SAMMLUNG GÖSCHEN BAND 1131

EINFÜHRUNG IN DIE ZAHLENTHEORIE

von

DR. ARNOLD SCHOLZ †
Dozent der Mathematik an der Universität Kiel

überarbeitet und herausgegeben von

DR. BRUNO SCHOENEBERG
Privatdozent der Mathematik an der Universität Hamburg

2. Auflage

WALTER DE GRUYTER & CO.
vormals G. J. Göschen'sche Verlagshandlung · J. Guttentag,
Verlagsbuchhandlung · Georg Reimer · Karl J. Trübner · Veit & Comp.
BERLIN 1955

Archiv-Nr. 11 11 31
Druck: Kahmann-Druck, Berlin-Steglitz
Printed in Germany

Inhalt

Literatur

Dickson-Bodewig: Einführung in die Zahlentheorie. Leipzig 1931.

Dirichlet-Dedekind: Vorlesungen über Zahlentheorie. 3. Aufl. 1879; 4. Aufl. 1894 (Braunschweig).
S. auch Dedekind, Ges. Werke.

Gauß: Disquisitiones Arithmeticae. Leipzig 1801. Übersetzung von Maser: Untersuchungen über höhere Arithmetik. Berlin 1889.

Hasse: Vorlesungen über Zahlentheorie. Berlin 1950.

Hecke: Vorlesungen über die Theorie der algebraischen Zahlen. Leipzig 1923. 2. Aufl. 1954.

Hilbert: Bericht über die Theorie der algebraischen Zahlkörper. Jahresber. d. Dtsch. Math. Vgg. 4 (1894).
S. auch Hilbert, Ges. Werke.

Kraitchik: Théorie des nombres I. Paris 1922, II 1926. Récherches sur la . . .; 1924.

Nagell: Introduction to Number Theory. Stockholm 1951.

Trost: Primzahlen. Basel 1953.

I. Teilbarkeitseigenschaften

§ 1. Der Ring der ganzen Zahlen

Gegenstand der elementaren Zahlentheorie sind in erster Linie die natürlichen Zahlen 0, 1, 2, 3, 4 .... Die axiomatische Grundlegung der Lehre von den natürlichen Zahlen ist indes nicht Aufgabe der Zahlentheorie. Für sie stehen Existenz der natürlichen Zahlen und ihre Hauptverknüpfungsarten, Addition und Multiplikation, mit ihren Gesetzen schon fest. Auch die Erweiterung des Bereichs der natürlichen Zahlen zum Bereich der ganzen Zahlen ..., -3, -2, -1, 0, 1, 2, 3, ... mit seinen Gesetzen der Anordnung und Rechnung wird als vollzogen angesehen. Wir wollen alles zusammenstellen, was wir von den ganzen Zahlen als bekannt voraussetzen, und zwar in einer Form, die eine axiomatische Grundlegung der Lehre von den ganzen Zahlen andeutet. Dabei haben wir gleichzeitig Gelegenheit, später häufig auftretende Begriffe zu erklären.

A. Definition der natürlichen Zahlen

1. Die natürlichen Zahlen bilden eine Menge Z von unterschiedenen Elementen. Je zwei ihrer Elemente a, b sind entweder identisch, $a = b$, oder voneinander verschieden, $a \neq b$.

2. Je zwei verschiedene Elemente a, b aus Z stehen zueinander in einer durch „vor" oder „kleiner" ausgedrückten Beziehung derart, daß entweder „a vor b" oder „b vor a" gilt.

Für „a vor b" schreiben wir $a < b$. Die Schreibweisen $a < b$ und $b > a$ sollen dasselbe bedeuten, und $a \leqq b$ ist eine abkürzende Schreibweise für „$a < b$ oder $a = b$".

3. Wenn für Elemente aus Z die Beziehungen $a < b$ und $b < c$ gelten, dann gilt auch $a < c$.

Die Elemente aus Z erfüllen die Forderungen, die man an eine geordnete Menge stellt.

