

■ Reinhold Remmert
■ Peter Ullrich

Elementare Zahlentheorie

Dritte Auflage



Birkhäuser



■ Reinhold Remmert
■ Peter Ullrich

Elementare Zahlentheorie

Dritte Auflage

Birkhäuser
Basel · Boston · Berlin

Autoren:

Reinhold Remmert
Westfälische Wilhelms-Universität
Mathematisches Institut
Einsteinstraße 62
D-48149 Münster

Peter Ullrich
Universität Koblenz-Landau
Campus Koblenz
Mathematisches Institut
Universitätsstraße 1
D-56070 Koblenz

Erste Auflage 1987
Zweite Auflage 1995

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über <<http://dnb.ddb.de>> abrufbar.

ISBN 978-3-7643-7730-4 Birkhäuser Verlag, Basel – Boston – Berlin

Das Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechts.

© 2008 Birkhäuser Verlag, Postfach 133, CH-4010 Basel, Schweiz
Ein Unternehmen von Springer Science+Business Media
Gedruckt auf säurefreiem Papier, hergestellt aus chlorfrei gebleichtem Zellstoff. TCF ∞
Printed in Germany

ISBN 978-3-7643-7730-4

e-ISBN 978-3-7643-7731-1

9 8 7 6 5 4 3 2 1

www.birkhauser.ch

Vorwort

Die Mathematik ist die Königin
der Wissenschaften, und die Arithmetik ist
die Königin der Mathematik.

C. F. GAUSS

„Gegenstand der elementaren Zahlentheorie sind in erster Linie die *natürlichen Zahlen* $1, 2, 3, \dots$. Nach KRONECKER hat sie der liebe Gott geschaffen, nach DEDEKIND der menschliche Geist. Das ist je nach Weltanschauung ein unlösbarer Widerspruch oder ein und dasselbe. Für die Zahlentheorie ist es gleichgültig, wer die natürlichen Zahlen geschaffen hat. Sie stellt sich auf den Standpunkt, daß sie jedenfalls da sind und uns wohlbekannt sind.“

Mit diesen eindrucksvollen Sätzen beginnt H. HASSE seine „Vorlesungen über Zahlentheorie“ [7]. Der von HASSE bezogene Standpunkt wird heute von nahezu allen Autoren, die über Zahlentheorie schreiben, geteilt. Auch wir sehen es in diesem Buch nicht als unsere Aufgabe an, den Begriff der natürlichen Zahl axiomatisch einzuführen, sondern setzen das Rechnen mit diesen Zahlen als bekannt voraus.

Das unvergängliche Problem der Zahlentheorie ist das der Teilbarkeit:
Ist eine Zahl durch eine andere teilbar oder nicht?

Alle in diesem Buch behandelten Fragen sind Variationen dieses einen Themas.

Sätze und Begriffsbildungen der elementaren Zahlentheorie, die seit alters her auch höhere Arithmetik genannt wird, bedürfen kaum einer Motivierung. Jeder Leser ist bereits vom Grundschul- und Gymnasialunterricht mit vielen Fragestellungen der Zahlentheorie (bewußt oder unbewußt) wohlvertraut: Wir alle haben schon große Zahlen in Primfaktoren zerlegt, Hauptnenner als kleinste gemeinsame Vielfache bestimmt und irgendwann auch Divisionen mit Rest durchgeführt. So ist es leicht und vielfach sogar überflüssig, den Leser noch besonders für die Probleme des Textes zu motivieren.

Das vorliegende Buch umfaßt den Stoff einer vierstündigen Vorlesung im Sommersemester. Es richtet sich an

- Dozenten und Studenten der Mathematik,
- Lehrer an Realschulen und Gymnasien,
- jeden, der sich für ein weit über dreitausend Jahre altes Teilgebiet der Mathematik interessiert.

Der Leser lasse sich nicht durch die relative Länge des Textes irritieren: Wir haben es vorgezogen, auch solche Begriffe, die an sich bekannt sind, noch einmal zu besprechen. Insbesondere setzen wir beim Leser an Vorkenntnissen neben elementarem Schulstoff nur eine gewisse Vertrautheit mit der Mengenschreibweise voraus. Diese Ausführlichkeit der Darstellung macht den Text auch zum

Selbststudium geeignet; hierzu tragen ebenfalls die Aufgaben am Ende eines jeden Paragraphen bei, die den behandelten Stoff einüben und vertiefen.

