Zahlentheorie

Von
Prof. Dr. Heinz Lüneburg (1935-2009)

Aus dem Nachlass des Autors
herausgegeben von

Prof. Dr. Theo Grundhöfer
apl. Prof. Dr. Huberta Lausch
Prof. Dr. Karl Strambach

Oldenbourg Verlag München

Prof. Dr. Heinz Lüneburg (1935–2009) lehrte von 1970 bis zu seiner Emeritierung 2003 als Professor an der Universität Kaiserslautern; Rufe nach Bayreuth bzw. Hamburg lehnte er ab. Seine Forschungsinteressen waren v.a. das Gebiet der endlichen Geometrie, wo sein Einfluss bis heute spürbar ist; später widmete er sich vermehrt auch der Untersuchung algorithmischer Fragen in Algebra und Kombinatorik sowie der Geschichte der Mathematik. Seine Forschung war insbesondere pädagogisch motiviert und zeichnet sich durch inhaltliche und formale Perfektion aus.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

© 2010 Oldenbourg Wissenschaftsverlag GmbH
Rosenheimer Straße 145, D-81671 München
Telefon: (089) 45051-0
oldenbourg.de

Das Werk einschließlich aller Abbildungen ist urheberrechtlich geschützt. Jede Verwertung außerhalb der Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Bearbeitung in elektronischen Systemen.

Lektorat: Kathrin Mönch
Herstellung: Sarah Voit
Coverentwurf: Kochan & Partner, München
Gedruckt auf säure- und chlorfreiem Papier
Gesamtherstellung: Books on Demand GmbH, Norderstedt

ISBN 978-3-486-59680-9

Vorwort

> Dans le monde, il y a mauvaise grâce à parler de soi ou des siens. Dans une préface, c'est la loi, loi dont on a beaucoup médit, dont on médira toujours, — par convenance,— mais qui fait trop joli jeu à la vanité des auteurs, pour jamais mourir. On me permettra donc d'insister un peu sur ce livre.
>
> Édouard Lucas, Récréations mathématiques 1882

Euklid hat in seinen Elementen nicht nur über Geometrie geschrieben. Es gibt in ihnen auch drei Bücher, die die zahlentheoretischen heißen. Einige ihrer Ergebnisse werden im zehnten Buch dazu verwendet, die Existenz gewisser irrationaler Strecken sicherzustellen. Sie sind aber auch für sich gesehen interessant und bieten einiges an sehr schöner Mathematik, die es wert ist, lebendig gehalten zu werden. Daher stehen diese Bücher am Anfang meiner Ausführungen als Einladung zur Zahlentheorie.

Der Division mit Rest ist das zweite Kapitel gewidmet. Sie wird normalerweise nur dazu benutzt, den größten gemeinsamen Teiler zweier Zahlen auszurechnen und zu beweisen, dass der Ring der ganzen Zahlen ein euklidischer Ring und damit ein Hauptidealring ist. Hier wird gezeigt, dass man noch mehr mit ihr anfangen kann, indem sie benutzt wird, um natürliche Zahlen in Mischbasen darzustellen. Dabei sind Darstellungen von natürlichen Zahlen in Mischbasen, vom heutigen Standpunkt aus betrachtet, Verallgemeinerungen der Darstellungen von natürlichen Zahlen im Dezimal- bzw. Dualsystem. Historisch gesehen, sind die Darstellungen von natürlichen Zahlen in Mischbasen jedoch die älteren. Man denke nur an das vor etwa dreißig Jahren aufgegebene englische Währungssystem, wo das Pfund zwanzig Schillinge und der Schilling zwölf Pfennige hatte, oder an die Zeitmessung, wo der Tag vierundzwanzig Stunden, die Stunde sechzig Minuten und die Minute sechzig Sekunden hat. Die Sekunde ist dann wieder dezimal unterteilt.

Das Thema vollkommene Zahlen, welches im ersten Kapitel schon Gegenstand der Untersuchungen ist, wird im vierten Kapitel wieder aufgenommen. Zur Konstruktion gerader vollkommener Zahlen benötigt man mersennesche Primzahlen, also Primzahlen der Form $2^p - 1$. Der Exponent p muss eine Primzahl sein, damit $2^p - 1$ eine Chance hat, seinerseits Primzahl zu sein. Wann dann $2^p - 1$ eine Primzahl ist, kann man mit dem Lucas-Lehmer-Test entscheiden. Der hier vorgeführte Beweis dieses Testes benötigt das quadratische Reziprozitätsgesetz, das im vierten Kapitel vorgestellt wird und das wir im Folgenden immer wieder einmal benutzen werden. Beim Beweis des Lucas-Lehmer-Testes kommt auch der Ring $\mathbf{Z}[\sqrt{3}]$ der ganzen algebraischen Zahlen im Körper $\mathbf{Q}[\sqrt{3}]$ ins Spiel. Dies zeigt, dass es immer wieder auch nützlich ist, allgemeinere Ringe als nur den Ring der ganzen Zahlen in die Untersuchungen einzubeziehen, will man

