Hamburger Beiträge zur Mathematik

Nr. 428, Dezember 2011

Über Addition und Multiplikation

von Ernst Kleinert

Über Addition und Multiplikation

von Ernst Kleinert

1

Unter den (nicht-logischen) Grundbegriffen, mit denen wir unsere Erfahrung beschreiben, ist derjenige der Quantität einer der am meisten fundamentalen, von Aristoteles und Kant mit Recht in den Rang des Kategorialen gerückt. Diskrete Quantität, oder Anzahl, ist schon beteiligt, wo wir überhaupt einzelne Erfahrungsinhalte unterscheiden. Kontinuierliche Quantität ist, in ihrer extensiven Form, bei jeder räumlichen Wahrnehmung beteiligt, als Ausdehnung in verschiedenen Richtungen, bei jedem zeitlichen Erleben als Dauer; in ihrer intensiven Form kommt sie jeder Empfindung zu, als Grad oder Stärke [1].

Addition und Multiplikation sind Operationen, mit denen wir Quantitäten theoretisch bearbeiten; zusammen mit ihren Umkehrungen konstituieren sie, was man die vier Grundrechenarten nennt. Wir fragen nach ihren Ursprüngen, nach ihrem Verhältnis zueinander, und warum es keine weiteren Basisoperationen algebraischer Natur gibt. Letzte Antworten können nicht erwartet werden, allein schon deshalb, weil die mathematische Arbeit nicht abgeschlossen ist, früher oder später auch neue Grundbegriffe hervorbringen wird, von denen dann neues Licht auf die Verhältnisse fällt. Einem so tiefen Gewässer kann man höchstens dann auf den Grund schauen, wenn es zum Stehen gekommen ist. Jedoch weckt die Vielfalt des Erreichten das Bedürfnis nach einem Überblick, auch wenn dieser nur vorläufig und unvollständig sein kann. Ein solcher soll hier unternommen werden, dazu ein paar Gedanken zur Interpretation.

2

Jede Änderung von Quantität ist Vermehrung oder Verminderung; es gibt „strukturell“ betrachtet nur *eine* Art der Veränderung (und ihre Umkehrung). Diese triviale Feststellung beleuchtet die Sonderstellung der Quantität im gesamten theoretischen Agieren: sie ist am leichtesten (theoretisch) zu bearbeiten. Ein erster mathematischer Reflex davon ist, daß die einschlägigen mathematischen Objekte, linear (oder total) geordnete Mengen, „zuviele“ Endomorphismen haben, was immer auf „schwache Struktur“ hinweist; zum Beispiel können sie fast beliebig deformiert werden; jede monoton wachsende Funktion von $\mathbb{R}$ in sich ist ein Endomorphismus von $(\mathbb{R}, \leq)$, jede abgeschlossene Teilmenge ein mögliches Bild. Ein zweiter ist formallogischer Natur: die Theorie der natürlichen Zahlen nur mit der Anordnung (oder nur mit der Addition) ist entscheidbar [2].

Dagegen kann sich alles, was die Sinne uns sonst bieten, Wahrnehmung von Farbe und Gestalt, Klang und Rhythmus, Empfindung von Druck und Festigkeit, Geschmack und Geruch, in mannigfacher Weise ändern, die Möglichkeiten der Änderung bilden selbst Kontinua (vor allem bei Gestalt und Klang). Überall finden sich dabei, in verschiedenen Hinsichten, diskrete und kontinuierliche Quantitäten. Weil alles Erkennen ein Beziehen ist, die einfachsten Beziehungen aber die zwischen Größen sind, ist es eine natürliche

Tendenz des theoretischen Agierens, möglichst viele Verhältnisse in quantitative zu übersetzen, möglichst viel von Eigenart, Struktur, „Wesen“ der Dinge quantitativ zu fassen. Der Geldwert von Dingen ist das verbreitetste Beispiel; auf andere werden wir zu sprechen kommen.

Im folgenden werden wir nur von extensiver Quantität handeln. Mit intensiven Größen ist schlecht rechnen, vor allem Addition scheint unangemessen; mehr Licht entsteht nicht, indem man neben eine trübe Lampe eine zweite stellt. Vermehrung, besser Steigerung intensiver Quantität denken wir eher als Multiplikation (ganz trivial: „Sonnenschutz Faktor 10“), und sie wird leicht als Umschlag in der Qualität empfunden. Etwas steigern ist ein Anderes, und meistens schwerer, als es zu vergrößern (man denke an das Weber-Fechnersche Gesetz). Wo es davon Mathematik gibt, wird sie eher kombinatorischer Art sein.

3

Ein Quantum ändert sich durch Wachstum oder Schrumpfung oder andere „natürliche“ Prozesse, oder aber durch Wegnehmen oder Hinzufügen eines gleichartigen Quantums. Nur das zweite ist mathematischer Betrachtung zunächst zugänglich. Die heutige Mathematik macht daraus eine binäre, assoziative und kommutative Operation auf der Menge der Quanta. Auf Binarität kann man sich beschränken, weil sich jede endliche Zusammensetzung als Sukzession von binären denken läßt, meistens auch so stattfindet; wo das nicht der Fall ist, wie beim Zusammenstellen von drei Zeltstangen, wird es nicht um Quantität allein gehen, sondern wesentlich um andere Struktur. Die Kommutativität ist schon eine stärkere Idealisierung, denn es kommt nicht selten vor, daß die Reihenfolge beim Hinzufügen oder Wegnehmen durchaus eine Rolle spielt; für die erste mathematische Betrachtung ist sie aber gleichgültig, da es in ihr nur um das entstehende neue Quantum gehen kann. Bei der Assoziativität ist die Sachlage komplizierter, findet aber letztlich dieselbe Rechtfertigung; die Gruppierung einer Sukzession von Zusammensetzungen in ein Aggregat von binären (ohne Eingriff in die Reihenfolge) ändert „prinzipiell“ nichts am Resultat [3]. Eine weitere Idealisierung liegt in einer gewissen Homogenitätseigenschaft, die man der Menge der Quanta unterlegt, wenn man sie als kommutative Halbgruppe denkt: jedes Element kann überall angefügt werden; realiter ist das Zusammenfügen meist nur partiell definiert.

4

Die Addition hat also ihren Ursprung in einer Klasse elementarer Handlungen, wie sie jedem aus dem Alltag geläufig sind. Für die Multiplikation finden wir solche nicht ohne weiteres, selbst wenn wir sie zunächst nur als Vervielfachung ansehen, also einen Spezialfall, genauer eine Abkürzung von Addition. Betrachten wir das einfachste denkbare Beispiel. Wenn man eine Gesellschaft verköstigen will, kann man Lebensmittel herbeischaffen, bis jeder genug hat. Dieses Verfahren bedarf keiner theoretischen Aktion (nicht einmal ein Zahlbegriff wird vorausgesetzt) und findet ja auch im Tierreich statt, etwa wenn ein Vogel seine Jungen füttert. Auch Tiere operieren mit Quantitäten, wobei sich entweder aus der Situation selbst ergibt, wann „es genug ist“, oder aber im Instinkt, der die Handlung leitet, auch bestimmte Quanta festgelegt sind. Das andere Verfahren ist,

die Zahl der Esser zu ermitteln, für jeden eine Portion zu veranschlagen und ein entsprechendes Quantum zu besorgen; hier ist der Zahlbegriff offensichtlich unentbehrlich, auch wenn er nur in seiner einfachsten Funktion auftritt (nämlich bijektive Beziehbarkeit von Mengen durch ihre Anzahl auszudrücken). Addition ist, als mathematischer, natürlich auch ein theoretischer Akt, aber er ist eine einfache Abstraktion aus einer konkreten Handlung. Multiplikation dagegen, auch wo sie nur als abgekürzte Addition auftritt, setzt mindestens die Bestimmung einer Einheit voraus, und dieser theoretische Akt ist keine Abstraktion, sondern ein Eingriff des theoretischen Agierens; in unserm Beispiel bedeutet er, bei aller Simplizität, die Unterlegung eines mathematischen Modells. Wir schreiben einem Tier nicht die Fähigkeit zu, Größen zu Gegenständen eines Kalküls zu machen, obwohl natürlich unsere theoretische Rekonstruktion manchen tierischen Verhaltens ein solches „als ob“ substituieren muß.

5

Multiplikative Struktur hat aber noch einen andern Ursprung, der von Addition, selbst vom Zahlbegriff unabhängig ist und im Begriff der Proportion bezeichnet wird. In gewissem Sinne ist die Wahrnehmung von Größer und Kleiner überhaupt an Proportion geknüpft, denn daß etwas größer wird, sehen wir nur dadurch, daß ein Anderes nicht größer wird, also eine Proportion sich ändert. Der multiplikative Charakter von Proportion ist evident; Veränderung von Proportion denken wir nicht als Addition (obwohl sie natürlich durch solche zustandekommen kann), sondern als Multiplikation (geometrisch als Dilatation einzelner Längen, aber mit verschiedenen Faktoren; bei gleicher Veränderung aller Längen bleibt Proportion gerade unverändert). Das Gewahrwerden von Proportion, der Umgang mit und die Arbeit an Proportionen geht der mathematischen Betrachtung weit voran; vor aller Mathematik erreichten Skulptur und Architektur höchste Grade proportionaler Verfeinerung (und nicht allein in Griechenland). Ein Wesen aber, das auf theoretische Aktion angewiesen ist, kann nicht beim bloß additiven, sozusagen naiven Umgang mit Größen stehen bleiben, sondern braucht eine Wissenschaft von den Verhältnissen zwischen Größen.

Das einfachste solche Verhältnis ist dasjenige, das von Größen gleicher Art konstituiert wird. Als erster hat Eudoxos erkannt, wie sich Proportion auf ganzzahlige Vervielfachung und damit auf Addition zurückführen läßt, und damit ein frühes Beispiel für die Reduktion von Qualität auf Quantität gegeben. Zwei Paare (a,b) und (c,d) gleichartiger Größen bestimmen dieselbe Proportion, wenn für alle natürlichen m und n gilt:

$$ma \leq nb \quad (ma \geq nb) \text{ genau dann, wenn } mc \leq nd \quad (mc \geq nd).$$

Für uns sind Proportionen reelle Zahlen r = a:b, s = c:d, und die Definition sagt einfach, daß r = s ist, wenn die rationalen Zahlen n:m , die kleiner (größer) als r sind, auch kleiner (größer) als s sind, was richtig ist, weil zwischen zwei verschiedenen reellen Zahlen eine rationale Zahl liegt ($\mathbb{Q}$ liegt „dicht“ in $\mathbb{R}$). Die Definition läßt übrigens die Möglichkeit offen, daß die beiden Paare verschiedenen Größenarten angehören, so daß sich zum Beispiel zwei Längen zueinander verhalten können wie zwei Zeitabschnitte.

