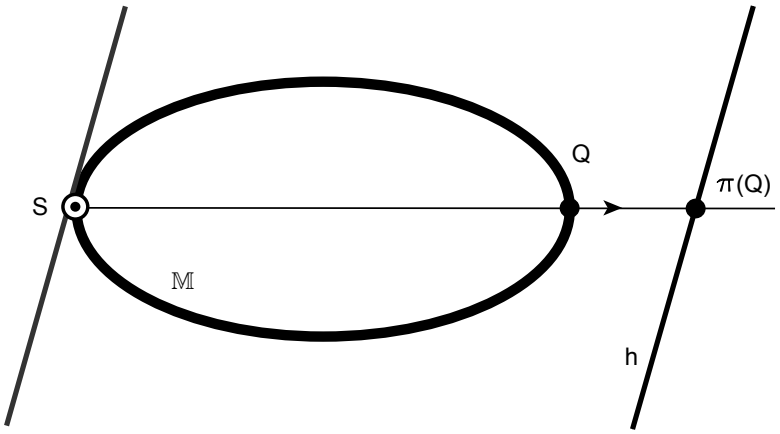


Abbildung 10.12: Stereographische Projektion einer Quadrik

Wichtig ist dabei, dass die Projektion π bijektiv auf ihr Bild ist, also injektiv. Dies bedeutet, dass für jeden Punkt $Q \in \mathbb{M}\backslash\{S\}$ die Gerade durch das Projektionszentrum S und durch Q keine weiteren Schnittpunkte mit $\mathbb{M}$ hat.

B) Man kann nun versuchen, π durch eine andere Art von Projektion zu ersetzen. Wählt man eine Zentralprojektion, so muss deren Zentrum wegen der geforderten Injektivität zu $\mathbb{M}$ gehören und man erhält nichts neues.

Man könnte natürlich versuchen, π durch eine Parallelprojektion zu ersetzen. Wegen der geforderten Injektivität dürfte dann jede Gerade, welche die Projektionsrichtung hat, die Quadrik $\mathbb{M}$ in höchstens einem Punkt schneiden. Die Projektionsrichtung müsste

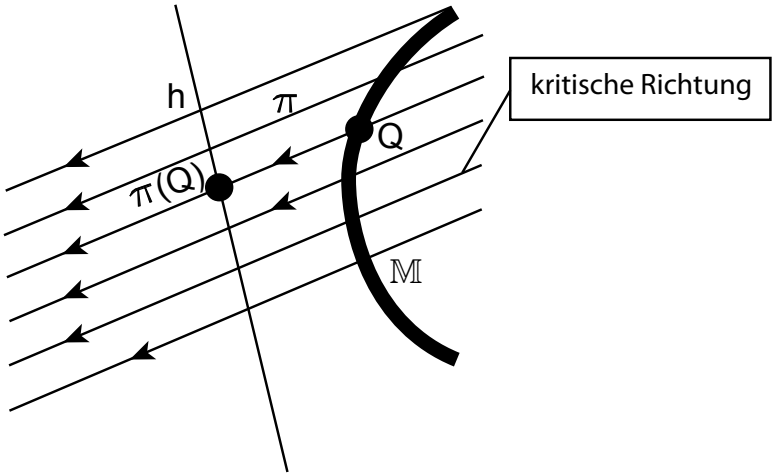


Abbildung 10.13: Projektion aus kritischer Richtung

deshalb bezüglich der Quadrik f kritisch sein. Mit anderen Worten müsste π eine Parallelprojektion aus einer bezüglich f kritischen Richtung auf eine Hilfsgerade h sein, welche etwa senkrecht zur Projektionsrichtung steht.

•

Um aus dem in 10.26 B) beschriebenen Verfahren wieder eine Parameterstellung von $\mathbb{M} = \mathbb{M}(f)$ zu gewinnen, muss man lediglich für h eine Parameterdarstellung wählen und die Umkehrabbildung von π in Koordinaten ausdrücken. Wir wollen dies nur im *parabolischen Fall* tun, d.h. im Fall wo unsere Quadrik $f(u, v)$ eine Parabel ist, also genau eine kritische Richtung hat. Dazu zunächst eine Vorbetrachtung.

Bemerkung 10.27. A) Wir betrachten die nichtausgeartete Quadrik $f(u, v) = Au^2 + Buv + Cv^2 + Du + Ev + F$. Dabei wollen wir annehmen, f sei eine Parabel, d.h. es sei $\mathbb{M}(f) \neq \emptyset$ und es gäbe genau eine kritische Richtung bezüglich f. Nach 10.15 und gemäss der Definition 10.5 B) gilt demnach

a) $\quad B^2 = 4AC; \Delta_f = BDE - AE^2 - CD^2 \neq 0.$

Wir wollen zusätzlich annehmen, es sei $C \neq 0$. Nach 10.15 b) zeigt dann der Vektor $(\alpha, \beta) := (2C, -B)$ in die kritische Richtung, d.h. es gilt $A\alpha^2 + B\alpha\beta + C\beta^2 = 0$.

Nun betrachten wir die Hilfsgerade h, parametrisiert durch

$$h : t \mapsto P_t := (Bt, 2Ct).$$

Es handelt sich um eine Gerade durch den Punkt $(0, 0)$, welche senkrecht zur kritischen Richtung verläuft. Zu jedem Parameterwert $t \in \mathbb{R}$ definieren wir nun eine Gerade g_t, parametrisiert durch

$$g_t : s \mapsto (Bt + 2Cs, 2Ct - Bs).$$

Es handelt sich um die Gerade durch P_t, welche in der kritischen Richtung verläuft, also um eine kritische Gerade bezüglich f. Wir wählen nun einen Punkt $Q = (u, v) \in \mathbb{R}^2$. Dann gibt es zwei eindeutig bestimmte Zahlen $t, s \in \mathbb{R}$ mit

$$Q = (u, v) = (Bt + 2Cs, 2Ct - Bs).$$

B) Natürlich gilt $Q \in \mathbb{M}(f)$ genau dann, wenn $f(u, v) = 0$, also genau dann, wenn

$$\begin{aligned} A(Bt + 2Cs)^2 + B(Bt + 2Cs)(2Ct - Bs) + C(2Ct - Bs)^2 \\ + D(Bt + 2Cs) + E(2Ct - Bs) + F = 0. \end{aligned}$$

Die linke Seite dieser Gleichung lässt sich aber schreiben in der Form

$$\begin{aligned} (AB^2 + 2B^2C + 4C^3)t^2 + (4AC^2 - B^2C)s^2 + (4ABC + 4BC^2 - B^3 - 4BC^2)st \\ + (BD + 2CE)t + (2CD - BE)s + F. \end{aligned}$$

Beachtet man, dass $B^2 = 4AC$ (s. A) a)), so lässt sich dieser Ausdruck auch schreiben als

$$4C(A + C)^2t^2 + (BD + 2CE)t + (2CD - BE)s + F.$$

Wir erhalten also:

a) $Q \in \mathbb{M}(f) \iff 4C(A + C)^2t^2 + (DB + 2CE)t + (2CD - BE)s + F = 0.$ •

Als nächstes beweisen wir das folgende Hilfsresultat:

Lemma 10.28. *Sei $f(u, v) = Au^2 + Buv + Cv^2 + Du + Ev + F$ eine nichtausgeartete Quadrik mit $B^2 = 4AC$. Dann gilt:*

a) $A + C \neq 0$.

b) *Ist $C \neq 0$, so besteht die Äquivalenz*

$$\mathbb{M}(f) = \emptyset \iff BE - 2CD = 0.$$

Beweis: „a)“: Nehmen wir an, es sei $A + C = 0$, also $C = -A$. Dann folgt $B^2 = 4AC = 4A(-A) = -4A^2$, also $B^2 = -(2A)^2$. Damit ist $A = B = 0$, also auch $C = 0$ und es ergibt sich der Widerspruch, dass $\Delta_f = BDE - AE^2 - CD^2 = 0$ (s. 10.27 A) a)).

„b)“: „$\Longrightarrow$“: Sei $\mathbb{M}(f) = \emptyset$. Nach 10.27 B) a) gilt dann für jede Wahl von t und s

$$4C(A + C)^2t^2 + (BD + 2CE)t + (2CD - BE)s + F \neq 0.$$

Anders gesagt: Wie immer auch $s \in \mathbb{R}$ gewählt wird, die Gleichung

$$(\alpha) \qquad 4C(A+C)^2t^2 + (BD+2CE)t + ((2CD-BE)s+F) = 0$$

hat keine Lösung t. Wegen $C \neq 0$ gilt gemäss Aussage a) aber $4C(A+C)^2 \neq 0$. Es handelt sich bei (α) also um eine quadratische Gleichung für t. Da diese Gleichung keine Lösung hat, muss gelten

$$(BD+2CE)^2 - 4(4C(A+C)^2)((2CD-BE)s+F) < 0,$$

und zwar für alle $s \in \mathbb{R}$. Da der erste Summand in dieser Ungleichung gar nicht von s abhängt, folgt $2CD - BE = 0$ (denn sonst könnte der zweite Summand durch geeignete Wahl von s ja beliebig gross gemacht werden).

„$\Longleftarrow$“: Sei $BE - 2CD = 0$. Nehmen wir an, es sei $\mathbb{M} = \mathbb{M}(f) \neq \emptyset$. Dann gibt es einen Punkt $S \in \mathbb{M}$. Mit 10.20 folgt, dass $\sharp\mathbb{M} = \infty$. Gemäss 10.27 B) a) besteht nun (wegen $BE - 2CD = 0$) für jeden Punkt $Q = (Bt + 2Cs, 2Ct - Bs) \in \mathbb{M}$ die Gleichung

$$4C(A+C)^2t^2 + (BD+2CE)t + F = 0.$$

Wählt man zwei verschiedene Punkte aus $\mathbb{M}$, so können diese nicht auf der gleichen (bezüglich f) kritischen Geraden g_t liegen, denn eine kritische Gerade kann $\mathbb{M}$ höchstens einmal schneiden (s. 10.14). Also gehören zu verschiedenen Punkten $Q \in \mathbb{M}$ auch verschiedene Parameterwerte t. Daraus können wir schliessen, dass die Gleichung (β) für unendlich viele verschiedene Werte von t besteht. Daraus folgt aber $4C(A+C)^2 = 0$. Da wir $C \neq 0$ vorausgesetzt haben, ergibt sich $A + C = 0$. Dies steht im Widerspruch zur schon bewiesenen Aussage a). Also ist $\mathbb{M} = \emptyset$. ■

Nun können wir endlich unser Zielergebnis formulieren und beweisen:

Satz 10.29. *Sei $f(u,v) = Au^2 + Buv + Cv^2 + Du + Ev + F$ eine nichtausgeartete Quadrik mit $B^2 = 4AC, C \neq 0$ und $BE - 2CD \neq 0$. Wir setzen*

$$s(t) := \frac{4C(A+C)^2t^2 + (DB+2CE)t + F}{BE - 2CD}.$$

Dann besteht die bijektive Abbildung:

$$\delta : \mathbb{R} \xrightarrow{\approx} \mathbb{M};\ t \mapsto \delta(t) := (Bt + 2Cs(t), 2Ct - Bs(t)).$$

Beweis: Seien $s, t \in \mathbb{R}$. Es gilt genau dann $s = s(t)$, wenn die Gleichung aus 10.27 B) a) gilt, also genau dann, wenn $Q := (Bt + 2Cs, 2Ct - Bs) \in \mathbb{M}$. Dies zeigt, dass die Abbildung $\delta : \mathbb{R} \to \mathbb{M}$ tatsächlich definiert ist – aber auch, dass diese Abbildung surjektiv ist.

In den Bezeichnungen von 10.27 A) gilt immer $\delta(t) \in g_t$. Ist $t \neq t'$, so ist aber $g_t \neq g_{t'}$, also $g_t \cap g_{t'} = \emptyset$ (denn die Geraden g_t und $g_{t'}$ haben ja die gleiche Richtung). Aus $t \neq t'$ folgt deshalb insbesondere, dass $\delta(t) \neq \delta(t')$. Also ist $\delta : \mathbb{R} \to \mathbb{M}$ auch injektiv. ■

Für den Fall, dass die Quadrik aus 10.29 rational ist, gilt eine zu 10.21 analoge Aussage, nämlich:

Korollar 10.30. *Es gelten die Voraussetzungen und Bezeichnungen von 10.29. Zudem sei die Quadrik f rational. Weiter sei $t \in \mathbb{R}$. Dann gilt*

$$t \in \mathbb{Q} \Longleftrightarrow \delta(t) \in \mathbb{Q}^2.$$

Beweis: „$\Longrightarrow$“: Sei $t \in \mathbb{Q}$. Wegen $A, B, C, D, E, F \in \mathbb{Q}$ ist dann $s(t) \in \mathbb{Q}$, also auch $Bt + 2Cs(t) \in \mathbb{Q}$ und $2Ct - Bs(t) \in \mathbb{Q}$ und damit $\delta(t) \in \mathbb{Q}^2$.

„$\Longleftarrow$“: Sei $\delta(t) \in \mathbb{Q}$. Dann gelten $Bt + 2Cs(t) \in \mathbb{Q}$ und $2Ct - Bs(t) \in \mathbb{Q}$. Es folgt

$$(4C^2+B^2)t = 4C^2t-2BCs(t)+B^2t+2BCs(t) = 2C(2Ct-Bs(t))+B(Bt+2Cs(t)) \in \mathbb{Q}.$$

Wäre $4C^2 + B^2 = 0$, so gälte $B = C = 0$ im Widerspruch zu unserer Voraussetzung, dass $C \neq 0$. Also gilt $4C^2 + B^2 \in \mathbb{Q} \setminus \{0\}$. Daraus folgt aber $t \in \mathbb{Q}$. ■

Als Anwendung ergibt sich

Korollar 10.31. *Sei $f(u, v) = Au^2 + Buv + Cv^2 + Eu + Dv + F$ eine nichtausgeartete rationale Quadrik mit $B^2 = 4AC, C \neq 0$ und $BE - 2CD \neq 0$. Dann gilt in den Bezeichnungen von 10.29:*

a) *Durch Einschränkung der Abbildung $\delta : \mathbb{R} \to \mathbb{M} = \mathbb{M}(f)$ erhält man eine bijektive Abbildung*

$$\delta\restriction: \mathbb{Q} \xrightarrow{\approx} \mathbb{Q}^2 \cap \mathbb{M}.$$

b) $\mathbb{Q}^2 \cap \mathbb{M} = \{(Bt + 2Cs(t), 2Ct - Bs(t)) \,\big|\, t \in \mathbb{Q}\}$.

Beweis: Ergibt sich leicht aus 10.30 und der Bijektivität von δ. ■

Bemerkung 10.32. A) Sei $f(u, v) = Au^2 + Buv + Cv^2 + Du + Ev + F$ eine Parabel, also eine nichtausgeartete Quadrik mit $B^2 = 4AC$. Sind $C \neq 0$ und $BE - 2CD \neq 0$, so nennen wir die bijektive Abbildung $\delta : \mathbb{R} \xrightarrow{\approx} \mathbb{M}(f) = \mathbb{M}$ eine *kritische rationale Parametrisierung* von f. Ähnlich wie im Falle der zu einem Punkt gehörigen Standard-Parametrisierung kann man im Fall wo f rational ist mit Hilfe einer kritischen Parametrisierung alle rationalen Punkte von $\mathbb{M}$ bestimmen.

B) Ist $f(u,v)$ eine Parabel mit $C = 0$, so muss gemäss 10.28 a) $A \neq 0$ gelten. Man gelangt nun zu einer kritischen Parametrisierung von f, indem man die Rollen von u und v vertauscht. Es ergibt sich so eine bijektive Abbildung

$$\delta' : \mathbb{R} \xrightarrow{\approx} \mathbb{M}; t \mapsto \delta'(t) := (Bt + 2As'(t), 2At - Bs'(t))$$

mit

$$s'(t) := \frac{4A(A+C)^2t^2 + (EB + 2AE)t + F}{BD - 2AE}.$$

•

Aufgaben 10.33. A) Bestimmen Sie die kritische Parametrisierung von

a) $f = f(u,v) := u^2 - 2uv + v^2 + u + 2v - 1$,

b) $f = f(u,v) := u^2 - 3u + 2v + 2$

und skizzieren Sie die Situation.

B) Sei $f(u,v) = Au^2 + Buv + Cv^2 + Du + Ev + F$ eine Parabel mit $C \neq 0$ und $BE - 2CD \neq 0$. Bestimmen Sie den *Scheitel* der Parabel $\mathbb{M} = \mathbb{M}(f)$, d.h. dem Punkt $\delta(t_0)$ zum Parameterwert t_0 für den die Funktion $s(t)$ aus 10.29 ein Extremum hat.

C) Zeigen Sie, dass die Tangente im Scheitel (vgl. B)) senkrecht steht zur kritischen Richtung.

D) Zeigen Sie, dass die Parabel aus B) bezüglich der kritischen Geraden g_{t_0} durch den Scheitel symmetrisch ist.

E) Bestimmen Sie $\mathbb{Q}^2 \cap \mathbb{M}(f)$ und $\mathbb{Z}^2 \cap \mathbb{M}(f)$ für die beiden Quadriken f aus A). •

Zur Existenz rationaler Punkte

Der Hauptsatz 10.24 besagt, dass sich aus einem einzigen rationalen Punkt einer nichtausgearteten rationalen Quadrik f alle rationalen Punkte dieser Quadrik bestimmen lassen. Unbeantwortet bleibt dabei die Frage, ob und wann die Quadrik f überhaupt einen rationalen Punkt besitzt – also die *Frage nach der Existenz rationaler Punkte auf einer nichtausgearteten Quadrik*. wir haben uns – in episodischer Weise – bereits am Ende von Kapitel 9 mit dieser Frage befasst. Eine allgemeine Antwort war uns dabei nicht möglich.

Für Parabeln ist diese Frage allerdings leicht zu beantworten. Es gilt nämlich:

Satz 10.34. *Für eine rationale Parabel, d.h. eine nichtausgeartete rationale Quadrik $f(u,v) = Au^2 + Buv + Cv^2 + Du + Ev + F$ mit $B^2 = 4AC$, sind äquivalent:*

(i) $\mathbb{M}(f) \neq \emptyset$*;*

(ii) $\mathbb{Q}^2 \cap \mathbb{M}(f) \neq \emptyset$*;*

(iii) Es gilt mindestens eine der beiden Aussagen

(α) $C \neq 0$ *und* $BE - 2CD \neq 0$,

(β) $A \neq 0$ *und* $BD - 2AE \neq 0$.

Beweis: „(i) $\Longrightarrow$ (iii)“ist klar nach 10.28 b) und 10.32 B).

„(iii) $\Longrightarrow$ (ii)“ist klar nach 10.31 b) und nach 10.32 B).

„(ii) $\Longrightarrow$ (i)“ist sofort klar. ■

Teil E
Lösungen zu den Aufgaben

Teil A

Aufgaben 1.3 A) Zählen der Elemente einer Menge $\mathbb{M}$ heisst eine bijektive Abbildung $\mathbb{M} \to \mathbb{N}_{\leq n}$ von $\mathbb{M}$ auf einen Anfangsabschnitt $\mathbb{N}_{\leq n} := \{m \in \mathbb{N} | m \leq n\}$ der natürlichen Zahlen angeben (vgl. Kapitel 3). Was eine Zahl ist und ob es Zahlen überhaupt gibt sind philosophische und keine mathematischen Fragen.
B) Für jede natürliche Zahl n gilt $n < n+1 \in \mathbb{N}$. Daher gibt es keine grösste natürliche Zahl. Allerdings könnte man eine " unendlich grosse" (nichtnatürliche) Zahl zum Beispiel mit ∞ bezeichnen und statt in $\mathbb{N}$ in $\mathbb{N} \cup \{\infty\}$ rechnen, indem man die Regeln

$$\infty + n = n + \infty = \infty,\ \infty \cdot n = n \cdot \infty = \infty \text{ und } \infty + \infty = \infty \cdot \infty = \infty$$

einführt (für $n \in \mathbb{N}$). Dabei verliert man aber Einiges, was im Rechenbereich $\mathbb{N}$ gilt, z. B. die Aussage $x < x + 1$.
C) Im Sinne der mathematischen Definition handelt es sich um eine natürliche Zahl. Allerdings ist es unmöglich, alle Ziffern der Dezimaldarstellung dieser Zahl hinzuschreiben.
D) Ja, denn es gibt eine Bijektion $\varphi : \mathbb{N} \to \mathbb{Z}$. Diese kann zum Beispiel definiert werden durch

$$\varphi(n) := \frac{n}{2} - 1 \text{ für gerades } n \text{ und } \varphi(n) := -\frac{n+1}{2} \text{ für ungerades } n.$$

E) Nein, denn es gibt eine Bijektion $\mathbb{N} \to \mathbb{Q}$ (vgl. Vorlesung „Grundbegriffe der Mathematik").
F) Ja, denn es gibt keine Bijektion $\mathbb{N} \to \mathbb{R}$ (vgl. Vorlesung „Grundbegriffe der Mathematik") und somit auch keine Bijektion $\mathbb{Q} \to \mathbb{R}$, da diese sonst komponiert mit der Bijektion aus E) eine Bijektion $\mathbb{N} \to \mathbb{R}$ liefern würde.

Aufgaben 1.5 A) Seien

$$\mathbb{A} := \{19m + 4 | m \in \mathbb{N}_0\} \text{ und } \mathbb{B} := \{8m + 5 | m \in \mathbb{N}_0\}.$$

Die gesuchten Zahlen sind genau die Elemente von $\mathbb{L} := \mathbb{A} \cap \mathbb{B}$. Es gelten

$$\mathbb{A} = \{4, 23, 42, 61, 80, 99, ...\} \text{ und } \mathbb{B} = \{5, 13, 21, 29, 37, 45, 53, 61, ...\},$$

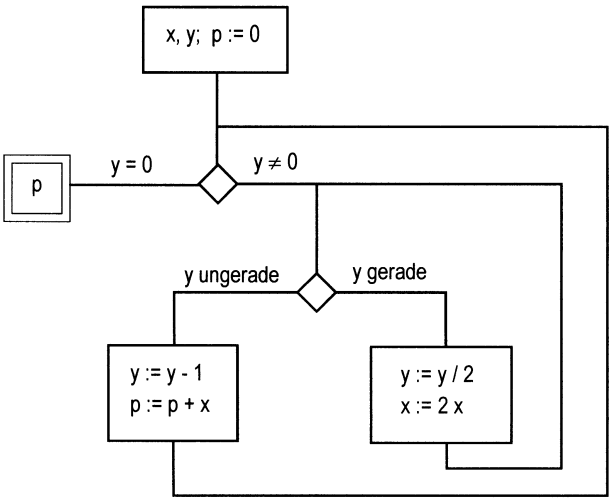
und man sieht, dass 61 die kleinste Zahl in $\mathbb{L}$ ist. Ist $x \in \mathbb{L}$, so ist $x - 61$ ein Vielfaches von $8 \cdot 19 = 152$ und umgekehrt. Also gilt

$$\mathbb{L} = \{61 + 152n | n \in \mathbb{N}_0\}.$$

B) Für beide Ausdrücke gibt es einfache Formeln:

$$1 + 2 + 3 + \cdots + 129 = \frac{129(129+1)}{2},\ 1 + 2^2 + 3^2 + \cdots + 87^2 = \frac{87(87+1)(2 \cdot 87 + 1)}{6}.$$

C) Auf jeder Zeile gilt $p + xy = 273$. Berechnet wurde $13 \cdot 21$ mit einem Verfahren, bei dem nur addiert, 1 subtrahiert, verdoppelt und halbiert werden muss. Somit lässt sich die Frage 1.4 D) bejahen, falls man zusätzlich noch das Halbieren erlaubt.