Eigenschaften des Ringes der ganzen Zahlen etablieren. Ein weiteres Beispiel für diese Situation ist der Ring $\mathbf{Z}[\sqrt{-1}]$ der ganzen gaußschen Zahlen, der ein euklidischer Ring ist und den man benutzen kann, um den fermatschen Satz zu beweisen, dass jede Primzahl, die durch 4 geteilt den Rest 1 hat, sich als Summe zweier Quadrate darstellen lässt.

Die Ringe A_D der ganzen algebraischen Zahlen in den Körpern $\mathbf{Q}[\sqrt{D}]$ sind aber auch für sich gesehen hochinteressant. Ihnen ist ein gut Teil dieses Buches gewidmet. Sie liefern Beispiele für Ringe, die keine Hauptidealringe sind. Nun, das sind die Polynomringe über dem Ring $\mathbf{Z}$ der ganzen Zahlen auch nicht. Im Gegensatz zu diesen gilt in jenen aber nicht der Satz von der eindeutigen Primfaktorzerlegung. Unter den Ringen A_D gibt es andererseits Hauptidealringe, die keinen, aber auch wirklich gar keinen euklidischen Algorithmus gestatten. Dies werden wir mithilfe einer von Motzkin stammenden internen Kennzeichnung der euklidischen Ringe beweisen. Vier solcher Ringe werden wir kennenlernen und in ihnen dennoch das rechnerische Problem lösen, den größten gemeinsamen Teiler zweier Elemente zu berechnen und ihn aus den gegebenen Elementen linear zu kombinieren. Hierzu werden uns quadratische Formen gute Dienste leisten. Überhaupt bieten die Ringe A_D viel Gelegenheit zum Rechnen und ich kann dem Leser nur empfehlen, die Rechenverfahren, die das Buch bietet, zu implementieren. Insbesondere die Algorithmen, die mit Kettenbrüchen zu tun haben, sind sehr reizvoll. Mit ihrer Hilfe kann man auch den fermatschen Zwei-Quadrate-Satz ins Konstruktive wenden. Wer die Rechenverfahren implementiert und auch die Übungsaufgaben löst, wird zu einem besseren Verständnis des Stoffes kommen.

Kaiserslautern 2003 *Heinz Lüneburg*

Aus dem Nachlass des Autors herausgegeben von Theo Grundhöfer, Huberta Lausch und Karl Strambach.

Inhaltsverzeichnis

Vorwort **V**

I. Zahlentheorie bei Euklid **1**

1. Die natürlichen Zahlen 1
2. Vollkommene Zahlen 10
3. Teilbarkeit 14
4. Stetige Proportion 20
5. Primzahlen 25

Aufgaben 26

II. Mischbasen **30**

1. Division mit Rest 30
2. Darstellungen natürlicher Zahlen in Mischbasen 32
3. Aufsteigende Kettenbrüche 37
4. Der cantorsche Algorithmus 40

Aufgaben 45

III. Der größte gemeinsame Teiler **47**

1. Der größte gemeinsame Teiler 47
2. ZPE-Bereiche 54
3. Euklidische Ringe 58

Aufgaben 62

IIII. Das quadratische Reziprozitätsgesetz **64**

1. Der chinesische Restsatz 64
2. Die eulersche Totientenfunktion 66
3. Das quadratische Reziprozitätsgesetz 69
4. Ganze Elemente 74

5. Der Test von Lucas-Lehmer 78
6. Der fermatsche Zwei-Quadrate-Satz 81
Aufgaben 81

V. Kettenbrüche **83**
1. Kettenbrüche 83
2. Der Kettenbruch der eulerschen Zahl 89
3. Nochmals der Zwei-Quadrate-Satz 92
4. Die modulare Gruppe 95
5. Periodische Kettenbrüche 97
Aufgaben 104

VI. Die Ringe A_D **105**
1. Die Einheitengruppe von A_D 105
2. Die Berechnung der Fundamentaleinheit 108
3. Die Klassenzahl 112
4. Weitere Hauptidealbereiche 120
5. Klassenzahl 1 121
Aufgaben 128

VII. Rechnen in A_D **129**
1. Rechnen mit Idealen 129
2. Der Schnitt zweier Ideale 135
3. Die quadratische Form eines Ideals 139
Aufgaben 145

Literatur **147**

Index **149**

I.