4. Die Menge Z besitzt ein erstes, allen vorangehendes Element, die Null.

5. Zu jedem Element aus Z gibt es ein unmittelbar folgendes Element.

6. Jeder echte Abschnitt von Z besitzt ein letztes Element.

Dabei verstehen wir unter einem Abschnitt von Z jede Teilmenge von Z, die mit irgendeinem Element auch jedes kleinere enthält, und unter einem echten Abschnitt einen solchen, der weder leer noch die volle Menge Z ist.

Die natürlichen Zahlen bilden eine geordnete Menge Z mit den drei Eigenschaften 4., 5., 6. Das ist eine der möglichen Definitionen der natürlichen Zahlen.

Endlich heißt eine Menge, die auf einen echten Abschnitt der natürlichen Zahlenreihe umkehrbar eindeutig abbildbar ist.

B. Sätze über die natürlichen Zahlen

1. Satz vom kleinsten Element: *Jede nicht leere Menge von natürlichen Zahlen hat ein kleinstes Element.*

2. Prinzip der vollständigen Induktion: *Ist eine Behauptung für die Zahl 0 richtig und folgt aus ihrer Richtigkeit für alle natürlichen Zahlen n' mit $n' \leqq n$ (oder auch nur für n) ihre Richtigkeit für die auf n unmittelbar folgende Zahl, so ist die Behauptung für jede natürliche Zahl richtig.*

3. Anzahlsatz: *Verschiedene Abschnitte der natürlichen Zahlenreihe haben verschiedene Anzahlen, d. h. es lassen sich ihre Elemente auch außer der Reihenfolge nicht gegenseitig eindeutig zuordnen.*

4. Dirichletsches Schubfächerprinzip: *Verteilt man n Dinge auf m Klassen und ist $m < n$, so kommen in irgendeiner Klasse mindestens zwei Dinge vor.*

C. Die negativen Zahlen

Zur Einführung der negativen Zahlen wird der natürliche Ordnungstypus, den wir auch in der Form $+0, +1, +2, \ldots$ schreiben, ergänzt zum symmetrischen Ordnungstypus

$$\cdots -3, -2, -1, \pm 0, +1, +2, +3, \ldots .$$

Die neuen Elemente $-m$, wo m eine natürliche Zahl ist, sind voneinander und von den alten Elementen verschieden, abgesehen von $-0 = +0$. Die Gesamtheit der alten und neuen Elemente, die Gesamtheit der ganzen Zahlen, wird geordnet durch

$$-n < -m < -0 = +0 < +m < +n$$

für alle natürlichen Zahlen m, n mit $0 < m < n$, wodurch eben

der symmetrische Ordnungstypus entsteht. Die Forderungen, die man an eine geordnete Menge stellt, sind erfüllt.

Diese so geordnete Reihe Γ der ganzen Zahlen besitzt folgende kennzeichnende Eigenschaften:

1. Jedes Element hat ein unmittelbar vorangehendes und ein unmittelbar folgendes Element.

2. Jeder echte Abschnitt besitzt ein letztes, jeder echte Rest ein erstes Element.

Dabei verstehen wir unter Rest jede Teilmenge von Γ, die mit irgendeinem Element auch jedes größere enthält, und unter einem echten Rest einen solchen, der weder leer noch gleich Γ ist.

Man nennt jetzt eine ganze Zahl $a > 0$ positiv, ein $a < 0$ negativ und bezeichnet als absoluten Betrag $|a|$ die natürliche Zahl n, für die $a = +n$ oder $a = -n$ ist.

D. Der Ring der ganzen Zahlen

In der geordneten Menge Γ der ganzen Zahlen lassen sich zwei Verknüpfungsarten erklären, die gewissen Gesetzen genügen. Die Menge Γ wird damit zum Ring Γ. Die Erklärung der Verknüpfungsarten setzen wir als bekannt voraus. Wir geben aber eine Definition des allgemeinen Ringes. Seine Elemente besitzen gewisse, gleich anzugebende Eigenschaften; von einer inhaltlichen Bedeutung wird abgesehen.