6

Der Gedanke, daß es sinnvoll sein kann, auch Quanta verschiedener Art zu vergleichen, führt zu einer weiteren Quelle multiplikativer Struktur, einen „abstrakteren“ Begriff von Proportion, der nicht auf Addition zurückgeführt werden kann. Es ist anschaulich evident, daß die Fläche eines Rechtecks proportional zu den beiden Seitenlängen ist; von da ist es nur ein Schritt zur Festlegung eines Flächenmaßes als Produkt von Längenmaßen, und entsprechend für ein Raummaß. Wir wissen nicht, wann und wo dieser Schritt zum erstenmal getan wurde; die griechische Mathematik hat ihn jedenfalls von Anfang an hinter sich. Ähnlich naheliegend ist der Gedanke, daß zurückgelegte Strecke, dividiert durch die Dauer der Bewegung, als Maß für die Geschwindigkeit dienen kann. Mit diesem Gedanken hat erst die neuzeitliche Mechanik ernst gemacht und in der Folge alle physikalischen Grundbegriffe auf Länge, Masse und Zeit zurückgeführt, zunächst Beschleunigung als Änderung der Geschwindigkeit, dividiert durch die Dauer der Änderung, sodann Kraft als Masse $\times$ Beschleunigung, Arbeit als Kraft $\times$ Weg, Druck als Kraft pro Fläche usw. Das cgs-System ist eine rein multiplikativ formulierte physikalische Dimensionstheorie, ein Begriff wie „Kilowattstunde“ ist schon sprachlich von sozusagen multiplikativer Struktur. Länge und Dauer zu addieren, ergibt keinen Sinn, wohl aber sie zu multiplizieren oder zu dividieren; addieren kann man nur Quanta derselben Dimension. Natürlich kommen nicht alle Potenzprodukte von c, g und s vor; aber das System leistet eine Quantifizierung von Eigenschaften, denen man diese Möglichkeit nicht ohne weiteres ansieht, wie Dichte, Viskosität oder Leitfähigkeit.

Die griechische Proportionenlehre, dieser erste ernsthafte Griff der Mathematik nach dem Kontinuum, hätte dafür den mathematischen Boden abgeben können, aber erst nach zwei Erweiterungen. Die erste hätte sein müssen, Proportionen auch für Größen verschiedener Arten zu definieren; das setzt voraus, für jede Art eine Maßeinheit festzulegen, statt der Quanta nur die Maßzahlen zu betrachten und die Proportionen als Quotienten dieser Maßzahlen. Das ist auch die Voraussetzung für den zweiten Schritt, nämlich für die Proportionen Rechenoperationen wie für Zahlen einzuführen, schließlich die Zahlen selbst als spezielle Proportionen aufzufassen und damit das umfassende, „rechenfähige“ System abstrakter Größen zu schaffen, das uns heute als reelles Zahlsystem geläufig ist. Aus unserer Sicht erscheinen diese Schritte „natürlich“; sie schaffen die Synthese der beiden Quellen multiplikativer Struktur, Organisation von Addition sowie Proportion. Aber die Griechen haben offenbar die Proportionen mehr als an sich und zeitlos Bestehendes angesehen (nur von solchem kann es nach griechischer Auffassung Wissenschaft geben), nicht als Objekte eines Kalküls und schon gar nicht als Operatoren, während „Zahl“ immer „natürliche Zahl“ blieb und in der Proportionenlehre nur als Faktor der Vervielfachung auftritt. Das zeigt, nebenbei gesagt, wie wenig selbstverständlich die Verrechnung der Welt ist, an die wir uns gewöhnt haben[4].

7

Von verschiedenen Seiten haben wir nun schon die fundamentale Asymmetrie zwischen additiver und multiplikativer Struktur in den Blick bekommen: diese ist die „mehr theoretische“ von beiden. Mit konkreten Quanta kann man nur additiv umgehen; die Multiplikation, selbst wo sie als abgekürzte Addition erscheint, ist genau besehen eine

Operation auf der Addition, nämlich eine bestimmte Art ihrer Organisation, und setzt immer einen theoretischen Akt voraus, die Setzung einer Anzahl oder eines bestimmten Quantums als neuer Einheit. Wir finden ein Gleiches beim zweiten Basisbeispiel eines Paars von Operationen additiven und multiplikativen Charakters, das der Geometrie entstammt. Der Addition entspricht die Translation, der Multiplikation die linearen affinen Operationen, die man in Dilatation, Rotation und Spiegelung aufteilen kann. Auch hier ist der theoretisch höhere Charakter der multiplikativen Operationen erkennbar: während Translation, als einfache Bewegung eines Punkts nach einem andern auf dem kürzesten Wege, keiner Vorüberlegung bedarf, setzt Dilatation die Wahl eines Nullpunkts, Rotation die einer Achse und Spiegelung die eines Zentrums voraus, alles Vorentwürfe zur Handlung, also theoretisches Agieren.

Der einfachste Reflex dieses „mehr theoretischen" Charakters der Multiplikation ist, daß sie schwieriger zu lernen war und auch die schwierigere Operation bleibt. Man kommt mit kleinen Faktoren leichter zu großen Zahlen, aber um den Preis höherer algorithmischer Komplexität; die Addition 621 + 185 ist leichter „im Kopf" auszuführen als die Multiplikation 31 $\times$ 26, obwohl beide dasselbe Ergebnis liefern. Noch mehr gilt das für die inversen Operationen: Subtraktion ist kaum schwieriger als Addition, Division aber deutlich schwieriger als Multiplikation; die Geometrie zeigt es durch den Unterschied zwischen der Geraden $x \to ax$ und der Hyperbel $x \to a/x$. Die numerische Mathematik präzisiert die größere Zahl der elementaren Operationen, den höheren Bedarf an Speicherplatz (was beides man schon an unserm kleinen Beispiel sieht), die stärkere Fortpflanzung von Fehlern: sind die Größen A und B mit Fehlern ΔA, ΔB behaftet, hat die Summe A + B den Fehler $\Delta A + \Delta B$, das Produkt aber den Fehler $A\Delta B + B\Delta A + \Delta A\Delta B$. Geometrische Veranschaulichung der Addition braucht nur eine Dimension, für die Multiplikation aber werden zwei benötigt. In der axiomatischen Mengentheorie ist die Definition der Vereinigungsmenge leicht; die Konstruktion der Produktmenge erfordert einen Kunstgriff. Schließlich zeigt die mathematische Logik, welch qualitativer Schritt mit der Einführung der Multiplikation vollzogen wird: während, wie wir schon erwähnt haben, die Theorie von $(\mathbb{N}, +)$ entscheidbar ist, gilt für die volle Peanoarithmetik der Unvollständigkeitssatz von Gödel.

8

Wir wollen nun näher sehen, wie sich dieses Grundverhältnis mathematisch weiter auswirkt, und beginnen mit dem Standardaufbau des Zahlensystems. Zugrunde liegt eine Menge, die wir $\mathbb{N}$ und deren Elemente wir „natürliche Zahlen" nennen, mit einem ausgezeichneten Element, 1 genannt, und einer injektiven Selbstabbildung $s: \mathbb{N} \to \mathbb{N}$, der Nachfolgerabbildung, derart, daß 1 nicht im Bild von s liegt und das Induktionsaxiom erfüllt ist: ist $M \subset \mathbb{N}$ eine Teilmenge mit $1 \in M$ und $s(M) \subset M$, so ist $M = \mathbb{N}$. Dies präzisiert die Intuition, daß man von der Eins ausgehend jede Zahl durch sukzessive Anwendung von s erreicht. Die Existenz eines solchen Tripels ($\mathbb{N}$, 1, s) wird durch die üblichen Mengenaxiome garantiert; der Rekursionssatz von Dedekind sagt, daß es bis auf einschlägige Isomorphie eindeutig bestimmt ist [5]. Der Rekursionssatz erlaubt (daher sein Name) die rekursive Definition von Funktionen auf $\mathbb{N}$ mit Werten in beliebigen andern solchen Tripeln, und seine erste Anwendung ist die Definition von Addition und Multiplikation der Zahlen. Bei festem m definiert man m + n durch

$$m + 1 = s(m) \quad \text{sowie} \quad m + s(n) = s(m + n) = (m + n) + 1$$

und nach demselben Schema das Produkt $m \times n$ durch

$$m \times 1 = m,\ m \times s(n) = m \times n + m\ .$$

Da m beliebig war, sind somit binäre Operationen $+, \times : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ durch die unäre Operation s definiert; die üblichen Rechenregeln werden nun induktiv verifiziert. Die Multiplikation ist damit auf die Addition und diese auf die Nachfolgerabbildung s zurückgeführt. Ersichtlich ist die Reihenfolge nicht umkehrbar: während Addition und Nachfolgerabbildung gleichwertig sind (man braucht ja nur die Gleichung $m + 1 = s(m)$ von rechts nach links zu lesen), kann man nicht die Multiplikation direkt aus der Nachfolgerabbildung ableiten; ein neuer Aspekt ihres „theoretisch späteren" Charakters, der fundamentalen Asymmetrie.