Zahlentheorie bei Euklid

Bis tief ins 19. Jahrhundert hinein waren die Elemente Euklids den Mathematikern vertraut. Heute sind sie dagegen weitgehend vergessen. Das ist schade, findet sich in ihnen doch so manches Juwel. Insbesondere auch in den arithmetischen Büchern, das sind die Bücher VII, VIII und VIIII der Elemente. Da ist einmal die Lehre vom Geraden und Ungeraden zu nennen, die darauf hinausläuft zu zeigen, dass sich jede Zahl auf genau eine Weise als eine Potenz von 2 mal einer ungeraden Zahl darstellen lässt. Dieses Resultat ist Vorläufer des Satzes von der eindeutigen Primfaktorzerlegung. Mit seiner Hilfe ist es möglich, den Bau der geraden vollkommenen Zahlen völlig in den Griff zu bekommen. Ein weiteres spektakuläres Resultat ist, dass für natürliche Zahlen a, b und n genau dann a^n Teiler von b^n ist, wenn a Teiler von b ist. Das Spektakuläre daran ist, dass Euklid dies beweist, ohne den Satz von der eindeutigen Primfaktorzerlegung zu benutzen, was wir heute tun. Eine Folgerung hieraus ist, die Euklid aber nicht formuliert, dass eine rationale Zahl, deren n-te Potenz eine ganze Zahl ist, selbst schon ganz ist. Ein weiterer Höhepunkt ist die Bestimmung aller pythagoreischen Tripel, d.h. aller Tripel (x, y, z) von natürlichen Zahlen mit $x^2 + y^2 = z^2$. All dies fließt bei ihm aus seiner Theorie von in stetiger Proportion stehenden Folgen. Dies möchte ich hier vortragen, wobei ich aber ganz und gar nicht philologisch vorgehen, vielmehr den euklidischen Text nach meinem Gutdünken interpretieren werde.

Für Euklid sind Zahlen Ansammlungen von Einheiten. Wie mit ihnen umzugehen ist, sagt er nicht. Um seine Ergebnisse auf eine etwas bessere Grundlage zu stellen, beginne ich mit der dedekindschen Grundlegung der natürlichen Zahlen, die ihrerseits ein Juwel ist. Sie axiomatisiert das Zählen und leitet daraus dann die uns allen vertraute Addition, Multiplikation und Anordnung der natürlichen Zahlen her. Dieser Grundlegung ist der erste Abschnitt gewidmet.

1. Die natürlichen Zahlen. Arithmos ist das griechische Wort für Haufen und Haufen von Steinen repräsentierten Zahlen, sodass dieses Wort schließlich auch die Bedeutung „Zahl“ annahm, wobei Zahl im Altertum und lange danach nur natürliche Zahl bedeutete. Für die Griechen also waren Zahlen so etwas wie Haufen von Steinen, Ansammlungen von Einheiten, wie es bei Euklid steht, wobei Euklid nirgendwo sagt, wie mit diesen Ansammlungen von Einheiten umzugehen sei. Vielleicht ist ihm nie bewusst geworden, dass man dazu etwas sagen muss. Fremd war ihm ein solches Vorgehen aber nicht, wie man an seinen geometrischen Postulaten sieht, wo er sehr wohl sagt, wie man mit Strecken, Kreisen und rechten Winkeln umzugehen hat. Man sieht es auch an seinem Hantieren mit Größen, bei denen er die Gültigkeit gewisser Postulate nachweist,

nachdem er die Vervielfachung von Größen erklärt hat. Es handelt sich dabei um einige der Postulate, die wir bei der Definition von Moduln stellen. Eine uns befriedigende Begründung für das Operieren mit natürlichen Zahlen hat aber erst das 19. Jahrhundert gegeben und da vor allem Dedekind. Er hat das Zählen im Rahmen der damals im Entstehen begriffenen Mengenlehre axiomatisiert. Seinem Vorbild werden wir nun folgen.

Es sei N eine Menge. Ferner sei $1 \in N$ und $'$ sei eine Abbildung von N in sich. Wir nennen $(N, 1, ')$ *Dedekindtripel*, falls gilt

a) Es ist $1 \notin N'$.

b) Die Abbildung $'$ ist injektiv.

c) Ist T eine Teilmenge von N, ist $1 \in T$ und gilt $T' \subseteq T$, so ist $T = N$.

Die Eigenschaft c) ist natürlich das Induktionsprinzip.

Grundlegend für alles Weitere ist der folgende Rekursionssatz von Dedekind.

Rekursionssatz. *Es sei $(N, 1, ')$ ein Dedekindtripel, A sei eine Menge und R sei eine Abbildung von A in sich, die sogenannte* Rekursionsregel. *Ist dann $a \in A$, so gibt es genau eine Abbildung f von N in A mit $f(1) = a$ und*

$$f(n') = R\big(f(n)\big)$$

für alle $n \in N$.

