Erster Abschnitt

Zahlentheorie

1. Zahlentheorie

1.1. Zahlbegriff und Zahlentheorie

Die Fähigkeit des Menschen, Dinge zu zählen und von ihnen losgelöste Zahlbegriffe herauszubilden, scheint erst in historischer Zeit entwickelt zu sein.[1, 2] Die Entwicklung des zum vom Gegenstand lösgelösten Zahlwort (Zahlbegriff) und zur strukturierten Zählreihe verlief über Stufen und war nicht ohne Brüche. Die Tatsache, daß z.B. in den indogermanischen Sprachen drei bzw. in deren ältesten überlieferten Sprachen die ersten vier Numeralia deklinierbar sind, rückt sie in die Nähe der Kategorie des Adjektivs. Außerdem spricht die Flexion von Nomina nach Singular, Dual und Plural ebenso dafür, daß zunächst die quantitative Ausprägung als eine den Dingen selbst zuzuordnende Eigenschaft gedeutet wurde, ohne diese in einem Zahlbegriff zu abstrahieren. Erst die Neuzeit erlebt den Siegszug der indischen Zahlen und der Stellenwertschreibung. Die Aufgabe der Zahlentheorie ist es, Eigenschaften von Zahlen und deren Darstellung zu beschreiben. Erste Anliegen der Zahlentheorie sind die Beschreibung verschiedener Zahlensysteme, die Beschreibung der verschiedenen sogenannten *b-adischen* Stellenwertsysteme als gleichwertige Darstellungsmöglichkeiten additiver und nicht-additiver Zahlensysteme. Das 17. Jahrhundert von dem deutschen Mathematiker *GOTTFRIED WILHELM LEIBNIZ* eingeführte Dualsystem gelangte bei der späteren Entwicklung elektronischer Rechenmaschinen das Dualsystem zu seiner großen Bedeutung für die Informationstechnik. Diese basiert auf einer zweiwertigen Logik, die mit Bits, deren Wert entweder 1 oder 0 ist, arbeitet und die sich in der Digitaltechnik durch elektrische Zustände, bevorzugt durch komplementäre Zustände wie *"Strom an/Strom aus"* oder "*Spannung/Masse"* darstellen lassen. Die durch das Dualsystem dargestellten Zahlen heißen *Dualzahlen* oder *Binärzahlen*. Auf der Theorie der Verbände, Ringe und Körper bauen die arithmetischen Operationen auf. Aus ihr ergeben sich die Lehre von der Teilbarkeit und der Restklassenarithmetik, die Beschreibung von Primzahlen, Primfaktoren und der Hauptsatz der elementaren Zahlentheorie.

[1] Menninger. Karl: Zahlwort und Ziffer. *Eine Kulturgeschichte der Zahl*, 2 Bände, Göttingen 1979

[2] Ifrah, Georges.: Universalgeschichte der Zahlen, Frankfurt am Main 1987

1.1.1. Natürliche Zahlen

Die natürlichen Zahlen werden axiomatisch begründet. Ihre Existenz und Eigenschaften werden durch die PEANO-Axiome[3] gefordert.

1,1,2, Zahlensysteme

Ein Zahlensystem wird zur *Darstellung* von Zahlen verwendet. Eine Zahl wird dabei entsprechend dem Regelsystems (der "*Grammatik*") des jeweiligen Zahlensystems als Folge von Symbolen ("*Ziffern*") dargestellt. Die Mathematik unterscheidet zwischen

- additiven,
- hybriden und
- positionellen Zahlensystemen.

1.1.2.1. Addititive Zahlensysteme (Additionssysteme)

In einem Additionssystem ergibt sich die Zahl als Summe der Werte der verschiedenen Symbole (Ziffern). Dabei spielt die Position der einzelnen Symbole (Ziffern) keine Rolle für deren Wert.

1.1.2.1.1. Additionssysteme

1.1.2.1.1.1 Das Unärsystem

Das *Unärsystem* verwendet ein einziges Symbol zur Darstellung einer Zahl. Ein Beispiel eines solchen Unärsystems ist das *Strichsystem*, in dem die natürliche Zahl n durch n Striche dargestellt wird. Dieses vermutlich älteste Zahlensystem ist bis heute in verschiedenen Alltagssituationen gebräuchlich, erlaubt aber wegen der Umständlichkeit der Zahlendarstellung keine komplexen Berechnungen.