In einer andern Hinsicht verhält sich die multiplikative Struktur zur additiven wie diese zur Nachfolgestruktur: man zeigt leicht, daß in der Kategorie der Mengen mit einer Selbstabbildung

$$\text{End}\,(\mathbb{N}, s) \simeq (\mathbb{N}_0, +) \qquad (\text{mit } \mathbb{N}_0 = \mathbb{N} \cup \{0\})$$

gilt; jede Abbildung $f: \mathbb{N} \to \mathbb{N}$ mit $f\,s = s\,f$ ist eine Addition (ist $f(1) = 1 + a$, so ist $f(n) = n + a$ für alle n), und analog ist jede additive Abbildung $f: \mathbb{N} \to \mathbb{N}$ eine Multiplikation (ist $f(1) = a$, so ist $f(n) = an$ für alle n). Hier muß nun beachtet werden, daß $\text{End}\,(\mathbb{N}, +)$ als Endomorphismenmenge einer kommutativen Halbgruppe die Struktur eines Halb*rings* hat, mit der wertweisen Verknüpfung als Addition und der Hintereinanderausführung als Multiplikation; damit ergibt sich vermöge der Abbildung $a \to (n \to an)$ ein Isomorphismus

$$\text{End}\,(\mathbb{N}, +) \simeq (\mathbb{N}, +, \times)$$

von Halbringen. Die multiplikative Halbgruppe operiert auf der additiven; naive Umkehrung dieser Beziehung würde die duale Distributivität

$$a + (b \times c) = (a + b) \times (a + c)$$

erfordern, die falsch ist („Multiplikation bindet stärker als Addition"), allgemeiner in beliebigen Ringen R schnell zu $R = \{0\}$ führt. Die Booleschen Algebren zeigen, daß auf einer Menge sehr wohl wechselseitig distributive, dabei kommutative monoidale Strukturen bestehen können, aber keine kann eine Gruppenstruktur sein [6]. Jedoch operiert die additive Halbgruppe auf der multiplikativen durch Potenzbildung, und die Regeln der Potenzrechnung lassen sich zusammenfassen zu der Aussage, daß die Abbildung, die jedem n die Potenzierung mit n zuordnet, einen Homomorphismus von $(\mathbb{N}_0, +, \times)$ in $\text{End}\,(\mathbb{N}, \times)$, der natürlich injektiv ist und als Bild gerade das Zentrum des Halbrings $\text{End}\,(\mathbb{N}, \times)$ hat (wie gleich klar werden wird),

$$Z(\text{End}\,(\mathbb{N}, \times)) \simeq (\mathbb{N}_0, +, \times)$$

(die 0 muß hinzugenommen werden, weil ($\mathbb{N}$, $\times$) ein Einselement hat und damit den trivialen Endomorphimus, der alles auf 1 abbildet).

9

Bemerkenswert ist nun, daß diese reichhaltigen, in ihrer wechselseitigen Verwobenheit geradezu dialektisch zu nennenden operativen Verhältnisse beim nächsten Schritt abbrechen. Zunächst folgt aus der Primzerlegung der natürlichen Zahlen, daß ($\mathbb{N}$, $\times$) eine unendliche direkte Summe von Kopien von ($\mathbb{N}_0$, +) ist, der Halbring der Endomorphismen von ($\mathbb{N}$, $\times$) sich darum identifizieren läßt mit dem Halbring der unendlich-dimensionalen Matrizen mit Koeffizienten aus $\mathbb{N}_0$, die in jeder Spalte nur endlich oft von Null verschieden sind [8]; sein Zentrum besteht aus den Skalarmatrizen. Andererseits führt die Fortsetzung des rekursiven Definitionsschemas zu

$$m \circ s(n) = (m \circ n) \times m ,$$

mit der Normierung $m \circ 1 = m$ also zur exponentiellen Struktur $m \circ n = m^n$. Während die Exponentialfunktion (bei fester Basis) eine schwer zu überschätzende Bedeutung hat (sie wird auch uns noch begegnen), scheint die *binäre* exponentielle Struktur kaum eine Rolle zu spielen. Der nächstliegende Grund ist wohl der, daß sie keine physikalische Interpretation hat. Während man Quanta gleicher Art addieren und subtrahieren, im cgs-System auch Quanta verschiedener Art multiplizieren und dividieren kann, hat eine Exponentiation physikalischer Dimensionen keinen greifbaren Sinn. Ein weiterer naheliegender Grund ist, daß die $\circ$ - Produkte sehr schnell sehr groß werden; in der Tat so groß, daß sie keine physikalische Bedeutung mehr haben können. Das würde ihre Brauchbarkeit für theoretische Zwecke der Mathematik nicht ausschließen. Aber die exponentielle Struktur steht abseits aller geläufigen Strukturen; obwohl aus der multiplikativen Struktur in natürlicher Weise hervorgehend, weist sie keinen „brauchbaren“ Bezug zu ihr auf. Zunächst ist sie weder kommutativ noch assoziativ, sogar in einem strikten Sinn, indem nämlich die Gleichungen

$$m \circ n = n \circ m \quad \text{und} \quad (k \circ n) \circ m = k \circ (n \circ m)$$

nur in ein paar Trivialfällen gelten. Nur die Relationen

$$(k \circ n) \circ m = (k \circ m) \circ n \quad \text{und} \quad (...(k \circ n) \circ n) ....) \circ n = k \circ (n \circ m)$$

wobei in der zweiten links m Faktoren n stehen, habe ich finden können [9] . Sei A ein Monoid und f ein Morphismus ($\mathbb{N}$, $\circ$) $\rightarrow$ A. Wegen

$$n \circ 1 = n, \quad 1 \circ n = 1$$

gilt notwendig

$$f(1) = f(1)f(n), \; f(n) = f(n)f(1) = f(n)f(1)f(n) = f(n)f(1)f(n)f(1) ,$$

damit ist $f(n) = f(n)f(1)$ idempotent. Gilt in A die Kürzungsregel, folgt $f \equiv 1$; daher kann $(\mathbb{N}, \circ)$ auf keiner Struktur, gleich welcher Art, durch Automorphismen operieren, aber auch nicht z.B. auf $(\mathbb{N}, +)$. Die Abbildung, die der Zahl n die Potenzierung mit n zuordnet, ist auch kein Morphismus $(\mathbb{N}, \circ) \rightarrow \mathrm{End}\,(\mathbb{N}, \times)$, denn das würde die Gleichung

$$m \circ (n \circ k) = (m \circ n) \circ k$$

erfordern, die Bedingung dafür, daß die operierende Struktur durch die Operation „dargestellt" wird. Nur „schwache" Operationen von $(\mathbb{N}, \circ)$ auf $(\mathbb{N}, \times)$ lassen sich vermittels geeigneter Idempotente konstruieren, worauf aber hier nicht weiter eingegangen werden soll.

Am merkwürdigsten ist vielleicht, daß unsere exponentielle Struktur auch keine nichttrivialen Endomorphismen hat, damit in besonderer Weise „rigide" ist, ohne Symmetrien (wie übrigens auch $(\mathbb{N}, +, \times)$ selbst). Ist nämlich $f: \mathbb{N} \rightarrow \mathbb{N}$ eine Funktion mit

$$f(m \circ n) = f(m) \circ f(n),$$

so muß wegen $(m \circ n) \circ k = m \circ (nk)$ (wir schreiben jetzt wie üblich $n \times k = nk$) auch

$$(f(m) \circ f(n)) \circ f(k) = f(m) \circ f(nk)$$

gelten, was $f(m) = 1$ oder $f(n)f(k) = f(nk)$ erzwingt. Ist also f nicht $\equiv 1$, ist f multiplikativ. Ist $f(m) \neq 1$, folgt weiter für beliebiges n die Gleichung

$$f(m) \circ n = f(m \circ n) = f(m) \circ f(n)$$

und damit $f(n) = n$ und $f = \mathrm{id}$. Die exponentielle Struktur ist nicht nur unfähig zu „eigentlichen" Operationen, sondern verschließt sich auch jeder Operation durch andere Strukturen.

10

Die Exponentiation ist der natürliche Kandidat für eine weitere algebraische Basisoperation jenseits der Multiplikation. Wir sehen nun aber, daß die Folge

$$(\mathbb{N}, s) - (\mathbb{N}, +) - (\mathbb{N}, \times) - (\mathbb{N}, \circ),$$

im Unhintergehbaren beginnend, zu etwas führt, das ein Grieche vielleicht als απειρον bezeichnet hätte; hier bleiben Probleme offen [10]. Natürlich läßt sich das rekursive Definitionsschema beliebig weiterführen zu „hyperexponentiellen" Strukturen mit (vermutlich) noch exotischeren Eigenschaften. Aber nach der Multiplikation bricht die „Verständlichkeit" ab, die Strukturen scheinen in keinem „inneren", durch wechselseitige Operationen begründeten Zusammenhang mehr zu stehen. Darin liegt sicher ein Teil der Antwort auf die Frage, warum wir über Addition und Multiplikation keine weiteren „Grundrechenarten" haben. Ein anderer liegt darin, daß man mit diesen beiden und den

aus ihnen abgeleiteten Operationen ziemlich weit kommt, was sich auf verschiedene Weisen mathematisch präzisieren läßt.

Durch eine bilineare Verschränkung von Addition und Multiplikation von Zahlen entsteht die Matrixmultiplikation (so geheißen, weil sie im Fall eindimensionaler Matrizen die gewöhnliche Multiplikation ist), und damit die ganze Welt linearer Gruppen, als welche sich die meisten „wichtigen“ Gruppen realisieren lassen, darunter Permutationen und geometrische Operationen; Gruppen ohne (injektive) lineare Darstellungen, oder wenigstens Realisierung als Limites von solchen sind exotische Objekte (aus dem Museum der Gegenbeispiele). Allgemeinen Erwartungen zufolge (Langlands-Funktorialität) wird alle „spektrale“ Information motivischen wie automorphen Ursprungs von den GL(n) produziert. Eine zweite Präzisierung bietet der Approximationssatz von Weierstraß: auf kompakten Intervallen kann jede stetige Funktion (und damit auch eine große Klasse nichtstetiger Funktionen) durch polynomiale Funktionen beliebig genau approximiert werden; diese sind aber aus Addition und Multiplikation zusammengesetzt (derived operators im Sinn der universellen Algebra). Schließlich bestätigt die mathematische Logik, nämlich kraft der Gödelisierung, daß wir mit Addition und Multiplikation auf $\mathbb{N}$ schon genug haben, um alle Theorie zu formalisieren, und kraft des Unvollständigkeitssatzes sogar mehr, als wir bewältigen können.