Beweis. Es sei Φ die Menge aller binären Relationen g auf $N \times A$ mit den Eigenschaften

a) Es ist $(1, a) \in g$.

b) Ist $n \in N$, $b \in A$ und $(n, b) \in g$, so ist $(n', R(b)) \in g$.

Setze

$$f := \bigcap_{g \in \Phi} g.$$

Dann leistet f das Verlangte, wie wir nun zeigen werden. Zunächst ist klar, dass $f \in \Phi$ gilt. Wir müssen zeigen, dass f eine Abbildung ist. Dazu müssen wir zeigen, dass es zu $n \in N$ genau ein $b \in A$ gibt mit $(n, b) \in f$. Um dieses zu zeigen, sei T die Menge der $n \in N$, für die es genau ein $b \in A$ gibt mit $(n, b) \in f$. Wir zeigen zunächst, dass $1 \in T$ gilt. Das einzige, was wir ja wirklich zur Verfügung haben, ist das Induktionsprinzip, sodass wir auf seine Anwendung hinsteuern.

Es gilt $(1, a) \in f$. Es sei $a \neq w \in A$ und $(1, w) \in f$. Wir setzen $f^* := f - \{(1, w)\}$. Wegen $w \neq a$ ist dann $(1, a) \in f^*$, sodass a) gilt. Es sei weiter $(n, b) \in f^*$. Dann ist $(n, b) \in f$ und folglich $(n', R(b)) \in f$. Nun ist $1 \notin N'$ und daher $(n', R(b)) \neq (1, w)$, sodass sogar $(n', R(b)) \in f^*$ gilt. Folglich ist $f^* \in \Phi$ und daher $f \subseteq f^*$. Wegen $(1, w) \in f$ folgt der Widerspruch $(1, w) \in f^*$. Dieser Widerspruch zeigt, dass $1 \in T$ gilt.

Es gelte $n \in T$. Es gibt dann genau ein $b \in A$ mit $(n, b) \in f$. Es folgt $(n', R(b)) \in f$. Es sei $R(b) \neq w \in A$ und es gelte $(n', w) \in f$. Wir setzen wieder $f^* := f - \{(n', w)\}$. Wegen $n' \neq 1$ ist dann $(1, a) \in f^*$. Es sei $m \in N$ und es gebe ein $x \in A$ mit $(m, x) \in f^*$. Ist $m \neq n$, so folgt aus der Injektivität von $'$, dass auch $m' \neq n'$ ist. Dies hat wiederum $(m', R(x)) \neq (n', w)$ zur Folge, sodass $(m', R(x)) \in f^*$ ist, da ja $(m, x) \in f$ gilt. Ist

$m = n$ so folgt $x = b$ und damit $(n', R(b)) \in f^*$. Es folgt wieder der Widerspruch $f \subseteq f^*$. Also gilt auch $n' \in T$. Aufgrund des Induktionsprinzips ist daher $T = N$, sodass f in der Tat eine Abbildung ist.

Schreibt man nun $f(n) = b$ an Stelle von $(n, b) \in f$, so gilt also $f(1) = a$. Ist $f(n) = b$, so bedeutet das in der ursprünglichen Schreibweise $(n, b) \in f$. Es folgt $(n', R(b)) \in f$, d.h. $f(n') = R(f(n))$. Damit ist die Existenzaussage des Satzes bewiesen.

Um die Einzigkeitsaussage zu beweisen, sei g eine Abbildung von A in sich und es gelte $g(1) = a$ und $g(n') = R(g(n))$ für alle $n \in N$. Es sei T die Menge aller $n \in N$ mit $f(n) = g(n)$. Dann ist $1 \in T$. Ist $n \in T$, so folgt

$$f(n') = R\big(f(n)\big) = R\big(g(n)\big) = g(n')$$

und damit $n' \in T$. Mittels des Induktionsprinzips folgt $T = N$ und weiter $f = g$. Damit ist alles bewiesen.

Korollar. *Sind $(N, 1_N, ')$ und $(M, 1_M, ')$ Dedekindtripel, so gibt es einen Isomorphismus von $(N, 1_N, ')$ auf $(M, 1_M, ')$.*

Beweis. Definiere die Abbildung R_M von M in sich durch $R_M(x) := x'$. Aufgrund des Rekursionssatzes gibt es dann genau eine Abbildung σ von N in M mit $\sigma(1_N) = 1_M$ und

$$\sigma(n') = R\big(\sigma(n)\big) = \sigma(n)'.$$

Dies zeigt, dass σ ein Homomorphismus ist. Ebenso gibt es einen Homomorphismus τ von $(M, 1_M, ')$ in $(N, 1_N, ')$, d.h. eine Abbildung τ von M in N mit $\tau(1_M) = 1_N$ und $\tau(m') = \tau(m)'$. Es folgt

$$\tau\sigma(1_N) = \tau(1_M) = 1_N.$$

Es sei $n \in N$ und $\tau\sigma(n) = n$. Dann ist

$$\tau\sigma(n') = \tau\big(\sigma(n)'\big) = \big(\tau\sigma(n)\big)' = n'.$$

Das Induktionsprinzip besagt daher, dass $\tau\sigma = \mathrm{id}_N$ ist. Analog folgt auch $\sigma\tau = \mathrm{id}_M$. Folglich ist σ bijektiv und τ ist die zu σ inverse Abbildung. Somit ist σ ein Isomorphismus.

Es gibt also bis auf Isomorphie nur ein Dedekindtripel, falls es überhaupt eins gibt. Ein solches nennen wir in Zukunft $\mathbf{N}$ und sprechen von ihm als der *Menge der natürlichen Zahlen*.

Auf $\mathbf{N}$ wollen wir nun Addition und Multiplikation definieren. Beginnen wir mit der Addition.

Es sei $m \in \mathbf{N}$. Wir definieren R durch $R(n) := n'$. Es gibt dann genau eine Abbildung π_m von $\mathbf{N}$ in sich mit $\pi_m(1) = m'$ und

$$\pi_m(n') = R\big(\pi_m(n)\big) = \pi_m(n)'.$$

Hier haben wir π_m geschrieben, um den Anschluss an das Vorige zu erhalten. Um das gewohnte Bild zu bekommen, schreiben wir statt π_m nun $m+$ und lassen die Klammern um das Argument der Abbildung weg. Dann gilt also

a) Es ist $m + 1 = m'$ für alle $m \in \mathbf{N}$.

b) Es ist $m + n' = (m + n)'$ für alle m, $n \in \mathbf{N}$.

Man ist gewohnt, $+$ als binäre Operation auf $\mathbf{N}$ aufzufassen. So wie die Addition hier definiert ist, ist aber zu jedem $m \in \mathbf{N}$ eine unäre Operation $m+$ definiert. Da diese unären Operationen aber auf ganz $\mathbf{N}$ operieren, kann man $+$ dann wieder als binäre Operation auf $\mathbf{N}$ auffassen, da ja zu jedem m, $n \in \mathbf{N}$ der Ausdruck $m + n$ erklärt ist.

Es ist nun zu zeigen, dass die so definierte Addition den gewohnten Rechenregeln gehorcht.

Satz 1. *Es ist $m' + n = m + n' = (m + n)'$ für alle m, $n \in \mathbf{N}$.*

Beweis. Die zweite Aussage des Satzes ist nur eine Wiederholung von b).

Um die erste zu beweisen, machen wir Induktion über n. Es gilt

$$m' + 1 = m'' = (m + 1)' = m + 1'.$$

Es sei $n \in \mathbf{N}$ und es gelte $m' + n = m + n'$. Dann folgt

$$m' + n' = (m' + n)' = (m + n')' = m + n'',$$

sodass die Aussage auch für n' gilt. Damit ist der Satz bewiesen.

Satz 2. *Es ist $m + n = n + m$ für alle m, $n \in \mathbf{N}$.*

Beweis. Wir zeigen zunächst, dass $1+n = n+1$ ist für alle $n \in \mathbf{N}$. Dies gilt sicherlich für $n = 1$. Es sei $n \in \mathbf{N}$ und es gelte $1 + n = n + 1$. Dann ist nach b) und Satz 1

$$1 + n' = (1 + n)' = (n + 1)' = n' + 1,$$

sodass in der Tat $1 + n = n + 1$ für alle $n \in \mathbf{N}$ gilt.

Um die allgemeine Aussage zu beweisen, machen wir nun Induktion nach m. Für $m = 1$ ist die Aussage richtig, wie gerade gesehen. Sie gelte für m. Dann ist

$$m' + n = m + n' = (m + n)' = (n + m)' = n + m'.$$

Damit ist Satz 2 bewiesen.

Die Addition ist also kommutativ. Sie ist auch assoziativ.

Satz 3. *Es ist $(m + n) + p = m + (n + p)$ für alle m, n, $p \in \mathbf{N}$.*

Beweis. Wir machen Induktion nach p. Es ist

$$(m + n) + 1 = (m + n)' = m + n' = m + (n + 1).$$

Also gilt die Aussage für $p = 1$. Sie gelte für p. Dann ist

$$\begin{aligned}(m + n) + p' &= \big((m + n) + p\big)' = \big(m + (n + p)\big)' = m + (n + p)' \\ &= m + (n + p'),\end{aligned}$$

sodass sie auch für p' gilt. Damit ist Satz 3 bewiesen.