Ein **Ring** ist eine Menge R von mindestens zwei unterschiedenen Elementen, für die zwei Verknüpfungsarten definiert sind. Jedem geordneten Elementepaar a, b aus R ist durch die erste Verknüpfung ein Element c und durch die zweite Verknüpfung ein Element d aus R zugeordnet. Die erste Verknüpfung nennen wir Addition und schreiben $a + b = c$ und die zweite Verknüpfung Multiplikation, $a \cdot b = d$.

Von diesen beiden Verknüpfungen wird verlangt, daß sie für beliebige Elemente aus R folgenden Gesetzen genügen:

1. $a + b = b + a$, 2. $ab = ba$ (*Kommutativgesetze*);
3. $(a + b) + c = a + (b + c)$,
4. $(ab)c = a(bc)$ (*Assoziativgesetze*);
5. $(a + b)c = ac + bc$ (*Distributivgesetz*).

6. *Zu jedem geordneten Elementepaar a, b aus R existiert ein eindeutig bestimmtes Element c aus R, so daß $a + c = b$ ist (Gesetz der unbeschränkten und eindeutigen Substraktion).*

Aus diesen Gesetzen können die bekannten Regeln des Buchstabenrechnens hergeleitet werden, ohne daß den auftretenden Zeichen eine inhaltliche Bedeutung beigelegt wird.

Man spricht auch von einem Ring, wenn die Gültigkeit des Kommutativgesetzes der Multiplikation nicht gefordert wird. Den hier definierten Ring nennt man dann kommutativen Ring.

E. Monotoniegesetze

Für die ganzen Zahlen gelten folgende Gesetze:

1. *Es ist $a + c < b + c$, wenn $a < b$ ist (Monotoniegesetz der Addition).*

2. *Es ist $ac < bc$, wenn $a < b$ und $c > 0$ ist (Monotoniegesetz der Multiplikation).*

Insbesondere gilt $ab > 0$, wenn $a > 0$ und $b > 0$ ist. Allgemein gilt $ab \neq 0$, wenn $a \neq 0$ und $b \neq 0$ ist. In Γ ist ein Produkt von zwei Faktoren dann und nur dann gleich Null, wenn mindestens ein Faktor gleich Null ist. Daraus folgt sofort die

Eindeutigkeit der Division: *Aus $ab = ab'$ und $a \neq 0$ folgt $b = b'$.* Anders formuliert: Die Gleichung $ax = c$ besitzt für $a \neq 0$ höchstens eine Lösung.

Ist für $a \neq 0$ die Gleichung $ax = c$ in Γ lösbar, so liegt eine Besonderheit vor, die uns ausführlich beschäftigen wird. Wir sagen dann, daß c durch a teilbar ist.

Einen Ring, in dem ein Produkt von zwei Elementen nur dann gleich 0 ist, wenn mindestens ein Faktor gleich 0 ist, bezeichnet man als „Ring ohne Nullteiler". In ihm ist die Gleichung $ax = c$ bei $a \neq 0$ auf höchstens eine Weise lösbar. Denn aus $ax = ax'$ folgt $a(x - x') = 0$ und wegen der Nullteilerfreiheit $x - x' = 0$. Gibt es außerdem in dem Ring ein „Einselement" e, so daß $ae = a$ für alle Elemente a des Ringes ist, so bezeichnet man den Ring als **Integritätsbereich.** Der Ring Γ der ganzen Zahlen ist Integritätsbereich.