Wir haben uns bemüht, das Wechselspiel zwischen konkretem und abstraktem Schließen herauszustellen. Der Leser wird – je nach Veranlagung – konkretes oder abstraktes Vorgehen besonders schätzen. Ein Werturteil, welcher Art von Zahlentheorie der Vorrang gegeben werden muß, ist objektiv nicht möglich: Der uralte Streit, welcher Zugang der didaktisch bessere ist, wird immer aufs neue entflammen; er erscheint vielen Mathematikern heute ebenso unverständlich wie der Streit der Byzantiner über das Geschlecht der Engel.

Wir sehen uns außerstande, dem Leser einen Königsweg zu beschreiben, der unmittelbar zum Verständnis dieses Textes führt. Die von Didaktikern seit eh und je diskutierte Frage: „Wie lernt man Mathematik?“ wird wohl allen Bemühungen zum Trotz niemals eine allgemein zufriedenstellende Antwort finden. Die Situation scheint immer noch dieselbe zu sein, wie für d’ALEMBERT, der einem zweifelnden Anfänger gesagt haben soll: „Allez en avant, la foi vous viendra“.*

Dem einen Leser wird das Verständnis der Begriffe und Sätze vorrangig sein, und er wird Beweise nicht bis in letzte Detail analysieren; dem anderen Leser wird gerade das volle Erfassen der Beweise oberstes Ziel sein. Gut beraten ist natürlich jeder, der sich diese beiden Gesichtspunkte gleichberechtigt zu eigen macht.

Wir haben ein ausführliches Inhaltsverzeichnis zusammengestellt, das aufgrund seiner spezifizierten Untergliederung einen detaillierten Überblick über den Gesamttext gibt. Auf einige Besonderheiten des Inhalts möchten wir dennoch an dieser Stelle hinweisen, so auf

- die Untersuchung der quadratischen Zahlbereiche $\mathbb{Z}[\sqrt{m}]$ und $\mathbb{Q}[\sqrt{m}]$, insbesondere der Gaußschen Zahlbereiche $\mathbb{Z}[i]$ und $\mathbb{Q}[i]$ und des Dedekindschen Ringes $\mathbb{Z}[\sqrt{-5}]$,
- den g -adischen Algorithmus, der die Verallgemeinerung der wohlvertrauten Dezimalbruchentwicklung für beliebige Grundzahlen g liefert,
- die Verwendung des Satzes von FERMAT-EULER als Verschlüsselungsverfahren.

Außerdem haben wir mehr als sonst üblich

- historische Bemerkungen

in den Text eingewoben.

Das Buch ist aus Vorlesungen entstanden, die der ältere von uns mehrfach gehalten hat. Wertvolle Hinweise erhielten wir von Herrn M. KOECHER. Bei der Herstellung des Manuskriptes haben uns Frau U. PETERNELL und Herr M. STEINSIEK unterstützt. Ihnen gilt unser Dank.

Der Birkhäuser Verlag hat die Drucklegung des Textes mit bewährter Sorgfalt betreut.

* ..Arbeiten Sie nur tüchtig, der Glaube wird Ihnen schon kommen.“

Wir schließen diese einleitenden Bemerkungen mit jenen denkwürdigen Sätzen, die GAUSS 1847 Abhandlungen“ schrieb:

„Die Höhere Arithmetik bietet einen unerschöpflichen Reichthum an interessanten Wahrheiten dar, und zwar an solchen, die nicht vereinzelt, sondern in in-nigem Zusammenhange stehen, und immer neue, ja unerwartete Verknüpfungen erkennen lassen, je weiter die Wissenschaft sich ausbildet. Ein großer Theil ihrer Lehren gewinnt auch einen neuen Reiz durch die Eigenthümlichkeit, daß ge-wichtige Lehrsätze in einfach ausgeprägtem Inhalt uns leicht durch Induction zu-geführt werden, deren Begründung doch so tief liegt, daß man erst nach vielen vergeblichen Versuchen dazu gelangt, und dann meistens erst auf beschwerlichen künstlichen Wegen, während die einfacheren Methoden lange verborgen bleiben. [...]