Nimmt man also Grenzwertbildung als ein weiteres konstitutives Prinzip hinzu, hat man ein Instrumentarium, mit dem man alle Quantitätsverhältnisse zu fassen bekommt. Die nächsten Schritte dazu sind der Ausbau des Zahlsystems, zunächst algebraisch durch Konstruktion von negativen, gebrochenen, schließlich algebraischen Zahlen, alles am Leitfaden zunehmender Lösbarkeit polynomialer Gleichungen; erst der letzte Schritt bringt ein neues Prinzip, die Komplettierung zum komplexen Zahlkörper [11] . Weitere, verwandte „kanonische“ Konstruktionen (Restklassenbildung, Komplettierung nach beliebigen Bewertungen, Konstruktion beliebiger transzendenter Erweiterungen) konstituieren das Gesamtfeld der „abstrakten Algebra“.

11

Diese stellt nun, in der Axiomatik der Ringe und Körper, Addition und Multiplikation unvermittelt nebeneinander, mit der einzigen (allerdings sehr einschneidenden) Kompatibilitätsbedingung, die im Distributivgesetz $a(b + c) = ab + ac$ sowie $(b + c)a = ba + ca$ ausgesprochen wird: die multiplikative (Halb-) Gruppe operiert von rechts und links auf der additiven Gruppe [12], die fundamentale Asymmetrie in abstracto. Dies erzwingt schon die Kommutativität der additiven Struktur: einerseits ist nämlich

$$2(a + b) = 2a + 2b = (1 + 1)a + (1 + 1)b = (a + a) + (b + b) ,$$

andererseits

$$2(a + b) = (1 + 1)(a + b) = (a + b) + (a + b) ,$$

und Vergleich der beiden Resultate liefert $a + b = b + a$. Eine vergleichbare Restriktion in umgekehrter Richtung besteht nicht, denn jede Gruppe G ist Untergruppe der

Einheitengruppe von $\mathbb{Z}[G]$. Die allgemeine Theorie kennt auch keine Operation der additiven auf der multiplikativen Struktur durch Potenzbildung, wie bei den natürlichen Zahlen.

Anders als bei den natürlichen Zahlen zieht diese Konstellation keine „innere Verwandtschaft“ der beiden Strukturen nach sich, im Gegenteil gilt in der Kategorie der affinen Gruppenschemata

$$\mathrm{Hom}\,(G_a, G_m) = \mathrm{Hom}\,(G_m, G_a) = 0\ ;$$

das bedeutet, daß es keine *universellen*, für alle kommutativen Ringe R definierten Morphismen zwischen $(R, +)$ und $(R, \times)$ gibt, so wie es etwa einen universellen Homomorphismus $GL(2) \rightarrow GL(1) = G_m$ gibt (die Determinante); in diesem Sinne sind Addition und Multiplikation „prinzipiell“ inkompatibel [13]. Das schließt natürlich nicht aus, daß es in Einzelfällen Isomorphismen zwischen additiven und multiplikativen Untergruppen gibt. Zum Beispiel enthalten $(\mathbb{Q}, +)$ und $(\mathbb{Q}, \times)$ unendlich zyklische Gruppen ($(\mathbb{Q}, +)$ ist unendliche Vereinigung von solchen, nämlich aller $1/n\,\mathbb{Z}$, $(\mathbb{Q}, \times)$ mod (± 1) ist unendliches direktes Produkt, erzeugt von den Primzahlen); aber $(\mathbb{Q}, +)$ ist divisibel, und um eine divisible multiplikative Gruppe zu erhalten, muß man eine sehr große Erweiterung bilden (Adjunktion aller Wurzeln). In Körpern positiver Charakteristik $p > 0$ gibt es keine partiellen Isomorphismen, weil die additive Gruppe p-elementar ist, aber multiplikative p-Torsion nicht existiert.

Überhaupt ist in Körpern ist die additive Struktur stets (vergleichsweise) einfach, nämlich ein Vektorraum über dem Primkörper (so daß Körper derselben Dimension über diesem isomorphe Additionsgruppen haben), während die multiplikative schon in Zahlkörpern intrikat wird (wenn die Klassenzahl > 1 ist [14]). Der additive Vektorraum erscheint geradezu als Arena für die verschiedenen Auftritte multiplikativer Struktur, und das wird noch sichtbarer, wenn man von Körpern zu Algebren übergeht. Die Darstellungstheortie systematisiert diesen Aspekt: derselbe Vektorraum als Träger verschiedener linearer Strukturen; schon der eindimensionale Fall hat größte Bedeutung. Die Möglichkeit multiplikativer Strukturen auf $\mathbb{R}^n$ bildeten, seit Hamilton 1843 die Quaternionen entdeckte, lange ein offenes Problem, das erst 1958 abschließend gelöst werden konnte: nur in den Dimensionen 1,2,4 und 8 gibt es nullteilerfreie bilineare Multiplikationen (und jeweils nur eine).

12

Eine Art Übergang von der Addition zur Multiplikation scheint die Algebra mit den elementaren symmetrischen Funktionen zu bieten, die in der Ausrechnung

$$(x - a_1)...(x - a_n) = x^n - s_1(\underline{a})\, x^{n-1} + ... + (-1)^n\, s_n(\underline{a}) \quad (\underline{a} = (a_1,...,a_n))$$

auftreten. Ersichtlich sind die s_k „Mischformen“, welche die Summe s_1 in das Produkt s_n der a_i überführen, und mit der Variablenzahl n wächst die Anzahl der Zwischenschritte. Wenn diese Mischformen eine größere Rolle spielen sollen als bisher, müßte man zuerst Funktionalgleichungen für sie herleiten. Um davon die „richtige“ Vorstellung zu

gewinnen, denke man die a_i als die Eigenwerte einer Matrix A; es ist dann

$$s_1(\underline{a}) = Tr(A),\ \ s_n(\underline{a}) = Det(A),$$

und bekanntlich ist

$$Tr(A + B) = Tr(A) + Tr(B),\ \ Det(AB) = Det(A)Det(B).$$

Die gesuchten Verallgemeinerungen (für die wir uns auf Diagonalmatrizen beschränken können) bestünden demnach in binären, für beliebige Ringe definierten und mit n und k zu indizierenden Operationen $\square : R^n \times R^n \rightarrow R^n$ derart, daß

$$s_k(A \square B) = s_k(A) \square s_k(B)$$

gilt. Freilich, etwas Neues erhält man erst für $n > 2$, nämlich $s_2(a,b,c) = ab + ac + bc$, und die s_k sind n-stellige Operationen; die Prädominanz binärer Operationen dämpft die Erwartung, daß auf diesem Wege bedeutende neue Aufschlüsse zu gewinnen sind. Auch sind die Operationen $\square$ kaum anders vorstellbar als polynomial (und über $\mathbb{Z}$ definiert), also „Abkömmlinge“ von Addition und Multiplikation. Aber vielleicht sind die Möglichkeiten tatsächlich noch nicht ausgelotet.

13

Der Übergang von der Ring- zur Körperaxiomatik hat einschneidende Folgen kategorialer Natur, die hier Erwähnung verdienen. Ein Körper hat keine echten Ideale, daher sind alle Morphismen injektiv, jedes Bild eines Körpers eine isomorphe Kopie, während ein Ring, der kein Körper ist, immer auch nichtisomorphe Restklassenringe besitzt. Eine direkte Komplementarität zwischen Größe der Einheitengruppe und Abbildbarkeit zeigt der Prozeß der Lokalisierung von Ringen: wenn Elemente invertierbar werden, verschwinden mögliche Restklassenringe und damit Moduln. Ein mehr systematischer Unterschied ist der folgende. Die Axiome für Gruppen und Ringe können rein „pfeiltheoretisch“ durch kommutative Diagramme ausgedrückt werden, so die Assoziativität der binären Operation

$$m:\ A \times A \rightarrow A$$

durch die Kommutativität des Diagramms

$$\begin{array}{ccc} & \overset{id \times m}{\rightarrow} & \\ A \times A \times A & & A \times A \\ {\scriptstyle m \times id}\ \downarrow & & \downarrow\ {\scriptstyle m} \\ A \times A & \underset{m}{\rightarrow} & A \end{array} .$$

Ist E ein Endobjekt der jeweiligen Kategorie, so kann ein „Element“ von A durch einen Pfeil $E \to A$ wiedergegeben werden [15], die neutrale Eigenschaft eines Elements durch ein entsprechend gebildetes Diagramm, das sich der Leser selbst überlegen mag. Man nennt solcherart gebildete Kategorien „algebraisch“ oder „gleichungsdefiniert“; sie zeichnen sich aus durch Reichtum an Limiten und adjungierten Funktoren [16]. Ein Körper ist nun ein Ring (verschieden vom Nullring), indem alle Elemente $\neq 0$ ein multiplikatives Inverses haben [17], und diese Bedingung ist nicht diagrammatisch formulierbar, die Kategorie der Körper ist (was leicht paradox erscheint) nicht algebraisch. Das ist ein Metatheorem zu der elementaren Tatsache, daß in der Kategorie der Körper (anders als in derjenigen der kommutativen Ringe) nur wenige Produkte und gar keine Summen existieren.

14

Die Theorie der linearen algebraischen Gruppen bringt uns zu weiteren Unterschieden, die hier erwähnt werden sollen, auch wenn nicht leicht zu sehen ist, was sie für unsere Fragestellung hergeben. Wie die Realisierung von G_a als zweidimensionale lineare Gruppe zeigt (a operiert durch $(x,y) \to (x + ay, y)$), ist die additive Gruppe unipotent, bei allen möglichen (algebraischen) Realisierungen in linearen Gruppen sind alle Eigenwerte $= 1$, was man auch aus $\mathrm{Hom}(G_a, G_m) = 0$ schließen kann (man betrachte die Jordanform). Sie ist deshalb auch nicht reduktiv; in der angegebenen zweidimensionalen Realisierung bilden die $(x,0)$ einen invarianten Unterraum ohne Komplement. Dagegen ist $G_m = GL(1)$ reduktiv; das „paßt“ zu der Tatsache, daß G_m sozusagen von Hause aus eine Gruppe linearer Operatoren ist, während G_a nur „indirekt“ so dargestellt werden kann; beachte, daß G_a auf sich selbst durch Translationen nicht linear wirkt, nur affin.