§ 2. Teilbarkeit, Primzahlen, Fundamentalsatz

Wir wenden uns jetzt der Teilbarkeitslehre im Integritätsbereich Γ zu. Alle vorkommenden kleinen lateinischen Buchstaben sollen Zahlen aus Γ bedeuten. Wir nennen die Zahl a durch b teilbar oder ein Vielfaches von b, wenn die Gleichung $a = b\,x$ lösbar ist. Zugleich heißt b ein Teiler von a oder eine in a aufgehende Zahl. Daß b ein Teiler von a ist, bezeichnen wir durch $b \mid a$; das Gegenteil bezeichnen wir durch $b \nmid a$. Für die Teilbarkeit gelten folgende Beziehungen, die unmittelbar aus ihrer Definition und den Eigenschaften von Γ folgen:

$\pm a \mid a$, $\pm 1 \mid a$, $a \mid 0$ für jedes a,
$0 \mid a$ nur für $a = 0$, $a \mid \pm 1$ nur für $a = \pm 1$,
aus $c \mid b$ und $b \mid a$ folgt $c \mid a$,
aus $b_1 \mid a_1$, $b_2 \mid a_2$ folgt $b_1 b_2 \mid a_1 a_2$,
aus $cb \mid ca$ folgt $b \mid a$, wenn $c \neq 0$,
aus $b \mid a_1$, $b \mid a_2$ folgt $b \mid m a_1 + n a_2$ für beliebige m, n,
aus $b \mid a$ und $a \mid b$ folgt $b = \pm a$.

Jedes a hat die *trivialen Teiler* $\pm 1, \pm a$. Gilt $t \mid a$, so nennt man t einen *wesentlichen Teiler* von a, wenn $t \neq \pm 1$ ist, und einen *echten Teiler* von a, wenn $t \neq \pm a$ ist. Besteht für $a \neq 0$ die Gleichung $a = b\,c$, also auch die Gleichung $|a| = |b|\,|c|$, so folgt $|b| \leqq |a|$. Jedes $a \neq 0$ hat also nur endlich viele Teiler. Es gibt Zahlen, die nur triviale Teiler besitzen: $\pm 1, \pm 2, \pm 3, \pm 5, \ldots$. Da für jedes a aus Γ eine der beiden Zahlen $\pm a$ eine natürliche Zahl ist und mit $b \mid a$ auch $-b \mid a$ gilt, beschränken wir uns für Teiler und Vielfache auf den Bereich der natürlichen Zahlen.

Wir stellen uns die Aufgabe, für eine gegebene natürliche Zahl $n > 1$ eine Darstellung als Produkt von möglichst vielen Faktoren, die alle größer als eins sind, aufzusuchen. Zu diesem Zweck teilen wir die natürlichen Zahlen $n > 1$ ein:

Eine natürliche Zahl p heißt **Primzahl**, *wenn $p > 1$ ist und nur triviale Teiler besitzt.*

Die übrigen natürlichen Zahlen $n > 1$ heißen zusammengesetzte oder zerlegbare Zahlen.

Satz 1: *Jede natürliche Zahl $a > 1$ besitzt mindestens einen Primteiler.*

Beweis: Die Menge aller natürlichen Teiler $t > 1$ von a ist nicht leer, denn $a \mid a$. In ihr gibt es ein kleinstes Element q. Gilt nun $p \mid q$, so folgt $p \mid a$. Da q der kleinste wesentliche Teiler von a ist, folgt $p = q$, wenn $p > 1$ ist. Also ist q ein Primteiler von a.

Die Menge der Primzahlen ist entweder endlich, d. h. auf einen echten Abschnitt der natürlichen Zahlenreihe abbildbar oder sie ist unendlich und auf die ganze natürliche Zahlenreihe abbildbar. Wir beweisen mit Euklid

Satz 2: *Es gibt unendlich viele Primzahlen.*

Beweis: Ist q eine Primzahl, in der mit 2, 3, 5, 7 beginnenden natürlichen Reihenfolge etwa die n-te, $q = p_n$, so bilde man das Produkt $P = p_1 p_2 \ldots p_n$ der ersten n Primzahlen bis q. Der kleinste wesentliche Teiler von $P + 1$ ist dann eine neue Primzahl $r > q$. Denn r ist ein Primteiler von $P + 1$, und alle Primzahlen $p_1, p_2, \ldots, p_n = q$ gehen in P, aber, weil sie größer als 1 sind, nicht in $P + 1$ auf. Also haben wir in r eine Primzahl $> q$, und daraus folgt die Existenz einer unmittelbar auf q folgenden Primzahl. (Das ist nicht notwendig r.)