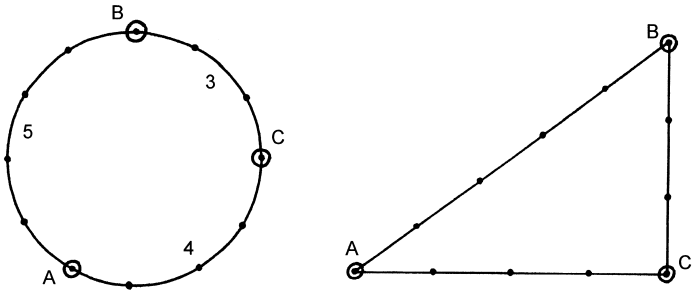
Aufgabe 1.5 C)

Aufgaben 1.6 A) Siehe Zeichnung.
B) Gesucht sind jeweils vier Zahlen $s, x, y, z \in \mathbb{N}$ so, dass $x + y + z = s$ und dass ein Dreieck mit den Seitenlängen x, y, z rechtwinklig ist, d.h. dass $x^2 + y^2 = z^2$ gilt (Satz von Pythagoras). Für $s = 30$ gelten

$$30 = 5 + 12 + 13 \text{ und } 5^2 + 12^2 = 13^2.$$

Für $s = 40$ gelten

$$40 = 8 + 15 + 17 \text{ und } 8^2 + 15^2 = 17^2.$$



Aufgabe 1.6 A)

C) Für $s = 60$ gelten

$$60 = 15 + 20 + 25 \text{ und } 15^2 + 20^2 = 25^2,$$

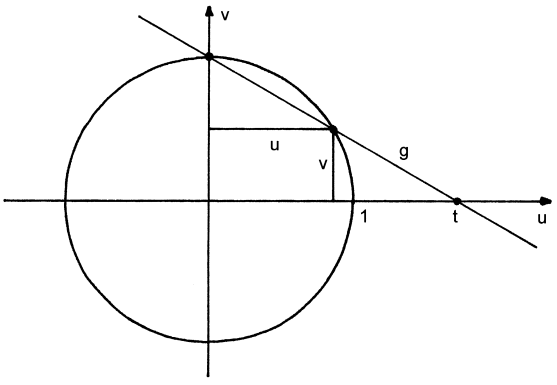
$$60 = 10 + 24 + 26 \text{ und } 10^2 + 24^2 = 26^2.$$

Die beiden zugehörigen Winkelmasse sind in dem Sinne wesentlich verschieden, dass die entsprechenden rechtwinkligen Dreiecke nicht ähnlich sind.
D) Gesucht ist nach den Überlegungen in B) die Menge

$$\{s \in \mathbb{N} | \exists x, y, z \in \mathbb{N} : x + y + z = s \wedge x^2 + y^2 = z^2\} =$$

$$\{s \in \mathbb{N} | \exists x, y \in \mathbb{N} : x^2 + y^2 = (s - x - y)^2\}.$$

Aufgaben 1.7 A)



Aufgabe 1.7 A)

B) Aus der Zeichnung in A) liest man (z. B. mit Hilfe der Strahlensätze) ab, dass die Verhältnisse $t : 1$ und $u : (1 - v)$ gleich sind, dass also gilt:

$$(*) \qquad t = \frac{u}{1 - v}.$$

C) Wegen $(u,v) \in \mathbb{S}$ gilt $u^2+v^2=1$, also $v=\sqrt{1-u^2}$ (wobei verwendet wurde, dass $v \geq 0$). Zusammen mit Gleichung $(*)$ erhalten wir $t-t\sqrt{1-u^2}=u$, also $t-u=t\sqrt{1-u^2}$ und durch Quadrieren $-2tu+u^2=-t^2u^2$. Wegen $0 \leq v < 1$ gilt $u \neq 0$, woraus $-2t+u=-t^2u$ und somit $u(1+t^2)=2t$ folgt. Schliesslich folgt

$$(**) \qquad u=\frac{2t}{1+t^2}.$$

Weiter erhalten wir

$$v \overset{(*)}{=} 1-\frac{u}{t} \overset{(**)}{=} 1-\frac{2}{1+t^2}=\frac{t^2-1}{t^2+1},$$

also

$$(***) \qquad v=\frac{t^2-1}{t^2+1}.$$

D) Summen, Differenzen, Produkte (und insbesondere Quadrate) und Quotienten rationaler Zahlen sind wieder rational (vgl. 1.12 C)). Vermöge der Formeln $(*), (**)$ und $(***)$ folgt daraus leicht die Behauptung.
E) Sei $t \in \mathbb{Q}$ mit $t>0$. Wir definieren

$$u:=u(t):=\frac{2t}{1+t^2},\ v:=v(t):=\frac{t^2-1}{t^2+1}.$$

Es gilt dann $u,v \in \mathbb{Q}$ nach E). Wir machen u und v gleichnamig. Sei dazu $z:=z(t)$ der kleinste gemeinsame Nenner von u und v. Es gelten dann $z \in \mathbb{N}$ und $uz, vz \in \mathbb{N}_0$ (vgl. 2.6). Setzen wir $x:=x(t):=uz$ und $y:=y(t):=vz$, so folgt

$$x^2+y^2=(uz)^2+(vz)^2=u^2z^2+v^2z^2=(u^2+v^2)z^2=z^2,$$

wobei im letzten Schritt verwendet wurde, dass $(u,v) \in \mathbb{S}$, also $u^2+v^2=1$.
Bemerkungen: a) Es wurde verlangt, dass $x,y,z \in \mathbb{N}$. Wählt man $t=1$, so liefert obiges Verfahren $y=0 \notin \mathbb{N}$. Dies entspricht genau dem Fall $(u,v)=(0,1)$, welcher in den Teilaufgaben A)–D) ausgeschlossen wurde.
b) Ein Tripel (x,y,z) natürlicher Zahlen mit $x^2+y^2=z^2$ heisst ein *pythagoräisches Tripel* (vgl. Kapitel 8). Wir haben also zu jeder positiven rationalen Zahl t (mit $t \neq 1$, vgl. a)) ein pythagoräisches Tripel konstruiert.
F) Die in 1.6 D) gesuchte Menge kann mit den Bezeichnungen von E) geschrieben werden als

$$\{x(t)+y(t)+z(t) | t \in \mathbb{Q} \setminus \{1\}, t>0\}.$$

Aufgaben 1.10 A) Pierre de Fermat (1601–1665) hat behauptet, dass es keine solchen natürlichen Zahlen x,y,z (mit $xyz \neq 0$) gebe (die *Fermatsche Vermutung*). Erst 1994 haben R. Taylor und A. Wiles einen Beweis dieser Vermutung geliefert.
B) Erhöhung des Exponenten. (Streng genommen ist dies keine Verallgemeinerung, da

der vorherige Fall mit Exponent 2 nicht mehr „darin enthalten“ ist.)

Aufgaben 2.3 A) Wir nehmen an, es gäbe ein Minimum x von $\mathbb{M}$. Wegen $x \in \mathbb{M}$ gälte $x > 1$. Mit $y := \frac{x+1}{2}$ folgten $y \in \mathbb{Q}$ und $1 < y < x$, ein Widerspruch.
B) Wir nehmen an, es gäbe ein Minimum u von $\mathbb{U}$. Dann gäbe es ein $n \in \mathbb{N}$ mit $u = \frac{1}{n}$, und es folgte der Widerspruch $u = \frac{1}{n} > \frac{1}{n+1} \in \mathbb{U}$.
C) Durch quadratische Ergänzung erhält man

$$x^2 - x + 2 = x^2 - 2 \cdot \frac{1}{2}x + \left(\frac{1}{2}\right)^2 + 2 - \frac{1}{4} = \left(x - \frac{1}{2}\right)^2 + \frac{7}{4}.$$

Dieser Ausdruck wird minimal, wenn $\left(x - \frac{1}{2}\right)^2$ minimal wird, also für $x = \frac{1}{2}$. Dann hat der Ausdruck den Wert $\frac{7}{4}$, also gilt $\min(\mathbb{M}) = \frac{7}{4}$. (Natürlich kann man $\min(\mathbb{M})$ auch bestimmen, indem man die Nullstelle der Ableitung von $x^2 - x + 2$ sucht und sich überlegt, dass an dieser Stelle wirklich ein Minimum vorliegt.)
D) a) Sei $a \in \mathbb{Q}$. Wegen $a \leq a$ gilt dann $a \in \mathbb{Q}_{\geq a}$, und für alle $q \in \mathbb{Q}_{\geq a}$ gilt nach Definition $a \leq q$. Somit folgt $a = \min(\mathbb{Q}_{\geq a})$.
b) Sei $a \notin \mathbb{Q}$. Angenommen es gäbe ein q mit $q = \min(\mathbb{Q}_{\geq a})$, so gälte $a \leq q \in \mathbb{Q}$, also $a < q$. Somit gäbe es ein $q' \in \mathbb{Q}$ mit $a < q' < q$, und es folgte der Widerspruch $q > q' \in \mathbb{Q}_{\geq a}$.
E) Seien $u := \min(\mathbb{U})$ und $v := \min(\mathbb{V})$. Nach Definition gelten $u \in \mathbb{U}, v \in \mathbb{V}$, also $u, v \in \mathbb{U} \cup \mathbb{V}$. Sei

$$w := \min(\{u, v\}) = \min(\{\min(\mathbb{U}), \min(\mathbb{V})\}).$$

Falls $w = u$, so gelten

$$\forall x \in \mathbb{U} : w = u \leq x \text{ und } \forall x \in \mathbb{V} : w = u \leq v \leq x.$$

Daraus folgt, dass $w \leq x$ für alle $x \in \mathbb{U} \cup \mathbb{V}$ und somit $w = \min(\mathbb{U} \cup \mathbb{V})$. Der Fall $w = v$ wird analog behandelt.
F) Banale Beispiele erhält man folgendermassen: Seien

$$\mathbb{U} := \left\{ \frac{1}{n} \middle| n \in \mathbb{N} \right\} \cup \{0\} \text{ und } \mathbb{V} := \left\{ \frac{1}{n} \middle| n \in \mathbb{N} \right\} \cup \{-1\}.$$

Offensichtlich gelten $\min(\mathbb{U}) = 0$ und $\min(\mathbb{V}) = -1$ sowie

$$\mathbb{U} \cap \mathbb{V} = \left\{ \frac{1}{n} \middle| n \in \mathbb{N} \right\} \neq \emptyset,$$

und diese Menge besitzt nach B) kein Minimum.
Ein etwas weniger banales Beispiel erhält man mit

$$\mathbb{U} := \{x \in \mathbb{R} | x \geq \pi\} \text{ und } \mathbb{V} := \{x \in \mathbb{Q} | x \geq 3\}.$$

Dann gelten $\min(\mathbb{U}) = \pi, \min(\mathbb{V}) = 3$ und

$$\mathbb{U} \cap \mathbb{V} = \{x \in \mathbb{Q} | x \geq \pi\} \neq \emptyset.$$

Wegen $\pi \notin \mathbb{Q}$ besitzt diese Menge nach D)b) kein Minimum.

Aufgaben 2.7 A)

$$\{q \in \mathbb{Q} | 0 \leq q \leq 1 \wedge \eta(q) = 36\} =$$
$$\left\{ \frac{n}{36} \middle| \, n = 0 \vee (1 \leq n \leq 36 \wedge n \text{ und } 36 \text{ sind teilerfremd} \right\}$$
$$= \left\{ 0, \frac{1}{36}, \frac{5}{36}, \frac{7}{36}, \frac{11}{36}, \frac{13}{36}, \frac{17}{36}, \frac{19}{36}, \frac{23}{36}, \frac{25}{36}, \frac{29}{36}, \frac{31}{36}, \frac{35}{36} \right\}.$$

B)

$$\eta(1.648) = \eta\left(\frac{1648}{1000}\right) = \eta\left(\frac{206}{125}\right) = 125; \; \eta\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{7}\right) = \eta\left(\frac{363}{140}\right) = 140.$$

Aufgaben 2.11 A) Nach 2.3 D) besitzt $\mathbb{Q}_{\geq\sqrt{n}} := \{q \in \mathbb{Q} | q \geq \sqrt{n}\}$ genau dann keine kleinste Zahl, wenn $\sqrt{n} \notin \mathbb{Q}$. Offensichtlich ist $\sqrt{1} = 1 \in \mathbb{Q}$, also $n > 1$. Aber wegen $1 < \sqrt{2} < 2$ gilt $\sqrt{2} \notin \mathbb{N}$. Aus 2.8 folgt damit $\sqrt{2} \notin \mathbb{Q}$ und somit $n = 2$.
B) Nach 2.3 D) ist das kleinste $n \in \mathbb{Q}$ mit $n > 23$ gesucht so, dass $\sqrt{n-4} \in \mathbb{Q}$. Nach 2.8 ist dies das kleinste $n \in \mathbb{Q}$ mit $n > 23$ so, dass $\sqrt{n-4} \in \mathbb{N}$. Ausprobieren ergibt $n = 29$.
C) a) Liegt das Produkt zweier reeller Zahlen x, y in $\mathbb{Q} \setminus \{0\}$, so gilt entweder $x, y \in \mathbb{Q}$ oder $x, y \notin \mathbb{Q}$. (Dies sieht man durch Multiplikation mit dem Kehrwert.) Wegen $m \neq n$ gilt

$$\left(\sqrt{m} + \sqrt{n}\right)\left(\sqrt{m} - \sqrt{n}\right) = m - n \in \mathbb{Q} \setminus \{0\},$$

und obige Überlegung liefert die Behauptung.
b) „$\Rightarrow$“ : Es gelte $\sqrt{m} + \sqrt{n} \in \mathbb{Q}$. Nach a) gilt $\sqrt{m} - \sqrt{n} \in \mathbb{Q}$. Damit erhalten wir $\sqrt{m} = \frac{1}{2}\left((\sqrt{m} + \sqrt{n}) + (\sqrt{m} - \sqrt{n})\right) \in \mathbb{Q}$ und somit $\sqrt{n} = (\sqrt{m} + \sqrt{n}) - \sqrt{m} \in \mathbb{Q}$, also $\sqrt{m}, \sqrt{n} \in \mathbb{Q}$. Mit 2.8 folgt die Behauptung.
„$\Leftarrow$“ : Klar wegen $\mathbb{N} \subseteq \mathbb{Q}$.

Aufgaben 2.12 A) Für jede natürliche Zahl muss eindeutig festgelegt sein, ob die Eigenschaft auf sie zutrifft oder nicht, und es kann nur eines davon der Fall sein (vgl. Vorlesung „Grundbegriffe der Mathematik“).
B) Mit Hilfe der Rechenregeln für logische Konnektoren (vgl. Vorlesung „Grundbegriffe der Mathematik“) sieht man, dass für $n \in \mathbb{N}$ gelten

$$\chi_{\mathcal{E}\wedge\mathcal{F}}(n) = \chi_{\mathcal{E}}(n) \cdot \chi_{\mathcal{F}}(n), \; \chi_{\neg\mathcal{E}}(n) = 1 - \chi_{\mathcal{E}}(n),$$

$$\chi_{\mathcal{E}\vee\mathcal{F}}(n) = \chi_{\neg(\neg\mathcal{E}\wedge\neg\mathcal{F})}(n) = 1 - (1 - \chi_{\mathcal{E}}(n))(1 - \chi_{\mathcal{F}}(n)) = \chi_{\mathcal{E}}(n) + \chi_{\mathcal{F}}(n) - \chi_{\mathcal{E}}(n) \cdot \chi_{\mathcal{F}}(n).$$

Aufgaben 2.14 A) Wir nehmen an es gäbe ein Maximum x von $\mathbb{M}$. Wegen $x \in \mathbb{M}$ gälte $x < 1$. Mit $y := \frac{1+x}{2}$ folgte $y \in \mathbb{R}$ und $x < y < 1$, ein Widerspruch.
B) a) Sei $a \in \mathbb{Q}$. Wegen $a \leq a$ folgt $a \in \mathbb{Q}_{\leq a}$, und für alle $q \in \mathbb{Q}_{\leq a}$ gilt $a \geq q$, also $a = \max(\mathbb{Q}_{\geq a})$.
b) Sei $a \notin \mathbb{Q}$. Angenommen es gäbe ein q mit $q = \max(\mathbb{Q}_{\leq a})$, so gälte $a \geq q \in \mathbb{Q}$, also $a > q$. Somit gäbe es ein $q' \in \mathbb{Q}$ mit $a > q' > q$, und es folgte der Widerspruch $q < q' \in \mathbb{Q}_{\leq a}$.
C) Nach 2.8 und B) sind alle $n \in \mathbb{N}$ mit $n \leq 20$ so, dass $\sqrt{n} \in \mathbb{N}$ und deren Quadratwurzeln gesucht. Durch Ausprobieren erhält man

$$\max(\mathbb{Q}_{\leq \sqrt{1}}) = 1,\ \max(\mathbb{Q}_{\leq \sqrt{4}}) = 2,\ \max(\mathbb{Q}_{\leq \sqrt{9}}) = 3,\ \max(\mathbb{Q}_{\leq \sqrt{16}}) = 4.$$

D) Seien $\mathbb{U}, \mathbb{V} \subseteq \mathbb{R}$ zwei Mengen, welche ein Maximum haben. Dann gilt

$$\max(\mathbb{U} \cup \mathbb{V}) = \max(\{\max(\mathbb{U}), \max(\mathbb{V})\}).$$

Beweis: Seien $u := \max(\mathbb{U})$ und $v := \max(\mathbb{V})$. Nach Definition gelten $u \in \mathbb{U}, v \in \mathbb{V}$, also $u, v \in \mathbb{U} \cup \mathbb{V}$. Sei

$$w := \max(\{u, v\}) = \max(\{\max(\mathbb{U}), \max(\mathbb{V})\}).$$

Falls $w = u$, so gelten

$$\forall x \in \mathbb{U} : w = u \geq x \text{ und } \forall x \in \mathbb{V} : w = u \geq v \geq x.$$

Daraus folgt, dass $w \geq x$ für alle $x \in \mathbb{U} \cup \mathbb{V}$ und somit $w = \max(\mathbb{U} \cup \mathbb{V})$. Der Fall $w = v$ wird analog behandelt.
E) Gesucht sind zwei Mengen $\mathbb{U}, \mathbb{V} \subseteq \mathbb{R}$ so, dass gleichzeitig folgende Aussagen gelten:

$$\max(\mathbb{U}) \text{ und } \max(\mathbb{V}) \text{ existieren, } \mathbb{U} \cap \mathbb{V} \neq \emptyset \text{ und } \max(\mathbb{U} \cap \mathbb{V}) \text{ existiert nicht.}$$

Wie in Aufgabe 2.3 F) erhält man banale Beispiele, indem man zu einer Menge ohne Maximum zwei jeweils verschiedene Maxima hinzufügt. Auch das zweite Beispiel in 2.3 F) lässt sich anpassen, indem man die Zeichen $\geq$ und $\leq$ vertauscht und die Zahl 3 durch 4 ersetzt.

Aufgaben 2.18 A) Ja, obwohl es vermutlich „anschaulich klar“ ist, was eine endliche Menge natürlicher Zahlen sein soll. Denn nur mit exakt definierten Begriffen kann vernünftig weitergearbeitet werden.
B) $\emptyset$ ist endlich, was man sich wie folgt überlegen kann. Sicher ist $\emptyset \subseteq \mathbb{N}$. Um zu zeigen, dass $\emptyset$ endlich ist, müssen wir ein $m \in \mathbb{N}$ angeben so, dass für alle $n \in \emptyset$ gilt $n \leq m$. Es gibt aber gar kein $n \in \emptyset$ und somit können wir ein beliebiges $m \in \mathbb{N}$ wählen um obige Bedingung zu erfüllen.
C) Zur Diskussion stehen nur die Zahlen $10^{28}, 2^{101}$ und 3^{67}. Es gelten

$$2^{101} = 2 \cdot 2^{100} = 2 \cdot \left(2^{10}\right)^{10} = 2 \cdot 1024^{10} > 2 \cdot \left(10^3\right)^{10} = 2 \cdot 10^{30} > 10^{28}$$

und

$$\frac{3^{67}}{2^{101}} = \frac{3 \cdot 3^{66}}{4 \cdot 2^{99}} = \frac{3}{4} \cdot \left(\frac{9}{8}\right)^{33} = \frac{3}{4} \cdot \left(\frac{9}{8}\right)^{3} \cdot \left(\frac{9}{8}\right)^{30} > \frac{3}{4} \cdot \left(\frac{9}{8}\right)^{3}$$

$$= \frac{3}{4} \cdot \left(1+\frac{1}{8}\right)^{3} = \frac{3}{4} \cdot \left(1+\frac{3}{8}+\frac{3}{64}+\frac{1}{512}\right) > \frac{3}{4} \cdot \left(1+\frac{3}{8}\right) = \frac{3}{4} \cdot \frac{11}{8} = \frac{33}{32} > 1,$$

also $3^{67} > 2^{101}$. Es folgt $\max(\mathbb{S}) = 3^{67}$, und nach 2.16 ist $\mathbb{S}$ endlich.

Aufgaben 3.4 A) (*Induktionsverankerung* $n = 1$) $1 = \frac{(1+1)1}{2}$.
(*Induktionsschritt* $n \to n+1$) Es gelte

$$(*) \qquad 1 + 2 + \cdots + n = \frac{(n+1)n}{2}.$$

Dann folgt

$$1 + 2 + \cdots + n + (n+1) \overset{(*)}{=} \frac{(n+1)n}{2} + (n+1)$$

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

B) (*Induktionsverankerung* $n = 1$) $1 = 1^2$.
(*Induktionsschritt* $n \to n+1$) Es gelte

$$(*) \qquad 1 + 3 + \cdots + (2n-1) = n^2.$$

Dann folgt

$$1+3+\cdots+(2n-1)+(2(n+1)-1) = 1+3+\cdots+(2n-1)+(2n+1) \overset{(*)}{=} n^2+2n+1 = (n+1)^2.$$

C) (*Induktionsverankerung* $n = 1$) $2^{1-1} = 2^0 = 1 \leq 1 = 1!$.
(*Induktionsschritt* $n \to n+1$) Es gelte

$$(*) \qquad 2^{n-1} \leq n!.$$

Dann folgt

$$2^n = 2^{n-1} \cdot 2 \overset{(*)}{\leq} n! \cdot 2 \leq n! \cdot (n+1) = (n+1)!.$$

D) Die Bernoulliungleichung aus 3.3 liefert für $b = 1$:

$$(*) \qquad n + 1 \leq 2^n.$$

(*Induktionsverankerung* $n = 1$) $1! = 1 < 2 = 2^{(1^2)}$.
(*Induktionsschritt* $n \to n+1$) Es gelte

$$(**) \qquad n! < 2^{(n^2)}.$$

Dann folgt

$$(n+1)! = n! \cdot (n+1) \overset{(**)}{<} 2^{(n^2)} \cdot (n+1) \overset{(*)}{\leq} 2^{(n^2)} \cdot 2^n = 2^{n^2+n} < 2^{((n+1)^2)}.$$

E) (*Induktionsverankerung* $n = 1$) $e_1 = 1 = 1 \cdot \frac{1}{1} = 1! \cdot \frac{1}{1!}$.
(*Induktionsschritt* $n \to n+1$) Es gelte

$$(*) \qquad e_n = n! \left(\frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} \right).$$

Dann folgt

$$e_{n+1} = e_n \cdot (n+1) + 1 \overset{(*)}{=} n! \left(\frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} \right)(n+1) + 1$$

$$= (n+1)! \left(\frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} \right) + \frac{(n+1)!}{(n+1)!} = (n+1)! \left(\frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} + \frac{1}{(n+1)!} \right).$$

Aufgaben 3.5 A) Sei $n \in \mathbb{N}$. Dann gilt

$$\sqrt{n} < 1 + \sqrt{n} = 1 + n \cdot \frac{1}{\sqrt{n}} \overset{3.3A)}{\leq} \left(1 + \frac{1}{\sqrt{n}} \right)^n.$$

B) Sei $n \in \mathbb{N}$. Für $a, b \in \mathbb{R}$ mit $0 \leq a \leq b$ gelten bekanntlich $a^2 \leq b^2$ und $\sqrt[n]{a} \leq \sqrt[n]{b}$. Damit erhalten wir

$$\sqrt[n]{n} = \sqrt[n]{\sqrt{n}^2} \overset{A)}{<} \sqrt[n]{\left(\left(1 + \frac{1}{\sqrt{n}} \right)^n \right)^2} = \sqrt[n]{\left(1 + \frac{1}{\sqrt{n}} \right)^{2n}}$$

$$= \left(1 + \frac{1}{\sqrt{n}} \right)^2 = 1 + \frac{2}{\sqrt{n}} + \frac{1}{n} \leq 1 + \frac{2}{\sqrt{n}} + \frac{1}{\sqrt{n}} = 1 + \frac{3}{\sqrt{n}}.$$

C) Mit den Überlegung zu Beginn von B) erhalten wir für $n \in \mathbb{N}$, da natürlich $1 \leq n$ gilt,

$$1 = \sqrt[n]{1} \leq \sqrt[n]{n}.$$

Die Abschätzung in B) liefert

$$\sqrt[n]{n} < 1 + \frac{3}{\sqrt{n}}.$$

Jetzt betrachten wir $\lim_{n\to\infty} \left(1 + \frac{3}{\sqrt{n}} \right)$. Wenn n beliebig gross wird (also $n \to \infty$), so wird auch $\sqrt{n}$ beliebig gross (vgl. die Überlegung zu Beginn von B)). Damit wird aber

$\frac{3}{\sqrt{n}}$ beliebig klein, also $\lim_{n\to\infty}\left(\frac{3}{\sqrt{n}}\right) = 0$. Die Grenzwertbildung vertauscht mit der Addition, und wir erhalten

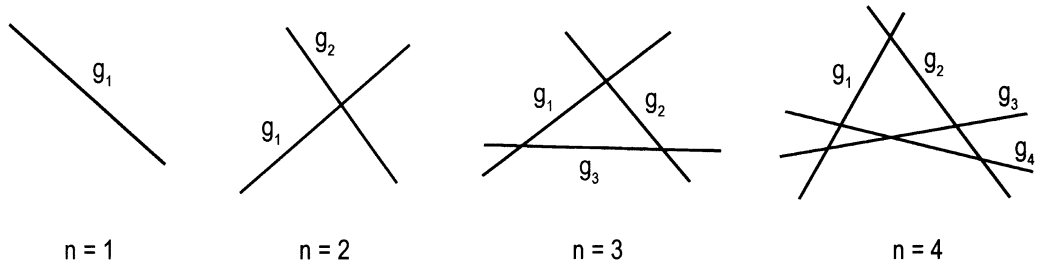
$$\lim_{n\to\infty}\left(1+\frac{3}{\sqrt{n}}\right) = \lim_{n\to\infty}(1) + \lim_{n\to\infty}\left(\frac{3}{\sqrt{n}}\right) = 1+0 = 1.$$

Wir haben also

$$1 \le \sqrt[n]{n} < 1 + \frac{3}{\sqrt{n}},$$

und für $n \to \infty$ werden die äusseren Terme zu 1. Dann gilt dies natürlich auch für den mittleren Term, und es folgt die Behauptung.

Aufgaben 3.6 A)



Aufgabe 3.6 A)

B) Da sich je zwei Geraden genau einmal schneiden, entspricht jeder Schnittpunkt einem Paar von Geraden. Somit ist zu bestimmen, wieviele mögliche Geradenpaare man mit n Geraden bilden kann. Etwas abstrakter heisst das: Wieviele zweielementige Teilmengen hat eine Menge von n Elementen? Diese Zahl kann bekanntlich durch den Binomialkoeffizienten $\binom{n}{2} = \frac{n(n-1)}{2}$ ausgedrückt werden.
C) (*Induktionsverankerung* $n = 1$) Eine Gerade zerlegt $\mathbb{E}$ in 2 Gebiete, und es gilt $2 = \frac{1^2+1+2}{2}$.
(*Induktionsschritt* $n-1 \to n$) Sei $n > 1$, und $\mathbb{E}$ werde durch $n-1$ Geraden $g_1, g_2, \ldots, g_{n-1}$ in $\frac{(n-1)^2+(n-1)+2}{2}$ Gebiete zerlegt. Legen wir nun eine n-te Gerade g_n dazu, so trifft diese jede der Geraden $g_1, g_2, \ldots, g_{n-1}$ so, dass dabei $n-1$ Schnittpunkte entstehen. Durch diese $n-1$ Schnittpunkte wird g_n in n Teilstücke zerlegt. Jedes dieser Teilstücke zerlegt eines der schon vorhandenen Teilgebiete von $\mathbb{E}$ in zwei Gebiete. Es gibt also n neue Gebiete. Somit beträgt die Anzahl Gebiete bei n Geraden

$$\frac{(n-1)^2+(n-1)+2}{2} + n = \frac{(n-1)^2+(n-1)+2+2n}{2} = \frac{n^2+n+2}{2}.$$

Aufgabe 3.8 Wir betrachten die Aussage „$x = x+1$“. Es ist klar, dass sie einer Eigenschaft entspricht, die auf eine natürliche Zahl zutrifft oder nicht. Trifft sie zu für

ein $n \in \mathbb{N}$, so gilt $n = n + 1$, und man sieht sofort, dass damit der Induktionsschritt $n + 1 = (n + 1) + 1$ durchgeführt werden kann. Allerdings trifft die Aussage auf $n = 1$ nicht zu, d.h. die Induktionsverankerung kann nicht gemacht werden. (Auch wenn man die Induktion bei einer natürlichen Zahl grösser als 1 verankern wollte, so klappt dies offensichtlich nicht.)

Aufgaben 3.26 A) $\mathbb{U} \cap \mathbb{V}$ ist als Teilmenge der endlichen Menge $\mathbb{U}$ nach 3.22 endlich. Sei $\mathbb{W} := \mathbb{V} \setminus \mathbb{U} \subseteq \mathbb{V}$. Leicht sieht man, dass $\mathbb{U} \cap \mathbb{W} = \emptyset$ und dass

$$(*) \qquad \mathbb{U} \cup \mathbb{W} = \mathbb{U} \cup \mathbb{V} \text{ und } \mathbb{W} = \mathbb{V} \setminus (\mathbb{U} \cap \mathbb{V}).$$

Weiter ist $\mathbb{W}$ als Teilmenge der endlichen Menge $\mathbb{V}$ nach 3.22 endlich. Aus 3.21 folgt, dass $\mathbb{U} \cup \mathbb{W}$ endlich ist und dass

$$\sharp(\mathbb{U} \cup \mathbb{W}) = \sharp\mathbb{U} + \sharp\mathbb{W}.$$

Nach $(*)$ bedeutet dies, dass $\mathbb{U} \cup \mathbb{V}$ endlich ist und dass

$$(**) \qquad \sharp(\mathbb{U} \cup \mathbb{V}) = \sharp\mathbb{U} + \sharp(\mathbb{V} \setminus (\mathbb{U} \cap \mathbb{V})).$$

Nach Korollar 3.22 gilt

$$\sharp(\mathbb{U} \cap \mathbb{V}) + \sharp(\mathbb{V} \setminus (\mathbb{U} \cap \mathbb{V})) = \sharp\mathbb{V},$$

woraus mit $(**)$ die Behauptung folgt.
B) (*Induktionsverankerung*) Es ist klar, dass die Aussage für $n = 1$ gilt.
(*Induktionsschritt* $n \to n + 1$) Es gelte

$$(*) \qquad \sharp(\mathbb{M}_1 \cup \cdots \cup \mathbb{M}_n) = \sharp\mathbb{M}_1 + \cdots + \sharp\mathbb{M}_n.$$

Nach Voraussetzung gilt

$$(\mathbb{M}_1 \cup \cdots \cup \mathbb{M}_n) \cap \mathbb{M}_{n+1} = (\mathbb{M}_1 \cap \mathbb{M}_{n+1}) \cup \cdots \cup (\mathbb{M}_n \cap \mathbb{M}_{n+1}) = \emptyset.$$

Somit erhalten wir

$$\sharp(\mathbb{M}_1 \cup \cdots \cup \mathbb{M}_n \cup \mathbb{M}_{n+1}) = \sharp((\mathbb{M}_1 \cup \cdots \cup \mathbb{M}_n) \cup \mathbb{M}_{n+1})$$

$$\overset{(3.21)}{=} \sharp(\mathbb{M}_1 \cup \cdots \cup \mathbb{M}_n) + \sharp\mathbb{M}_{n+1} \overset{(*)}{=} \sharp\mathbb{M}_1 + \cdots + \sharp\mathbb{M}_n + \sharp\mathbb{M}_{n+1}.$$

C) Nach B) gilt

$$\sharp(\mathbb{M}_1 \cup \cdots \cup \mathbb{M}_n) = \sharp\mathbb{M}_1 + \cdots + \sharp\mathbb{M}_n = \underbrace{r + \cdots + r}_{n \text{ Summanden}} = nr.$$

D) Seien $n := \sharp\mathbb{U}$ und $m := \sharp\mathbb{V}$. Nach 3.25 B) lässt sich $\mathbb{U}$ in der Form $\mathbb{U} = \{u_1, \ldots, u_n\}$ schreiben. Es gilt

$$\mathbb{U} \times \mathbb{V} = \{(u, v) | u \in \mathbb{U}, v \in \mathbb{V}\}$$

$$= \{(u_i, v) | i \in \{1, \ldots, n\}, v \in \mathbb{V}\} = \{(u_1, v) | v \in \mathbb{V}\} \cup \cdots \cup \{(u_n, v) | v \in \mathbb{V}\}.$$

Für $i, j \in \{1, \ldots, n\}$ mit $i \neq j$ gilt offenbar $\{(u_i, v) | v \in \mathbb{V}\} \cap \{(u_j, v) | v \in \mathbb{V}\} = \emptyset$. Weiter ist für $i \in \{1, \ldots, n\}$ die Abbildung

$$\{(u_i, v) | v \in \mathbb{V}\} \to \mathbb{V}, (u_i, v) \mapsto v$$

bijektiv, wie man leicht nachrechnet; es gilt also $\sharp\{(u_i, v) | v \in \mathbb{V}\} = \sharp\mathbb{V} = m$. Aus C) folgt jetzt die Behauptung.
E) Weil φ eine Abbildung ist, sind die Urbilder zweier verschiedener Elemente von $\mathbb{M}$ disjunkt. Weiter ist φ auf ganz $\mathbb{U}$ definiert. Also liegt jedes Element von $\mathbb{U}$ im Urbild eines Elements von $\mathbb{M}$. Dies bedeutet aber $\mathbb{U} = \varphi^{-1}(m_1) \cup \cdots \cup \varphi^{-1}(m_n)$, und aus B) folgt die Behauptung.
F) (*Induktionsverankerung* $n = 1$) Ist $\sharp\mathbb{M} = 1$, so gibt es eine Bijektion $\varphi : \mathbb{N}_{\leq 1} = \{1\} \to \mathbb{M}$, und es ist klar, das diese wachsend ist.
(*Induktionsschritt* $n \to n + 1$) Für jedes $\mathbb{M}' \subseteq \mathbb{R}$ mit $\sharp\mathbb{M}' = n$ gebe es eine wachsende Bijektion $\varphi : \mathbb{N}_{\leq n} \to \mathbb{M}'$. Seien $\sharp\mathbb{M} = n + 1$, $a := \max(\mathbb{M})$ und $\mathbb{M}' := \mathbb{M} \setminus \{a\}$. Nach 3.22 gilt dann $\sharp\mathbb{M}' = \sharp\mathbb{M} - \sharp\{a\} = n$. Nach Induktionsannahme gibt es eine wachsende Bijektion $\varphi : \mathbb{N}_{\leq n} \to \mathbb{M}'$. Wir definieren eine Abbildung

$$\tilde{\varphi} : \mathbb{N}_{\leq n+1} \to \mathbb{M}, m \mapsto \begin{cases} \varphi(n), & \text{falls } m \neq n + 1 \\ a, & \text{falls } m = n + 1. \end{cases}$$

Nun prüft man leicht nach, dass $\tilde{\varphi}$ eine wachsende Bijektion ist.
G)

$$\varphi_1 : \mathbb{N}_{\leq k+1} \to \{0, 1, \cdots, k\}, m \mapsto m - 1.$$

$$\varphi_2 : \mathbb{N}_{\leq 31} \to \{-7, -6, \cdots, 23\}, m \mapsto m - 8.$$

$$\varphi_3 : \mathbb{N}_{\leq 13} \to \{2k + 1 | k \in \{-4, -3, \cdots, 8\}\}, m \mapsto 2(m - 5) + 1 = 2m - 9.$$

$$\varphi_4 : \mathbb{N}_{\leq 5} \to \{(-2)^k | k \in \{2, 3, 4, 5, 6\}\} = \{4, -8, 16, -32, 64\} \text{ mit}$$

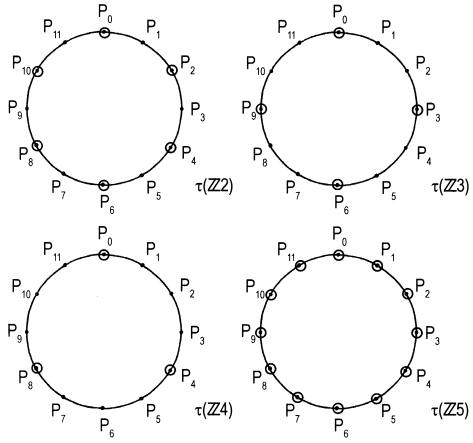
$$1 \mapsto -32,\ 2 \mapsto -8,\ 3 \mapsto 4,\ 4 \mapsto 16 \text{ und } 5 \mapsto 64.$$

$$\varphi_5 : \mathbb{N}_{\leq n} \to \left\{ \frac{1}{k} \middle| k \in \mathbb{N}_{\leq n} \right\}, m \mapsto \frac{1}{n - m + 1}.$$

Teil B

Aufgaben 4.4 A) Für $k \in \mathbb{N}$ gilt $\tau(\mathbb{Z}k) = \{P_{nk \bmod (12)} | n \in \mathbb{Z}\}$. Somit erhalten wir

$$\tau(\mathbb{Z}2) = \{P_0, P_2, P_4, P_6, P_8, P_{10}\},\ \tau(\mathbb{Z}3) = \{P_0, P_3, P_6, P_9\},$$
$$\tau(\mathbb{Z}4) = \{P_0, P_4, P_8\},\ \tau(\mathbb{Z}5) = \{P_i | i \in \{0, \ldots, 11\}\}.$$



Aufgabe 4.4 A)

B) Für $m, n \in \mathbb{N}$ gilt nach Definition

$$(*) \qquad n = m \cdot \left\lfloor \frac{n}{m} \right\rfloor + n \mod (m) \text{ mit } 0 \leq n \mod (m) < m.$$

Durch Division mit m erhalten wir

$$\frac{n}{m} = \left\lfloor \frac{n}{m} \right\rfloor + \frac{n \mod (m)}{m} \text{ mit } 0 \leq \frac{n \mod (m)}{m} < 1,$$

woraus die Behauptung a) folgt. Behauptung b) folgt direkt aus $(*)$ durch Subtraktion von $m \cdot \left\lfloor \frac{n}{m} \right\rfloor$.

C) Die erste Behauptung ist ein Spezialfall der zweiten ($k = 1$). Deshalb ist nur die zweite Behauptung zu zeigen. Das Bestehen der angegebenen Gleichung ist äquivalent dazu, dass ein $q \in \mathbb{Z}$ existiert mit $km^n = q(m-1) + k$, das heisst dass $k\frac{m^n-1}{m-1} \in \mathbb{Z}$. Nach 3.3 B) gilt aber

$$k\frac{m^n - 1}{m - 1} = k \sum_{i=0}^{n-1} m^i,$$

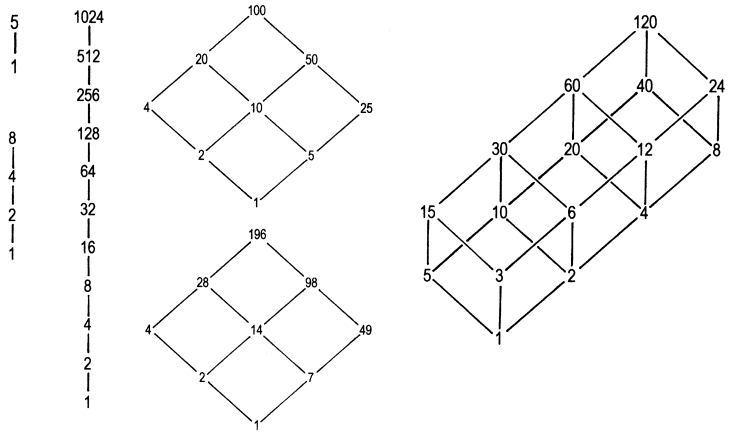
und diese Summe ist sicher eine ganze Zahl.

D) Sei $a \in \mathbb{N}$. Die Dezimaldarstellung von a hat die Form

$$a = a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n$$

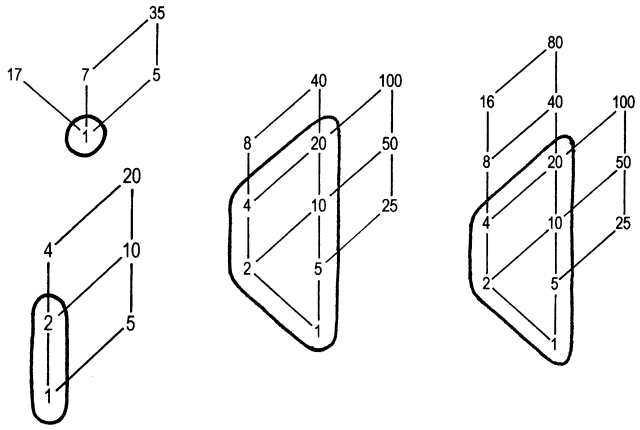
mit $n \in \mathbb{N}_0$ und Ziffern $a_0, \ldots, a_n \in \{0, \ldots, 9\}$ mit $a_n \neq 0$. Jeden der auftretenden Summanden können wir wegen C) in der Form $a_i \cdot 10^i = 9q_i + a_i$ schreiben mit $q_i \in \mathbb{Z}$. Somit erhalten wir $a = 9(q_0 + \cdots + q_n) + (a_0 + \cdots + a_n)$, und es folgt $a \bmod (9) = (a_0 + \cdots + a_n) \bmod (9)$, wobei die rechte Seite der letzten Gleichung gerade der „Neunerrest“ der Quersumme von a ist.

Aufgaben 4.10 A) i) Wegen $0 = m \cdot 0, n = 1 \cdot n$ und $m = m \cdot 1$ folgen die Behauptungen direkt aus der Definition.
ii) Aus $k|m$ und $m|n$ folgt, dass es $a, b \in \mathbb{Z}$ mit $n = am$ und $m = bk$ gibt. Dann gilt $n = am = a(bk) = (ab)k$ und somit $k|n$.
iii) Genau dann gilt $m|n$, wenn es ein $a \in \mathbb{Z}$ mit $n = am$ oder – äquivalent dazu – mit $-n = -(am) = (-a)m$ gibt, also wenn $m|(-n)$.
iv) Aus $m|n$ und $m|p$ folgt, dass es $a, b \in \mathbb{Z}$ mit $n = am$ und $p = bm$ gibt. Dann gilt $n + p = am + bm = (a + b)m$ und somit $m|(n + p)$.
v) Aus $m|n$ folgt, dass es ein $a \in \mathbb{Z}$ mit $n = am$ gibt. Dann gilt $np = (am)p = (pa)m$ und somit $m|np$.
vi) Aus $k|m$ und $k \neq m$ folgt, dass es ein $a \in \mathbb{Z} \setminus \{1\}$ mit $m = ak$ gibt. Nach Voraussetzung sind $k, m \in \mathbb{N}$, also $k, m \geq 1$. Somit gilt $a > 1$, und deshalb muss $k < m$ gelten, da sonst der Widerspruch $m = ak > k \geq m$ folgte.
vii) Gilt $km|n$, so gibt es ein $a \in \mathbb{Z}$ mit $n = a(km) = (ak)m$; also gilt $m|n$.
viii) Gilt $\mathbb{T}(m) \subseteq \mathbb{T}(n)$, so ist jeder Teiler von m auch ein Teiler von n. Wegen $m|m$ gilt also $m|n$. Gilt umgekehrt $m|n$ und ist k ein Teiler von m, so gilt nach 4.5 B)b) auch $k|n$, also $\mathbb{T}(m) \subseteq \mathbb{T}(n)$.
ix) Wegen $m|m$ gilt $m \in \mathbb{T}(m)$. Für $k \in \mathbb{T}(m) \setminus \{m\}$ gilt nach 4.5 B)f) $k < m$, woraus die Behauptung folgt.
B)



Aufgabe 4.10 B)

C)



Aufgabe 4.10 C)

D) Bezeichnen wir die kleinsten echten Teiler von n und p mit a und b, so liefert das Netz die Gleichungen $n = a^2b^2$ und $p = ab^4$. Durch Ausprobieren (d.h. Einsetzen kleiner Primzahlen für a und b) erhalten wir für (n, p) die Lösungen $(36, 48), (36, 162), (100, 80)$ und $(196, 112)$.

E) Der Euklidische Algorithmus liefert

$$\mathrm{ggT}(513, 10701) = \mathrm{ggT}(441, 513) = \mathrm{ggT}(72, 441) = \mathrm{ggT}(9, 72) = \mathrm{ggT}(0, 9) = 9;$$

$$\mathrm{ggT}(1716, 299) = \mathrm{ggT}(299, 1716) = \mathrm{ggT}(221, 299)$$
$$= \mathrm{ggT}(78, 221) = \mathrm{ggT}(65, 78) = \mathrm{ggT}(13, 65) = \mathrm{ggT}(0, 13) = 13.$$

F) Siehe Zeichnung.

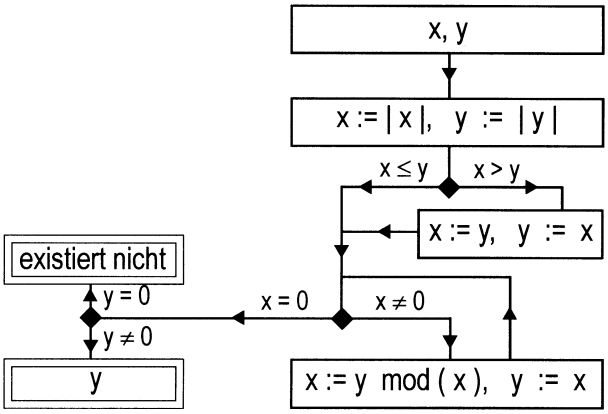
G) Der Abstand zwischen den Pfählen muss 36 und 52 teilen. Also ist der grösstmögliche Abstand gerade $\mathrm{ggT}(36, 52) = 4$. Mit diesem Abstand braucht man wegen $36 = 9 \cdot 4$ und $52 = 13 \cdot 4$ genau $2(9 + 13) = 44$ Pfähle.

H) Wir suchen zwei natürliche Zahlen m und n so, dass $mn = 1000$ und dass der Umfang $2(m + n)$ minimal wird. Ausprobieren liefert $(m, n) = (40, 25)$. Bei diesem Format des Platzes haben die Pfähle einen grösstmöglichen Abstand von $\mathrm{ggT}(40, 25) = 5$. Somit werden $2(8 + 5) = 26$ Pfähle benötigt.

I) Macht das kleine Zahnrad 78 Umläufe, so macht das grosse Zahnrad 13 Umläufe; also besteht das Übersetzungsverhältnis $\frac{13}{78} = \frac{1}{6}$. Nach sechs Umläufen des kleinen Zahnrades hat das grosse Zahnrad also genau einen Umlauf gemacht und es berühren sich erstmals wieder die gleichen Zähne. Somit werden während der sechs Umläufe des kleinen Zahnrades am grossen Zahnrad genau sechs Zähne zerkratzt, und danach wiederholt sich alles.

J) Für das Übersetzungsverhältnis gilt

$$\frac{m}{n} = \frac{\frac{m}{\mathrm{ggT}(m,n)}}{\frac{n}{\mathrm{ggT}(m,n)}}.$$



Aufgabe 4.10 F)

Die Anzahl zerkratzter Zähne ist $\frac{n}{\mathrm{ggT}(m,n)}$, und dies ist auch die minimale Anzahl Umläufe des „kleinen“ Zahnrades. Entsprechend ist die minimale Anzahl Umläufe des „grossen“ Zahnrades $\frac{m}{\mathrm{ggT}(m,n)}$.

Aufgaben 4.20 A) i) Es gilt $\mathrm{ggT}(2,3) = 1$, und wir finden

$$2 \cdot 2 + 3 \cdot (-1) = 1,$$

also $(u, v) = (2, -1)$.
ii) Es gilt $\mathrm{ggT}(39, 299) = 13$. Wir betrachten $\left(\frac{39}{13}, \frac{299}{13}\right) = (3, 23)$. Es gilt $\mathrm{ggT}(3, 23) = 1$, und wir finden

$$3 \cdot 8 + 23 \cdot (-1) = 1.$$

Indem wir diese Gleichung mit 13 multiplizieren erhalten wir

$$39 \cdot 8 + 299 \cdot (-1) = 13,$$

also $(u, v) = (8, -1)$.
iii) Es gilt $\mathrm{ggT}(72, 162) = 18$. Wir betrachten $\mathrm{ggT}\left(\frac{72}{18}, \frac{162}{18}\right) = \mathrm{ggT}(4, 9) = 1$ und finden

$$4 \cdot (-2) + 9 \cdot 1 = 1.$$

Multiplikation mit 18 liefert

$$72 \cdot (-2) + 162 \cdot 1 = 18,$$

also $(u, v) = (-2, 1)$.
B) i) Sei $m \in \mathbb{Z}$. Wegen $m = 1 \cdot m \in \mathbb{Z}m$ gilt $\mathbb{Z}m \neq \emptyset$. Sind $x, y \in \mathbb{Z}m$, so finden wir $a, b \in \mathbb{Z}$ mit $x = am$ und $y = bm$. Es folgt

$$x + y = am + bm = (a + b)m \in \mathbb{Z}m.$$

Für $z \in \mathbb{Z}$ gilt weiter

$$zx = z(am) = (za)m \in \mathbb{Z}m.$$

Damit ist gezeigt, dass $\mathbb{Z}m$ ein Ideal ist.
ii) Es gibt $u \in \mathbb{I}$ und $v \in \mathbb{J}$, und es gelten $vu \in \mathbb{I}$ und $uv \in \mathbb{J}$, also $uv \in \mathbb{I} \cap \mathbb{J} \neq \emptyset$. Seien $x, y \in \mathbb{I} \cap \mathbb{J}$ und $z \in \mathbb{Z}$. Dann gelten $x, y \in \mathbb{I}$ und $x, y \in \mathbb{J}$. Weil $\mathbb{I}, \mathbb{J}$ Ideale sind, folgen $x + y, zx \in \mathbb{I}$ und $x + y, zx \in \mathbb{J}$, also $x + y, zx \in \mathbb{I} \cap \mathbb{J}$. Somit ist $\mathbb{I} \cap \mathbb{J}$ auch ein Ideal.
iii) Es gibt $u \in \mathbb{I}$ und $v \in \mathbb{J}$, und es gilt $u + v \in \mathbb{I} + \mathbb{J} \neq \emptyset$. Seien $x, y \in \mathbb{I} + \mathbb{J}$ und $z \in \mathbb{Z}$. Es gibt dann $a, a' \in \mathbb{I}$ und $b, b' \in \mathbb{J}$ mit $x = a + b$ und $y = a' + b'$. Weil $\mathbb{I}$ und $\mathbb{J}$ Ideale sind, gelten $a + a', za \in \mathbb{I}$ und $b + b', zb \in \mathbb{J}$. Also folgen

$$x + y = (a + b) + (a' + b') = (a + a') + (b + b') \in \mathbb{I} + \mathbb{J}$$

und

$$z(a + b) = za + zb \in \mathbb{I} + \mathbb{J}.$$

Somit ist $\mathbb{I} + \mathbb{J}$ ein Ideal.
C) a) Sei $x \in \mathbb{I}$. Dann gilt $-x = (-1) \cdot x \in \mathbb{I}$.
b) Wegen $\emptyset \neq \mathbb{I} \neq \{0\}$ gibt es ein $x \in \mathbb{I}$ mit $x \neq 0$. Mit a) folgt $-x \in \mathbb{I}$, und wegen $x \neq 0$ gilt entweder $x \in \mathbb{N}$ oder $-x \in \mathbb{N}$, also die Behauptung.
c) Sei $x \in \mathbb{I}$. Division mit Rest liefert eine Darstellung $x = at + x \bmod (t)$ mit $a \in \mathbb{Z}$. Wegen $t \in \mathbb{I}$ gilt $at \in \mathbb{I}$, und aus a) folgt $-at \in \mathbb{I}$. Wegen $x \in \mathbb{I}$ folgt also $x \bmod (t) = x - at \in \mathbb{I}$.
d) Sei $x \in \mathbb{I}$. Division mit Rest liefert $x = at + y$ mit $a, y \in \mathbb{Z}$ und $0 \leq y < t$. Nach c) gilt $y \in \mathbb{I}$. Weil aber $t = \min(\mathbb{N} \cap \mathbb{I})$ gilt, muss $y \notin \mathbb{N}$ gelten. Also ist $y = 0$, und wir erhalten $x = at$. Dies bedeutet aber gerade, dass $x \in \mathbb{Z}t$.
e) Wegen $t \in \mathbb{I}$ gilt sicher $\mathbb{Z}t \subseteq \mathbb{I}$. Nach d) gilt auch die umgekehrte Inklusion, und es folgt die Behauptung.
D) Wir nehmen an, das vorliegende Netz wäre das Netz des gemeinsamen Teilerverbandes zweier natürlicher Zahlen. Insbesondere wäre es dann das Netz des Teilerverbandes des grössten gemeinsamen Teilers g dieser zwei Zahlen. Offenbar hätte dann g zwei verschiedene minimale echte Teiler a und b. Weiter müsste g, der „höchste Punkt“ des Netzes, sowohl gleich a^2b als auch ab^2 sein. Also erhielten wir den Widerspruch $a = b$.

Aufgaben 4.24 A) Es bezeichne a die Seitenlänge des Platzes in cm. Die Beschränkung der Kosten bedeutet $a^2 \leq 120000$, also $a \leq 346$. Das maximale a ist ein gemeinsames Vielfaches von 12 und 16, also ein Vielfaches von $\mathrm{kgV}(12, 16) = 48$, genauer

$$a = \max\{48n | n \in \mathbb{N} \wedge 48n \leq 346\} = 48 \cdot 7 = 336.$$

Dies entspricht einem Platz aus $\frac{336}{16} \cdot \frac{336}{12} = 21 \cdot 28 = 588$ Platten.
B) Es gelten $\mathrm{kgV}(10, 6) = 30$, $\mathrm{kgV}(10, 8) = 40$ und $\mathrm{kgV}(6, 8) = 24$, das heisst alle 30 bzw. 40 bzw. 24 Minuten fahren die Busse A und B bzw. A und C bzw. B und C

gemeinsam los. Während einer Dauer von insgesamt 14 Stunden geschieht dies also 28 bzw. 21 bzw. 35 mal. Dass alle drei Busse gleichzeitig losfahren geschieht höchstens alle $\mathrm{kgV}(30,40) = 120$ Minuten. Weil 120 auch ein Vielfaches von 24 ist, ist dies tatsächlich alle 120 Minuten der Fall und geschieht insgesamt 7 mal.
C) a) Sei $x \in \mathbb{Z}mn$. Dann gibt es $a \in \mathbb{Z}$ mit $x = a(mn) = (am)n = (an)m$ und es folgt $x \in \mathbb{Z}m \cap \mathbb{Z}n$.
b) Weil $\mathbb{Z}a = \mathbb{Z}(-a)$ für jedes $a \in \mathbb{Z}$ gilt können wir annehmen, es gelte $m, n \in \mathbb{N}$. Nach 4.23 ist $\mathbb{Z}m \cap \mathbb{Z}n = \mathbb{Z}mn$ äquivalent zu $mn = \mathrm{kgV}(m,n)$. Nach 4.22 ist dies aber äquivalent zu $\mathrm{ggT}(m,n) = 1$, und es folgt die Behauptung.
D) Die minimale Zeit zwischen zwei Vollmonden beträgt 42524 Minuten. Die Zeit zwischen zwei identischen Zuständen der Uhr beträgt mit Berücksichtigung des Wochentages $7 \cdot 24$ Stunden, also 10080 Minuten. Somit tritt die gezeichnete Situation alle $\mathrm{kgV}(42524, 10080)$ Minuten auf. Um diese Zahl zu berechnen kann man 4.22 verwenden. Es gilt $\mathrm{ggT}(42524, 10080) = 4$, also

$$\mathrm{kgV}(42524, 10080) = \frac{42524 \cdot 10080}{4} = 107160480.$$

Dies entspricht genau 74417 Tagen oder knapp 204 Jahren.
E) Ein Jahr hat 8766 Stunden und eine Woche hat 168 Stunden. Es gilt $\mathrm{ggT}(8766, 168) = 6$, und mit 4.22 folgt, dass die angegebene Situation alle

$$\mathrm{kgV}(8766, 168) = \frac{8766 \cdot 168}{6} = 245448$$

Stunden oder alle 28 Jahre eintritt.

Aufgaben 4.28 A)

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
ν_2	0	1	0	2	0	1	0	3	0	1	0	2	0	1	0	4	0	1
ν_3	0	0	1	0	0	1	0	0	2	0	0	1	0	0	1	0	0	2
ν_4	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	2	0	0
ν_6	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1

n	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
ν_2	0	2	0	1	0	3	0	1	0	2	0	1	0	5	0	1	0	2
ν_3	0	0	1	0	0	1	0	0	3	0	0	1	0	0	1	0	0	2
ν_4	0	1	0	0	0	1	0	0	0	1	0	0	0	2	0	0	0	1
ν_6	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	2

B) i) Für $u = 2, v = 3$ gelten $\nu_6(u) = \nu_6(v) = 0$ und $\nu_6(uv) = 1$. Weitere Beispiele für (u,v) sind $(3,4), (2,9), (3,8), (2,15), (3,10), (2,18), (3,12), (4,9)$.
ii) Für $w = 2$ gelten $2 \cdot \nu_4(w) = 0$ und $\nu_4(w^2) = 1$. Weitere Beispiele für w sind 6 und 8.
C) Wegen 4.27 c) ist nur „$\Rightarrow$“ zu zeigen. Sei also $\nu_2(u+v) = \min\{\nu_2(u), \nu_2(v)\}$. Wir

nehmen an, es gälte $n := \nu_2(u) = \nu_2(v)$. Dann gäbe es ungerade Zahlen a, b mit $u = 2^n a$ und $v = 2^n b$. Es wäre also $a + b$ gerade und

$$u + v = 2^n a + 2^n b = 2^n(a + b).$$

Daraus folgte aber der Widerspruch $\nu_2(u + v) > n$.
D) Offensichtlich erfüllt $(1, 1)$ die vorgegebenen Bedingungen. Ein anderes solches Paar kann es nicht geben, denn für $(u, v) \neq (1, 1)$ wäre $u + v > 2$, aber $\nu_{u+v}(u + v) = 1$ und $\nu_{u+v}(u) = \nu_{u+v}(v) = 0$.
E) Das in D) bestimmte Paar $(1, 1)$ liefert ein Gegenbeispiel.

Aufgaben 5.7 A)–F) Empfohlene Startseiten für die Suche im Internet sind:
http://mathworld.wolfram.com/PrimeNumber.html
http://primes.utm.edu
http://de.wikipedia.org/wiki/Primzahl
Geeignete Suchbegriffe: Mersenneprimzahlen, Primzahlzwillinge, Catalansche Vermutung, Goldbachsche Vermutung.
G) Wir nehmen an, p wäre keine Primzahl. Dann gäbe es ein $m, n \in \mathbb{N} \setminus \{1, p\}$ mit $p = mn$. Wir könnten ohne Einschränkung annehmen, es gälte $n \leq m$. So erhielten wir $2 \leq n$ und $n^2 \leq mn = p$, also den Widerspruch $n|p$ und $2 \leq n \leq \sqrt{p}$.
H) Es gilt

$$\mathbb{M}_n = \mathbb{N}_{\leq n^2} \setminus \{uv | u, v \in \mathbb{N}_{\leq n}\} = \left\{m \in \mathbb{N} | n < m \leq n^2 \wedge m \in \mathbb{P}\right\} = \mathbb{P}_n \cap \mathbb{N}_{>n},$$

denn Primzahlen $p \leq n$ können als $p = 1p$ geschrieben werden. Konkret für $n = 10$ und $n = 20$ findet man

$$\mathbb{P}_{10} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\},$$

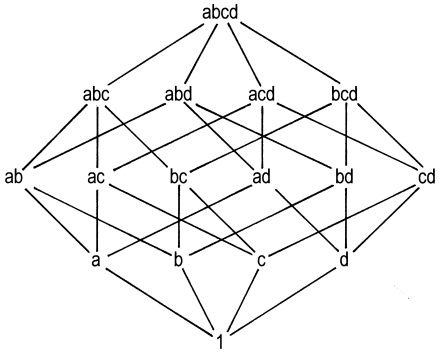
$$\mathbb{P}_{20} = \mathbb{P}_{10} \cup \{101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179,$$
$$181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281,$$
$$283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397\},$$

$$\mathbb{M}_{10} = \mathbb{P}_{10} \setminus \{2, 3, 5, 7\} \text{ und } \mathbb{M}_{20} = \mathbb{P}_{20} \setminus \{2, 3, 5, 7, 11, 13, 17, 19\}.$$

I) Siehe Zeichnung. Gesucht sind Zahlen der Form *abcd* mit verschiedenen Primzahlen a, b, c, d. Die kleinsten Beispiele sind $2 \cdot 3 \cdot 5 \cdot 7 = 210$ und $2 \cdot 3 \cdot 5 \cdot 11 = 330$.
J) Wir nehmen an, p wäre nicht prim. Dann fänden wir $r, s \in \mathbb{N} \setminus \{1\}$ mit $p = rs$. Nach 3.3 B) gälte

$$h^{rs} - 1 = (h^r - 1)\left(1 + h^r + \cdots + h^{(s-1)r}\right).$$

Diese beiden Faktoren wären aber wegen $r > 1$ und $s > 1$ beide in $\mathbb{N} \setminus \{1\}$, und somit wäre $h^{rs} - 1 = h^p - 1$ nicht prim.
K) Mit $h = 2$ folgt aus J), dass für $n \in \mathbb{N}$ gilt: Ist $2^n - 1$ prim, so ist n prim. Dies ist



Aufgabe 5.7 I)

eine notwendige Bedingung dafür, dass eine Mersennezahl prim ist (vgl. A)).

Aufgaben 5.11 A) Wir suchen zuerst die Primfaktorzerlegungen der gegebenen Zahlen. Es gelten

$$120 = 2^3 \cdot 3 \cdot 5,\ 1024 = 2^{10} \text{ und } 9999 = 3^2 \cdot 11 \cdot 101.$$

Damit erhalten wir nach Definition der Teilervielfachheit

$$\nu_p(120) = \begin{cases} 3 & \text{für} \quad p = 2 \\ 1 & \text{für} \quad p = 3 \\ 1 & \text{für} \quad p = 5 \\ 0 & \text{für} \quad p \in \mathbb{P} \setminus \{2,3,5\}; \end{cases}$$

$$\nu_p(1024) = \begin{cases} 10 & \text{für} \quad p = 2 \\ 0 & \text{für} \quad p \in \mathbb{P} \setminus \{2\}; \end{cases}$$

$$\nu_p(9999) = \begin{cases} 2 & \text{für} \quad p = 3 \\ 1 & \text{für} \quad p = 11 \\ 1 & \text{für} \quad p = 101 \\ 0 & \text{für} \quad p \in \mathbb{P} \setminus \{3,11,101\}. \end{cases}$$

B) a) Es gilt $\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1)$, also $\nu(1) = 0$.
b) Aus $\frac{m}{n} = \frac{m'}{n'}$ folgt $mn' = m'n$. Damit erhalten wir

$$\nu(m) + \nu(n') = \nu(mn') = \nu(m'n) = \nu(m') + \nu(n),$$

woraus die Behauptung folgt.
c) Was an dieser Definition problematisch sein könnte ist, dass die Darstellung $\frac{m}{n}$ eines Bruches nicht eindeutig ist. Betrachten wir $q \in \mathbb{Q} \setminus \{0\}$ und zwei verschiedene Bruchdarstellungen $\frac{m}{n} = q = \frac{m'}{n'}$, so folgt aber aus b), dass $\nu(m) - \nu(n)$ nur von q und nicht von der gewählten Bruchdarstellung abhängt. Somit ist die Definition von $\tilde{\nu}$ sinnvoll.