In der arithmetischen Theorie der linearen Gruppen spielt die Eigenschaft der „starken Approximation“ eine wichtige Rolle; sie besagt (im einfachsten Fall), daß die Gruppe der rationalen Punkte dicht in der Gruppe der Punkte über dem endlichen Adelring liegt, was man als eine Art arithmetischen Wohlverhaltens ansehen kann. Für G_a ist das (wie für alle unipotenten Gruppen) im wesentlichen der Chinesische Restsatz: für paarweise teilerfremde ganze m_i, $i = 1,...,r$, und beliebige ganze a_i ist das simultane System von Kongruenzen

$$x \equiv a_i \bmod m_i, \quad i = 1,...,r$$

stets durch ein ganzes x lösbar; das ist gleichbedeutend damit, daß $\mathbb{Z}$ dicht liegt in

$$\lim_I \mathbb{Z} \bmod I = \prod \mathbb{Z}_p ,$$

der Komplettierung nach der Idealtopologie. Für G_m ist die Approximationseigenschaft im Fall des rationalen Grundkörpers leicht als falsch zu erkennen, weil die Einheitengruppe von $\mathbb{Z}$ nur zwei Elemente hat; aber nicht das ist der „eigentliche“ Grund, denn auch in Zahlkörpern mit unendlicher Einheitengruppe ist die multiplikative starke Approximation nicht erfüllt [18]. Ist R der Ganzheitsbereich, läuft die Untersuchung darauf hinaus, wir groß das Bild der Einheitengruppe von R in den Einheitengruppen der

Restklassenringe von R ist, eine sehr schwierige, nicht allgemein beantwortbare Frage. Da die Restklassenringe durch Kongruenzen für die additive Struktur definiert sind, manifestiert sich hier eine gewisse „Unverträglichkeit“ von additiver und multiplikativer Struktur; dazu gleich mehr.

Erscheinen G_a und G_m in diesen Hinsichten als opposita, so kommen sie in einer weiteren hier einschlägigen Hinsicht überein. In jeder algebraischen $\mathbb{Q}$- Gruppe G ist der Kern der Reduktionsabildung

$$G(\mathbb{Z}) \rightarrow G(\mathbb{Z} \bmod m))$$

für beliebige natürliche m eine Untergruppe von endlichem Index in $G(\mathbb{Z})$, genannt eine (Haupt-)Kongruenzgruppe. Man sagt, daß G die Kongruenzeigenschaft habe, wenn jede Untergruppe von endlichem Index in $G(\mathbb{Z})$ eine Kongruenzgruppe enthält. Für $G = G_a$ ist das leicht zu beweisen, für $G = G_m$ im Fall des rationalen Grundkörpers trivial, für beliebige Zahlkörper aber ein nichttrivialer Satz von Chevalley [19].

15

Wir sahen, wie die abstrakte Algebra additive und multiplikative Struktur trennt und unterscheidet. Das erste und reichste Feld für unsere Untersuchung ist natürlich der Anfang dieser Algebra, die Lehre von den ganzen Zahlen. Die multiplikative Struktur produziert hier, sozusagen aus dem Nichts, eins der stärksten Faszinosa aller Mathematik, die Folge der Primzahlen, bis heute ein Gegenstand immer tiefer dringender Forschungen. Der ist kein Mathematiker, der noch nie darüber gestaunt hat, wie aus dem schlichten, scheinbar strukturlosen Eins-nach-dem-Anderen der Nachfolge- und Additionsstruktur die undurchschaubare Folge der multiplikativen Indivisibilien hervorgeht, im Kleinen gänzlich erratisch, dabei asymptotisch dem einfachen Gesetz folgend, das der Primzahlsatz ausspricht. Die Unvorhersehbarkeit der Primzahlfolge ist korreliert mit derjenigen der Primzerlegung; während die „kanonische“ additive Zerlegung einer Zahl die tautologische ist, nämlich ihre Definition als Summe von Einsen, kann ihre kanonische multiplikative Zerlegung so schwierig werden, daß man sie selbst im Zeitalter der Superrechner zur Verschlüsselung verwenden kann. Wir werden nun sehen, wie eine Reihe bekannter, teils gelöster, teils ungelöster Probleme der Zahlentheorie ihre Wurzel in einer gewissen „Inkompatibilität“ von additiver und multiplikativer Struktur hat.

Deren sicherlich einfachster Aspekt ist, daß uns die multiplikative Struktur zweier Zahlen, ihre Primzerlegung, noch nicht viel sagt über die ihrer Summe; wenn sie teilerfremd sind, wissen wir nur, daß die Primteiler der Summe jedenfalls verschieden sind von denen der Summanden. Leicht ist nur

$$v_p(a + b) \geq \min \{v_p(a), v_p(b)\}$$

wobei $v_p(a)$ den p-Exponenten von a bezeichnet, mit Gleichheit, wenn $v_p(a) \neq v_p(b)$; im andern Fall kann $v_p(a + b)$ jeden größeren Wert annehmen. In seiner naivsten Form würde das Problem sein, $v_p(a + b)$ als Funktion von a und b auszudrücken (in noch anderer Weise als durch die Definition), insbesondere $v_p(a + 1)$ als Funktion von a, was

man als hoffnungslos und vermutlich nicht sachgemäß gestellt ansehen wird. Man sieht sofortt, daß $v_p(a + b)$ nicht allein von $v_p(a)$ und $v_p(b)$ abhängen kann. Muß man noch andere Funktionen v_q heranziehen, oder die $v_p(c)$ für vorangegangene c, und wenn ja, welche? Man sieht, daß schon eine sinnvolle Fragestellung Schwierigkeiten macht. Das Problem wird sozusagen entschärft durch Lokalisieren an einer Primstelle p , denn im Lokalen ist die Ungleichung eine „starke“ Aussage, weil es nur das einzige Primelement p gibt. Auf dieser Aufteilung der Teilbarkeitsbeziehungen in einfachere (aber nicht triviale) lokale Beziehungen beruht die Durchschlagskraft der lokalen Methoden, die aus der heutigen Zahlentheorie nicht mehr wegzudenken sind. Jeder, der sich ernsthaft mit Zahlentheorie beschäftigt hat, kennt das unendlich subtile Ineinandergreifen von Teilbarkeits- und Größenbeziehungen, das manche Beweisführungen der „elementaren“ Zahlentheorie als Kunstwerke erscheinen läßt; im Lokalen wird alles „algebraischer“, es gibt weniger Überraschungen. Freilich sind nicht alle Probleme „lokalisierbar“.

16

Die additive Zahlentheorie befaßt sich mit der Frage, was für Zahlen sich als Summen aus vorgegebenen Zahlmengen schreiben lassen. Für uns interessant ist der Fall, in dem die erlaubten Summanden eine bestimmte multiplikative Struktur haben. Der einfachste Fall ist das Euler-Goldbach-Problem: ist jede gerade Zahl > 2 Summe von zwei Primzahlen? Es versteht sich, daß man dies heute bis in astronomische Höhen bestätigt hat; die besten bisher bewiesenen Resultate sind ein Satz von Chen: jede solche Zahl ist Summe einer Primzahl und einer Zahl mit höchstens zwei Primfaktoren, und ein Satz von Vinogradov: jede genügend große *ungerade* Zahl ist Summe von *drei* Primzahlen. Alles spricht also dafür, daß die Vermutung zutrifft; die Inkompatibilität von Addition und Multiplikation manifestiert sich hier in der Schwierigkeit des Beweises. Man hat keine Mühe, die Vermutung für kleine Zahlen zu verifizieren, aber es existiert kein „elementarer“ Beweisansatz (nur die sehr komplexen Siebmethoden führen zu Resultaten). In diesen Kontext gehört auch das nach wie vor ungelöste Problem der Primzahlzwillinge.

Eine andere sehr einfache multiplikative Eigenschaft einer Zahl ist, eine m-te Potenz zu sein (mit m > 1), und demnach ist die Frage, ob die Summe von zwei solchen wieder eine solche sein kann, ein anderer einfacher Test für die „Verträglichkeit“ von Addition und Multiplikation. Im Fall n = 2 führt dies zu den „pythagoreischen Tripeln“, deren Parametrisierung schon im Altertum bekannt war. Für größere Exponenten ist es, wie wir heute wissen, mit der Verträglichkeit vorbei: die Fermatsche Gleichung

$$x^m + y^m = z^m$$

hat für $m > 2$ keine nichttriviale Lösung in ganzen Zahlen [20]. An diesem Befund ändert sich wenig, wenn man die zu lösenden Gleichungen modifiziert. Die Fermatgleichung definiert eine rationale Kurve vom Geschlecht $(m-1)(m-2)/2$; die Vermutung, daß eine Kurve von einem Geschlecht > 1 über einem Zahlkörper nur endlich viele rationale Punkte haben kann, wurde 1922 von Mordell ausgesprochen und 1983 von Faltings bewiesen. Heute vermutet man weiter, daß alle Gleichungen der Form

$$ax^n + by^m = cz^k$$

bei festen a,b,c und $1/n + 1/m + 1/k < 1$ nur endlich viele Lösungen haben [21]. Lange Zeit wurde vermutet, daß die Gleichung

$$3^2 - 2^3 = 1$$

den einzigen Fall zeigt, in dem sich ein Quadrat und ein Kubus von ganzen Zahlen um 1 unterscheiden („Catalansche Vermutung"), bis 2002 der Beweis gelang.

Eine Modifikation unserer Fragestellung ergibt sich, wenn man die multiplikative Struktur der Summanden festlegt, aber ihre Anzahl variiert. Man weiß seit langem, welche Zahlen als Summen von zwei oder drei, und daß alle als Summen von vier Quadratzahlen geschrieben werden können. Schon im 18.Jahrhundert wurde die Frage aufgeworfen, ob man bei gebenem Exponenten n eine Zahl k so finden kann, derart daß jede Zahl eine k-fache Summe von n-ten Potenzen ist. Für $n = 2$ ist $k = 4$ wählbar, für $n = 3$ ist $k = 9$ die erforderliche Minimalzahl; man vergleiche das mit der Tatsache, daß kein Kubus einer ganzen Zahl eine Summe von zwei Kuben ist. Hilbert gelang 1909 der Nachweis, daß es stets ein kleinstes k gibt, so daß *jede genügend große Zahl* eine derartige Summe ist; sozusagen eine quantifizierte Verträglichkeit *on the long run.*

Das multiplikative Gegenstück zur additiven Zahlentheorie hätte zu fragen, welche Zahlen sich als Produkte von Faktoren mit „besonderer" additiver Struktur darstellen lassen. Dieser Gesichtspunkt scheint viel weniger ergiebig, vermutlich weil nicht zu sehen ist, was eine „besondere" additive Struktur einer Zahl sein soll, die nicht ihrerseits durch multiplikative Struktur der Summanden definiert ist; wodurch die Fragestellung an die additive Theorie zurückverwiesen würde.

Eine besonders subtile Kopplung von additiver und multiplikativer Struktur spricht die erst 1985 aufgestellte „abc-Vermutung" aus (so benannt einfach nach ihrer üblich gewordenen Formulierung). Es bezeichne rad a („Radikal" von a) das Produkt der verschiedenen Primteiler der natürlichen Zahl a; die Funktion rad „vergißt" also die Potenzen $v_p(a)$, indem sie alle = 1 setzt; a = rad a bedeutet, daß a durch keine Quadratzahl teilbar („quadratfrei") ist. Die Vermutung lautet: für jedes reelle $\varepsilon > 1$ gibt es eine Konstante $K = K(\varepsilon)$, derart daß, wenn a und b teilerfremd sind und $a + b = c$ ist,

$$c \leq K\,(\mathrm{rad}(abc))^{\varepsilon}$$

gilt. (Es ist klar, daß die Teilerfremdheit hier nötig ist, und man zeigt leicht, daß für $\varepsilon = 1$ keine solche Aussage gelten kann.) Um einen ersten Einblick in die Eigenart und Kraft dieser Aussage zu erhalten, denke man a und b als Potenzen p^n und q^m mit quadratfreien p und q. Die Ungleichung wird dann

$$p^n + q^m \leq K\,(p\,q\,\mathrm{rad}(p^n + q^m))^{\varepsilon}\,,$$

und denkt man sich n, m wachsend und ε nahe bei 1, so sieht man, daß $\mathrm{rad}(p^n + q^m)$ ungefähr von der Größenordnung von $p^n + q^m$ selbst sein muß, und das erzwingt, daß

Summen hoher Potenzen teilerfremder Zahlen dazu tendieren, quadratfrei zu sein oder wenigstens große Primfaktoren nur in erster Potenz zu enthalten. Dieses Phänomen war natürlich schon lange bekannt (zum Beispiel beschäftigte man sich schon lange mit Zahlen der Form $2^n \pm 1$), aber erst die Vermutung offeriert eine „strukturelle" Erklärung[22]. Auf die geradezu überwältigende Menge weiterer, vergleichsweise leicht zu ziehender Konsequenzen (darunter einige mit großer Mühe schon bewiesene Sätze) kann hier nicht weiter eingegangen werden [23]. Die abc-Vermutung spricht, zum ersten Mal in der Geschichte der Arithmetik, eine nichttriviale, in der Tat äußerst tiefliegende, gleichzeitig elementar formulierbare und, wenn wahr, überaus folgenreiche wechselseitige Restriktion zwischen der Sukzession der Zahlen und ihrer Primzerlegung aus; es ist gut vorstellbar, daß man eines Tages in dieser Entdeckung (und sei es auch nur die Entdeckung der Fragestellung) einen Wendepunkt der ganzen Entwicklung sehen wird.

18

Geht man von den gewöhnlichen ganzen Zahlen zu den „höheren", algebraischen Zahlbereichen über, wird die additive Struktur vervielfältigt (an die Stelle von $\mathbb{Z}$ tritt ein freier $\mathbb{Z}-$ Modul von endlichem Rang), während die multiplikative Struktur qualitative Veränderungen erfährt: die Primzerlegung der Elemente muß durch Primidealzerlegung ersetzt werden, und die Einheitengruppe wird (*einen* Fall ausgenommen) unendlich. Ein Satz von Brauer und Siegel [24] suggeriert eine Art Komplementarität zwischen der Komplexität der Primzerlegung (repräsentiert durch die Klassenzahl) und der Größe der Einheitengruppe (repräsentiert durch den Regulator); der einzige Fall ($\mathbb{Z}$ ausgenommen), in dem die letztere endlich ist (der imaginär-quadratische) ist gleichzeitig der einzige, von dem man weiß, daß die Primzerlegung nur endlich oft eindeutig ist.

Obwohl einige Probleme der additiven Zahlentheorie auf Zahlkörper übertragen werden können, verschiebt sich doch das Interesse auf die multiplikative Struktur. Der heute schon klassisch zu nennende Teil der Theorie gipfelt in der Klassenkörpertheorie, die man als eine multiplikative Theorie bezeichnet hat. Ihre zentrale Aussage läßt sich darin zusammenfassen, daß eindimensionale Charaktere der absoluten Galoisgruppe eines Zahlkörpers K vermöge der Artin-Reziprozität mit Idelklassencharakteren identifiziert werden können; die Idelgruppe aber ist einfach die multiplikative Gruppe $G_m(A(K))$ des Adelrings A(K) von K. Die natürliche Frage, ob eine vergleichbare Korrespondenz auch für die höherdimensionalen Charaktere der Galoisgruppe besteht und welche Gruppen dabei an die Stelle von G_m treten, wird im (sehr viel weiter greifenden) Programm von Langlands beantwortet: für n-dimensionale Charaktere ist $G_m = GL(1)$ durch $GL(n)$ zu ersetzen. In Termini der L-Reihen, in welchen die spektralen Data für beide Arten von Gruppen kodifiziert sind, heißt das: alle Artinschen L-Reihen sind automorphe L-Reihen. Die additive Gruppe G_a kann eine vergleichbare Rolle nicht spielen, da der Mechanismus der L-Funktionen nur für Darstellungen reduktiver Gruppen zu „funktionieren" scheint [25].

19

Wir haben gesehen, wie unsere beiden Operationen in Algebra und Zahlentheorie getrennt bleiben, ja einander gegenüberstehen. Gehen wir zur Komplettierung des

rationalen Körpers an seiner archimedischen „Stelle“ über, so finden wir durch Exponentialfunktion und Logarithmus vermittelte Isomorphismen zwischen der additiven Gruppe und der positiven Hälfte der multiplikativen (ihrer Einskomponente; für keinen Körper kann die *volle* Multiplikationsgruppe zur additiven Gruppe isomorph sein). Das Besondere daran ist nicht, daß additive Struktur in multiplikative übergeht; das kann man (wie gesehen) auch in natürlichen Zahlen durch $n \to a \circ n$ (bei festem a) haben, sondern daß das Bild so groß ist, daß eine Umkehrung möglich wird. Vergleichbares existiert in allen Körpern, die bezüglich einer Bewertung vollständig sind (wegen der Nenner in den Koeffizienten der Reihenentwicklungen von exp und log aber nur in Charakteristik 0); ist die Bewertung nichtarchimedisch und P das Primideal, erhält man (für genügend großes n) Isomorphismen zwischen der additiven Gruppe P^n und der multiplikativen der „höheren Einseinheiten“ $1 + P^n$. Die Komplettierung, so möchte man sagen, verklebt die diskreten Strukturen mit dem Leim des Kontinuums, der so dicht ist, daß sie ihre Eigenart aufgeben und ineinander überführbar werden. Als mehr strukturellen Hintergrund kann man die Tatsache ansehen, daß eine Liesche Gruppe bis auf lokale Isomorphie durch ihre Liealgebra bestimmt ist (und zwar gerade vermöge einer verallgemeinerten Exponentialabbildung), in der Dimension 1 aber nur *eine* Liealgebra existiert (die triviale); erst in höheren Dimensionen entfalten sich die strukturellen Möglichkeiten der kontinuierlichen Gruppen. Hier erscheint additive Struktur in einem neuen Verhältnis zur multiplikativen, nämlich als ihre Linearisierung; gleichzeitig liefert die Liealgebra eine „kanonische“ Darstellung der Gruppe (die adjungierte, die im Fall von G_m allerdings trivial ist): wieder Vektorraumstruktur als Schauplatz „multiplikativer“ Operation.

Eine dritte Erscheinungsform „der“ eindimensionalen Liegruppe muß an dieser Stelle genannt werden, die kompakte Kreisgruppe S^1, die vor dem Hintergrund unserer Fragestellung als eine Art Zwitterwesen erscheint: additiv, wenn man sie als $\mathbb{R}$ mod $\mathbb{Z}$, multiplikativ, wenn man sie als Gruppe der komplexen Zahlen vom Betrag 1 denkt, wobei natürlich die Exponentialfunktion den Übergang vermittelt. Durch die Restklassenbildung entsteht alle denkbare Torsion, algebraisch auf die sparsamste Weise, nämlich jede zyklische Gruppe genau einmal, topologisch als dichte, aber abzählbare Untergruppe, „eingewoben“ in ein Kontinuum. Die Kreisgruppe ist die einfachste Gruppe mit dieser Eigenschaft, und dies ist wohl der tiefere Grund für ihre besondere Rolle als Zielgruppe der (eindimensionalen) Charaktere *aller* Gruppen, die durch den Dualitätssatz von Pontrjagin ins Licht gestellt wird. In diesem Kontext erscheint sie als „schizophrenes“ Objekt [26]: während $(\mathbb{R}, +)$ und damit auch $(\mathbb{R}, \times)$ selbstdual sind, hat sie selbst als kompakte Gruppe das diskrete Dual $(\mathbb{Z}, +)$. Hier kann erwähnt werden, wie die Dualitätstheorie auch „virtuell isomorphe“ additive und multiplikative Struktur unterscheidet: in den nichtarchimedischen Lokalisierungen der globalen Körper sind die additiven Gruppen selbstdual, die multiplikativen (als Produkte einer diskreten und einer kompakten Gruppe) davon weit entfernt; das gilt auch noch adelisch.