[3] G. Peano, italienischer Mathematiker, vgl. (*in Vorbereitung*)

1.1.2.1.1.2. Entwickelte Additionssysteme

Bereits die ägyptische Sprache verwendete seit dem 3. vorchristlichen Jahrtausends ein Dezimalsystem.[4] Dabei werden verschiedene Symbole (Ziffern) für jede der verschiedenen Potenzen der Basis '10' verwendet. Bereits die hieratischen Hieroglyphenschrift gehorchte dem Prinzip der (im Dezimalsystem) jeweils neun verschiedenen Ziffern für jede verwendete Potenz der Basis. Das Bauprinzip dieses Systems verfügte für jede Potenz der Basis über eine Ziffer, also z. B.: für 10^0 (= 1, in der koptischen Orthographie ⲟⲩⲁ, für 10^1 (= 10, kopt. ⲙⲏⲧ), für 10^2 (= 100, kopt. ϣⲉ), für 10^3 (= 1000, kopt. ϣⲟ) und für 10^4 10000 (= 10000, kopt. ⲧⲃⲁ).[5] Allerdings war das ägyptische Zahlensystem zwar ein Dezimal- aber kein Stellenwertsystem.[6]

Ein weiteres Beispiel eines entwickelten Additionssystems stellen die Römischen Zahlen dar, die neben den lateinischen Buchstaben X, C und M als Symbolen (Ziffern)[7] für die ersten drei Zehnerpotenzen 10, 100 und 1000 auch noch die lateinischen Buchstaben I, V, L und D als Ziffernsymbole für 1, 5, 50 und 500 verwenden.

---

4 vgl. Plisch, Uwe-Karsten: Einführung in die koptische Sprache, Wiesbaden 1999, S. 19–21. Insbesondere zur Darstellung von Brüchen vgl. S. 21.

5 Ein Schwachpunkt des ägyptischen Systems war, dass die fehlende Möglichkeit der Stellenwertschreibung zur Wiederholung des gleichen Zeichens an der jeweiligen 'Stelle' zwang. Daher entwickelten die Ägypter bereits in Mitte des dritten vorchristlichen Jahrtausends hieratisch handschriftlich Techniken der Abkürzung, die den späteren entstandenen alphabetischen Zahlen zum Vorbild gedient haben mochten.

6 Vgl. kopt. ⲥⲉⲩ-(=6), ⲥⲉⲧⲁⲥⲉ (=66) und ⲥⲉⲩϣⲉ ⲥⲉⲧⲁⲥⲉ (=666). Zu den Einzelheiten der Morphologie des koptischen Zahlensystems vgl. U. Plisch, op.cit., S. 20.

7 Dabei dürfte das 'X' ein Relikt einer (älteren) unären Darstellungsweise anzusehen sein, die Symbole C und M dagegen als Kürzel der lateinischen Numeralia *CENTUM* und *MILLE*. Vgl. Menninger, op.cit., Bd. II, S. 46

Die Ziffern werden mit abnehmender Wertigkeit notiert und addiert. Beispiele römischer Zahlen sind:

(1) Die (dezimale) Zahl 1878 wird als *MDCCCLXXVIII* dargestellt.

(2) Die (römische) Zahl *MMCCXIII* besitzt den (dezimalen) Zahlenwert 2213.

(3) Die (römische) Zahl *MCMLIV* besitzt den (dezimalen) Zahlenwert 1954.

Im Beispiel (3) wird sichtbar, daß die Symbole je nach Kontext additiven oder subtraktiven Charakter haben: steht eine kleinere Zahl vor einem größeren Zahlensymbol, z.B. C vor M, wird der Wert des größeren Symbol um den des voranstehenden kleineren Symbols vermindert.[8] Noch im mittelalterlichen Europa war das römische Zahlensystem allgemein verbreitet und wurde erst im 16. Jahrhundert zu Gunsten des indisch-arabischen Stellenwertsystems endgültig aufgegeben.[9]

1.1.2.1.1.3. Hybridsysteme

In Hybridsystemen geht eine Grundzahl einem Zeichen das eine Potenz der Basis wiedergibt, voraus. Beide werden miteinander addiert oder multipliziert. In den europäischen Zahlensystemen sind solche Hybridsysteme selten.[10] Hybridsysteme existierten bereits seit Beginn des zweiten vorchristlichen Jahrtausends unter anderem in Mesopotamien und China. Hybride Systeme existierten auch in Äthiopien, Indien, aber auch in der Maya-Kultur. Mitte des vierten vorchristlichen Jahrhunderts schufen die Griechen, ausgehend von diesen hieratischen Zahlen, die sogenannten alphabetischen Zahlen indem sie die ersten hieratischen Zahlen durch die Buchstaben ih-