C) a) α) $\tilde{\nu}(n) = \tilde{\nu}\left(\frac{n}{1}\right) = \nu(n) - \nu(1) = \nu(n) - 0 = \nu(n)$.
β) Wir finden $m, s, n, t \in \mathbb{Z} \setminus \{0\}$ so, dass $q = \frac{m}{n}$ und $r = \frac{s}{t}$. Damit erhalten wir

$$\tilde{\nu}(qr) = \tilde{\nu}\left(\frac{m}{n}\frac{s}{t}\right) = \tilde{\nu}\left(\frac{ms}{nt}\right) = \nu(ms) - \nu(nt) = \nu(m) + \nu(s) - \nu(n) - \nu(t)$$

$$= \nu(m) - \nu(n) + \nu(s) - \nu(t) = \tilde{\nu}\left(\frac{m}{n}\right) + \tilde{\nu}\left(\frac{s}{t}\right) = \tilde{\nu}(q) + \tilde{\nu}(r).$$

b) Sei $\mu : \mathbb{Q} \setminus \{0\} \to \mathbb{Z}$ eine Abbildung mit den Eigenschaften (α) und (β). Wir müssen zeigen, dass dann $\mu = \tilde{\nu}$, d.h. dass für jedes $q \in \mathbb{Q} \setminus \{0\}$ gilt $\mu(q) = \tilde{\nu}(q)$. Sei $q \in \mathbb{Q} \setminus \{0\}$. Wir finden $m, n \in \mathbb{Z} \setminus \{0\}$ mit $q = \frac{m}{n}$ und erhalten

$$\nu(m) \overset{(\alpha)}{=} \mu(m) = \mu\left(\frac{m}{n} \cdot n\right) \overset{(\beta)}{=} \mu\left(\frac{m}{n}\right) + \mu(n) \overset{(\alpha)}{=} \mu\left(\frac{m}{n}\right) + \nu(n).$$

Dies liefert uns aber

$$\mu(q) = \mu\left(\frac{m}{n}\right) = \nu(m) - \nu(n) = \tilde{\nu}\left(\frac{m}{n}\right) = \tilde{\nu}(q).$$

c) Seien $q = \frac{m}{n}$ und $r = \frac{s}{t}$ wie in a). Damit erhalten wir

$$\tilde{\nu}(q + r) = \tilde{\nu}\left(\frac{m}{n} + \frac{s}{t}\right) = \tilde{\nu}\left(\frac{mt + ns}{nt}\right) = \nu(mt + ns) - \nu(nt)$$

$$\geq \min\{\nu(mt), \nu(ns)\} - \nu(nt) = \min\{\nu(mt) - \nu(nt), \nu(ns) - \nu(nt)\} =$$

$$\min\left\{\tilde{\nu}\left(\frac{mt}{nt}\right), \tilde{\nu}\left(\frac{ns}{nt}\right)\right\} = \min\{\tilde{\nu}(q), \tilde{\nu}(r)\}.$$

D) Wir schreiben $x^3 - 2x^2 = x \cdot x \cdot (x - 2)$ und erhalten

$$\mu_p\left(x^2 - 2x^2\right) = \begin{cases} 2 & \text{für} \quad p = 0 \\ 1 & \text{für} \quad p = 2 \\ 0 & \text{für} \quad p \in \mathbb{R} \setminus \{0, 2\}. \end{cases}$$

E) Seien $p \in \mathbb{R}, f(x) \in \mathbb{R}[x] \setminus \{0\}$ und $\mu := \mu_p(f)$. Es gibt also ein $g(x) \in \mathbb{R}[x]$ mit $g(p) \neq 0$ und $f(x) = (x - p)^\mu g(x)$. Falls $\mu = 0$, so gilt $f^{(\mu)}(p) = f(p) = g(p) \neq 0$. Sei nun $\mu > 0$, und für alle $h(x) \in \mathbb{R}[x] \setminus \{0\}$ mit $\mu_p(h) < \mu$ gelten

$$(*) \qquad h^{(0)}(p) = \cdots = h^{(\mu_p(h)-1)}(p) = 0 \text{ und } h^{(\mu_p(h))} \neq 0.$$

Sei $h(x) := (x - p)^{\mu-1} g(x)$. Dann gilt $\mu_p(h) < \mu$ und somit auch die Aussage $(*)$. Man überlegt sich mit Hilfe der Ableitungsregeln leicht, dass für alle $n \in \mathbb{N}_0$

$$f^{(n)}(x) = nh^{(n-1)}(x) + (x - p)h^{(n)}(x)$$

gilt (wobei wir $h^{(-1)} := 0$ vereinbaren). Mit $(*)$ folgt jetzt durch vollständige Induktion die Behauptung.
F) i) Sei $f(x) := x - p \in \mathbb{R}[x]$. Es gelten $f^{(0)}(p) = p - p = 0$ und $f^{(1)}(p) = 1 \neq 0$. Aus 5.10) B)b) folgt also $\mu_p(f) = 1$.
ii) Wir finden $\bar{f}(x), \bar{g}(x) \in \mathbb{R}[x]$ mit $f(x) = (x-p)^{\mu_p(f)}\bar{f}(x)$, $g(x) = (x-p)^{\mu_p(g)}\bar{g}(x)$, $\bar{f}(p) \neq 0$ und $\bar{g}(p) \neq 0$. Damit erhalten wir

$$(fg)(x) = (x-p)^{\mu_p(f)+\mu_p(g)}(\bar{f}\bar{g})(x)$$

und $(\bar{f}\bar{g})(p) \neq 0$, also die Behauptung.
iii) Es gelten die Bezeichnungen von ii). Ohne Einschränkung können wir annehmen, es gelte $\mu_p(f) \geq \mu_p(g)$. Wir erhalten

$$(f+g)(x) = (x-p)^{\mu_p(g)}\left((x-p)^{\mu_p(f)-\mu_p(g)}\bar{f}(x) + \bar{g}(x)\right)$$

und damit die Behauptung.

Aufgaben 5.14 A) $1024 = 2^{10},\ 8! = 2^7 \cdot 3^2 \cdot 5 \cdot 7,\ \binom{17}{4} = 2^2 \cdot 5 \cdot 7 \cdot 17,\ 99 = 3^2 \cdot 11,\ 999 = 3^3 \cdot 37,\ 9999 = 3^2 \cdot 11 \cdot 101,\ 99999 = 3^2 \cdot 41 \cdot 271.$
B) Es gilt

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1}$$

und damit $p \in \mathbb{P}\left(\binom{p}{k}\right)$. Sei $q \in \mathbb{P}\left(\binom{p}{k}\right)$. Dann gibt es ein $m \in \mathbb{Z}$ mit

$$qm = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1},$$

also mit

$$qmk(k-1)\cdots 1 = p(p-1)\cdots(p-k+1).$$

Daraus folgt $q | p(p-1)\cdots(p-k+1)$, und nach 5.3 teilt q einen der rechts stehenden Faktoren. Da diese aber alle kleiner oder gleich p sind, muss dies auch für q gelten. Somit ist p maximal in $\mathbb{P}\left(\binom{p}{k}\right)$.
C) Wir verwenden 3.3 B) und erhalten damit

$$2^{15} - 1 = 2^{3\cdot 5} - 1 \overset{3.3B)}{=} \left(2^5 - 1\right)\left(1 + 2^5 + 2^{2\cdot 5}\right) = 31 \cdot 1057 = 7 \cdot 31 \cdot 151.$$

D) Die Primzahlen kleiner oder gleich 11 sind $2, 3, 5, 7$ und 11. Also erhalten wir

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310,\ 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 4620,\ 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 6930,$$

$$2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 9240,\ 2 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 11 = 11550.$$

E) Sei $p \in \mathbb{P}$. Nach Definition der Teilervielfachheit ist $p \in \mathbb{P}(mn)$ äquivalent zu $0 < \nu_p(mn) = \nu_p(m) + \nu_p(n)$, also zu $\nu_p(m) > 0$ oder $\nu_p(n) > 0$, und dies ist wiederum

gleichbedeutend mit $p \in \mathbb{P}(m) \cup \mathbb{P}(n)$. Verwenden wir dir Darstellung aus 5.13 C)a), so erhalten wir

$$mn = \prod_{p\in\mathbb{P}} p^{\nu_p(mn)} = \prod_{p\in\mathbb{P}} p^{\nu_p(m)+\nu_p(n)}.$$

Aufgaben 5.19 A)

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$d(n)$	1	2	2	3	2	4	2	4	3	4	2	6	2	4	4	5	2	6
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28	14	24	24	31	18	39

n	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
$d(n)$	2	6	4	4	2	8	3	4	4	6	2	8	2	6	4	4	4	9
$\sigma(n)$	20	42	32	36	24	60	31	42	40	56	30	72	32	63	48	54	48	91

B) Nach 5.15 gilt $15 = \sharp\mathbb{T}(n) = (\alpha_1 + 1)\cdots(\alpha_r + 1)$, wobei $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ die Primfaktorzerlegung von n ist. Weil dabei $\alpha_1, \ldots, \alpha_r$ verschieden von 0 sind, besteht nur die Möglichkeit $r = 2$ und $\{\alpha_1 - 1, \alpha_2 - 1\} = \{3, 5\}$. Dies bedeutet, dass $n = p_1^2 p_2^4$ mit zwei verschiedenen Primzahlen p_1, p_2. Ausprobieren liefert

$$2^4 \cdot 3^2 = 144,\ 3^4 \cdot 2^2 = 324,\ 2^4 \cdot 5^2 = 400 \text{ und } 2^4 \cdot 7^2 = 784.$$

C) Seien $d := \sharp\mathbb{T}(n)$ und $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ die Primfaktorzerlegung von n. Nach 5.15 gilt dann $d = (\alpha_1 + 1)\cdots(\alpha_r + 1)$, und weil d prim ist folgt $r = 1$. Somit ist $n = p_1^{\alpha_1}$ eine Primzahlpotenz. Weil weiter $\alpha_1 + 1$ prim ist, ist α_1 entweder gerade oder gleich 1. Zusammengefasst erhalten wir also: n ist eine Primzahl oder eine Primzahlpotenz mit geradem Exponenten.
D) Seien $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ die Primfaktorzerlegung von n und $q \in \mathbb{P}$ mit $q^2 = \sharp\mathbb{T}(n)$. Nach 5.15 wissen wir, dass $q^2 = (\alpha_1 + 1)\cdots(\alpha_r + 1)$. Daraus folgt, dass entweder $r = 2$ und $\alpha_1 + 1 = \alpha_2 + 1 = q$ oder dass $r = 1$ und $\alpha_1 + 1 = q^2$.
Im Fall $r = 2$ müssen wir unterscheiden, ob q gerade (das heisst $q = 2$) oder ungerade ist. Ist $q = 2$, also $\alpha_1 = \alpha_2 = 1$, so erhalten wir $n = p_1 p_2$. Falls q ungerade ist, so ist $\alpha_1 = \alpha_2$ gerade und wir erhalten $n = (p_1 p_2)^\alpha$ mit geradem $\alpha \in \mathbb{N}$.
Im Fall $r = 1$ schreiben wir $\alpha_1 = q^2 - 1 = (q-1)(q+1)$. Falls $q = 2$, so gilt $\alpha_1 = 3$ und wir erhalten $n = p_1^3$. Ist q ungerade, so folgt schliesslich $n = p_1^\alpha p_2^{\alpha+2}$ mit geradem $\alpha \in \mathbb{N}$.
E) Sei $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ die Primfaktorzerlegung von n. Es gilt dann $r = \sharp\mathbb{P}(n)$ und wegen $\alpha_1, \ldots, \alpha_r \geq 1$ folgt

$$\sharp\mathbb{T}(n) \overset{(5.15)}{=} (\alpha_1 + 1)\cdots(\alpha_r + 1) \geq (1+1)\cdots(1+1) = 2^r = 2^{\sharp\mathbb{P}(n)}.$$

Ist n quadratfrei, so bedeutet dies $\alpha_1 = \cdots = \alpha_r = 1$ und in der obigen Ungleichung gilt Gleichheit.
F) a) Wir schreiben $g := \mathrm{ggT}(m, n)$, und nach 5.13 C)a) gilt $g = \prod_{p\in\mathbb{P}} p^{\nu_p(g)}$. Sei p ein Primteiler von g. Die Teilervielfachheit von p in g ist die maximale Potenz von p,

welche sowohl m als auch n teilt, das heisst $\nu_p(g) = \min(\{\nu_p(m), \nu_p(n)\})$, und aus obiger Darstellung folgt die Behauptung.
b) Sei $p \in \mathbb{P}$. Genau dann ist p ein Teiler von g, wenn $\nu_p(g) > 0$, wegen $\nu_p(g) = \min(\{\nu_p(m), \nu_p(n)\})$ also genau dann, wenn $\nu_p(m) > 0$ und $\nu_p(n) > 0$. Dies ist aber offenbar äquivalent zu $p \in \mathbb{P}(m) \cap \mathbb{P}(n)$.
c) m und n sind genau dann teilerfremd, wenn $g = 1$. Es ist klar, dass 1 die einzige natürliche Zahl ist, die keine Primteiler besitzt, weswegen obige Aussage äquivalent zu $\mathbb{P}(g) = \emptyset$ ist. Mit b) folgt nun die Behauptung.
G) a) Wir schreiben $k := \mathrm{kgV}(m, n)$. Sei p ein Primteiler von k. Die Teilervielfachheit von p in k ist die maximale Potenz von p, welche m oder n teilt, das heisst $\nu_p(k) = \max(\{\nu_p(m), \nu_p(n)\})$, und mit 5.13 C)a) folgt die Behauptung.
b) Sei $p \in \mathbb{P}$. Genau dann ist p ein Teiler von k, wenn $\nu_p(k) > 0$, wegen $\nu_p(k) = \max(\{\nu_p(m), \nu_p(n)\})$ also genau dann, wenn $\nu_p(m) > 0$ oder $\nu_p(n) > 0$. Dies ist aber offenbar äquivalent zu $p \in \mathbb{P}(m) \cup \mathbb{P}(n)$.

Aufgaben 5.21 A) Weil m und n teilerfremd sind, können wir 5.20 verwenden, welches insbesondere sagt, dass

$$\mathbb{P}(n-m) \subseteq \mathbb{P} \setminus (\mathbb{P}(m) \cup \mathbb{P}(n)) = \mathbb{P} \setminus \{2,3,5,7\} = \{p \in \mathbb{P} | p \geq 11\}.$$

Wegen $n-m > 1$ ist $\mathbb{P}(m-n) \neq \emptyset$, das heisst es gibt ein $q \in \mathbb{P}(n-m) = \{p \in \mathbb{P} | p \geq 11\}$. Wegen $q | n-m$ und $n-m \neq 0$ folgt $n-m \geq q \geq 11$.
Obige Voraussetzungen werden durch $n = 21$ und $m = 10$ erfüllt und es gilt $n-m = 11$.
B) Der Beweis von A) kann wörtlich übertragen werden. Ein Beispiel, bei welchem Gleichheit gilt, ist gegeben durch $n = 90$ und $m = 77$.

Aufgaben 5.23 A)

n	$\Pi(n)n^{-1}\ln(n)$	n	$\Pi(n)n^{-1}\ln(n)$	n	$\Pi(n)n^{-1}\ln(n)$	n	$\Pi(n)n^{-1}\ln(n)$	n	$\Pi(n)n^{-1}\ln(n)$
		21	1.160	41	1.178	61	1.213	81	1.194
2	0.347	22	1.124	42	1.157	62	1.198	82	1.182
3	0.732	23	1.227	43	1.225	63	1.184	83	1.225
4	0.693	24	1.192	44	1.204	64	1.170	84	1.213
5	0.966	25	1.159	45	1.184	65	1.156	85	1.202
6	0.896	26	1.128	46	1.165	66	1.143	86	1.191
7	1.112	27	1.099	47	1.229	67	1.192	87	1.181
8	1.040	28	1.071	48	1.210	68	1.179	88	1.170
9	0.977	29	1.161	49	1.191	69	1.166	89	1.210
10	0.921	30	1.134	50	1.174	70	1.153	90	1.200
11	1.090	31	1.219	51	1.156	71	1.201	91	1.190
12	1.035	32	1.191	52	1.140	72	1.188	92	1.180
13	1.184	33	1.166	53	1.199	73	1.234	93	1.170
14	1.131	34	1.141	54	1.182	74	1.221	94	1.160
15	1.083	35	1.117	55	1.166	75	1.209	95	1.151
16	1.040	36	1.095	56	1.150	76	1.197	96	1.141
17	1.167	37	1.171	57	1.135	77	1.185	97	1.179
18	1.124	38	1.149	58	1.120	78	1.173	98	1.170
19	1.240	39	1.127	59	1.175	79	1.217	99	1.160
20	1.198	40	1.107	60	1.160	80	1.205	100	1.151

Weiter gelten $\Pi(5000) = 669$ und $\Pi(5000)5000^{-1}\ln(5000) \approx 1.140$.
B) a) Wir machen Induktion über n. Für $n = 1$ ist die Behauptung klar, da a und b als teilerfremd vorausgesetzt werden. Seien nun $n > 1$ und $\mathrm{ggT}(a_i, b) = 1$ für $i \in \{1, \ldots, n-1\}$. Es gilt

$$g := \mathrm{ggT}(a_n, b) = \mathrm{ggT}(a_1 \cdots a_{n-1} + b, b) = \mathrm{ggT}(a_1 \cdots a_{n-1}, b).$$

Wir nehmen an, es gäbe es einen Primteiler p von g. Dieser teilte dann aber sowohl $a_1 \cdots a_{n-1}$ und nach 5.3 also ein a_i für ein $i \in \{1, \ldots, n-1\}$ wie auch b, was der Induktionsvoraussetzung widerspräche.
b) Ohne Einschränkung können wir annehmen, es gelte $n < m$. Wäre $g := \mathrm{ggT}(a_n, a_m) \neq 1$, so gäbe es einen Primteiler p von g. Es gälte also $p|a_1 \cdots a_{n-1} + b$ und $p|a_1 \cdots a_{m-1} + b$. Es gäbe somit ein $x \in \mathbb{Z}$ mit $a_1 \cdots a_{n-1} + b = xp$, und es folgte

$$p|a_1 \cdots a_{n-1} x p a_{n+1} \cdots a_{m-1} + b.$$

Also hätten wir $p|b$ und somit auch $p|a_1 \cdots a_{n-1}$. Wegen $p \in \mathbb{P}$ gäbe es einen Index $i \in \{1, \ldots, n-1\}$ mit $p|a_i$, und dies wäre ein Widerspruch zu a).
c) Wir nehmen an, $\bigcup_{n\in\mathbb{N}} \mathbb{P}(a_n)$ wäre endlich. Dann gäbe es ein $N \in \mathbb{N}$ mit

$$\bigcup_{n\in\mathbb{N}} \mathbb{P}(a_n) = \bigcup_{n=1}^{N} \mathbb{P}(a_n),$$

und a_{N+1} wäre im Widerspruch zu b) nicht teilerfremd zu $a_1, \ldots, a_N$.
C) Mit $a = 1$ und $b = 2$ gelten

$$a_1 = 1,\ a_2 = 3 = 2^{2^0} + 1,\ a_3 = 5 = 2^{2^1} + 1 \text{ und } a_4 = 17 = 2^{2^2} + 1.$$

Wir behaupten, dass für $n \geq 2$

$$a_n = 2^{2^{n-2}} + 1$$

gilt und zeigen dies durch Induktion über n. Für $n = 2$ ist dies klar. Seien also $n > 2$ und

$$(*) \qquad a_{n-1} = 2^{2^{n-3}} + 1.$$

Nach Definition gilt $a_{n-1} = a_1 \cdots a_{n-2} + 2$, also $a_1 \cdots a_{n-2} = a_{n-1} - 2$. Somit erhalten wir

$$a_n = a_1 \cdots a_{n-2} a_{n-1} + 2 = (a_{n-1} - 2)a_{n-1} + 2 = \left(a_{n-1}^2 - 2a_{n-1} + 1\right) + 1 = (a_{n-1} - 1)^2 + 1$$

$$\overset{(*)}{=} \left(2^{2^{n-3}} + 1 - 1\right)^2 + 1 = \left(2^{2^{n-3}}\right)^2 + 1 = 2^{2^{n-2}} + 1,$$

und durch vollständige Induktion folgt die Behauptung.
D) Adressen siehe 5.7, Stichwort *Primzahlsatz*.

Aufgaben 5.25 A)

r	n
1	$\in \mathbb{N}_{\leq 500}$
2	1,4,9,16,25,36,49,64,81,100,121,144,169,196,225,256,289,324,361,400,441,484
3	1,8,27,64,125,198,343
4	1,16,81,256
5	1,32,243
6	1,64
7	1,128
8	1,256
≥ 9	1

B) Wir nehmen an, es gälte $\sqrt[r]{n} \in \mathbb{Q}$. Nach 5.24 gälte dann sogar $\sqrt[r]{n} \in \mathbb{N}$, das heisst es gäbe ein $m \in \mathbb{N}$ mit $m^r = n$. Wegen $n \neq 1$ wäre auch $m \neq 1$. Wir hätten aber die Ungleichung $m^r = n < 2^r$ und wegen $r > 1$ auch $m < 2$, also den Widerspruch $m = 1$.

Teil C

Aufgaben 6.4 A) Für die Reste r und s gelten $r \in \{0, 1, 2\}$ und $s \in \{0, 1, 2, 3, 4\}$. Gesucht sind für jede Wahl von r und s ein $x \in \mathbb{Z}$ mit $0 \leq x \leq 14$ so, dass $x \bmod (3) = r$ und $x \bmod (5) = s$. Der Chinesische Restsatz sagt, dass wegen der Teilerfremdheit von 3 und 5 eine solche Zahl existiert. Zu ihrer Bestimmung verwenden wir das Vorgehen aus 6.3 und müssen zuerst $u, v \in \mathbb{Z}$ mit $3u+5v = 1$ finden. Durch Ausprobieren erhalten wir $u = 2$ und $v = -1$. Also erfüllt $x' := 6s-5r$ die beiden gegebenen Kongruenzen. Um die Bedingung $0 \leq x \leq 14$ zu erfüllen setzen wir $x_0 := x' \bmod (15) = (6s - 5r) \bmod (15)$ und erhalten die folgende Tabelle.

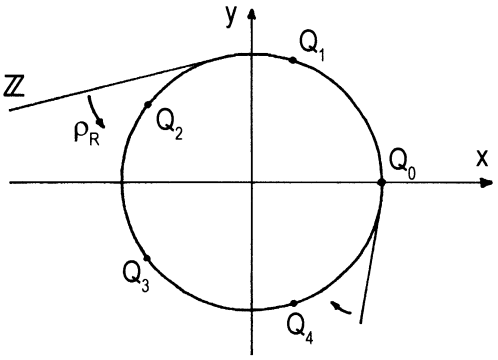
r	0	0	0	0	0	1	1	1	1	1	2	2	2	2	2
s	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
x_0	0	6	12	3	9	10	1	7	13	4	5	11	2	8	14

B) Gesucht ist ein $x \in \mathbb{Z}$ mit $0 \leq x < 60$ und mit $x \bmod (5) = 3$ und $x \bmod (12) = 7$. Da 5 und 12 teilerfremd sind besagt der Chinesische Restsatz, dass eine solche Zahl existiert. Wir suchen zuerst $u, v \in \mathbb{Z}$ mit $5u + 12v = 1$ und finden durch Ausprobieren $u = 5$ und $v = -2$. Dies liefert uns als Lösung der beiden Kongruenzen $x' := 7{\cdot}5{\cdot}5+3{\cdot}12{\cdot}(-2) = 103$ und somit $x = 103 \bmod (60) = 43$. Also trifft Hans um 9.43 Uhr am Zentralplatz ein und verpasst somit den Bus U von 9.40 Uhr um 3 Minuten und den Bus V von 9.36 Uhr um 7 Minuten.