Für die Addition gilt die Kürzungsregel.

Satz 4. *Sind m, n, $p \in \mathbf{N}$ und gilt $m + p = n + p$, so ist $m = n$.*

Beweis. Wir machen Induktion nach p. Ist $p = 1$, so folgt

$$m' = m + 1 = n + 1 = n'.$$

Weil $'$ injektiv ist, folgt weiter $m = n$.

Aus $m + p = n + p$ folge $m = n$ und es sei $m + p' = n + p'$. Dann ist

$$(m + p)' = m + p' = n + p' = (n + p)'.$$

Hieraus folgt weiter $m + p = n + p$ und dann auch $m = n$.

Ist $n \in \mathbf{N}$, so setzen wir

$$E_n := \{n + x \mid x \in \mathbf{N}\}.$$

Der Buchstabe E steht für Ende, da E_n, wie bald klar werden wird, aus allen natürlichen Zahlen besteht, die größer als n sind.

Satz 5. *Es ist $E_1 = \mathbf{N} - \{1\}$.*

Beweis. Es sei $T := E_1 \cup \{1\}$. Dann ist $1 \in T$. Es sei $n \in T$. Dann ist $n' = n + 1 = 1 + n \in E_1 \subseteq T$. Also ist $T = \mathbf{N}$. Wäre $1 \in E_1$, so gäbe es ein $w \in \mathbf{N}$ mit $1 = w + 1 = w'$ im Widerspruch zu $1 \notin \mathbf{N}'$. Also ist $E_1 = \mathbf{N} - \{1\}$.

Satz 6. *Ist $n \in \mathbf{N}$, so gilt*

a) Es ist $n' \in E_n$.

b) Ist $x' \in E_n$, so ist $E_x \subseteq E_n$.

c) Es ist $n \notin E_n$.

d) Es ist $E_n = E_{n'} \cup \{n'\}$.

Beweis. a) Es ist $n' = n + 1 \in E_n$.

b) Es sei $x' \in E_n$. Ferner sei $y \in E_x$. Es gibt dann a, $b \in \mathbf{N}$ mit $x' = n + a$ und $y = x + b$. Mit Satz 1 folgt

$$y' = x' + b = n + a + b.$$

Nun ist $a + b \neq 1$ (Beweis!). Nach Satz 5 gibt es daher ein $c \in \mathbf{N}$ mit $c' = c + 1 = a + b$. Also ist

$$y' = n + c' = (n + c)'$$

und damit $y = n + c \in E_n$.

c) Wäre $n \in E_n$, so gäbe es ein $w \in \mathbf{N}$ mit $n = n + w$. Es folgte

$$n + 1 = n' = (n + w)' = n + w'.$$

Hieraus folgte mit Satz 4 der Widerspruch $1 = w'$.

d) Nach a) ist $n' \in E_n$. Ferner ist $n'' = n + 1' \in E_n$. Mit $x = n'$ folgt mit b) daher $E_{n'} \subseteq E_n$. Also gilt

$$E_{n'} \cup \{n'\} \subseteq E_n.$$

Es sei umgekehrt $x \in E_n$. Es gibt dann ein $y \in \mathbf{N}$ mit $x = n + y$. Ist $y = 1$, so ist

$$x = n + 1 = n' \in E_{n'} \cup \{n'\}.$$

Ist $y \neq 1$, so folgt mit Satz 5, dass es ein $z \in \mathbf{N}$ gibt mit $y = 1 + z$. Es folgt

$$x = n + 1 + z = n' + z \in E_{n'} \cup \{n'\}.$$

Damit ist alles bewiesen.

Satz 7. *Sind m, $n \in \mathbf{N}$, so ist $E_m \subseteq E_n$ oder $E_n \subseteq E_m$.*

Beweis. Es sei T die Menge der $n \in \mathbf{N}$, für die $E_n \subseteq E_m$ oder $E_m \subseteq E_n$ gilt. Wegen

$$m' = m + 1 = 1 + m \in E_1$$

ist $E_m \subseteq E_1$ nach Satz 6 b) und daher $1 \in T$. Es sei $n \in T$. Ist $n'' \in E_m$, so folgt mit Satz 6 b), dass $E_{n'} \subseteq E_m$ ist, sodass $n' \in T$ gilt. Es sei also $n'' \notin E_m$. Nach Satz 6 a) ist $n' \in E_n$. Ferner ist $n'' = (n+1)' = n+1' \in E_n$. Folglich ist $E_n \not\subseteq E_m$. Wegen $n \in T$ folgt $E_m \subseteq E_n$. Wegen $n' \notin E_n$ ist dann auch $n' \notin E_m$. Nach Satz 6 d) ist

$$E_n = E_{n'} \cup \{n'\}.$$

Hieraus folgt zusammen mit $n' \notin E_m$, dass

$$E_m = E_m \cap E_n = E_m \cap \big(E_{n'} \cup \{n'\}\big) = E_m \cap E_{n'}.$$

ist. Also ist $E_m \subseteq E_{n'}$ und damit $n' \in T$, sodass $T = \mathbf{N}$ ist. Damit ist Satz 7 bewiesen.