---

[8] Grundsätzlich gilt für alle römischen Zahlensymbole: steht ein Symbol mit einem kleinere Wert vor einem Symbol mit einem höheren Wert, so wird der Wert des vorangehenden Symbols von dem Wert des folgenden Symbols abgezogen. Diese nicht ursprüngliche Darstellungstechnik führt zu einer kürzeren Zahlendarstellung: jede Ziffer darf nur noch dreimal hintereinander auftreten. VIIII wird auf diese Weise zu IX. Diese Subtraktionsregel innerhalb des römischen Additionssystems wird aber nicht konsequent angewendet.

[9] Vgl. Menninger, op.cit., S. Bd. 2, 265

[10] Zu erwähnen ist hier das Deutsche. Man betrachte *dreizehn* und *dreißig*.

res Alphabets ersetzten. Diese Art der Zifferndarstellung gelangte auch nach Italien zu den Etruskern.

1.1.2.1.2. Stellenwertsysteme

1.1.2.1.2.1. Zahlendarstellung im Stellenwertsystem

Ein *Stellenwertsystem*[11] ist ein Zahlensystem, das im Vergleich zu Additionssystemen mit wenigen Symbolen große Zahlen als Potenzsummen darstellt. In diesem Zusammenhang wird auch von der ***b-adischen Darstellung von Zahlen***[12] gesprochen. Dabei steht die Variable $b \in \mathbb{N}$ $(b \geqslant 2)$ für die Anzahl der Symbole. Der Wert von b heißt die *Basis* des Zahlensystems. Die als Nennwerte verwendeten Symbole werden als *Ziffern* bzw. *Zahlzeichen* bezeichnet.

Es gibt zwei Arten, die Zifferndarstellung einer Zahl zu betrachten:

- ***einerseits*** als eine von einer Grammatik G erzeugte Folge von Symbolen, d.h. als *Wörter* der Sprache L(G),
- ***andererseits*** als Folge von Zahlen, die diesen Symbolen entsprechen.[13]

Die Zuordnung zwischen Symbolen und Zahlen setzt beide Sichtweisen in eine enge Beziehung.

Die Ziffernfolge stellt den *Zahlenwert* durch eine (endliche oder unendliche) Potenzreihe dar. Im Stellenwertsystem bestimmt die Position den *Wert* der jeweiligen Ziffer. Die niederwertigste Position steht im Allgemeinen rechts. Jede Ziffernposition hat einen Wert, der einer Potenz der Basis b entspricht. Für die *k*-te Position $(k \in \mathbb{N}_0)$ ist dieser Wert das a_k-fache von b^k.

---

[11] *b-adische Systeme* heißen auch auch *Positionssysteme* oder *Polyadische* Zahlensysteme.

[12] Diese sind nicht zu verwechseln mit p-adischen Zahlensystemen!

[13] Für mathematische Anwendungen wie zum Beispiel Teilbarkeitsregeln wird im Allgemeinen die zweite Möglichkeit vorgezogen.

Die Berechnung des Zahlenwertes z_b einer (n+1) - stelligen Zahl $z_b \in \mathbb{N}_0$ in einem Stellenwertsystem mit der Basis b erfolgt durch Multiplikation des i-ten Koeffizienten a_i mit der zugehörigen Potenz b^i und anschließende Summierung der entsprechenden Produkte:

1.1.2.1.2.2. Ziffern

Die b-adische Darstellung einer Zahl verwendet genau b verschiedene Ziffern, mindestens jedoch zwei. Jeder der b Ziffern wird injektiv eine der Zahlen von 0 bis $b - 1$ zugeordnet.[14] Formeln für Ziffern und Operationen mit Ziffern[15] setzen die Teilbarkeitslehre voraus.[16]

---

14 Zur Unterscheidung sind im Folgenden Ziffernsymbole fett und ihre zugehörigen Zahlenwerte normal gesetzt. Beispiele:

- Im Dualsystem mit $b = 2$ werden gewöhnlich die Ziffern **0** und **1** verwendet und ihnen die Zahlen 0 und 1 zugeordnet.
- Im Dezimalsystem ist $b = 10$ und es werden gewöhnlich die 10 Ziffern **0**, **1**, **2**, **3**, **4**, **5**, **6**, **7**, **8** und **9** verwendet und diesen (in dieser Reihenfolge) die Zahlen 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 zugeordnet. Für eine Basis $b < 10$ werden gewöhnlich die ersten b Ziffern analog zum Dezimalsystem verwendet. Für $b > 10$ werden gewöhnlich zusätzlich zu den Ziffern des Dezimalsystems Buchstaben als weitere Ziffern eingesetzt. Beispielsweise werden im Hexadezimalsystem mit b = '16' zusätzlich die Ziffern **A**, **B**, **C**, **D**, **E** und **F** verwendet und diesen (wieder in dieser Reihenfolge) die Zahlen '10', '11', '12', '13', '14' und '15' zugeordnet.

15 Die letzte Ziffer der b-adischen Darstellung einer natürlichen Zahl n ist der Rest von n bei Division durch b. Dieser Rest ist auch durch den Ausdruck

$$(1) \quad n - b \left\lfloor {}^{n}/_{b} \right\rfloor$$

gegeben. Die Zahl '7' hätte im 5er-System die Darstellung 12_5. Die letzte Ziffer wäre dann nach (1) gleich

1.1.2.1.2.3. Darstellung natürlicher Zahlen

Eine natürliche Zahl $n \in \mathbb{N}$ wird in der *b*-adischen Darstellung durch eine (endliche) Folge

(1) $< a_n > = a_0, a_1, a_2, \ldots, a_n$

---

(2) $7 - 5 * \lfloor 7/5 \rfloor = 7 - 5*1 = 2$

Allgemein ist die durch die letzten *k* Ziffern von *n* gebildete Zahl der Rest von *n* bei Division durch b^k. Die *k*-te Ziffer (von rechts mit null beginnend gezählt) einer natürlichen Zahl *n* ist

(3) $\lfloor n/b^k \rfloor - b \lfloor n/b^{k+1} \rfloor$

gegeben. Die Zahl '7' hätte im 5er-System die Darstellung 12_5. Die zweite Ziffer wäre dann nach (3) gleich

(4) $\lfloor 27/5^2 \rfloor - 5 * \lfloor 27/5^3 \rfloor = 1 - 5*0 = 1$

Treten in (3) negative Exponenten *k* auf, so ergibt sich in (4) die entsprechende Nachkommastelle. Die Anzahl i der Ziffern der *b*-adischen Darstellung einer natürlichen Zahl *n* ist

(5) $i = \lfloor \ln(n)/\ln(5) \rfloor + 1$

Für 7_5 gilt also

(6) $i = \lfloor \ln(7)/\ln(5) \rfloor + 1 = 1 + 1 = 2$

[16] s. Zweiter Abschnit: *"Teilbarkeit"*

von Ziffern $a_i \in \{0, 1, ..., b-1\}$ dargestellt. Die traditionelle Darstellungskonvention ist allerdings der folgende von rechts nach links geordnete Ausdruck:

(2) $$a_n a_{n-1} a_{n-2,} \ldots a_0$$

Der Folge (1) wird nun die Zahl

(3) $$z_b = \sum_{i=n}^{0} a_i\, b^i = a_n\, b^n + a_{n-1} b^{n-1} + \ldots + a_0\, b^0$$

mit $a_i \in \{ 0, 1, ... b-1 \}$ zugeordnet.[17] Der Zahlenwert z_b ergibt sich in (3) also durch Summierung der Reihe aller mit ihrem jeweiligen *Stellenwert* multiplizierten Ziffernwerte.

1.1.2.1.2.4. Basen und Exponenten der Zahlensysteme

Mit der Beschränkung des niedrigsten Exponenten auf 0 kann man nur natürliche Zahlen darstellen. Läßt man auch negative Exponenten zu, dann lassen sich mit dem Stellenwertsystem auch rationale und reelle Zahlen darstellen. Auch muß die Basis b des Stellenwertsystems nicht notwendigerweise eine natürliche Zahl sein. Jede kom-

[17] Es läßt sich zeigen, daß zu jeder natürlichen Zahl n eine Folge von Ziffern existiert, deren zugeordneter Wert n ist. Man kann beliebig oft die Ziffer **0** = 0 anfügen (d.h. in der Schreibweise (2) voranstellen). Werden Folgen, die mit der Ziffer **0** enden (in der Schreibweise (2) mit führender **0**) nicht zugelassen, dann ist diese Zuordnung sogar eineindeutig. Das heißt, zu jeder natürlichen Zahl n existiert genau eine Folge, deren zugeordneter Wert n ist. Allerdings wird der Zahl 0 nicht die leere Folge ohne Folgenglied zugeordnet, sondern die Folge, die genau aus einem Folgenglied, und zwar der Ziffer besteht, der der Wert 0 zugeordnet wird (also **0**).

plexe Zahl c mit | c | > 1 kann als Basis eines Stellenwertsystems verwendet werden.

1.1.2.1.2.5. Darstellung ganzer Zahlen

Die ganze Zahl $z \in \mathbb{Z}$ wird wie eine natürliche Zahl durch endliche Ziffernfolgen dargestellt. Diesen wird das Symbol *signum(z)* vorangestellt. Negativen Zahlen wird der *Signum*-Wert "**-**" als Symbol vorangestellt. Darstellungen von von Null verschiedenen Zahlen, denen kein Minuszeichen vorangestellt wird, werden als positive Zahlen interpretiert. Der Ziffernfolge wird nun die negative Zahl z wie folgt zugeordnet:

$$(4) \qquad z_b = (-1) \sum_{i=n}^{0} a_i\, b^i = a_n\, b^n + a_{n-1} b^{n-1} + \ldots + a_0\, b^0$$

mit $a_i \in \{ 0, 1, \ldots b-1 \}$ zugeordnet. Der Zahlenwert z_b ergibt sich in (4) also durch Multiplikation des Vorzeichnens *signum*(z) mit dem Summenwert der Reihe aller mit ihrem jeweiligen *Stellenwert* multiplizierten Ziffernwerte.

1.1.2.1.2.6. Darstellung rationaler Zahlen

Läßt man auch negative Exponenten $i < 0$ zu, kann man auch rationale Zahlen in einem Stellenwertsystem b-adisch darstellen. Eine *rationale* Zahl $z \in \mathbb{Q}$ hat dann die Form

$$(5) \qquad a_n\, b^n + \ldots + a_1\, b^1 + a_0\, b^0 + a_{-1}\, b^{-1} \ldots + a_{-m}\, b^{-m}$$

Dabei markiert ein Trennzeichen[18] den Übergang vom nichtnegativen zum negativen Exponenten.[19] Der Exponent gibt *-i* die Position nach dem Komma an.
Der Reihe (5) wird nun die Zahl

$$z_b = \text{signum}(z) \sum_{I=n}^{-m} a_i\, b^i \tag{6}$$

$$= \text{signum}(z)\,(a_n\, b^n + \ldots + a_1\, b^1 + a_0\, b^0 + a_{-1}\, b^{-1} \ldots + a_{-m}\, b^{-m})$$

mit a_n, $a_{-m} \in \{ 0, 1, \ldots b-1 \}$ und $n \in \mathbf{N}_0$, $m \in \mathbf{N}$ zugeordnet. Der Zahlenwert z_b ergibt sich in (6) also wiederum durch Multiplikation des Vorzeichnens *signum(z)* mit dem Summenwert der Reihe aller mit ihrem jeweiligen *Stellenwert* multiplizierten Ziffernwerte.

1.1.2.1.2.7. Darstellung reeller Zahlen

Die Darstellung reeller Zahlen erfolgt ebenso so wie die Darstellung rationaler Zahlen durch b-adische Entwicklung. Liefert die b-adische Entwicklung im Falle rationaler Zahlen möglicherweise eine endliche Ziffernfolge, so ergibt die b-adische Entwicklung einer irrationalen Zahl dagegen grundsätzlich eine unendliche und nicht-periodische Ziffernfolge. Unter einer *b-adischen Darstellung einer reellen Zahl* ist folglich die bei der b-adischen Entwicklung entstehende Ziffernfolge zu verstehen, durch die dann jede reelle Zahl als (unter Umständen unendlicher) b-adischer Bruch angenähert wird.

[18] Im deutschen Sprachraum wird als Trennzeichen in der Regel das Dezimalkomma ",", im englischsprachigen Raum dagegen der Dezimalpunkt "." verwendet.

[19] Eine andere Darstellung für rationale und irrationale Zahlen ist der Kettenbruch, welcher bessere Approximationen liefert als die Stellenwertsysteme.

1.1.2.1.2.8. Verallgemeinerung

Für solche verallgemeinerten Stellenwertsysteme gelten einige der hier gemachten Aussagen über die endliche Darstellbarkeit rationaler und reeller Zahlen nicht. Dies gilt es später zu untersuchen.[20]

[20] *(in Vorbereitung)*