Die Bedeutung der Primzahlen für den multiplikativen Aufbau der natürlichen Zahlen zeigt der Satz von der eindeutigen Primzerlegung, der **Fundamentalsatz der elementaren Zahlentheorie.**

Satz 3: *Jede natürliche Zahl $a > 1$ ist als Produkt von Primzahlen darstellbar:*

$$a = p_1 p_2 \ldots p_s \qquad (s \geqq 1). \tag{1}$$

Die Darstellung ist, abgesehen von der Reihenfolge der Faktoren, eindeutig.

Beweis: Die Aussagen der Existenz und der Eindeutigkeit sind für $a = 2$ richtig. Wir setzen voraus, daß beide Aussagen für alle a', wo $2 \leqq a' < a$ ist, zutreffen.

Die Existenz einer Zerlegung in Primfaktoren folgt nun für jedes $a \geqq 2$ daraus, daß a einen kleinsten Primteiler besitzt. Entweder ist $a = p$ selbst Primzahl, womit eine

Zerlegung gegeben ist, oder es besitzt eine Zerlegung $a = p_1 a'$ mit dem kleinsten Primteiler p_1 von a und $1 < a' < a$. Nach Induktionsvoraussetzung besitzt a' eine Primzerlegung und damit auch a.

Dieser Beweis liefert zugleich ein bestimmtes Verfahren, eine Zerlegung für a zu gewinnen. Man spaltet vom übrigbleibenden Faktor a' wieder den kleinsten Primteiler p_2 ab, $a' = p_2 a''$, und wiederholt dieses Verfahren, bis nur noch ein Primfaktor übrigbleibt. So erhält man eine bestimmte Zerlegung $a = p_1 p_2 \dots p_s$, und zwar ist $p_1 \leqq p_2 \leqq \cdots \leqq p_s$. Denn hätte in einer Teilzerlegung $a = p_1 \dots p_e f$ der Restfaktor f einen Primteiler $p < p_e$, so wäre auch $p \mid p_e f$ und somit p_e nicht der kleinste Teiler von $p_e f$. Man braucht also für die Zerlegung von f nur Primzahlen $p \geqq p_e$ daraufhin zu untersuchen, ob sie in f aufgehen. Es genügen solche, deren Quadrat f nicht übersteigt; denn soll $f = p h$ zerlegbar sein, und ist $p^2 > f$, so ist h ein Teiler von f mit der Eigenschaft $h^2 < p$. Faßt man in dieser Zerlegung gleiche Primzahlen zu Potenzen zusammen, so erhält man die *kanonische Zerlegung von* a:

$$a = p_1^{a_1} \; p_2^{a_2} \dots p_r^{a_r} \tag{2}$$

mit $p_1 < p_2 < \cdots < p_r$ und positiven Exponenten. — Diese Zerlegung nach aufsteigenden Primfaktoren besagt aber noch nicht die Eindeutigkeit der Zerlegung (1) überhaupt.

Wir beweisen jetzt die *Eindeutigkeit* nach Zermelo. Angenommen, die Primzerlegung sei nicht für alle a eindeutig. Dann gibt es eine kleinste Zahl m, die wenigstens zwei verschiedene Zerlegungen besitzt. Eine Zerlegung ist die kanonische Zerlegung. In ihr kommt der kleinste Teiler q von m vor; dadurch ist sie eindeutig bestimmt. Denn in $m = q k$ gibt es für k, da $k < m$ ist, genau eine Zerlegung. Hat man eine zweite Zerlegung, eine Zerlegung mit dem Primteiler p, so ist $p > q$; sei $m = pl$. Jetzt bilde man

$$m' = m - q l = (p - q) l. \tag{3}$$

Wegen $p > q$ und $l \geqq 2$ ist $2 \leqq m' < m$, und m' ist eindeutig zerlegbar. Nun ist

$$m' = q (k - l).$$

Wegen der eindeutigen Zerlegbarkeit von m' kommt also q in der Zerlegung der rechten Seite von (3) vor. Da l nur Primteiler hat, die größer als q sind, tritt q in der Zerlegung von $p - q$ auf. Aus $p - q = q\,r$ folgt $p = q\,(r+1)$. Das ist ein Widerspruch zur Primzahleigenschaft von p. — Also hat auch m nur eine Zerlegung.