Eine fast unmittelbare Folgerung aus Satz 7 ist

Satz 8. *Sind m, $n \in \mathbf{N}$, so gibt es ein $c \in \mathbf{N}$ mit $m + c = n$ oder $n + c = m$, es sei denn, es ist $m = n$.*

Beweis. Wegen Satz 7 dürfen wir o.B.d.A. annehmen, dass $E_n \subseteq E_m$ ist. Wegen $n' \in E_n$ ist dann $n' \in E_m$, sodass es ein $d \in \mathbf{N}$ gibt mit $n' = m + d$. Ist $d = 1$, so folgt $n' = m + 1 = m'$ und damit $n = m$. ist $d \neq 1$, so folgt mit Satz 5, dass es ein $c \in N$ gibt mit $d = c + 1 = c'$. Es folgt

$$n' = m + c' = (m + c)'$$

und weiter $n = m + c$.

Es seien m, $n \in \mathbf{N}$; wir setzen $m < n$, falls es ein $c \in \mathbf{N}$ gibt mit $m + c = n$. Wir setzen $m \leq n$, falls entweder $m = n$ oder $m < n$ ist.

Nach dieser Definition ist

$$E_n = \{x \mid x \in \mathbf{N}, n < x\}.$$

Dies sagt zunächst noch nichts. Die Bedeutung dieses Sachverhalts wird aber durch den nächsten Satz sofort klar.

Satz 9. *Die soeben definierte Relation $\leq$ ist eine lineare Anordnung von $\mathbf{N}$, d.h. es gilt*
a) Es ist $m \leq m$ für alle $m \in \mathbf{N}$.
b) Sind m, $n \in \mathbf{N}$ und gilt $m \leq n$ sowie $n \leq m$, so ist $m = n$.
c) Sind m, n, $p \in \mathbf{N}$ und ist $m \leq n$ und $n \leq p$, so ist $m \leq p$.
d) Sind m, $n \in \mathbf{N}$, so ist $m \leq n$ oder $n \leq m$.

Beweis. a) ist Teil der Definition.

b) Es sei $m \neq n$. Dann ist $m < n$ und $n < m$. Es gibt also c, $d \in \mathbf{N}$ mit $m + c = n$ und $n + d = m$. Es folgt $m + d + c = m$ und weiter

$$m + (d + c)' = (m + d + c)' = m' = m + 1,$$

was wiederum den Widerspruch $1 = (d + c)'$ ergibt. Also ist doch $m = n$.

c) Ist $m = n$ oder $n = p$, so ist nichts zu beweisen. Wir dürfen daher annehmen, dass $m + c = n$ und $n + d = p$ ist mit c, $d \in \mathbf{N}$. Es folgt $m + c + d = p$ und damit $m \leq p$.

d) Dies ist nur eine Umformulierung von Satz 8.

Die Definition von $<$ besagt, dass stets $m < m + n$ gilt, und mit Satz 9 folgt, dass niemals $m + n \leq m$ ist.

Die auf $\mathbf{N}$ etablierte Anordnung ist sogar eine *Wohlordnung*. Dies besagt der nächste Satz.

Satz 10. *Ist X eine nicht leere Teilmenge von $\mathbf{N}$, so gibt es ein kleinstes Element in X, d.h. es gibt ein Element $k \in X$ mit $k \leq x$ für alle $x \in X$.*

Beweis. Für $n \in \mathbf{N}$ setzen wir

$$A_n := \{a \mid a \in \mathbf{N}, a \leq n\}.$$

Dann ist $A_{n+1} = A_n \cup \{n + 1\}$, da es zwischen n und $n + 1$ keine weitere natürliche Zahl gibt. Wir zeigen zunächst, dass für alle $n \in \mathbf{N}$ gilt, dass X ein kleinstes Element enthält, falls nur $A_n \cap X \neq \emptyset$ ist. Es sei T die Menge der natürlichen Zahlen, für die diese Aussage gilt. Dann ist $1 \in T$. Ist nämlich $A_1 \cap X$ nicht leer, so ist $A_1 \cap X = \{1\}$ und 1 ist als kleinstes Element von $\mathbf{N}$ kleinstes Element von X. Es sei $n \in T$ und es gelte $A_{n+1} \cap X \neq \emptyset$. Dann ist

$$\emptyset \neq A_{n+1} \cap X = (A_n \cap X) \cup \big(\{n + 1\} \cap X\big).$$

Ist $A_n \cap X \neq \emptyset$, so enthält X ein kleinstes Element, sodass in diesem Falle $n + 1 \in T$ gilt. Ist $A_n \cap X = \emptyset$, so ist

$$\emptyset \neq A_{n+1} \cap X = \big(\{n + 1\} \cap X\big).$$

Hieraus folgt $n + 1 \in X$. Ist nun $y \in \mathbf{N}$ und $y < n + 1$, so ist $y \in A_n$ und daher $y \notin X$. Es folgt, dass $n + 1$ das kleinste Element von X ist. Also ist auch hier $n + 1 \in T$, sodass $T = \mathbf{N}$ ist.

Weil wir vorausgesetzt haben, dass X nicht leer ist, gibt es ein $n \in X$. Es folgt $n \in A_n \cap X$, sodass X nach dem Bewiesenen ein kleinstes Element enthält. Damit ist der Satz bewiesen.

Der nächste Satz besagt, dass die auf $\mathbf{N}$ definierte Anordnung mit der Addition verträglich ist.

Satz 11. *Sind m, n, $p \in \mathbf{N}$, so gilt genau dann $m \leq n$, wenn $m + p \leq n + p$ ist.*

Beweis. Es sei $m = n$. Dann ist $m + p \leq n + p$ für alle $p \in \mathbf{N}$. Es sei also $m < n$. Dann gibt es ein $c \in \mathbf{N}$ mit $m + c = n$. Es folgt

$$m + p + c = m + c + p = n + p,$$

sodass $m + p < n + p$ ist.

Es sei umgekehrt $m+p \leq n+p$. Wäre $n < m$, so folgte nach dem bereits Bewiesenen der Widerspruch $n + p < m + p \leq n + p$.

Sind a, $b \in \mathbf{N}$ und ist $a < b$, so gibt es genau ein $d \in \mathbf{N}$ mit $a + d = b$. Für dieses d schreiben wir auch $b - a$. Die Gültigkeit der Rechenregeln $c - (a - b) = (c + b) - a$ und $c - (a + b) = (c - a) - b$ möge der Leser selbst nachweisen. Dabei sind die Beweise so zu führen, dass die Operationen niemals aus $\mathbf{N}$ herausführen. Die hier definierte Subtraktion ist ja nur definiert, wenn $a < b$ ist, nur dann wissen wir, was $b-a$ bedeutet.

Addition und partielle Subtraktion sind mittels der *Nachfolgerfunktion* $'$ definiert. Macht man das explizit, so erhält man folgende, nicht sehr effektive Rekursion um Summe und Differenz zu berechnen. Sind m, $n \in \mathbf{N}$, so ist $m + n = m + 1 = m'$, falls $n = 1$ ist, andernfalls ist

$$m + n = (m + 1) + (n - 1).$$

Entsprechend gilt

$$m - n = (m - 1) - (n - 1),$$

falls nur $m > n > 1$ ist.

Und nun zur Multiplikation. Für $a \in \mathbf{N}$ definieren wir die Rekursionsregel R_a durch $R_a(m) := a + m$. Aufgrund des Rekursionssatzes gibt es dann eine Abbildung μ_a von $\mathbf{N}$ in sich mit $\mu_a(1) = a$ und $\mu_a(m') = a + \mu_a(m)$. Setzt man nun $am := \mu_a(m)$, so gilt also $a1 = a$ und $a(m + 1) = a + am$ für alle a, $m \in \mathbf{N}$.

Satz 12. *Die soeben definierte Multiplikation auf $\mathbf{N}$ genügt den folgenden Rechenregeln:*

a) Es ist $a1 = 1a = a$ für alle $a \in \mathbf{N}$.

b) Es ist $a(b + c) = ab + ac$ für alle a, b, $c \in \mathbf{N}$.

c) Es ist $(a + b)c = ac + bc$ für alle a, b, $c \in \mathbf{N}$.

d) Es ist $a(bc) = (ab)c$ für alle a, b, $c \in \mathbf{N}$.

Beweis. a) Die Gültigkeit der Gleichung $a1 = a$ folgt aus der Konstruktion der Multiplikation. Um die Gültigkeit der Gleichung $1a = a$ zu etablieren, machen wir Induktion nach a. Für $a = 1$ gilt diese Gleichung. Sie gelte für a. Dann ist

$$1a' = 1 + 1a = 1 + a = a',$$

sodass sie auch für a' gilt. Also gilt sie für alle $a \in \mathbf{N}$.

b) Hier machen wir Induktion nach c. Für $c = 1$ folgt

$$ab + a1 = a1 + ab = a + ab = ab' = a(b + 1).$$