20

Der Antagonismus von Addition und Multiplikation wird also aufgehoben (durchaus im Hegelschen Doppelsinn) durch die Verdichtung der Zahlenfolge zum Kontinuum. Es geht über in Dualität durch den Abstraktionsprozeß, den die mathematische Kategorienlehre

vollzieht. Die kategoriale Summe zweier endlicher Mengen ist ihre disjunkte Vereinigung, ihr kategoriales Produkt das Mengenprodukt. Diese kategorialen Bezeichnungen haben ihren Ursprung darin, daß sie mit den Elementzahlen konform gehen: die Elementzahl der disjunkten Vereinigung ist die Summe der Elementzahlen der vereinigten Mengen, und Entsprechendes gilt für das Mengenprodukt. Erhalten bleibt auch die Asymmetrie, daß nur eine der zwei denkbaren Distributivitäten gilt,

$$(M \cup N) \times L \;=\; (M \times L) \cup (N \times L)\;;$$

in diesem Sinne sind die kategorialen Begriffsbildungen „natürliche“ Fortsetzungen der gewöhnlichen. Aber Summe und Produkt im kategorialen Sinn sind durch universelle Abbildungseigenschaften definiert, und diese gehen durch Dualisieren (Umkehrung der Pfeile) ineinander über: in der dualen Kategorie wird die Summe zum Produkt und umgekehrt. Die Asymmetrie wird nicht aufgehoben, sondern in der dualen Gegenwelt sozusagen gespiegelt; das ist ist aber nicht das „wahre“ Verhältnis von Addition und Multiplikation.

Auch gehen die gewöhnlichen Konnotationen von Summe und Produkt in andern Kategorien verloren; in abelschen Kategorien zum Beispiel fallen beide zusammen (wobei natürlich die Distributivität verschwindet). Man kann auch $(\mathbb{N}, \leq)$ als Kategorie auffassen [27]; die kategoriale Summe zweier Zahlen ist dann ihr Maximum, das Produkt ihr Minimum; ersetzt man die gewöhnliche Anordnung $\leq$ durch die Teilbarkeitsrelation, wird das kleinste gemeinsame Vielfache zur Summe, der größte gemeinsame Teiler zum Produkt. Daran zeigt sich, daß die kategorialen Benennungen letztlich doch metaphorisch sind; ich kenne keine Möglichkeit, die natürlichen Zahlen zu Objekten einer Kategorie zu machen, derart daß Summe und Produkt im gewöhnlichen und im kategorialen Sinne übereinstimmen [28] . Wir wollen darum die weiteren kategorialen Abenteuer unserer beiden Begriffe nicht weiter verfolgen.

21

Fassen wir zusammen. Addition und Multiplikation, dem ersten Blick vielleicht als ein „gleichberechtigt“ nebeneinander stehendes Paar von Operationen erscheinend, weisen tatsächlich in manchen Hinsichten komplementäres oder duales Verhältnis auf. Nähere Betrachtung jedoch, besonders ihrer Genese, bringt eine Hierarchie ans Licht: die Multiplikation ist die theoretisch „höhere“ und dominante Operation. Die Mathematik präzisiert dies in mannigfacher Weise, komplexitätstheoretisch, formallogisch, am deutlichsten in der Axiomatik der Ringe: die multiplikative Halbgruppe operiert auf der additiven Gruppe, diese fungiert geradezu als Schauplatz verschiedener möglicher Multiplikationen. Den operativen Charakter der Multiplikation spiegelt die Bezeichnung „Faktor“, das, was etwas bewirkt, während ein „Summand“ gemäß der Bedeutung des Gerundivums etwas ist, mit dem etwas geschehen soll. Das geht bis in die Notation: tritt eine Gruppe als Operatorgruppe auf, neigen wir zur multiplikativen Schreibweise (automatisch, wenn sie nicht kommutativ ist); eine kommutative Gruppe, auf der Operationen stattfinden, schreiben wir additiv[7]. In der Kategorie der Gruppenschemata, also von einem algebraisch universellen Gesichtspunkt aus, sind beide Strukturen gänzlich unverträglich, auch ihre konkreten Ausprägungen zeigen die Asymmetrie: die

multiplikative Struktur von Ringen ist in der Regel komplexer als die additive. Vollends in der Zahlentheorie läßt sich eine Inkompatibilität von Addition und Multiplikation ausmachen, die man als Quelle einer Reihe bekannter Probleme ansehen kann. Bleiben unsere beiden Operationen also in einem durchaus antagonistischen Verhältnis, solange die Strukturen diskret bleiben, werden sie ineinander überführbar, wenn man zu Komplettierungen übergeht. Mit einer Denkfigur im Stile von Cusanus: als wolle der mathematische Weltgeist, indem er das Diskrete, also Gesonderte zum Kontinuum zusammenschließt, im Unendlichen eine Versöhnung stiften, eine coincidentia oppositorum oder ein hegelsches „Übergehen“.

22

Es fragt sich nun, wie dieser Befund zu deuten ist, ja was überhaupt eine Deutung sein soll und was sie prinzipiell leisten kann. Das bringt uns zurück zum Anfang unserer Betrachtung und die dort gestellten Fragen. Die Ursprünge unserer Operationen haben wir erörtert, auch eine Antwort gefunden auf die Frage, warum es keine weiteren algebraischen Basisoperationen gibt. Wie können wir nun das sichtbarste Ergebnis unserer Materialsammlung verstehen, die fundamentale Asymmetrie? Ein verführerischer Gedanke ist, die multiplikative Operation der Zahlen auf der additiven Halbgruppe, als welche sie anfänglich selbst enstehen, als eine Art Selbstreferentialität auf niedrigster Stufe zu deuten. Wir haben ja gesehen, wie die Multiplikation als Organisator von Addition erschien, als planmäßige Ordnung eines (im Prinzip) auch begrifflos zu vollziehenden Vorgangs, und jede Operation multiplikativen Charakters einen Vorentwurf voraussetzt, einen Eingriff des theoretischen Agierens; hinzu kommt die „dialektische“ Verschränkung der Operationen. Daß die Analogie zur Selbstreferentialität keine ganz leere Spekulation ist, zeigt die mathematische Logik. Wir haben schon erwähnt, daß erst nach Einbeziehung der Multiplikation die Theorie von $\mathbb{N}$ unentscheidbar wird, vermöge des Unvollständigkeitssatzes. Die Formel, mit der man diesen Satz beweist, enthält nun eine charakteristische Selbstreferentialität: sie behauptet ihre eigene Unbeweisbarkeit. Der Selbstbezug aber ist von besonderem Gewicht, als ein Hauptmerkmal, welches das menschliche theoretische Agieren vom tierischen Handeln unterscheidet. Damit wird eine Grenze überschritten, zugleich eine neue und vorderhand unüberschreitbare vor uns aufgerichtet.

Man kann einwenden, daß auch schon die additive Struktur auf der Nachfolgerstruktur operiert. Aber damit wird die Komplexität nicht wesentlich vermehrt, weil die Addition durch die Gleichung $s(n) = n+1$ die Nachfolgerabbildung „enthält“; dagegen kann man nicht aus der multiplikativen die additive Struktur rekonstruieren, zum Beispiel weil auch der Halbring $\mathbb{N}\times\mathbb{N}$ und der Polynomring $\mathbb{Z}/2\mathbb{Z}[x]$ eine zu $(\mathbb{N}, \times)$ isomorphe multiplikative Halbgruppe besitzen [29] . Der Entstehung der Multiplikation aus der Addition sieht man eben nicht an, was mit ihr an Neuem ins Spiel kommt; erst die Primzerlegung enthüllt die erstaunliche Tatsache, daß sich in der multiplikativen Struktur die additive unendlich vervielfacht hat, und daß damit neue Qualitäten eintreten, erscheint ohne weiteres plausibel. Man darf natürlich nicht aus dem Blick verlieren, daß die Komplexität der Peanoarithmetik nicht durch die Multiplikation allein zustande kommt, sondern durch ihr Hinzutreten zur Addition.

23

Der Komplexitätssprung beim Übergang von $(\mathbb{N}, +)$ zu $(\mathbb{N}, +, \times)$ illustriert ein in der Mathematik häufiges Phänomen: die Zwei als Erzeugerin von Vielheit und Komplexität, das Aufkommen qualitativ neuer Phänomene, wenn man einen Parameter von 1 auf 2 erhöht; so entbindet der Übergang von einer zu zwei Dimensionen in der Geometrie die Fülle der (ebenen) Gestaltphänomene, ein funktionsfähiges Alphabet benötigt mindestens zwei Symbole, aber auch nicht mehr [30]. In unserem Fall ist der Parameter die Anzahl der Operationen, und noch deutlicher als der Unvollständigkeitssatz illustriert die Algebra diesen Sprung. Während eine Iteration von Additionen oder Multiplikationen wieder nur eine solche ist, schafft das Zusammenwirken der beiden Operationen die ganze Strukturvielfalt der Polynome, damit der klassischen Algebra und algebraischen Geometrie. Dabei sind die beiden Operationen in gewissem Sinne voneinander unabhängig, wie der Identitätssatz für Polynome präzisiert: sind die Polynome f und g als Abbildungen gleich, d.h. $f(a) = g(a)$ für alle Argumente a, so sind sie als Polynome identisch, d.h. haben dieselben Koeffizienten. Diese Unabhängigkeit kann man als einen weiteren Aspekt der Inkompatibilität verstehen; einen Ausgleich sozusagen bieten die zahllosen Polynomidentitäten, verschiedene Schreibweisen für denselben Ausdruck, wie die binomischen Formeln.

24

Wir haben nun auf unsere beiden Grundrechenarten einen volleren Blick gewonnen; haben wir sie „verstanden“? Was kann bedeuten, die kategoriale Verfassung zu „verstehen“? Wenn man nach unten gräbt, kommt man schnell zu einer Schicht, an der sich „der Spaten zurückbiegt“. In der Mathematik sind das Konstellationen von Grundbegriffen, die nicht hinterfragbar scheinen, auch wenn man sie wechselseitig durcheinander darstellen kann. Man kann Kategorien durch Mengen modellieren und umgekehrt; damit hat man aber nicht den *Begriff* der Kategorie auf den der Menge zurückgeführt, ebensowenig wie die Koordinatisierung den Raumbegriff auf den Zahlbegriff zurückführt. Jene Grundbegriffe und (ihre als Axiome formulierten) Konstellationen erscheinen als Vorgegebenes unserer kategorialen Organisation, zu dem Alternativen (wie höherdimensionale Räume) allenfalls denkbar, aber nicht erfahrbar sind. Wenn in diesem nicht hintergehbaren Faktischen und seiner Faktizität ein verstehbarer Sinn liegt (was immer auch der Sinn von „Sinn“ sein mag), dann kann er sich nur durch Entwicklung erschließen. Die Primzahlfolge versteht man nicht, indem man sich in ihren Ursprung versenkt, sondern indem man Sätze über Primzahlen beweist. Wie kommt es, daß sich immer wieder beste Köpfe an solchen Problemen abarbeiten, obwohl sie kaum je praktischen Nutzen bringen, wo hat diese nicht nachlassende Verführungskraft ihre Wurzel? Bloßes Vergnügen an Denksport würde seine Moden durch die Völker und Zeitalter haben. Die Antwort ist, daß die Grundprobleme der Zahlentheorie noch nahe am Ursprung entstehen, der kategorialen Verfassung, und damit keine beliebigen Exerzitien für die Leistungsfähigkeit des Denkens sind, sondern natürliche Aufgaben; keine sportliche Herausforderung, sondern eine, welche die Conditio Humana im Ganzen angeht.