Aufgaben 6.7 A) Es gelten $x \equiv y \bmod (m)$ und $z \equiv w \bmod (m)$. Nach 6.6 a) folgen $m|(x - y)$ und $m|(z - w)$, also $m|(xz - yz)$ und $m|(yz - yw)$. Daraus folgen $xz \equiv yz$

mod (m) und $yz \equiv yw \bmod (m)$, und 6.6 d) impliziert die Behauptung.
B) Es gelten $x \equiv y \bmod (m)$ und $z \equiv w \bmod (m)$. Nach 6.6 b) gilt $-1 \equiv -1 \bmod (m)$, und aus 6.6 g) folgt $-z \equiv -w \bmod (m)$. 6.6 f) liefert jetzt die Behauptung.

Aufgaben 6.14 A)



Aufgabe 6.14 A)

B) Ist ϱ_R längentreu, so wird das Intervall $[0, m] \subseteq \mathbb{R}$ längentreu auf den Kreis S^1_R abgebildet. Somit muss der Umfang von S^1_R gleich der Länge von $[0, m]$, also gleich m, sein. Es muss deshalb $2\pi R = m$ gelten, woraus $R = \frac{m}{2\pi}$ folgt.
C) „(i)⇒(ii)“ : Sei $\mathrm{ggT}(m, n) = 1$. Dann gibt es $u, v \in \mathbb{Z}$ mit $un + vm = 1$. In $\mathbb{Z}/m$ gilt somit

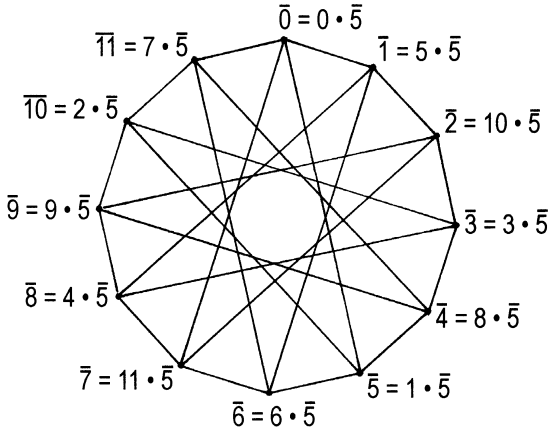
$$\overline{1} = \overline{un + vm} = un + rm + \mathbb{Z}m = un + \mathbb{Z}m = \overline{un},$$

wie wegen $un + rm - un = rm$ aus Satz 6.10 folgt.
„(ii)⇒(iii)“ : Es ist klar, dass $\overline{\mathbb{Z}n} \subseteq \mathbb{Z}/m$ gilt. Ein Element von $\mathbb{Z}/m$ hat die Form $x + \mathbb{Z}m$ mit $x \in \mathbb{Z}$. Nach Voraussetzung gibt es ein $u \in \mathbb{Z}$ mit $\overline{un} = \overline{1}$, das heisst mit $un \equiv 1 \bmod (m)$. Für $x \in \mathbb{Z}$ folgt mit Satz 6.6 b) und g), dass $unx \equiv 1x \bmod (m)$gilt. Damit erhalten wir

$$\overline{x} = \overline{1x} = \overline{unx} = \overline{(ux)n} \in \overline{\mathbb{Z}n},$$

also $\mathbb{Z}/m \subseteq \overline{\mathbb{Z}n}$.
„(iii)⇒(i)“ : Nach Voraussetzung gilt $\overline{1} \in \overline{\mathbb{Z}n}$. Es gibt also ein $u \in \mathbb{Z}$ mit $1 + \mathbb{Z}m = un + \mathbb{Z}m$. Dies heisst, dass es $a, b \in \mathbb{Z}$ gibt mit $1 + am = un + bm$. Wir erhalten $1 = un + (b - a)m$, und dies bedeutet nach 4.12, dass $\mathrm{ggT}(m, n) = 1$.
D) Siehe Zeichnung.

Aufgaben 6.16 A) Dass ε injektiv ist, ist gleichbedeutend damit, dass für $x, y \in \mathbb{Z}$ mit $\varepsilon(x + \mathbb{Z}mn) = \varepsilon(y + \mathbb{Z}mn)$ die Gleichung $x + \mathbb{Z}mn = y + \mathbb{Z}mn$ gilt. Dies wiederum ist äquivalent dazu, dass aus $(x + \mathbb{Z}m, x + \mathbb{Z}n) = (y + \mathbb{Z}m, y + \mathbb{Z}n)$ die Gleichheit $x + \mathbb{Z}mn = y + \mathbb{Z}mn$, nach Lemma 6.1 also die Beziehung $mn|(x - y)$, folgt. Dies ist



Aufgabe 6.14 D)

aber genau die Eindeutigkeitsaussage des Chinesischen Restsatzes.
B) 6.12 b) besagt, dass $\sharp(\mathbb{Z}/k) = k$ für jedes $k \in \mathbb{N}$. Unter Verwendung von Aufgabe 3.26 D) erhält man damit $\sharp(\mathbb{Z}/mn) = mn = \sharp(\mathbb{Z}/m)\sharp(\mathbb{Z}/n) = \sharp(\mathbb{Z}/m \times \mathbb{Z}/n)$. Will man nun beweisen, dass ε bijektiv ist, so genügt es zu zeigen, dass ε injektiv oder surjektiv ist. Die Bijektivität ergibt sich dann aus Satz 3.24.
C) Wir nehmen an, n wäre kein Teiler von m. Dann gäbe es $a, r \in \mathbb{Z}$ mit $m = an + r$ und $0 < r < n$, also insbesondere mit $r + \mathbb{Z}n \neq 0 + \mathbb{Z}n$. Nach Definition von φ gälte einerseits $\varphi(m+\mathbb{Z}m) = m+\mathbb{Z}n = r+\mathbb{Z}n$ und wegen $m+\mathbb{Z}m = 0+\mathbb{Z}m$ andererseits aber auch $\varphi(m+\mathbb{Z}m) = \varphi(0+\mathbb{Z}n) = 0+\mathbb{Z}n$. Das hiesse, dass dem Element $m+\mathbb{Z}m \in \mathbb{Z}/m$ durch φ zwei verschiedene Werte zugeordnet würden und φ somit gar keine Abbildung wäre, was wir im Widerspruch dazu aber vorausgesetzt haben.

Aufgaben 6.19 D) Eine Parameterdarstellung τ wie in 6.18 D) ist bestimmt durch die Wahl eines Paares $(m, n) \in \mathbb{N}^2$ mit $mn = k$ und $\mathrm{ggT}(m, n) = 1$, wobei die Reihenfolge berücksichtigt werden muss. Für $k = 28$ haben genau die vier Paare $(1, 28)$, $(4, 7)$, $(7, 4)$ und $(28, 1)$ diese Eigenschaft. Es gibt also 4 verschiedene Parameterdarstellungen. Für $k = 30$ und für $k = 120$ erhält man je 8 und für $k = 120$ erhält man 16 verschiedene Parameterdarstellungen nach denselben Überlegungen.

Aufgaben 7.6 A) Nach 6.11 C)a) ist $\overline{2} = \overline{7}$ gleichbedeutend mit $m|(7-2)$, also mit $m|5$. Somit gilt $m = 5$ oder $m = 1$.
B) $\overline{9} = \overline{5}$ ist gleichbedeutend mit $m|(9-5)$, also mit $m|4$. Somit gilt $m \in \{1, 2, 4\}$. Es gelten aber $26 \bmod (1) = 26 \bmod (2) = 0$ sowie $26 \bmod (4) = 2 \neq 0$, woraus $m = 4$ folgt.
C) Es gilt $\overline{1} = \overline{2} + \overline{2} = \overline{4}$. Dies ist gleichbedeutend mit $m|(4-1)$, und es folgt $m = 3$ oder $m = 1$.

D) Es gilt $\overline{11} = \overline{6} \cdot \overline{8} = \overline{48}$, und dies ist gleichbedeutend mit $m|(48-11)$, also mit $m|37$. Wegen $37 \in \mathbb{P}$ folgt $m = 37$ oder $m = 1$.
E) Es gilt $\overline{5} = \overline{2}\,\overline{x} = \overline{2x}$, und dies ist gleichbedeutend mit $7|(2x-5)$. Wegen $\mathbb{Z}/7 = \{\overline{x}|0 \leq x \leq 6\}$ liefert ausprobieren die Lösung $\overline{x} = \overline{6}$.
F) $\overline{1}^4 = \overline{1^4} = \overline{1}$; $\overline{2}^4 = \overline{2^4} = \overline{16} = \overline{1}$; $\overline{3}^4 = \overline{3^4} = \overline{81} = \overline{1}$; $\overline{4}^4 = \overline{4^4} = \overline{256} = \overline{1}$.
G) $\overline{-2} = -\overline{2} = \overline{x}^2 = \overline{x^2}$ ist gleichbedeutend mit $11|\,(x^2-(-2))$, also mit $11|\,(x^2+2)$. Wegen $\mathbb{Z}/11 = \{\overline{x}|0 \leq x \leq 10\}$ liefert ausprobieren die Lösungen $\overline{x} = \overline{3}$ oder $\overline{x} = \overline{8}$.
H) $\overline{0} = \overline{x} \cdot \overline{2} = \overline{2x}$ ist gleichbedeutend mit $16|2x$. Wegen $\mathbb{Z}/16 = \{\overline{x}|0 \leq x \leq 15\}$ liefert ausprobieren die Lösungen $\overline{x} = \overline{0}$ oder $\overline{x} = \overline{8}$.

Aufgaben 7.11 A) Es gilt $\mathbb{M}_{12} = \{1,5,7,11\}$ und somit $(\mathbb{Z}/12)^* = \left\{\overline{1},\overline{5},\overline{7},\overline{11}\right\}$. Es ist klar, dass $\overline{1}^{-1} = \overline{1}$. Weiter gelten $\overline{5} \cdot \overline{5} = \overline{25} = \overline{1}$, also $\overline{5}^{-1} = \overline{5}$, und $\overline{7} \cdot \overline{7} = \overline{49} = \overline{1}$, also $\overline{7}^{-1} = \overline{7}$, sowie $\overline{11} \cdot \overline{11} = \overline{121} = \overline{1}$, also $\overline{11}^{-1} = \overline{11}$. Somit ist jedes Element von $(\mathbb{Z}/12)^*$ zu sich selbst invers.
B) Es gilt

$$\mathbb{M}_{36} = \{1,5,7,11,13,17,19,23,25,29,31,35\}$$

und somit

$$(\mathbb{Z}/36)^* = \left\{\overline{1},\overline{5},\overline{7},\overline{11},\overline{13},\overline{17},\overline{19},\overline{23},\overline{25},\overline{29},\overline{31},\overline{35}\right\}.$$

Es ist klar, dass $\overline{1}^{-1} = \overline{1}$. Zur Bestimmung der weiteren Inversen verwenden wir das Verfahren von 7.10 B). Wir bestimmen also durch Ausprobieren oder unter Verwendung des Euklidischen Algorithmus zu jedem $x \in \mathbb{M}_{36}$ Zahlen $y, z \in \mathbb{Z}$ mit $xy + 36z = 1$. Es gilt dann $\overline{x}^{-1} = \overline{y}$. Wir erhalten vorerst

$$5(-7) + 36 \cdot 1 = 1, \text{ also } \overline{5}^{-1} = \overline{-7} = \overline{29};$$

$$7(-5) + 36 \cdot 1 = 1, \text{ also } \overline{7}^{-1} = \overline{-5} = \overline{31};$$

$$11 \cdot 23 + 36(-7) = 1, \text{ also } \overline{11}^{-1} = \overline{23};$$

$$13 \cdot 25 + 36(-9) = 1, \text{ also } \overline{13}^{-1} = \overline{25};$$

$$17 \cdot 17 + 36(-8) = 1, \text{ also } \overline{17}^{-1} = \overline{17};$$

$$19 \cdot 19 + 36(-10) = 1, \text{ also } \overline{19}^{-1} = \overline{19}.$$

Weil für jedes $\overline{x} \in (\mathbb{Z}/m)^*$ die Gleichung $(\overline{x}^{-1})^{-1} = \overline{x}$ gilt, sind die übrigbleibenden Fälle in obiger Aufstellung schon vorhanden, abgesehen von $\overline{35}$. Weil Inverse eindeutig bestimmt sind, ist die einzig übrigbleibende Möglichkeit jedoch $\overline{35}^{-1} = \overline{35}$.
C) „(i)⇒(iv)“ : Wäre μ bijektiv, so existierte die Umkehrabbildung μ^{-1}, und für $b \in \mathbb{Z}/m$ gälte $a\mu^{-1}(b) = b$. Für $b = \overline{1}$ folgte insbesondere $a\mu^{-1}\left(\overline{1}\right) = \overline{1}$, und a wäre im Widerspruch zur Voraussetzung invertierbar.
„(iv)⇒(iii)“ : Dies ist klar nach Satz 3.24.
„(iii)⇒(ii)“ : Ist μ nicht injektiv, so gibt es $c, d \in \mathbb{Z}/m$ mit $c \neq d$ und $ac = ad$. Es folgen

$c - d \in (\mathbb{Z}/m) \setminus \{\overline{0}\}$ und $\overline{0} = ac - ad = a(c-d)$.
„(ii)⇒(i)“ : Sei $b \in (\mathbb{Z}/m)\setminus\{\overline{0}\}$ mit $ab = \overline{0}$. Wäre $a \in (\mathbb{Z}/m)^*$, so existierte $a^{-1} \in (\mathbb{Z}/m)^*$ mit $aa^{-1} = 1$, und es folgte der Widerspruch

$$\overline{0} = \overline{0}a^{-1} = (ab)a^{-1} = b\left(aa^{-1}\right) = b\overline{1} = b.$$

D) Wir verwenden folgende Charakterisierung der Gleichheit zweier Polynome, den sogenannten *Koeffizientenvergleich*: Sind

$$f(x) = \sum_{i=0}^{d} a_i x^i,\ g(x) = \sum_{j=0}^{e} b_j x^j \in \mathbb{R}[x]$$

mit $d, e \in \mathbb{N}_0$, $a_0, \ldots, a_d, b_0, \ldots, b_e \in \mathbb{R}$, $a_d \neq 0$ und $b_e \neq 0$, so gilt $f(x) = g(x)$ genau dann, wenn $d = e$ und $a_i = b_i$ für alle $i \in \{0, \ldots, d\}$. Weiter wollen wir die konstanten Polynome in $\mathbb{R}[x]$, d.h. die Polynome der Form $f(x) = a$ mit $a \in \mathbb{R}$, mit den reellen Zahlen identifizieren; damit können wir schreiben $\mathbb{R} \subseteq \mathbb{R}[x]$. Insbesondere ist das konstante Polynom $f(x) = 1$ gerade das Einselement im Ring $\mathbb{R}[x]$.
Wir behaupten, dass $(\mathbb{R}[x])^* = \mathbb{R}\setminus\{0\}$ und zeigen, dass jede dieser Mengen in der jeweils anderen enthalten ist.
„$\supseteq$“ : Sei $a \in \mathbb{R} \setminus \{0\}$. Dann gelten $a^{-1} = \frac{1}{a} \in \mathbb{R} \setminus \{0\}$ und $aa^{-1} = 1$. Werden a und a^{-1} als (konstante) Polynome aufgefasst, so gilt also $a \in (\mathbb{R}[x])^*$.
„$\subseteq$“ : Sei $f(x) = \sum_{i=0}^{d} a_i x^i \in (\mathbb{R}[x])^*$. Dann gibt es ein zu $f(x)$ inverses Polynom $g(x) = \sum_{j=0}^{e} b_j x^j$ mit $f(x)g(x) = 1$, das heisst mit

$$\sum_{k=0}^{d+e} \left(\sum_{l=0}^{k} a_l b_{k-l} \right) x^k = 1 = \sum_{k=0}^{0} 1x^0.$$

Wegen $d, e \in \mathbb{N}_0$ liefert der Koeffizientenvergleich $d = e = 0$. Somit gelten $f(x) = a_0x^0 = a_0 \in \mathbb{R}$ und $g(x) = b_0x^0 = b_0$, und wegen $a_0b_0 = 1$ folgt $a_0 \neq 0$.

Aufgaben 7.16 A) In den Verknüpfungstabellen für die Subtraktion und die Division ist jeweils das erste Argument aus der Vertikalen und das zweite Argument aus der Horizontalen auszuwählen.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$-$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

$:$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{1}$

B)

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	0	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Aufgaben 7.21 A) Nach 7.20 B) gilt $\sharp(\mathbb{Z}/m)^* = \varphi(m)$ und wir erhalten die folgende Tabelle.

m	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\sharp(\mathbb{Z}/m)^*$	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8

m	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
$\sharp(\mathbb{Z}/m)^*$	16	6	18	8	12	10	22	8	20	12	18	12	28	8	

B) In $(\mathbb{Z}/5)^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ gelten $\overline{1}^2 = \overline{1}, \overline{2}^2 = \overline{4}, \overline{3}^2 = \overline{9} = \overline{4}$ und $\overline{4}^2 = \overline{16} = \overline{1}$. In $(\mathbb{Z}/8)^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ gelten $\overline{1}^2 = \overline{1}, \overline{3}^2 = \overline{9} = \overline{1}, \overline{5}^2 = \overline{25} = \overline{1}$ und $\overline{7}^2 = \overline{49} = \overline{1}$. In $(\mathbb{Z}/5)^*$ sind also alle Quadrate gleich $\overline{1}$, während dies in $(\mathbb{Z}/8)^*$ nicht gilt.
C) a) Wegen $\varphi(3) = \varphi(4) = 2$ ist φ sicher nicht injektiv. Sei $m \in \mathbb{N} \setminus \{1, 2\}$. Falls $\mathbb{P}(m) = \{2\}$, so gilt $\varphi(m) = 2^k$ für ein $k \in \mathbb{N}$; $\varphi(m)$ ist also gerade. Gibt es hingegen ein $p \in \mathbb{P}(m)$ mit $p \neq 2$, so besitzt $\varphi(m)$ einen geraden Faktor $p - 1$, ist also auch gerade. Berücksichtigt man, dass $\varphi(1) = \varphi(2) = 1$, so sieht man, dass φ Werte in $\{n \in \mathbb{N} | n = 1 \text{ oder } n \text{ gerade}\}$ annimmt und somit nicht surjektiv ist.
b) Falls $m = 1$ oder $n = 1$, so ist die Behauptung klar. Seien also $m, n \in \mathbb{N} \setminus \{1\}$ mit $\mathrm{ggT}(m, n) = 1$. Nach 7.20 B), 7.18 und 3.24 D) gilt

$$\varphi(mn) = \sharp(\mathbb{Z}/mn)^* = \sharp(\mathbb{Z}/m)^* \times \sharp(\mathbb{Z}/n)^* = \varphi(m)\varphi(n).$$

D) i) Sei $m \in \mathbb{N} \setminus \{1\}$ mit $\frac{\varphi(m)}{m} = \frac{4}{15}$, und sei $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die Primfaktorzerlegung von m. Dann gilt

$$15(p_1 - 1) \cdots (p_r - 1) = 4p_1 \cdots p_r,$$

und wegen der Eindeutigkeit der Primfaktorzerlegung folgt, dass m einen Primfaktor 5 besitzt. Ohne Einschränkung können wir annehmen, dass $p_1 = 5$ gilt. Somit erhalten wir

$$15 \cdot 4(p_2 - 1) \cdots (p_r - 1) = 4 \cdot 5p_2 \cdots p_r.$$

Wie oben folgt $p_2 = 3$, also

$$15 \cdot 4 \cdot 2(p_3 - 1) \cdots (p_3 - 1) = 4 \cdot 5 \cdot 3p_3 \cdots p_r.$$

Dieselbe Überlegung liefert $p_3 = 2$ und somit

$$15 \cdot 4 \cdot 2 \cdot 1(p_4 - 1) \cdots (p_r - 1) = 4 \cdot 5 \cdot 3 \cdot 2p_4 \cdots p_r.$$

Wäre $r > 3$, so folgte die Gleichung

$$(p_4 - 1) \cdots (p_r - 1) = p_4 \cdots p_r.$$

Da die Primfaktoren $p_1, \ldots p_r$ verschieden sind, stünde auf der rechten Seite eine ungerade und auf der linken Seite eine gerade Zahl, was nicht möglich ist. Das bedeutet, dass $r = 3$ gilt und somit, dass $\mathbb{P}(m) = \{2, 3, 5\}$. Folglich kann m nach einer Umnumerierung seiner Primfaktoren nur die Form $n = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3}$ haben. Sofort sieht man, dass für jedes m dieser Form gilt $\frac{\varphi(m)}{m} = \frac{4}{15}$.
ii) Sei $n \in \mathbb{N} \setminus \{1\}$ mit $\frac{\varphi(n)}{n} = \frac{8}{35}$, und sei $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die Primfaktorzerlegung von n. Dann gilt

$$35 \cdot (p_1 - 1) \cdots (p_r - 1) = 8p_1 \cdots p_r,$$

und die gleichen Überlegungen wie in i) liefern sukzessive $p_1 = 5, p_2 = 7, p_3 = 3$ und $p_4 = 2$. Übrig bleibt wieder eine Gleichung zwischen einer geraden und einer ungeraden Zahl, und es folgt nach einer Umnumerierung $n = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \cdot 7^{\alpha_4}$.
E) Seien $m \in \mathbb{U}$ und $m = p_1^{\alpha_1} \cdots p_4^{\alpha_4}$ die Primfaktorzerlegung von m. Dann gilt

$$\frac{\varphi(m)}{m} = \frac{(p_1 - 1)(p_2 - 1)(p_3 - 1)(p_4 - 1)}{p_1 p_2 p_3 p_4}$$

$$(*) \qquad = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)\left(1 - \frac{1}{p_4}\right)$$

$$\geq \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = \frac{48}{210} = \frac{8}{35},$$

also die Behauptung a). Ist $n \in \mathbb{N}$ und gilt $p_1, p_2, p_3, p_4 > n$, so folgt aus $(*)$ direkt Behauptung b).
F) Wegen $\mathbb{P} \subseteq \mathbb{N}$ und Satz 5.22 gibt es eine strikt wachsende Folge $(p_k)_{k \in \mathbb{N}}$ in $\mathbb{P}$. Für $n \in \mathbb{N}$ sei $m_n := p_{4n} \cdot p_{4n+1} \cdot p_{4n+2} \cdot p_{4n+3}$. Dann ist $(m_n)_{n \in \mathbb{N}}$ eine Folge in $\mathbb{U}$, und für $n \in \mathbb{N}$ gilt

$$\frac{\varphi(m_n)}{m_n} = \left(1 - \frac{1}{p_{4n}}\right)\left(1 - \frac{1}{p_{4n+1}}\right)\left(1 - \frac{1}{p_{4n+2}}\right)\left(1 - \frac{1}{p_{4n+3}}\right).$$

Es folgt $\lim_{n\to\infty}(\frac{\varphi(m)}{m}) = \lim(1 - \frac{1}{p_{4n}}) \lim(1 - \frac{1}{p_{4n+1}} \lim(1 - \frac{1}{p_{4n+2}}) \lim(1 - \frac{1}{p_{4n+3}}) = (1 - \lim(\frac{1}{p_{4n}}))(1 - \lim(\frac{1}{p_{4n+1}}))(1 - \lim(\frac{1}{p_{4n+2}}))(1 - \lim(\frac{1}{p_{4n+3}})) = 1$.
G) Wir behalten die Bezeichnungen von F) bei. Ohne Einschränkung können wir die

Folge $(p_k)_{k\in\mathbb{N}}$ in $\mathbb{P}\setminus\{p\}$ wählen. Für $n\in\mathbb{N}$ definieren wir $m_n := p_{3n}\cdot p_{3n+1}\cdot p_{3n+2}\cdot p \in \mathbb{U}$. Wir erhalten damit $\lim_{n\to\infty}(\frac{\varphi(m)}{m}) = \lim(1-\frac{1}{p_{3n}})\lim(1-\frac{1}{p_{3n+1}})\lim(1-\frac{1}{p_{3n+2}})\lim(1-\frac{1}{p}) = (1-\lim(\frac{1}{p_{3n}}))(1-\lim(\frac{1}{p_{3n+1}}))(1-\lim(\frac{1}{p_{3n+2}}))(1-\lim(\frac{1}{p})) = (1-\frac{1}{p})$.

Aufgaben 7.24 A) Die Elemente a von $(\mathbb{Z}/m)^*$ können mit 7.9 oder für $m\neq 4$ mit 7.12 bestimmt werden. Aus den Definitionen ergibt sich dann die folgende Tabelle.

m	a	$\langle a\rangle$	$\mathrm{ord}(a)$
2	$\bar{1}$	$\{\bar{1}\}$	1
3	$\bar{1}$	$\{\bar{1}\}$	1
	$\bar{2}$	$\{\bar{1},\bar{2}\}$	2
4	$\bar{1}$	$\{\bar{1}\}$	1
	$\bar{3}$	$\{\bar{1},\bar{3}\}$	2
5	$\bar{1}$	$\{\bar{1}\}$	1
	$\bar{2}$	$\{\bar{1},\bar{2},\bar{4},\bar{3}\}$	4
	$\bar{3}$	$\{\bar{1},\bar{3},\bar{4},\bar{2}\}$	4
	$\bar{4}$	$\{\bar{1},\bar{4}\}$	2

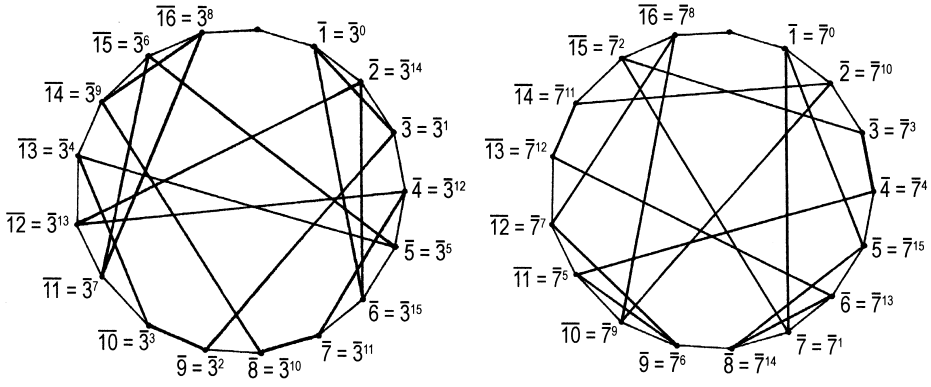
B) Der Fall $m=5$ lässt sich aus Aufgabe A) ablesen. Nach 7.9 gilt $(\mathbb{Z}/8)^* = \{\bar{1},\bar{3},\bar{5},\bar{7}\}$, und man berechnet $\bar{3}^2 = \bar{5}^2 = \bar{7}^2 = \bar{1}$. Folglich haben genau die Restklassen $\bar{3},\bar{5},\bar{7}$ die Ordnung 2.

Aufgaben 7.30 A) Wir potenzieren die Elemente von $(\mathbb{Z}/7)^*$ solange, bis wir $\overline{1}$ erhalten.

a	a^2	a^3	a^4	a^5	a^6	$\mathrm{ord}(a)$
$\overline{1}$						1
$\overline{2}$	$\overline{4}$	$\overline{1}$				3
$\overline{3}$	$\overline{2}$	$\overline{6}$	$\overline{4}$	$\overline{5}$	$\overline{1}$	6
$\overline{4}$	$\overline{2}$	$\overline{1}$				3
$\overline{5}$	$\overline{4}$	$\overline{6}$	$\overline{2}$	$\overline{3}$	$\overline{1}$	6
$\overline{6}$	$\overline{1}$					2

B) Siehe Zeichnung.
C) Sei $\overline{\bullet} : \mathbb{Z}\to\mathbb{Z}/p$ die Restklassenabbildung. Weil p kein Teiler von n ist, gilt $\mathrm{ggT}(p,n)=1$. Nach 7.10 folgt daraus $\overline{n}\in(\mathbb{Z}/p)^*$, und nach 7.29 folgt $\overline{n}^{p-1}=\overline{1}$, was äquivalent ist zur Behauptung.
D) Weil p kein Teiler von n ist, folgt aus dem Kleinen Satz von Fermat, dass es ein $b\in\mathbb{Z}$ mit $n^{p-1}=bp+1$ gibt. Weil p auch kein Teiler von $n-1$ ist gilt $n\neq 1$, und mit 3.3 B) erhalten wir

$$n^{p-2}+\cdots+1 = \frac{n^{p-1}-1}{n-1} = \frac{bp+1-1}{n-1} = \frac{b}{n-1}\cdot p.$$



Aufgabe 7.30 B)

Die Behauptung folgt, wenn wir zeigen, dass $\frac{b}{n-1} \in \mathbb{Z}$. Dazu nehmen wir $\frac{b}{n-1} \notin \mathbb{Z}$ an. Wegen $\frac{b}{n-1}p \in \mathbb{Z}$ wäre dann $\mathrm{ggT}(n-1,p) \neq 1$, und es folgte der Widerspruch $p|n-1$.
E) Wir potenzieren $\overline{3}$ fortlaufend und erhalten

$$\overline{3}^0 = \overline{1},\ \overline{3}^1 = \overline{3},\ \overline{3}^2 = \overline{9},\ \overline{3}^3 = \overline{27} = \overline{5},\ \overline{3}^4 = \overline{81} = \overline{4},\ \overline{3}^5 = \overline{243} = \overline{1}.$$

Die höheren Potenzen von $\overline{3}$ liefern keine weiteren Werte. Somit existiert $n(a)$ nur für $a \in \{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\}$, und es gelten

$$n(\overline{1}) = 0,\ n(\overline{3}) = 1,\ n(\overline{4}) = 4,\ n(\overline{5}) = 3,\ n(\overline{9}) = 2.$$

Teil D

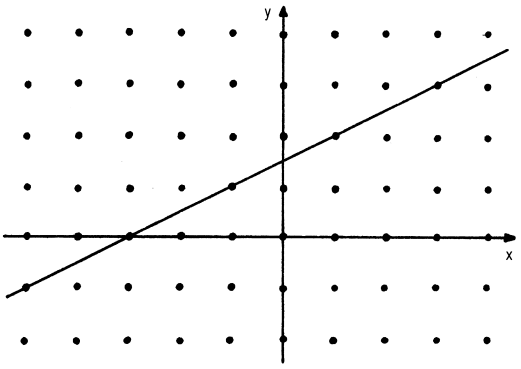
Aufgaben 8.4 A) Siehe Zeichnung. Wegen $\mathrm{ggT}(-1,2) = 1$ und $1|3$ existieren nach 8.2 Lösungen. Wir wenden das Verfahren aus 8.3 an, um die Lösungsmenge $\mathbb{L}$ zu bestimmen. Wir suchen $u, v \in \mathbb{Z}$ mit $-u + 2v = 1$. Ausprobieren liefert $u = 1$ und $v = 1$, und es folgt $\mathbb{L} = \{(3 + 2t, 3 + t) | t \in \mathbb{Z}\}$.
B) Eine lineare diophantische Gleichung mit mindestens zwei Lösungen in

$$\{(x,y) | 0 \leq x \leq 2, 0 \leq y \leq 1\}$$

entspricht geometrisch einer Geraden, welche durch mindestens zwei der Gitterpunkte

$$(0,0), (0,1), (1,0), (1,1), (2,0), (2,1)$$

geht. Wie man der Skizze entnimmt, gibt es elf solcher Geraden. Da die zugehörigen Gleichungen jeweils mit einer von 0 verschiedenen ganzen Zahl multipliziert werden können ohne dass sich dabei die Lösungsmenge ändert, erhalten wir die folgenden Typen

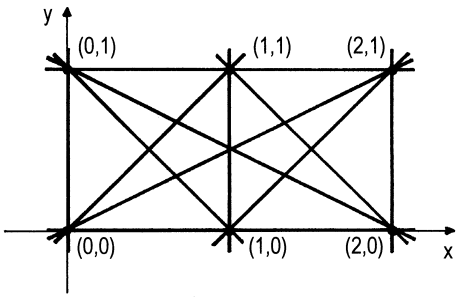


Aufgabe 8.4 A)

von Gleichungen, wobei $\lambda \in \mathbb{Z} \setminus \{0\}$.

I :	$\lambda x = 0$	V :	$\lambda y = \lambda$	IX :	$\lambda x - \lambda y = 0$
II :	$\lambda x = \lambda$	VI :	$\lambda x + 2\lambda y = 2\lambda$	X :	$\lambda x + \lambda y = 2\lambda$
III :	$\lambda x = 2\lambda$	VII :	$\lambda x - 2\lambda y = 0$	XI :	$\lambda x - \lambda y = \lambda$
IV :	$\lambda y = 0$	VIII :	$\lambda x + \lambda y = 0$		

Einen zwölften Typ Gleichung, der die Bedingungen erfüllt, liefert die Wahl $a = b = c = 0$.



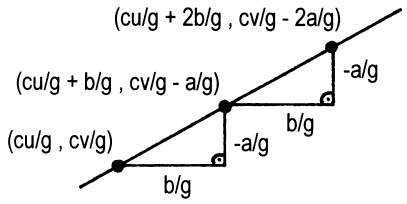
Aufgabe 8.4 B)

C) Damit überhaupt Lösungen existieren, muss $\mathrm{ggT}(a, b) = 1$ gelten. Ist (x, y) eine Lösung, so ist auch $(x + tb, y - ta)$ mit $t \in \mathbb{Z}$ eine Lösung. Aus der Skizze ist ersichtlich, das zwei verschiedene solche Lösungen minimalen Abstand haben, wenn $t = 1$ gilt. Ihr Abstand beträgt dann

$$\sqrt{(x - (x + b))^2 + (y - (y + a))^2} = \sqrt{a^2 + b^2}.$$

Es soll somit $\sqrt{a^2 + b^2} < 4$, also $a^2 + b^2 < 16$ gelten. Ausprobieren liefert für (a, b) die Möglichkeiten

$$(\pm 1, \pm 1),\ (\pm 1, \pm 2),\ (\pm 1, \pm 3),\ (\pm 2, \pm 1),\ (\pm 2, \pm 3),\ (\pm 3, \pm 1),\ (\pm 3, \pm 2).$$



Aufgabe 8.4 C)

D) Seien $g := \mathrm{ggT}(a,b)$ und $u, v \in \mathbb{Z}$ mit $au + bv = g$. Zwei „benachbarte“ Lösungen haben die Form $(\frac{cu}{g} + \frac{tb}{g}, \frac{cv}{g} - \frac{ta}{g})$ und $(\frac{cu}{g} + \frac{(t+1)b}{g}, \frac{cv}{g} - \frac{(t+1)a}{g})$ mit $t \in \mathbb{Z}$ (s. Skizze zu C)). Ihr Abstand beträgt

$$\sqrt{\left(\frac{cu}{g} + \frac{tb}{g} - \left(\frac{cu}{g} + \frac{(t+1)b}{g}\right)\right)^2 + \left(\frac{cv}{g} - \frac{ta}{g} - \left(\frac{cv}{g} - \frac{(t+1)a}{g}\right)\right)^2} =$$

$$\sqrt{\frac{a^2+b^2}{g^2}} = \frac{1}{g}\sqrt{a^2+b^2}.$$

E) a) Sei G die durch $ax + by = c$ definierte Gerade. Für einen beliebigen Punkt (x, y) auf G gilt $y = \frac{c}{b} - \frac{a}{b}x$, und somit beträgt sein Abstand vom Nullpunkt

$$f(x) := \sqrt{x^2+y^2} = \sqrt{\frac{a^2+b^2}{b^2}x^2 - \frac{2ac}{b^2}x + \frac{c^2}{b^2}}.$$

Wir wollen einen Punkt $(x_0, y_0) \in G$ so bestimmen, dass sein Abstand von $(0,0)$ minimal wird. Dazu genügt es, wenn das Quadrat seinen Abstandes minimal wird, weswegen wir im obigen Ausdruck die Wurzel weglassen können. Bekanntlich ist x_0 die Nullstelle der Ableitung von f. Es gilt also $x_0 = \frac{ac}{a^2+b^2}$, und es folgt $y_0 = \frac{bc}{a^2+b^2}$. Einsetzen und umformen ergibt

$$f(x_0) = \sqrt{x^2+y^2} = \sqrt{\frac{c^2\left(a^2+b^2\right)}{\left(a^2+b^2\right)^2}} = \left|\frac{c\sqrt{a^2+b^2}}{a^2+b^2}\right| = |\delta|.$$

b) Sei weiterhin (x_0, y_0) ein Punkt auf G mit minimalem Abstand $|\delta|$ vom Nullpunkt. sei $g := \mathrm{ggT}(a,b)$. Es bezeichne $d := \frac{1}{g}\sqrt{a^2+b^2}$ den Abstand zwischen zwei „benachbarten“ Lösungen (vgl. D)). Läge keine Lösung in einem Abstand von höchstens $\frac{d}{2}$ von (x_0, y_0), so gäbe es zwei „benachbarte“ Lösungen mit einem Abstand grösser als d. Lägen drei Lösungen in einem Abstand von höchstens $\frac{d}{2}$ von (x_0, y_0), so wären zwei davon „benachbart“, hätten aber einen echt kleineren Abstand voneinander als d. Somit liegen mindestens eine und höchstens zwei Lösungen in einem Abstand von $\frac{d}{2}$ von (x_0, y_0). Da

Abstände zwischen einer Geraden und einem Punkt jeweils rechtwinklig zur Geraden gemessen werden, liefert der Satz des Pythagoras die Behauptung.
F) Durch Ausprobieren findet man die Faktorisierung

$$2x^2 - 3y^2 - 5xy + x + 11y - 6 = (2x + y - 3)(x - 3y + 2).$$

Eine Lösung der gegebenen Gleichung ist ein Paar $(x, y) \in \mathbb{Z}^2$, welches eingesetzt in obigen Ausdruck 0 ergibt. Dies ist genau dann der Fall, wenn $2x + y - 3 = 0$ oder $x - 3y + 2 = 0$. Somit sind diese beiden linearen diophantischen Gleichungen zu lösen. Für die erste Gleichung finden wir mit dem Verfahren aus 8.3 die Lösungsmenge

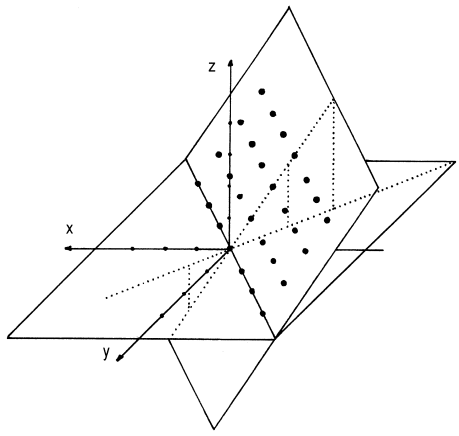
$$\mathbb{L}_1 = \{(3 + t, -3 - 2t) | t \in \mathbb{Z}\}.$$

Analog finden wir für die zweite Gleichung

$$\mathbb{L}_2 = \{(-8 - 3s, -2 - s) | s \in \mathbb{Z}\},$$

und es gilt für die Lösungsmenge $\mathbb{L}$ der gegebenen Gleichung $\mathbb{L} = \mathbb{L}_1 \cup \mathbb{L}_2$.

Aufgaben 8.6 A) Wir verwenden das Verfahren aus 8.5. Es gilt $g := \text{ggT}(1, 1) = 1$. Sei $f(z) := z$. Für jedes $z \in \mathbb{Z}$ gilt $g | f(z)$, weswegen für jede Wahl von z eine Lösung existiert. Mit $u = 1$ und $v = 0$ gilt $u+v = 1$ und wir erhalten $\mathbb{L} = \{(z+t, -t, z) | t, z \in \mathbb{Z}\}$.



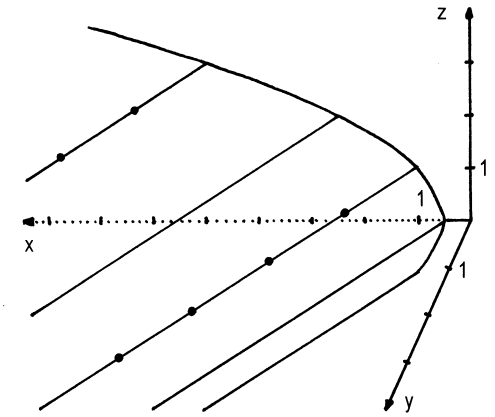
Aufgabe 8.6 A)

B) Wir verwenden das Verfahren aus 8.5. Es gilt $g := \text{ggT}(-1, 1) = 1$. Sei $f(z) := z^2$. Für jedes $z \in \mathbb{Z}$ gilt $g | f(z)$, weswegen für jede Wahl von z eine Lösung existiert. Mit $u = 0$ und $v = 1$ gilt $-u + v = 1$ und wir erhalten $\mathbb{L} = \{(t, z^2 + t, z) | t, z \in \mathbb{Z}\}$. Geometrisch liegt genau die Situation aus Abbildung 8.2 vor.

C) Wir verwenden das Verfahren von 8.5 und bestimmen zuerst $(u, v) \in \mathbb{Z}^2$ mit $2u - 6v = \text{ggT}(2, -6) = 2$. Das Paar $(u, v) = (4, 1)$ erfüllt dies, und wir erhalten damit die Lösungsmenge

$$\left\{ \left(\frac{z^2+1}{2} \cdot 4 + t \cdot \frac{-6}{2}, \frac{z^2+1}{2} \cdot 1 - t \cdot \frac{2}{2}, z \right) \middle| \, t, z \in \mathbb{Z} \wedge 2 | z^2 + 1 \right\} =$$

$$\left\{ \left(2z^2 + 2 - 3t, \frac{z^2+1}{2} - t, z \right) \middle| \, t, z \in \mathbb{Z} \wedge z \text{ ungerade} \right\}.$$



Aufgabe 8.6 C)

D) Damit die Lösungsmenge leer ist, darf $g := \text{ggT}(5, -b) = \text{ggT}(5, b)$ für kein $z \in \mathbb{Z}$ ein Teiler von $f(z) := 10z^4 - 11$ sein. Es gilt sicher $g \in \{1, 5\}$. Für $g = 1$ gilt $g | f(z)$ für jedes $z \in \mathbb{Z}$. Also bleibt nur noch $g = 5$ übrig. Wegen $5 | 10z^4$ ist 5 für kein $z \in \mathbb{Z}$ ein Teiler von $f(z)$. Die Bedingung $g = 5$ erreichen wir mit $b \in \{0, 5\}$.
Für die übrigen Fälle, das heisst für $b \in \{1, 2, 3, 4\}$, kann das Verfahren aus 8.5 angewendet werden und es ergeben sich die Lösungsmengen

$$\mathbb{L}_{b=1} = \{(10z^4 - t - 11, 40z^4 - 5t - 44, z) | t, z \in \mathbb{Z}\};$$

$$\mathbb{L}_{b=2} = \{(10z^4 - 2t - 11, 20z^4 - 5t - 22, z) | t, z \in \mathbb{Z}\};$$

$$\mathbb{L}_{b=3} = \{(-10z^4 + 3t + 11, -20z^4 - 5t + 22, z) | t, z \in \mathbb{Z}\};$$

$$\mathbb{L}_{b=4} = \{(10z^4 + 4t - 11, 10z^4 - 5t - 11, z) | t, z \in \mathbb{Z}\}.$$

Aufgaben 8.9 A) Für jedes $n \in \mathbb{N}$ mit $n \geq 3$ sind die Schnittpunkte mit den Koordinatenachsen die einzigen rationalen Punkte auf der n-ten Fermatkurve.
B) Wir nehmen an, es wäre $b := \sqrt[n]{1 - a^n} \in \mathbb{Q}$. Dann gälte $b \neq 0$. Es folgte $a^n + b^n = a^n + \left(\sqrt[n]{1 - a^n}\right)^n = a^n + 1 - a^n = 1$, also $(a, b) \in \mathbb{Q} \cap \mathbb{M}_n$ mit $ab \neq 0$ im Widerspruch zu

A).
C) Für $a = \frac{3}{5}$ erhält man $\sqrt[2]{1-a^2} = \sqrt[2]{1-\frac{3^2}{5^2}} = \sqrt[2]{\frac{16}{25}} = \frac{4}{5} \in \mathbb{Q}$.
D) Ist $(a_n, a_n) \in \mathbb{M}_n$, so gilt $1 = a_n^n + a_n^n = 2a_n^n$, also $a_n = \sqrt[n]{\frac{1}{2}}$. Wird n beliebig gross, strebt $\frac{1}{n}$ gegen 0. Somit strebt $a_n = \left(\frac{1}{2}\right)^{\frac{1}{n}}$ gegen $\left(\frac{1}{2}\right)^0 = 1$, es gilt also $\lim_{n\to\infty}(a_n) = 1$.
E) Ist $(u, v_n) \in \mathbb{M}_n$, so gilt $v_n^n = 1 - u^n$, und es folgt $v_n = \sqrt[n]{1-u^n}$. Wird n beliebig gross, so strebt u^n wegen $|u| < 1$ gegen 0. Somit strebt $1 - u^n$ gegen 1 und zudem $\frac{1}{n}$ gegen 0, also $\lim_{n\to\infty}(v_n) = 1$.
F) Ist $(u, w_k) \in \mathbb{M}_{2k+1}$, so gilt $w_k^{2k+1} = 1-u^{2k+1}$. Wird k beliebig gross, so können wir wegen $|u| > 1$ den Summanden 1 vernachlässigen und erhalten $\lim_{k\to\infty}\left(\left(-u^{2k+1}\right)^{\frac{1}{2k+1}}\right) = \lim_{k\to\infty}(-u) = -u$.

Aufgaben 8.11 A) Die Werte von d sind klein, weswegen wir das Verfahren von 8.10 D) anwenden. Wir berechnen also die Werte von $dy^2 + 1$ für kleine $y \in \mathbb{N}$ und prüfen, ob $\sqrt{dy^2+1} \in \mathbb{N}$. Ist dies der Fall, so ist $(\sqrt{dy^2+1}, y)$ die kleinste nichttriviale Lösung der gegebenen Gleichung.
i) Es gelten $2 \cdot 1^2 + 1 = 3$, $2 \cdot 2^2 + 1 = 9$ und $\sqrt{9} = 3 \in \mathbb{N}$. Minimale Lösung: $(3, 2)$.
ii) Es gelten $3 \cdot 1^2 + 1 = 4$ und $\sqrt{4} = 2 \in \mathbb{N}$. Minimale Lösung: $(2, 1)$.
iii) Es gelten $7 \cdot 1^2 + 1 = 8$, $7 \cdot 2^2 + 1 = 29$, $7 \cdot 3^2 + 1 = 64$ und $\sqrt{64} = 8 \in \mathbb{N}$. Minimale Lösung: $(8, 3)$.
iv) Es gelten $6 \cdot 1^2 + 1 = 7$, $6 \cdot 2^2 + 1 = 25$ und $\sqrt{25} = 5 \in \mathbb{N}$. Minimale Lösung: $(5, 2)$.
v) Es gelten $8 \cdot 1^2 + 1 = 9$ und $\sqrt{9} = 3 \in \mathbb{N}$. Minimale Lösung: $(3, 1)$.
vi) Es gelten $10 \cdot 1^2 + 1 = 11$, $10 \cdot 2^2 + 1 = 41$, $10 \cdot 3^2 + 1 = 91$, $10 \cdot 4^2 + 1 = 161$, $10 \cdot 5^2 + 1 = 251$, $10 \cdot 6^2 + 1 = 361$ und $\sqrt{361} = 19 \in \mathbb{N}$. Minimale Lösung: $(19, 6)$.
D) $(d+1)^2 - d\left(\sqrt{d+2}\right)^2 = d^2 + 1 + 2d - d(d+2) = d^2 + 1 + 2d - d^2 - 2d = 1$.
I) i) Wegen $\sqrt{14+2} = 4 \in \mathbb{N}$ ist $(x_1, y_1) := (15, 4)$ nach Aufgabe D) eine Lösung von $x^2 - 14y^2 = 1$. Weitere Lösungen erhalten wir mit dem Verfahren von Aufgabe C) wie folgt:

$$x_2 := x_1^2 + 14y_1^2 = 449,\ y_2 := 2x_1y_1 = 120;$$

$$x_3 := x_1x_2 + 14y_1y_2 = 13455,\ y_3 := x_1y_2 + x_2y_1 = 3596.$$

Dies gibt die Lösungen $(449, 120)$ und $(13455, 3596)$.
ii) Wegen $\sqrt{34+2} = 6 \in \mathbb{N}$ ist $(x_1, y_1) := (35, 6)$ nach Aufgabe D) eine Lösung von $x^2 - 34y^2 = 1$. Weitere Lösungen erhalten wir mit dem Verfahren von Aufgabe C) wie folgt:

$$x_2 := x_1^2 + 34y_1^2 = 2449,\ y_2 := 2x_1y_1 = 420;$$

$$x_3 := x_1x_2 + 34y_1y_2 = 171395,\ y_3 := x_1y_2 + x_2y_1 = 29394.$$

Dies gibt die Lösungen $(2449, 420)$ und $(171395, 29394)$.

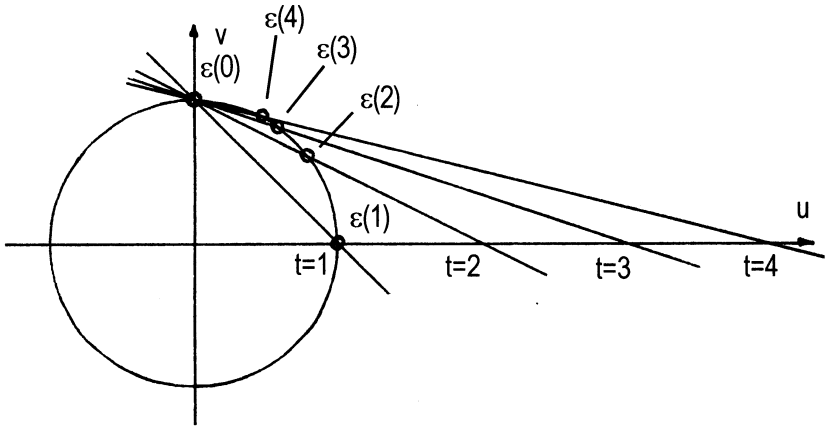
Aufgaben 9.2 A) Eine geschlossene Schnur mit 12, 30 oder 40 Knoten in regelmässigen Abständen erlaubt die Messung eines rechten Winkels (vgl. 1.6 A), B)). Beträgt die Anzahl der Knoten 60, so erhält man zwei wesentlich verschiedene Winkelmasse (vgl. 1.6 C)). Bei der Berechnung des Preises des Modelles Duplex werden offenbar beide möglichen Masse berechnet, was einer Gesamtzahl von 120 Knoten entspricht und bei einer Reduktion um 25% einen Preis von 90 ¶ ergibt.
B) Sei $(x, y, z) \in \mathbb{N}^3$ ein pythagoräisches Tripel mit $x \in \mathbb{P}$. Dann gilt $x^2 = z^2 - y^2 = (z + y)(z - y)$, und es folgt $z + y, z - y \in \mathbb{T}(x^2) = \{1, x, x^2\}$, da x eine Primzahl ist. Gälte $z + y = 1$, so folgte $z \notin \mathbb{N}$ oder $y \notin \mathbb{N}$. Gälte $z + y = x$ und somit $z - y = x$, so folgte $z + y = z - y$, also $y = 0 \notin \mathbb{N}$. Somit müssen $z + y = x^2$ und $z - y = 1$ gelten, woraus man sofort die Behauptung erhält.
C) Sei $(x, y, z) \in \mathbb{N}^3$ ein pythagoräisches Tripel mit $x \leq y$. Wir nehmen an, es gälte $x = y$. Dann folgte $z^2 = x^2 + y^2 = 2x^2$. Daraus erhielten wir durch Wurzelbildung $\sqrt{2}x = \sqrt{2x^2} = \sqrt{z^2} = z \in \mathbb{N}$, also den Widerspruch $\sqrt{2} = \frac{z}{x} \in \mathbb{Q}$. Also gilt $x < y$.
Wir nehmen an, es gälte $y \in \mathbb{P}$. Wenden wir 9.2 B) mit vertauschten Rollen von x und y an, so folgte $x = \frac{y^2-1}{2} < y$, also $y^2 - 2y + 1 = (y - 1)^2 < 2$. Dies lieferte aber den Widerspruch $y = 1$.

Aufgaben 9.4 D) Die explizite Formel für die Abbildung ε aus 9.3 B)a) liefert

$$\varepsilon(0) = (0, -1),\ \varepsilon(1) = (1, 0),\ \varepsilon(2) = \left(\frac{4}{5}, \frac{3}{5}\right),\ \varepsilon(3) = \left(\frac{3}{5}, \frac{4}{5}\right),$$

$$\varepsilon(4) = \left(\frac{8}{17}, \frac{15}{17}\right),\ \varepsilon(5) = \left(\frac{5}{13}, \frac{12}{13}\right).$$

Sicher gilt



Aufgabe 9.4 D)

$$\lim_{n\to\infty}(\varepsilon(n)) = \lim_{n\to\infty}\left(\frac{2n}{n^2+1}, \frac{n^2-1}{n^2+1}\right) = \left(\lim_{n\to\infty}\left(\frac{2n}{n^2+1}\right), \lim_{n\to\infty}\left(\frac{n^2-1}{n^2+1}\right)\right).$$

Die Summanden $+1$ und -1 können für genügend grosse n vernachlässigt werden. Durch Kürzen erhalten wir somit

$$\lim_{n\to\infty}(\varepsilon(n)) = \left(\lim_{n\to\infty}\left(\frac{2}{n}\right), \lim_{n\to\infty}(1)\right) = (0,1) = S,$$

was sich auch aufgrund der Skizze vermuten lässt (vgl. die geometrische Konstruktion der Abbildung ε in 9.3 A)).
E) Sei $n \in \mathbb{Z}$. Wegen

$$(2n)^2 + \left(n^2-1\right)^2 = 4n^2 + n^4 + 1 - 2n^2 = n^4 + 2n^2 + 1 = \left(n^2+1\right)^2$$

gilt für $(x,y,z) := (2n, n^2-1, n^2+1)$ die Gleichung $x^2+y^2=z^2$. Gilt zusätzlich $n \geq 2$, so folgt $(x,y,z) \in \mathbb{N}^3$, und (x,y,z) ist ein pythagoräisches Tripel.

Aufgaben 9.7 D) Wir betrachten hier nur das Produkt der ersten vier Primzahlen. Ein analoges Vorgehen löst aber auch die Aufgabe für acht Primfaktoren.
Sei also $u = 2\cdot 3\cdot 5\cdot 7 = 210$. Nach 9.7 A) müssen wir teilerfremde $m, k \in \mathbb{Z}$ mit $m < k < 2m$ bestimmen so, dass k ungerade ist und dass $u = 2mk$. Dies bedeutet aber, dass $2mk = 210$, also dass $mk = 105$. Es folgt aus der obigen Ungleichungskette durch Multiplikation mit m, dass $m^2 < 105 < 2m^2$. Wurzelziehen erlaubt nun die Abschätzungen $m \leq 10 < \sqrt{2}m$. Weiter muss $m \in \{3,\ 3\cdot 5,\ 3\cdot 5\cdot 7,\ 5,\ 5\cdot 7,\ 7\}$ gelten. Wegen $m \leq 10$ erhalten wir damit $m \in \{3,5,7\}$. Aber in diesen drei Fällen gilt $\sqrt{2}m < 10$. Also gibt es kein primitives und somit überhaupt kein pythagoräisches Tripel mit Umfang 210.
E) i) Sei $n \in \mathbb{N}_{\geq 2}$. Dann gilt nach Definition des Umfanges eines pythagoräischen Tripels $x_n + y_n + z_n = 2^n\left(2^{n-1}+1\right)$. Weil (x_n, y_n, z_n) primitiv ist, gibt es nach dem Satz von Diophantos zwei teilerfremde Zahlen $m, k \in \mathbb{N}$ mit $k < m$, wovon eine gerade und die andere ungerade ist so, dass

$$(x_n, y_n, z_n) = \left(2mk, m^2-k^2, m^2+k^2\right).$$

Es folgt

$$2^n\left(2^{n-1}+1\right) = 2mk + m^2 - k^2 + m^2 + k^2 = 2m(m+k),$$

das heisst

$$2^{n-1}\left(2^n+1\right) = m(m+k).$$

Weil $m+k$ ungerade ist, folgt $2^{n-1}|m$, also $m = 2^{n-1}l$ für ein $l \in \mathbb{N}$. Wir erhalten

$$2^{n-1}+1 = l(m+k) = l\left(2^{n-1}l + k\right),$$

was wegen $l, k \in \mathbb{N}$ nur geht, wenn $l = k = 1$. Schliesslich erhalten wir

$$(x_n, y_n, z_n) = \left(2^n, 2^{2n-2} - 1, 2^{2n-2} + 1\right).$$

ii) Es gilt $\frac{y_n}{x_n} = \frac{2^{2n-2}-1}{2^n}$. Für genügend grosse n kann der Summand -1 vernachlässigt werden, und Kürzen liefert

$$\lim_{n\to\infty}\left(\frac{y_n}{x_n}\right) = \lim_{n\to\infty}\left(2^{n-2}\right) = \infty.$$

Analog erhält man

$$\lim_{n\to\infty}\left(\frac{z_n}{x_n}\right) = \infty.$$

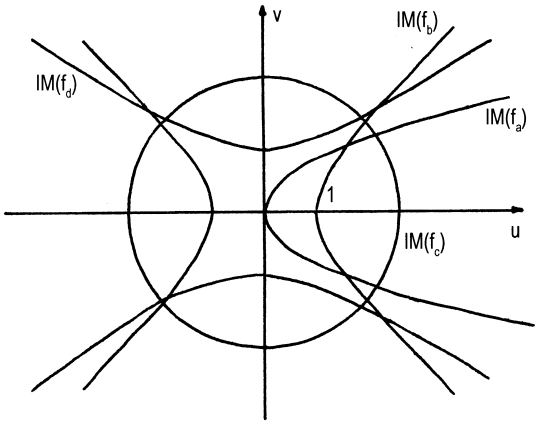
Es gilt $\frac{z_n}{y_n} = \frac{2^{2n-2}+1}{2^{2n-2}-1}$. Für genügend grosse n können die Summanden $+1$ und -1 vernachlässigt werden, und Kürzen liefert

$$\lim_{n\to\infty}\left(\frac{z_n}{y_n}\right) = \lim_{n\to\infty}(1) = 1.$$

Aufgaben 9.9 A) Mit Hilfe des Satzes von Diophantos bestimmt man alle primitiven pythagoräischen Tripel, deren Umfang höchstens 60 beträgt. Es sind dies $(4, 3, 5)$, $(8, 15, 17)$, $(12, 5, 13)$ und $(24, 7, 25)$. Ist (x, y, z) ein pythagoräisches Tripel, so ist $\left(\frac{x}{z}, \frac{y}{z}\right)$ ein rationaler Punkt auf dem Einheitskreis, und es gilt $(x, y, z) = \left(z\frac{x}{z}, z\frac{y}{z}, z\right)$. Die Abbildung ι aus 9.3 B)b), welche die Umkehrabbildung von ε ist, liefert zu jedem solchen rationalen Punkt $\left(\frac{x}{z}, \frac{y}{z}\right)$ ein $t = \iota\left(\frac{x}{z}, \frac{y}{z}\right) \in \mathbb{Q}$ mit $\left(\frac{x}{z}, \frac{y}{z}\right) = (u(t), v(t))$, also mit $(x, y, z) = (zu(t), zv(t), z)$ wie gewünscht. Wie man leicht sieht, wird hierbei zwei Tripeln der Form (x, y, z) und (kx, ky, kz) mit $k \in \mathbb{N}$ dasselbe t zugeordnet. Somit können wir uns auf die schon bestimmten primitiven pythagoräischen Tripel beschränken.
Für $(x, y, z) = (4, 3, 5)$ finden wir $\left(\frac{x}{z}, \frac{y}{z}\right) = \left(\frac{4}{5}, \frac{3}{5}\right)$ und damit $\iota\left(\frac{4}{5}, \frac{3}{5}\right) = \frac{\frac{4}{5}}{1-\frac{3}{5}} = 2$. Analog erhält man für die übrigen primitiven pythagoräischen Tripel in der obenstehenden Reihenfolge für t die Werte 4, $\frac{3}{2}$ und $\frac{4}{3}$.

Aufgaben 9.12 C) Setzt man $z = 1$, so errät man leicht eine Lösung indem man x oder y gleich 0 oder 1 wählt. Dies ergibt zum Beispiel: a) $(1, 0, 1)$; b) $(1, 0, 1)$; c) $(0, 0, 1)$; d) $(2, 1, 1)$; f) $(1, 1, 1)$.
D) Die Gleichung e) liefert für $z = 1$ eine Pell'sche Gleichung. Das Paar $(1, 0)$ ist eine Lösung jeder Pell'schen Gleichung, und so finden wir die Lösung $(1, 0, 1)$.

Aufgaben 9.14 B) Es gelten $f_a(u, v) = u - v^2$, $f_b(u, v) = u^2 - v^2 - 1$, $f_c(u, v) = u^2 + v^2 - 7$ und $f_d(u, v) = -u^2 + 2v^2 - 3$. $\mathbb{M}(f_a)$ ist eine Parabel parallel zur u-Achse mit Scheitelpunkt im Ursprung. $\mathbb{M}(f_b)$ ist eine gleichseitige Hyperbel mit Mittelpunkt im Ursprung und Halbachsen (!) der Länge 1. $\mathbb{M}(f_c)$ ist ein Kreis um den Ursprung mit Radius $\sqrt{7}$.



Aufgabe 9.14 B)

$\mathbb{M}(f_d)$ ist eine Hyperbel mit Mittelpunkt im Ursprung und Halbachsen der Längen $\sqrt{3}$ und $\sqrt{\frac{3}{2}}$.

Aufgaben 9.17 A) a) Wir behaupten, es sei $\mathbb{L} := \mathbb{L}\left(x^2+y^2-3z^2\right) = \emptyset$ und gehen vor wie in 9.15. Wir nehmen an, es gäbe ein $(x,y,z) \in \mathbb{L}$. Ohne Einschränkung könnten wir annehmen, x, y und z hätten keinen gemeinsamen Primfaktor. Wir fänden also $m,n,r,s \in \mathbb{Z}$ mit $0 \leq r,s \leq 2$ und $(r,s) \neq (0,0)$ so, dass $x = 3m+r$ und $y = 3n+s$ gälten. Wegen $(x,y,z) \in \mathbb{L}$ erhielten wir $3z^2 = x^2+y^2 = (3m+r)^2+(3n+s)^2 = 3\left(3m^2+2mr+3n^2+2ns\right)+r^2+s^2$, also $3|r^2+s^2$. Man sieht aber leicht (zum Beispiel anhand einer Tabelle wie in 9.15), dass dies für keine Wahl von (r,s) mit $0 \leq r,s \leq 2$ mit $(r,s) \neq (0,0)$ erfüllt wäre, und somit erhielten wir einen Widerspruch. Also folgt die Behauptung.
b) $\mathbb{M}\left(u^2+v^2-3\right)$ ist ein Kreis mit Mittelpunkt im Ursprung und Radius $\sqrt{3}$.
B) Wir formulieren das Vorgehen von 9.15 allgemein. Für

$$(x,y,z) \in \mathbb{L}_c := \mathbb{L}\left(x^2+y^2-cz^2\right)$$

so, dass x, y und z keinen gemeinsamen Primfaktor haben, gibt es $m,n,r,s \in \mathbb{Z}$ mit $0 \leq r,s \leq c-1$, $(r,s) \neq (0,0)$ so, dass $x = cm+r$ und $y = cn+s$, und weiter gilt

$$(*) \qquad cz^2 = x^2+y^2 = c\left(cm^2+2mr+cn^2+2ns\right)+r^2+s^2,$$

also $c|r^2+s^2$. Wir stellen eine Tabelle mit den Werten von r^2+s^2 auf, welche wir aus Symmetriegründen nicht vollständig auszufüllen brauchen.

	0	1	2	3	4	5	6	7	8	9
0	0									
1	1	2								
2	4	5	8							
3	9	10	13	18						
4	16	17	20	25	32					
5	25	26	29	34	41	50				
6	36	37	40	45	52	61	72			
7	49	50	53	58	65	74	85	98		
8	64	65	68	73	80	89	100	113	128	
9	81	82	85	90	97	106	107	145	145	162

Betrachtet man nun einen quadratischen Ausschnitt dieser Tabelle, ausgehend von der linken oberen Ecke mit einer Seitelänge von c Zellen, so genügt es zu sehen, dass c keinen der darin enthaltenen von 0 verschiedenen Einträge teilt. Dies ist für alle $c \in \{1, 3, 7\}$ der Fall, und es folgt also $\mathbb{L}_1 = \mathbb{L}_3 = \mathbb{L}_7 = \emptyset$.
In den Fällen $c \in \{2, 4, 5, 8, 9, 10\}$ finden wir ein $(x, y, z) \in \mathbb{L}_c$, indem wir im entsprechenden Tabellenausschnitt einen Eintrag wählen, der ein Vielfaches von c ist. Wir bestimmen die entsprechenden Werte für r und s und setzen $x = r$ und $y = s$, was in den Darstellungen $x = cm + r$ und $y = cn + s$ der Wahl von $m = n = 0$ entspricht. Nun findet man leicht ein passendes z so, dass $(x, y, z) \in \mathbb{L}_c$. Konkret erhält man zum Beispiel $(1, 1, 1) \in \mathbb{L}_2$, $(2, 0, 1) \in \mathbb{L}_4$, $(2, 1, 1) \in \mathbb{L}_5$, $(2, 2, 1) \in \mathbb{L}_8$, $(3, 0, 1) \in \mathbb{L}_9$ und $(3, 1, 1) \in \mathbb{L}_{10}$.
Übrig bleibt jetzt nur noch der Fall $c = 6$. Die obenstehende Tabelle liefert nicht direkt einen Widerspruch, denn es gilt $6|(3^2 + 3^2)$. Die dadurch bestimmte Wahl von $(r, s) = (3, 3)$ ist aber die einzig mögliche. Nach $(*)$ folgt

$$6(6(m(m+1) + n(n+1))) + 18 = 6z^2,$$

nach Kürzen mit 6 also

$$6(m(m+1) + n(n+1)) + 3 = z^2.$$

Deswegen sind z^2 und somit auch z ein Vielfaches von 3. Es gibt also ein $w \in \mathbb{Z}$ mit $z = 3w$. Damit können wir obige Gleichung mit 3 kürzen und erhalten

$$2(m(m+1) + n(n+1)) = 3w^2 - 1.$$

Die linke Seite dieser Gleichung ist sicher gerade, und deshalb sind $3w^2$ und damit auch w ungerade. Dies heisst, dass es ein $t \in \mathbb{Z}$ gibt mit $w = 2t + 1$. Damit erhalten wir

$$2(m(m+1) + n(n+1)) = 3(2t+1)^2 - 1 = 12t^2 + 12t + 2.$$

Dividieren wir diese Gleichung mit 2, so folgt

$$m(m+1) + n(n+1) = 6t^2 + 6t + 1 = 6t(t+1) + 1.$$

Hierbei ist aber die linke Seite gerade und die rechte Seite ungerade. Dieser Widerspruch zeigt, dass $\mathbb{L}_6 = \emptyset$ gilt.