Der Fundamentalsatz gibt uns Aufschluß über sämtliche Teiler einer Zahl a, wenn ihre Primzerlegung (2) bekannt ist. Alle Zahlen

$$m = p_1^{c_1}\ p_2^{c_2} \dots p_r^{c_r} \text{ mit } 0 \leqq c_i \leqq a_i \tag{4}$$

und nur diese sind Teiler von a. Daß diese m Teiler von a sind, ist klar. Daß andere Primteiler als $p_1, \dots, p_r$ in der Zerlegung eines Teilers t von a nicht vorkommen, folgt aus dem Fundamentalsatz. Und schließlich treten in der Zerlegung eines Teilers t keine Exponenten $c_i > a_i$ auf; denn sonst hätten wir etwa

$$p_1^{a_1+1} \mid t \mid a \text{ und damit } a = p_1^{a_1+1} v;$$

daraus würde der Widerspruch $p_1 \mid p_2^{a_2} \dots p_r^{a_r}$ folgen. Die Anzahl aller Teiler von a einschließlich a und 1 ist daher

$$\tau(n) = (a_1+1)(a_2+1)\dots(a_r+1), \tag{5}$$

dem Produkt der Zahlen, die angeben, wieviel Möglichkeiten für das einzelne c_i bestehen.

§ 3. Größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches

Wir fragen jetzt nach den natürlichen Zahlen, die zugleich Teiler von zwei positiven Zahlen a und b sind. Die verschiedenen Primzahlen, die entweder Teiler von a oder von b sind, seien $p_1, p_2, \dots, p_r$. Dann lassen sich a und b eindeutig in folgender Form schreiben:

$$\begin{aligned} a &= p_1^{\alpha_1}\ p_2^{\alpha_2} \dots p_r^{\alpha_r}, \\ b &= p_1^{\beta_1}\ p_2^{\beta_2} \dots p_r^{\beta_r}. \end{aligned} \tag{6}$$

Hier sind die α_i und β_i natürliche Zahlen, die gleich 0 sind,

wenn p_i in der Zerlegung von a oder b nicht vorkommt. Damit eine Zahl t zugleich die Zahlen a und b teilt, ist nach (4) notwendig und hinreichend, daß t die Form

$$t = p_1^{t_1} \; p_2^{t_2} \cdots p_r^{t_r}$$

hat, wo gleichzeitig $0 \leqq t_i \leqq \alpha_i$ und $0 \leqq t_i \leqq \beta_i$ erfüllt sind. Die größte unter diesen Zahlen hat die Exponenten $t_i = \min(\alpha_i, \beta_i)$; sie ist ein Vielfaches jedes gemeinsamen Teilers von a und b. Damit gilt

Satz 4: *Zu zwei positiven Zahlen a und b gibt es eine und nur eine positive Zahl d mit den beiden Eigenschaften: 1. $d|a$, $d|b$, 2. aus $t|a$, $t|b$ folgt $t|d$ und umgekehrt. Sie ist der größte gemeinsame Teiler der Zahlen a und b und wird mit $d = (a, b)$ bezeichnet.*

Aus diesen beiden Eigenschaften folgt schon, ohne daß die Primzerlegung herangezogen wird, die eindeutige Bestimmtheit von d. Denn wenn d' auch 1. und 2. erfüllt, folgt $d'|d$ und $d|d'$, also $d' = d$.