Von den eigenthümlichen Schönheiten dieser Gebiete haben Alle sich angezogen gefühlt, die darin beschäftigt gewesen sind: keiner aber hat es wohl so oft ausgesprochen wie Euler, der namentlich in fast allen seinen zahlreichen, zur Höhe-ren Arithmetik gehörenden Aufsätzen die Erklärung wiederholt, wie viele Freude ihm diese Forschungen machen, und wie sehr er darin eine Erholung von und eine Stärkung zu ändern der unmittelbaren practischen Anwendung näher liegenden Arbeiten finde.“

Münster/Westf., 18. September 1986

R. REMMERT, P. ULLRICH

Vorwort zur 2. Auflage

Gegenüber dem Erstdruck wurden nur Fehler und Unebenheiten beseitigt. Für diesbezügliche Hinweise danken wir insbesondere den Herren B. ARTMANN (Darmstadt), W. GREVE-KRAMER (Göttingen), M. KNESER (Göttingen), M. PETERS (Münster), H. RÖSCHLAU (Kappeln) und St. SPRINGMANN (Göttingen).

Münster/Westf., 26. Januar 1995

R. REMMERT, P. ULLRICH

Vorwort zur 3. Auflage

Neben einigen Ergänzungen wurden wieder Glättungen vorgenommen. Für Hin-weise danken wir den Herren J. ELSTRODT (Münster), M. KNESER (†), H. MÖLLER (Münster) und M. PETERS (Münster).

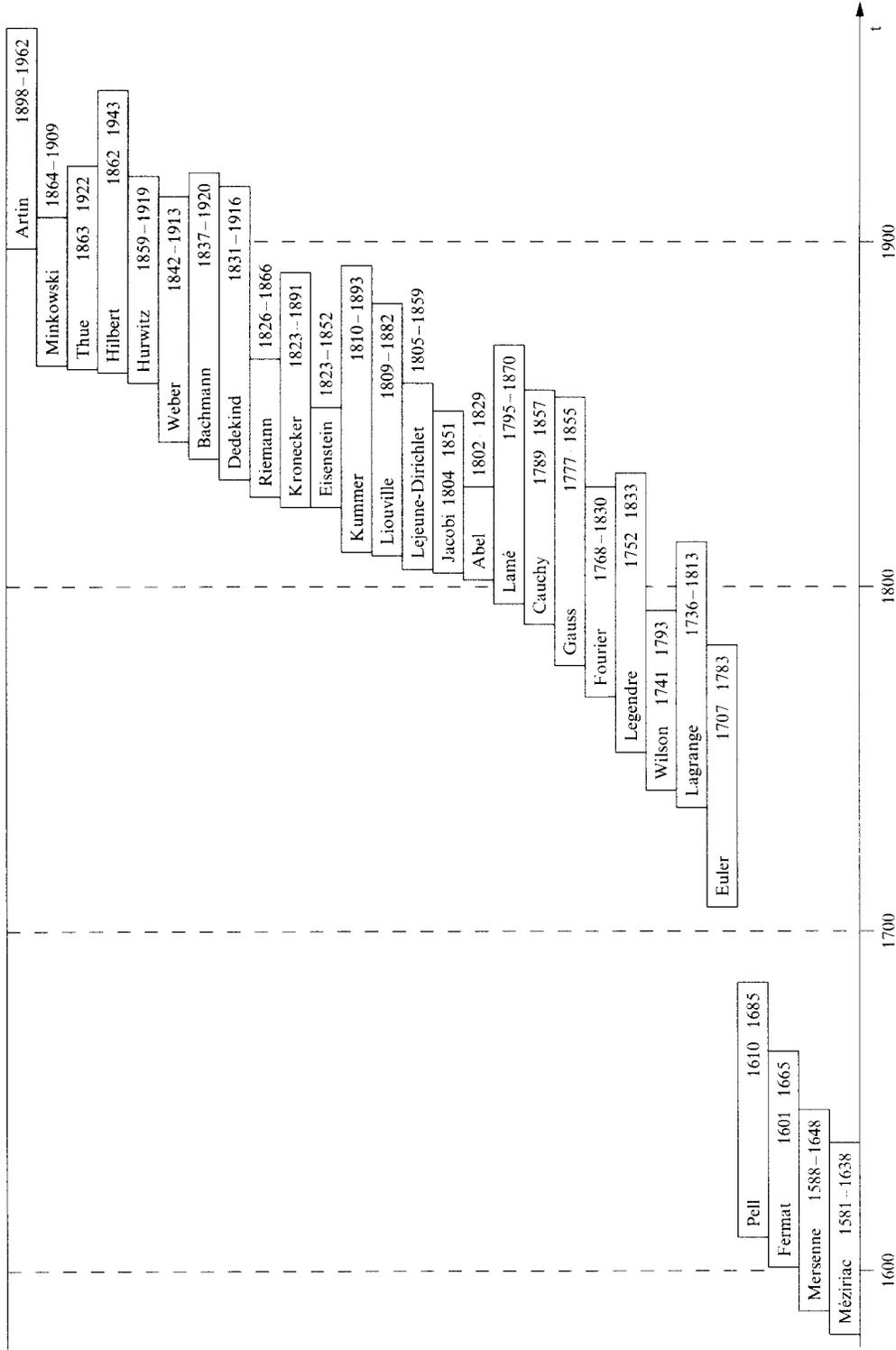
Münster/Westf. und Koblenz, 30. April 2007

R. REMMERT, P. ULLRICH

Lesehinweise

Ein Zitat 3.4.2 bedeutet Abschnitt 2 im Paragraphen 4 des Kapitels 3; entsprechend wird die Aufgabe 2) zu Paragraph 4 in Kapitel 3 als „Aufgabe 3.4.2“ zitiert. Innerhalb eines Kapitels wird die Kapitelnummer, innerhalb eines Paragraphen auch die Paragraphennummer we-gelassen. Die mit * gekennzeichneten Paragraphen bzw. Abschnitte können bei der ersten Lektüre übergangen werden.

Zeittafel



Inhaltsverzeichnis

Kapitel 1

Primzerlegung in \mathbb{Z} und \mathbb{Q}

Einleitung

§ 0	Natürliche, ganze und rationale Zahlen	13
	1. Der Ring \mathbb{Z} der ganzen und der Körper \mathbb{Q} der rationalen Zahlen – 2. Anordnung von \mathbb{Z} und \mathbb{Q} – 3. Prinzip vom kleinsten Element und Induktionsprinzip – 4. Division mit Rest	
§ 1	Teilbarkeit, Primzahlen	22
	1. Teilbarkeitsbegriff – 2. Primzahlen – 3. Existenz unendlich vieler Primzahlen – 4. Unzerlegbarkeit und Primeigenschaft	
§ 2	Der Hauptsatz der elementaren Zahlentheorie	28
	1. Existenz einer Primzerlegung – 2. Eindeutigkeit der Primzerlegung – 3*. Der Eindeutigkeitsbeweis von ZERMELO – 4*. Kritische Bemerkungen	
§ 3	Anwendungen des Hauptsatzes	33
	1. Anzahl aller positiven Teiler – 2. Produkt aller positiven Teiler – 3. Summe aller positiven Teiler – 4. Vollkommene Zahlen – 5. Mersennesche Primzahlen – 6. Fermatsche Primzahlen	
§ 4	Zahlentheorie im Körper \mathbb{Q}	42
	1. Primzerlegung in \mathbb{Q} – 2. Irrationalitätsaussagen – 3*. Zur Irrationalität und Transzendenz von e und π – 4. Die Vielfachheitsfunktion $w_p(a)$ – 5*. Ägyptische Bruchdarstellungen, Fibonaccimethode	

Kapitel 2

Theorie des größten gemeinsamen Teilers in \mathbb{Z}

Einleitung

§ 1	Größter gemeinsamer Teiler	55
	1. Größter gemeinsamer Teiler zweier ganzer Zahlen – 2. Euklidischer Algorithmus – 3. Idealtheoretische Charakterisierung des größten gemeinsamen Teilers – 4. Größter gemeinsamer Teiler endlich vieler ganzer Zahlen – 5. Teilerfremdheit – 6. Reduzierte Bruchdarstellung – 7. Kleinstes gemeinsames Vielfaches	
§ 2	Über die Verteilung und Darstellung von Primzahlen	70
	1. Elementare Verteilungssätze – 2. Großer Primzahlsatz – 3*. Die Chebyshevsche Abschätzung – 4. Große Primzahlen – 5. Primzahlen in arithmetischen Progressionen – 6. Primzahlen als Werte von Polynomen	
§ 3	Zahlentheoretische Funktionen	81
	1. Multiplikative Funktionen – 2. Eulersche φ -Funktion – 3. DIRICHLET-Faltung – 4. Summatorfunktionen	

Kapitel 3

Zahlentheorie in allgemeinen Integritätsringen

Einleitung

- § 0 Integritätsringe 95
 1. Allgemeine Begriffe der Ringtheorie – 2. Polynomringe –
 3. Quadratische Zahlbereiche
- § 1 Teilbarkeitstheorie in Integritätsringen 101
 1. Grundbegriffe der Teilbarkeitstheorie – 2. Normfunktionen
 3. Zerlegungssatz für Integritätsringe mit monotoner Normfunktion
- § 2 Faktorielle Ringe, Hauptidealringe und euklidische Ringe 111
 1. Faktorielle Ringe – 2. Hauptidealringe – 3. Euklidische Ringe –
 4. Beispiele – 5*. Weiterführende Ergebnisse – 6. Zerlegung von
 Primzahlen in quadratischen Zahlbereichen – 7. Charakterisierung von
 Primzahlen in quadratischen Zahlbereichen
- § 3 Zahlentheorie in faktoriellen Ringen und in Hauptidealringen 126
 1. Zahlentheorie in faktoriellen Ringen – 2. Theorie des größten
 gemeinsamen Teilers – 3. Integritätsringe mit ggT – 4. Charakterisierung
 faktorieller Ringe. Zerlegungssatz für noethersche Ringe

Kapitel 4

Der g -adische Algorithmus

Einleitung

- § 1 g -adische und Cantorsche Darstellung natürlicher Zahlen 139
 0. Historisches Präludium – 1. Existenz und Eindeutigkeit der g -adischen
 Darstellung – 2. Rechnen im g -adischen System – 3*. Cantorsche
 Darstellung natürlicher Zahlen
- § 2 g -adische Darstellung rationaler Zahlen 148
 1. g -adischer Algorithmus – 2. Endliche g -adische Darstellungen –
 3. Periodische g -adische Darstellungen
- § 3 Periodizitätssätze. Satz von FERMAT-EULER 158
 1. Kriterien für reine Periodizität – 2. Charakterisierung von Vorperioden
 und Perioden – 3. Zyklische Ziffernverschiebung – 4. Satz von
 FERMAT-EULER
- § 4* (Anhang) g -adische Entwicklung als Approximationsverfahren 168
 1*. Approximationskriterium – 2*. Konstruktion von Brüchen zu
 g -periodischen Folgen – 3*. g -adische Entwicklungen und unendliche
 Reihen

Kapitel 5

Kongruenzen und Restklassenringe

Einleitung

- § 1 Kongruenzenrechnung 179
 1. Kongruenzrelation. Elementares Rechnen mit Kongruenzen –
 2. Kongruenzen zu verschiedenen Moduln – 3. Neuner- und Elferprobe –

4. Der Satz von FERMAT-EULER als Kongruenzsatz – 5. Anwendung des Satzes von FERMAT-EULER in der Kryptographie

§ 2 Satz von WILSON. Chinesischer Restsatz 192
 1. Lineare Kongruenzen – 2. Der Satz von WILSON – 3. Ein Satz von EULER – 4. Chinesischer Restsatz

§ 3 Restklassenringe und Polynomkongruenzen 201
 1. Restklassenringe – 2. Primideale und maximale Ideale –
 3. Polynomkongruenzen und Polynomgleichungen – 4. Satz von LAGRANGE

Kapitel 6
Prime Restklassengruppen

Einleitung

§ 1 Elementare Gruppentheorie 213
 1. Gruppenbegriff. Beispiele aus der Zahlentheorie – 2. Untergruppen, Kongruenz, Ordnung einer Gruppe – 3. Ordnung eines Gruppenelementes – 4. Verallgemeinerungen der Sätze von FERMAT-EULER und WILSON

§ 2 Zyklische prime Restklassengruppen 223
 1. Allgemeines Zyklizitätskriterium – 2. Existenz von Primitivwurzeln zu Primzahlen – 3. Zyklizität der Gruppen $\mathbb{Z}_{p^n}^*$ – 4. Kleine Primitivwurzeln zu p^n – 5. Zyklizität der Gruppen $\mathbb{Z}_{2p^n}^*$ – 6. Bestimmung aller zyklischen Gruppen \mathbb{Z}_m^*

Kapitel 7
Theorie der quadratischen Reste

Einleitung

§ 1 Quadratische Reste 237
 1. Quadratische Reste modulo einer beliebigen Zahl $m > 1$ –
 2. Quadratische Reste modulo Primzahlpotenzen – 3. Quadratische Reste modulo einer ungeraden Primzahl – 4. Legendresches Restsymbol –
 5. Gaußsches Lemma

§ 2 Quadratisches Reziprozitätsgesetz 248
 1. Formulierung des Reziprozitätsgesetzes. Beispiele – 2. Beweis des Reziprozitätsgesetzes – 3*. Analytischer Beweis des Reziprozitätsgesetzes nach EISENSTEIN – 4. Das Reziprozitätsgesetz für das Jacobische Restsymbol – 5. Anwendungen des allgemeinen Reziprozitätsgesetzes

Literatur 266
 Namenverzeichnis 267
 Sachverzeichnis 269
 Symbolverzeichnis 274

Kapitel 1

Primzerlegung in \mathbb{Z} und \mathbb{Q}

In diesem Kapitel wird Stoff dargestellt, der zum Teil aus dem Schulunterricht bekannt ist. Insbesondere stellt der Paragraph 0 die dem Leser wohlvertrauten Eigenschaften der natürlichen, ganzen und rationalen Zahlen zusammen, die wir im weiteren unbewiesen voraussetzen.

Den Schwerpunkt des Kapitels bildet der Paragraph 2, wo der Hauptsatz der elementaren Zahlentheorie behandelt wird, d.h. der Satz von der eindeutigen Darstellbarkeit jeder natürlichen Zahl $\neq 0$ als Produkt von Primzahlen. Dieser Satz wird im elementaren Rechenunterricht stillschweigend als richtig unterstellt, da auf jener Stufe ja überhaupt noch nicht von mathematischer Strenge die Rede sein kann. Leider wird dadurch, wie die Erfahrung immer aufs neue lehrt, bei manchem Leser der ganz unberechtigte Eindruck entstanden sein, daß dieser Darstellungssatz unmittelbar einsichtig sei und keiner Begründung bedürfe. Es ist ein Hauptanliegen des ersten Kapitels, diesen irrigen Eindruck, der sich bei vielen für immer festgesetzt hat, zu korrigieren.

Die Anwendungen des Hauptsatzes der elementaren Zahlentheorie, die in den letzten beiden Paragraphen besprochen werden, demonstrieren dessen mathematische Kraft. Die getroffene Auswahl ist naturgemäß willkürlich: Der Leser sollte vor allem ein Gefühl dafür bekommen, wie häufig der Hauptsatz bei der Lösung von Fragen, die auch einem mathematischen Laien nahegebracht werden können, verwendet werden muß.

§ 0 Natürliche, ganze und rationale Zahlen

In diesem Paragraphen stellen wir für uns wichtige Tatsachen über natürliche, ganze und rationale Zahlen zusammen. Da unser Thema „Zahlentheorie“ und nicht „Aufbau des Zahlensystems“ heißt, sind wir nicht an einer streng logischen Begründung des Zahlenbegriffs ab ovo interessiert. Vielmehr soll dieser Paragraph dem Leser all jene Dinge in Erinnerung bringen, die er schon von der Schule her kennt und die zu den allgemeinen mathematischen Grundkenntnissen gehören.

1. Der Ring \mathbb{Z} der ganzen und der Körper \mathbb{Q} der rationalen Zahlen. Die Zahlen $1, 2, 3, \dots$ heißen seit altersher *natürliche Zahlen*. Wir vereinbaren, daß auch die Null eine natürliche Zahl ist, und bezeichnen die so erweiterte Menge mit \mathbb{N} , also

$$\mathbb{N} := \{0, 1, 2, 3, \dots, 1001, 1002, \dots\}.$$

Da häufig die Menge $\{1, 2, 3, \dots\}$ aller von 0 verschiedenen natürlichen Zahlen betrachtet wird, ist es zweckmäßig, auch für diese Menge ein Symbol einzuführen. Wir verabreden folgende Bezeichnung:

$$\mathbb{N}^\times := \{1, 2, 3, \dots\}.$$

Es gilt also: $\mathbb{N} = \{0\} \cup \mathbb{N}^\times$. Die Menge \mathbb{N} ist eine echte Teilmenge der Menge

$$\mathbb{Z} := \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

aller *ganzen Zahlen*. Es gibt gute Gründe dafür, die zahlentheoretischen Untersuchungen sofort in \mathbb{Z} (und nicht in \mathbb{N}) durchzuführen: Zum einen läßt sich in \mathbb{Z} uneingeschränkt subtrahieren und daher einfacher rechnen als in \mathbb{N} ; zum anderen ist für spätere Verallgemeinerungen \mathbb{Z} und nicht \mathbb{N} der richtige Ausgangsbereich. Wir setzen das Rechnen mit ganzen Zahlen als bekannt voraus, stellen aber die grundlegenden Rechenregeln in zwei Aussagen zusammen:

Additionsregeln: In \mathbb{Z} gibt es eine Addition $+$, d.h. je zwei Elementen $a, b \in \mathbb{Z}$ ist ein (drittes) Element $a + b \in \mathbb{Z}$ zugeordnet. Für alle $a, b, c \in \mathbb{Z}$ gilt:

- 1) $(a + b) + c = a + (b + c)$ (Assoziativgesetz).
- 2) $a + b = b + a$ (Kommutativgesetz).
- 3) Zu jedem Paar $a, b \in \mathbb{Z}$ gibt es genau ein $x \in \mathbb{Z}$ mit $x + b = a$, man schreibt $x = a - b$.

Der Leser beachte, daß die Aussage 3) i.a. nicht in \mathbb{N} gilt, da $a - b$ nicht notwendig eine natürliche Zahl ist: So gibt es z.B. kein x in \mathbb{N} mit $x + 4 = 3$. Man faßt die Additionsregeln zusammen, indem man sagt: *Die Menge \mathbb{Z} ist bzgl. der Addition $+$ eine kommutative Gruppe*. Statt kommutative Gruppe sagt man auch *abelsche Gruppe* (zu Ehren des norwegischen Mathematikers Niels Henrik ABEL, 1802–1829).

Multiplikationsregeln: In \mathbb{Z} gibt es eine Multiplikation \cdot , d.h. je zwei Elementen $a, b \in \mathbb{Z}$ ist ein (drittes) Element $a \cdot b \in \mathbb{Z}$ zugeordnet. Für alle $a, b, c \in \mathbb{Z}$ gilt:

- 1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativgesetz).
- 2) $a \cdot b = b \cdot a$ (Kommutativgesetz).
- 3) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (Distributivgesetz).
- 4) $1 \cdot a = a$.

Statt $a \cdot b$ schreibt man auch einfach ab . Man faßt die Additionsregeln und die Multiplikationsregeln dahin zusammen, daß man sagt: *Die Menge \mathbb{Z} ist bzgl. der Addition $+$ und der Multiplikation \cdot ein kommutativer Ring mit Einselement*. Eine wichtige Eigenschaft von \mathbb{Z} ist die *Nullteilerfreiheit*: Aus $ab = 0$ mit $a, b \in \mathbb{Z}$ folgt $a = 0$ oder $b = 0$ (in Worten: ein Produkt ist nur dann null, wenn wenigstens ein Faktor null ist). Die Nullteilerfreiheit impliziert die

Kürzungsregel: Seien $a, b, c \in \mathbb{Z}$; es gelte $ab = ac$ und $a \neq 0$. Dann gilt: $b = c$.

Beweis: Aus $ab = ac$ folgt $a(b - c) = 0$. Wegen $a \neq 0$ muß gelten $b - c = 0$, d. h. $b = c$. \square

Der Ring \mathbb{Z} läßt sich erweitern zum Bereich \mathbb{Q} der *rationalen Zahlen*

$$\{0, \pm 1, \pm 2, \pm \frac{1}{2}, \pm 3, \pm \frac{1}{3}, \pm \frac{2}{3}, \pm 4, \pm \frac{3}{2}, \dots\}.$$

Jede rationale Zahl γ gestattet (auf mannigfache Weise) eine *Bruchdarstellung*

$$\gamma = \frac{a}{b} \text{ mit einem Zähler } a \in \mathbb{Z} \text{ und einem Nenner } b \in \mathbb{Z}, b \neq 0;$$

dabei gilt: Zwei rationale Zahlen $\gamma = \frac{a}{b}$, $\gamma' = \frac{a'}{b'}$ mit $a, a', b, b' \in \mathbb{Z}$, $b \neq 0$, $b' \neq 0$, sind genau dann gleich, wenn gilt $ab' = a'b$.

Statt „rationale Zahl“ sagen wir auch „Bruch“. Wir bezeichnen im folgenden rationale Zahlen i. a. mit kleinen lateinischen Buchstaben und benutzen den griechischen Buchstaben γ vorwiegend dann, wenn die Zahl in einer Bruchdarstellung $\gamma = \frac{a}{b}$ mit $a, b \in \mathbb{Z}$ gegeben wird.

Die Additionsregeln und die Multiplikationsregeln für \mathbb{Z} gelten unverändert für den Bereich \mathbb{Q} ; überdies gilt für \mathbb{Q} auch die

Divisionsregel: Zu jedem Paar $a, b \in \mathbb{Q}$ mit $b \neq 0$ gibt es genau ein $x \in \mathbb{Q}$ mit $bx = a$; man schreibt $x = b^{-1}a$ oder auch $x = \frac{a}{b}$.

Beispiel: Für $a = \frac{2}{3}$, $b = \frac{5}{7}$ ist $x = \frac{14}{15}$.

Die Additionsregeln, Multiplikationsregeln und die Divisionsregel beschreiben erschöpfend die Rechengesetze für die vier elementaren Rechenoperationen der Addition, Subtraktion, Multiplikation und Division im Zahlensystem \mathbb{Q} . Man faßt sie wie folgt zusammen: *Die Menge \mathbb{Q} ist bezüglich der Addition $+$ und der Multiplikation \cdot ein Körper.*

Wir werden im Ring \mathbb{Z} und im Körper \mathbb{Q} unbekümmert und wie seit früher Jugend gewohnt rechnen. Wir schreiben durchweg $ab + cd$ statt $(ab) + (cd)$. Auch verwenden wir die gebräuchlichen Redeweisen wie *Summe* bzw. *Differenz*

bzw. *Produkt* bzw. *Quotient* für $a + b$ bzw. $a - b$ bzw. ab bzw. $\frac{a}{b}$.

Sind die rationalen Zahlen $\gamma_1 = \frac{a_1}{b_1}$, $\gamma_2 = \frac{a_2}{b_2}$ in Bruchdarstellung vorgegeben, so sind

$$\gamma_1 \pm \gamma_2 = \frac{a_1 b_2 \pm a_2 b_1}{b_1 b_2}, \quad \gamma_1 \gamma_2 = \frac{a_1 a_2}{b_1 b_2}$$

Bruchdarstellungen für Summe, Differenz und Produkt. Falls

$$\gamma_1 \neq 0, \quad \text{so gilt } a_1 \neq 0, \quad \text{und } \gamma_1^{-1} = \frac{b_1}{a_1}$$

ist eine Bruchdarstellung des „Inversen“ von γ_1 (*Kehrwert*).

Sind a_1, \dots, a_n endlich viele Elemente aus \mathbb{Q} , so sind (auf Grund der Assoziativgesetze) die *endliche Summe* $a_1 + a_2 + \dots + a_n$ und das *endliche Produkt* $a_1 a_2 \cdot \dots \cdot a_n$ in \mathbb{Q} wohldefiniert. Wir verwenden die bekannte Schreibweise

$$\sum_{v=1}^n a_v = a_1 + \dots + a_n, \quad \prod_{v=1}^n a_v = a_1 \cdot \dots \cdot a_n$$

für Summe und Produkt. Falls $a_1 = a_2 = \dots = a_n = a$, so gilt $\sum_{v=1}^n a_v = na$ und $\prod_{v=1}^n a_v = a^n$, wobei $a^0 := 1$ gesetzt wird.

Wir erinnern an die

Summenformel der endlichen geometrischen Reihe: Für alle $x \in \mathbb{Q}$ und alle natürlichen Zahlen $n \geq 1$ gilt:

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

Der *Beweis* ergibt sich durch Ausmultiplizieren der linken Seite. \square

Wir machen stillschweigend Gebrauch von den Inklusionen

$$\mathbb{N}^* \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}.$$

2. Anordnung von \mathbb{Z} und \mathbb{Q} . Die Menge \mathbb{Z} ist in natürlicher Weise *angeordnet*:

$$\dots < -3 < -2 < -1 < 0 < 1 < 2 < 3 \dots.$$

Man schreibt allgemein $b < a$ und liest „ b ist kleiner als a “, wenn $b \in \mathbb{Z}$ in dieser Zahlenreihe links von $a \in \mathbb{Z}$ steht. (Das läßt sich auch so ausdrücken: Es gilt $b < a$ genau dann, wenn es eine natürliche Zahl $n \neq 0$ gibt, so daß gilt: $b + n = a$.) Statt „ b ist kleiner als a “ sagt man auch „ a ist größer als b “, man schreibt $a > b$ anstelle von $b < a$. Wir werden vorwiegend mit der Relation $>$ arbeiten.

Die Anordnung von \mathbb{Z} setzt sich zu einer Anordnung von \mathbb{Q} fort: So ist z. B. $\frac{1}{7} > \frac{2}{15}$. Allgemein gilt für zwei Zahlen $\gamma, \gamma' \in \mathbb{Q}$ genau dann $\gamma > \gamma'$, wenn die Differenz $\gamma - \gamma'$ ein Bruch der Form $\frac{a}{b}$ mit von 0 verschiedenen natürlichen Zahlen a, b ist. Wir stellen die für das Rechnen unerläßlichen Eigenschaften der Anordnungsrelation $>$ zusammen, verzichten aber auch hier bewußt auf eine strenge Begründung.

Anordnungsregeln: Seien $a, b, c \in \mathbb{Q}$.

- 1) Es gilt entweder $a > b$ oder $a = b$ oder $b > a$.
- 2) Aus $a > b$ und $b > c$ folgt $a > c$ (Transitivität).