Nach Cusanus kommt der Geist, mens, auf uns im Zustand einer vom Urheber bewirkten „Einwicklung“ (complicatio) und offenbart sich erst in der explicatio, der Auswicklung im historischen Prozeß. Für Cusanus stand der Urheber fest und auch das Ziel des Prozesses: die Annäherung des Geschöpfs an den Schöpfer. Ziehen wir die Glaubensartikel ab, bleiben das Vorgegebene, die kategoriale Verfassung, und das Aufgegebene, nämlich sie denkend und handelnd zu entwickeln. Die mathematische Entfaltung ist ein Teil dieser Aufgabe: nec est aliud numerus quam ratio explicata[31]. Die Mathematik von heute birgt unerwartete Einlösungen dieses dictums.

Anmerkungen und Nachweise

1 Kritik der reinen Vernunft, B 202 (Axiome der Anschauung), B 207 (Antizipationen der Wahrnehmung).

2 Siehe M.Rabin, Decidable Theories, in J.Barwise (edt.), Handbook of Mathematical Logic, Amsterdam 1977, S.603 ff. Ist die Anordnung gegeben, kann der Nachfolger als das (axiomatisch zu fordernde) kleinste größere Element definiert werden; wie man die Anordnung durch die Addition definiert, ist bekannt. Siehe zu diesem Thema auch meine Ausführungen in „Von Zahlen und Figuren“, 18ff.

3 Näheres in meinem Aufsatz „Über Assoziativität und Kommutativität“, Mathem. Sem.-Ber. 50 (2003).

4 Man mustere die Sätze über Proportionen, die Euklid im Buch V seiner „Elemente“ bietet. Immerhin kennt er:

$$\text{wenn } a:b = c:d = r, \text{ dann auch } (a+c):(b+d) = r ,$$

was man als eine Form der Distributivität auffassen kann; man beachte aber, daß hier keine *Proportionen* addiert werden.

5 Genauer: ein Anfangsobjekt in der Kategorie dieser Tripel.

6 Wenn man eine Boolesche Algebra zu einem Ring macht, verschwindet die Dualität der beiden Booleschen Operationen.

7 Auch der außermathematische Gebrauch von „Summe“ und „Produkt“ zeigt diese Tendenz: in jeder Art Produkt sind „Faktoren“ beteiligt, die etwas Neues bewirken, während eine Summe nicht mehr sein muß als die Gesamtheit der Teile.

8 Man bemerke, daß $(\mathbb{N}, \times)$ eine große Automorphismengruppe besitzt (beliebige Permutationen der Primzahlen), während $(\mathbb{N}, s)$ und $(\mathbb{N}, +)$ jeweils nur den trivialen Automorphismus haben.

9 Ich würde gern wissen, ob diese definierend sind.

10 Denkbar ist anstelle des binären exp eine ternäre Operation (siehe 12 unten).

11 Üblich ist eine etwas andere Reihenfolge, nämlich $\mathbb{N} - \mathbb{Z} - \mathbb{Q} - \mathbb{R} - \mathbb{C}$; das hat praktische und didaktische Gründe.

12 Ist der Ring (d.h. seine Multiplikation) kommutativ, fallen natürlich beide zusammen.

13 Siehe W.Waterhouse, Introduction to Affine Group Schemes, Springer 1979, S. 19. Nach Abzug der Gruppenstrukturen (Vergißfunktor), nur als algebraische Kurven gesehen, werden G_m und G_a birational äquivalent, $G_a = P^1 \setminus \{\infty\}$, $G_m = P^1 \setminus \{ \infty , 0\}$.

14 Beachte aber: alle reell-quadratischen Zahlkörper mit eindeutiger Primzerlegung haben isomorphe Multiplikations- und Additionsgruppen; sind aber natürlich als Körper nicht isomorph.

15 Die Objekte A brauchen keine Mengen zu sein!

16 Näheres bei B.Pareigis, Kategorien und Funktoren, Stuttgart 1969.

17 Aus $0 + 0 = 0$ folgt mit der Distributivität $0a + 0a = 0a$ und damit $0a = 0$. Das Argument benutzt außer der Distributitivität nur die Tatsache, daß jede Gleichung $a + x = b$ eine eindeutige Lösung hat; weder Assoziativität noch Kommutativität kommen ins Spiel. Es gilt also in großer Allgemeinheit für Paare binärer Operationen mit einer Distributivität, daß das neutrale Element als Nullelement für die operierende Struktur fungiert.

18 Siehe Platonov/Rapinchuk, Algebraic Groups and Number Theory, Academic Press 1994, Ch. 7. Eine reduktive Gruppe über einem Zahlkörper besitzt höchstens dann starke Approximation, wenn sie halbeinfach ist, und das ist für G_m wieder „tautologisch“ falsch.

19 C.Chevalley, Deux Theoremes d´ Arithmetique, J.Math.Soc.Japan 3 (1951), S.36 – 44. Siehe die Diskussion des Kongruenzproblems bei Platonov/Rapinchuk (Anm.18).

20 Von unserm Gesichtspunkt erscheint Kummers Zugang als der natürliche: im Körper der m-ten Einheitswurzeln kann man die linke Seite in ein Produkt linearer Faktoren zerlegen, wodurch das Problem ein rein multiplikatives wird und mit Kenntnis der Primzerlegung angegangen werden kann. Daß es dennoch auf diesem Wege (bisher) nicht vollständig gelöst, sondern als eher zufälliges Produkt einer tiefen Vermutung über elliptische Kurven sozusagen mitbewiesen wurde, ist eine Kapriole des mathematischen Weltgeistes.

21 Als Foglerugn aus der abc-Vermutung (siehe 17 unten); A.Nitaj, La Conjecture abc, L´ Enseignement Mathematique, 42 (1996), S. 3 – 24.

22 Der Leser kann sich selbst überzeugen, indem er Quadratsummen teilerfremder $a \leq 10$ bildet. Es entstehen viel mehr quadratfreie Zahlen, als man nach der Größe der Stichprobe

im Bereich $\leq$ 181 erwarten sollte.

23 Siehe die abc-conjecture homepage.

24 Siehe S.Lang, Algebraic Number Theory, Springer 1986.

25 Natürlich kann man auch Dirichletsche Reihen zu additiven Charakteren bilden; das erste echte Beispiel zum Charakter $n \to (-1)^n$. Es ist nicht schwer zu sehen, daß diese L-Reihe nicht das „richtige" Eulerprodukt hat und auch keiner Funktionalgleichung genügt.

26 Vgl. MacLane/Moerdijk, Sheaves in Geometry and Logic, Springer 1992, S.482.

27 Jede partiell geordnete Menge $(M, \leq)$ kann als Kategorie aufgefaßt werden, mit den Elementen von M als Objekten und genau einem Morphismus $x \to y$, falls $x \leq y$.

28 Die nächstliegende Approximation scheint die folgende zu sein: bezeichnen wir mit $\mathscr{E}$ die Kategorie der endlichen Mengen mit den *injektiven* Abbildungen als Morphismen, so erhalten wir einen Funktor

$$|\ |\ :\ \mathscr{E} \to\ (\mathbb{N},\ \leq),$$

indem wir die Menge M auf ihre Elementanzahl |M| und alle Injektionen $M \to N$ auf den einzigen Pfeil $|M| \to |N|$ in $(\mathbb{N}, \leq)$ abbilden. Aber $\mathscr{E}$ hat weder Summen noch Produkte. (Man sieht das am leichtesten, indem man die skeletale Unterkategorie mit Objekten $[n] = \{1,...,n\}$ betrachtet. Als Summe von $[m]$ und $[n]$ kommt nur $[\max\{m,n\}]$ in Betracht (also das „falsche" Objekt), aber dieses Objekt erfüllt nicht die geforderte Abbildungseigenschaft; analog für Produkte.)

29 Umgekehrt ist allerdings die gewöhnliche Multiplikation die einzige, die aus $(\mathbb{N}, +)$ einen Halbring macht (siehe Abschnitt 8); erst in $\mathbb{N}\times\mathbb{N}$ erscheint hier Vielfalt (quadratische Zahlbereiche). Am Rande sei hier notiert, daß der Halbring $\mathbb{N}[x]$ keine eindeutige Primzerlegung besitzt, das dort unzerlegbare Polynom $x^3 + 1$ teilt das Produkt $(x + 1)(x^4 + x^2 + 1)$, aber keinen der Faktoren. – Der nichtinitiierte Leser hat sich vielleicht schon gefragt, wie dieser Übergang einen Komplexitätssprung bewirken kann, wenn doch die Multiplikation aus der Addition abgeleitet wird. Die Ableitung vermittels des Rekursionssatzes setzt das „umgebende" Mengenuniversum voraus; in der Peanoarithmetik, die das vermeidet, müssen daher Addition und Multiplikation einzeln gefordert werden (zusätzlich zu s). Siehe die Diskussion in meinem Buch „Mathematik für Philosophen", Leipziger Universitätsverlag 2004.

30 Siehe zu diesem Thema meinen Aufsatz „Über die 2 und Dualität", in: „Drei Studien zur Struktur der Mathematik", Hamburger Beiträge zur Mathematik, Nr.229 (2005). Man sollte darüber aber nicht vergessen, daß die Gruppentheorie auch mit nur einer Operation zu größter Komplexität kommt (Unlösbarkeit des Wortproblems).

31 De Coniecturis I, 2.