Der gr. g. T. von mehr als zwei positiven Zahlen, auch von unendlich vielen, wird entsprechend definiert: $d = (a_1, a_2, \ldots, a_n)$.

Ergänzend definieren wir $(a_1, a_2, \ldots, a_n)$ für den Fall, daß ein $a_i = 0$ ist. Man streiche alle $a_i = 0$ und bilde den gr. g. T. für die übrigen Zahlen, falls es solche gibt; sonst wird $(a_1, a_2, \ldots, a_n) = 0$ gesetzt. Auch für diese Ergänzungen treffen 1. und 2. zu. Dagegen ist $(0, 0, \ldots, 0)$ nicht mehr der gr. g. T. im Sinne der Anordnung.

Die Frage nach den gemeinsamen natürlichen Vielfachen zweier positiven Zahlen a und b ist in analoger Weise zu beantworten. Schreiben wir wieder a und b in der eben verwendeten Form, so hat eine Zahl v, die zugleich Vielfaches von a und b ist, offensichtlich die Gestalt

$$v = p_1^{v_1} \; p_2^{v_2} \ldots p_r^{v_r},$$

wo die v_i gleichzeitig $v_i \geqq a_i$, $v_i \geqq b_i$ erfüllen. Das kleinste derartige v hat die Exponenten $v_i = \max(\alpha_i, \beta_i)$ und ist ein Teiler aller gemeinsamen Vielfachen von a und b. Damit gilt

Satz 5: *Zu zwei natürlichen Zahlen a und b gibt es eine und nur eine positive Zahl e mit den beiden Eigenschaften: 1.* $a|e, b|e$, *2. aus* $a|v, b|v$ *folgt* $e|v$ *und umgekehrt. Sie ist das kleinste gemeinsame Vielfache der Zahlen a, b und wird mit* $[a, b]$ *bezeichnet.*

Das kl. g. V. von mehr als zwei, aber endlich vielen Zahlen wird entsprechend definiert.

Durch die Eigenschaften 1. und 2. ist e eindeutig festgelegt.

Für beliebige ganze a_i sollen das kl. g. V. und der gr. g. T. eingeführt werden durch die Forderung, daß sie sich nicht ändern, wenn ein a_i durch $-a_i$ ersetzt wird. Im übrigen werden als gemeinsame Vielfache und Teiler nur die natürlichen betrachtet.

Aus den Definitionen des gr. g. T. und kl. g. V. ergeben sich ohne Schwierigkeiten folgende *Rechenregeln* bei beliebigen ganzen a_i und t:

$(a_1, \ldots, a_n)$ und $[a_1, \ldots, a_n]$ sind unabhängig von der Reihenfolge der a_i,

$(a_1, \ldots, a_n) = (a_1, (a_2, \ldots, a_n)), [a_1, \ldots, a_n] = [a_1, [a_2, \ldots, a_n]],$
$(ta_1, \ldots, ta_n) = |t|\,(a_1, \ldots, a_n), [ta_1, \ldots, ta_n] = |t|\,[a_1, \ldots, a_n],$
$(a_0, a_1, \ldots, a_n) \mid (a_1, \ldots, a_n), [a_1, \ldots, a_n] \mid [a_0, a_1, \ldots, a_n],$
$(0, a_1, \ldots, a_n) = (a_1, \ldots, a_n), [1, a_1, \ldots, a_n] = [a_1, \ldots, a_n],$
$(1, a_1, \ldots, a_n) = 1, [0, a_1, \ldots, a_n] = 0.$

Diese Regeln sind für die Bestimmung des gr. g. T. und kl. g. V in konkreten Fällen oft von Nutzen.

Zwischen dem kl. g. V. und dem gr. g. T. zweier natürlicher Zahlen besteht die Beziehung

$$ab = (a, b)\,[a, b]$$

durch welche die Bestimmung des kl. g. V. auf die Bestimmung des gr. g. T. zurückgeführt wird. Sie ist enthalten in dem

Satz 6: Für $A = a_1 q_1 = a_2 q_2 = \cdots = a_n q_n \geqq 0$ *gilt* $A = (a_1, \ldots, a_n)\,[q_1, \ldots, q_n] = [a_1, \ldots, a_n]\,(q_1, \ldots, q_n)$.

Beweis: Für $A = 0$ folgt die Behauptung unmittelbar aus unseren Definitionen. Für $A \neq 0$ schreiben wir unter Verwendung des Produktzeichens

$$A = \prod_{\nu=1}^{r} p_\nu^{\alpha_\nu}, \quad a_i = \prod_{\nu=1}^{r} p_\nu^{\alpha_{i\nu}}, \quad q_i = \prod_{\nu=1}^{r} p_\nu^{\alpha_\nu - \alpha_{i\nu}}.$$

Dann ist

$$(a_1, \ldots, a_n) = \prod p_\nu^{\delta_\nu}, \; \delta_\nu = \min(\alpha_{1\nu}, \ldots, \alpha_{n\nu}),$$

$$[a_1, \ldots, a_n] = \prod p_\nu^{\varepsilon_\nu}, \; \varepsilon_\nu = \max(\alpha_{1\nu}, \ldots, \alpha_{n\nu}),$$

$$(q_1, \ldots, q_n) = \prod p_\nu^{\delta'_\nu}, \; \delta'_\nu = \min(\alpha_\nu - \alpha_{1\nu}, \ldots, \alpha_\nu - \alpha_{n\nu}),$$

$$[q_1, \ldots, q_n] = \prod p_\nu^{\varepsilon'_\nu}, \; \varepsilon'_\nu = \max(\alpha_\nu - \alpha_{1\nu}, \ldots, \alpha_\nu - \alpha_{n\nu}).$$

Wegen $\min(\alpha_\nu - \alpha_{1\nu}, \ldots, \alpha_\nu - \alpha_{n\nu}) = \alpha_\nu - \max(\alpha_{1\nu}, \ldots, \alpha_{n\nu})$ und $\max(\alpha_\nu - \alpha_{1\nu}, \ldots, \alpha_\nu - \alpha_{n\nu}) = \alpha_\nu - \min(\alpha_{1\nu}, \ldots, \alpha_{n\nu})$ ist $\delta_\nu + \varepsilon'_\nu = \varepsilon_\nu + \delta'_\nu = \alpha_\nu$, womit die Behauptung bewiesen ist. Für $n = 2$ und $a_1 = q_2 = a$, $a_2 = q_1 = b$ ist das $(a, b)\,[a, b] = ab$. Für $n = 3$ lautet die entsprechende Regel $a\,b\,c = (a, b, c)\,[bc, ac, ab] = [a, b, c]\,(bc, ac, ab)$.

Wenn zwei Zahlen a und b keinen andern gemeinsamen Teiler als 1 besitzen, wenn also $(a, b) = 1$ ist, nennt man a und b „teilerfremd", „relativ prim" oder „prim zueinander". Auch n Zahlen heißen teilerfremd, wenn $(a_1, \ldots, a_n) = 1$ ist, dagegen „paarweise teilerfremd", wenn je zwei der Zahlen $a_1, \ldots, a_n$ teilerfremd sind, was schon für $n = 3$ mehr bedeutet. Z. B. ist $(481, 629, 663) = 1$, aber $(481, 629) = 37$, $(481, 663) = 13$, $(629, 663) = 17$.

Ein Kriterium für Teilerfremdheit und paarweise Teilerfremdheit haben wir in

Satz 7: *Die Zahlen $a_1, a_2, \ldots$ sind dann und nur dann teilerfremd, wenn sie keinen gemeinsamen Primteiler haben. Sie sind dann und nur dann paarweise teilerfremd, wenn die Primteiler von $a_1, a_2 \ldots$ lauter verschiedene Primzahlen sind.*

Der Beweis dieses Satzes und der gleich folgenden Sätze ergibt sich unmittelbar aus unserer Übersicht über die Teiler einer Zahl. Es gelten: