Es ist für die moderne Entwicklung der Algebra charakteristisch, daß die oben genannten Hilfsmittel zu selbständigen umfangreichen Theorien Anlaß gegeben haben, die gegenüber der vorstehend angeführten Grundaufgabe der klassischen Algebra immer mehr in den Mittelpunkt des Interesses getreten sind. So ist denn in moderner Auffassung die Algebra nicht mehr bloß die Lehre von der Auflösung der Gleichungen, sondern die Lehre von den formalen Rechenbereichen, wie Körpern, Gruppen u.a., und ihre Hauptaufgabe ist die Gewinnung von Einsichten in die Struktur solcher Bereiche (siehe dazu S. 24). Im beschränkten Rahmen der vorliegenden Bändchen ist es uns jedoch nicht möglich, diesen allgemeineren, modernen Gesichtspunkt in den Vordergrund zu stellen. Wir nehmen daher die vorstehend ausgesprochene Grundaufgabe der klassischen Algebra als wegweisenden Leitfaden und abgrenzenden Rahmen für unsere Darlegungen, werden aber dabei in der Tat, vor allem in **2**, auch zu strukturellen Aussagen im Sinne der modernen Algebra geführt werden.

I. Ringe, Körper, Integritätsbereiche

§ 1. Definition der Ringe, Körper, Integritätsbereiche

Als das formal-charakteristische, von der inhaltlichen Bedeutung der Zeichen als Zahlen befreite an den drei elementaren Rechenoperationen Addition, Substraktion, Multiplikation — die vierte, Division, ziehen wir erst später hinzu — ist folgender Tatbestand anzusehen:

(a) *Es liegt eine* Menge B von unterschiedenen Elementen *in irgendeiner endlichen Anzahl* (*mindestens zwei*) *oder in unendlicher Anzahl vor.*

Wir verwenden Buchstaben $a, b, \ldots$ und kompliziertere Zeichen (z.B. die späterhin erklärten Zeichen $a + b$, $ab, \ldots$), um die Resultate logischer Setzungen von Elementen aus B mitzuteilen, und sagen dann auch einfach, $a, b, \ldots$ seien *Elemente aus* B. Auf Grund der in (a) geforderten Unterschiedenheit steht für je zwei solche logische Setzungen a, b fest, ob es sich um dasselbe oder um verschiedene Elemente aus B handelt, was wir durch die Bezeichnungen $a = b$ bzw. $a \neq b$ angeben.

(b) *Für je zwei in bestimmter Reihenfolge gegebene, nicht notwendig verschiedene Elemente a, b aus B sind* zwei Verknüpfungen *definiert, d. h. jedem geordneten Elementpaar a, b aus B ist irgendwie ein Element c (erste Verknüpfung) und ein Element d (zweite Verknüpfung) aus B zugeordnet.*

(a) und (b) sind z. B. realisiert, wenn B die Menge aller geraden, oder aller ganzen, oder aller rationalen, oder aller reellen, oder aller komplexen Zahlen, oder aller positiven von einer dieser Zahlsorten (mit Ausnahme der letztgenannten) ist und als Verknüpfungen die Addition ($c = a + b$) und Multiplikation ($d = ab$) gewählt werden. In Anlehnung an diese als Ausgangspunkt unserer Abstraktion anzusehenden Spezialfälle wollen wir die beiden Verknüpfungen in (b) auch allgemein *Addition* und *Multiplikation*, die dem Paar a, b zugeordneten Elemente c und d *Summe* und *Produkt* nennen und $c = a + b$, $d = ab$ schreiben, obwohl natürlich die rein formale Forderung (b) (und ebenso auch die gleich folgende Forderung (c) an unsere Verknüpfungen) keinerlei Anlaß zu der inhaltlichen Annahme gibt, daß diese Verknüpfungen, wenn B eine Zahlenmenge ist, mit der gewöhnlichen Addition und Multiplikation übereinstimmen.

(c) *Die in* (b) *genannten beiden Verknüpfungen genügen für beliebige Elemente aus B den Gesetzen:*

(1) $a + b = b + a$, **(2)** $ab = ba$
(kommutatives Gesetz);

(3) $(a + b) + c = a + (b + c)$, **(4)** $(ab)c = a(bc)$
(assoziatives Gesetz);

(5) $(a + b)\, c = ac + bc$
(distributives Gesetz);

(6) *Zu jedem geordneten Elementpaar a, c aus B existiert ein eindeutig bestimmtes Element b aus B derart, daß $a + b = c$ ist*

(Gesetz der unbeschränkten und eindeutigen Subtraktion).

Wie schon in der beigefügten Benennung des Gesetzes (6) zum Ausdruck gebracht ist, bezeichnet man die nach (6) in B unbeschränkt und eindeutig ausführbare Operation der Bestimmung von b aus $a + b = c$ als *Subtraktion* und führt daher in sinngemäßer Fortsetzung der unter (b) verwendeten Terminologie die Bezeichnung $b = c - a$ (*Differenz*) ein.

Definition 1. *Wenn für eine Menge* B *die unter* (a), (b), (c) *aufgeführten Tatsachen realisiert sind, heißt* B *ein* Ring *bezüglich der Verknüpfungen* (b).

Den letzten Zusatz muß man machen, weil eine Menge B a priori bezüglich je zweier verschiedenartig erklärter Verknüpfungen, also in mehrfacher Weise Ring sein kann (siehe dazu **3**, 1, § 1, Aufg. 4, 5). Unter einem Ring B schlechthin versteht man immer die Menge B mit Einschluß der für sie definierten Verknüpfungen. — Wir bezeichnen Ringe stets mit großen griechischen, Elemente aus Ringen mit kleinen lateinischen oder griechischen Buchstaben[1]).

Wir beweisen nun zunächst einige in Ringen gültige Tatsachen.

Satz 1. *In jedem Ring* B *existiert ein eindeutig bestimmtes Element* 0, *das* Nullelement *oder* Null *von* B *heißt, mit der Eigenschaft*

$$a + 0 = a \quad \textit{für alle } a \textit{ aus } \mathsf{B}.$$

Beweis. Nach (6) existieren in B zu den Elementen $a, b, \ldots$ von B je die Differenzen $a - a, b - b, b - a, \ldots$, für die nach ihrer Erklärung gilt

$$a + (a - a) = a, \quad b + (b - b) = b, a + (b - a) = b, \ldots.$$

Vermöge der ersten und dritten dieser Relationen hat man, nun unter Beachtung von (1) und (3),

$$\begin{aligned} b + (a - a) &= [a + (b - a)] + (a - a) \\ &= [a + (a - a)] + (b - a) = a + (b - a) = b. \end{aligned}$$

Der Vergleich mit der zweiten jener Relationen ergibt dann, zufolge der Eindeutigkeit in (6),

$$a - a = b - b.$$

[1]) Die Buchstaben $i, k, l, m, n, p, q, r, s$; $\iota, \varkappa, \lambda, \mu, \nu, \varrho, \sigma$ behalten wir jedoch für gewöhnliche ganze Zahlen, z. B. Indizes und Exponenten, vor.

Also sind alle Differenzen $a - a, b - b, \ldots$ dasselbe Element 0 von B. Dieses hat die im Satz genannte Eigenschaft und ist nach (6) sogar schon durch eine einzige der Forderungen $a + 0 = a$ eindeutig bestimmt.

Satz 2. *Es gilt* $0c = 0$ *für jedes* c *aus* B.

Beweis. Nach (5) und Satz 1 ist für beliebiges c aus B

$$0c = (0 + 0)\,c = 0c + 0c,$$

also nach (6) und Satz 1 schließlich $0c = 0$.

Wir ziehen jetzt die bisher noch unberücksichtigte Division in den Kreis unserer Betrachtungen, indem wir den unter (c) genannten Forderungen (1)—(6) noch die folgende anreihen:

(7) *Zu jedem geordneten Elementpaar* a, c *aus* B, *in dem* $a \neq 0$ *ist, existiert ein eindeutig bestimmtes Element* b *aus* B *derart, daß* $ab = c$ *ist*

(Gesetz der unbeschränkten und eindeutigen Division).

Analog wie oben bei der Subtraktion bezeichnet man auch hier, wenn (7) in B erfüllt ist, die in B bis auf die Einschränkung $a \neq 0$ unbeschränkt und eindeutig ausführbare Operation der Bestimmung von b aus $ab = c$ als *Division* und führt die Bezeichnung $b = \dfrac{c}{a}$ (*Quotient*) ein.

Die in (7) gemachte Einschränkung $a \neq 0$ ist keine willkürliche Festsetzung, sondern notwendig, wenn (a), (b), (c) und (7) widerspruchsfrei nebeneinander bestehen sollen. Ohne diese Einschränkung folgte nämlich, wenn c ein beliebiges Element aus B ist, aus der Existenz eines b, so daß $0b = c$ ist, nach Satz 2, daß $c = 0$ wäre. Es enthielte also B nur das eine Element 0 im Widerspruch zu (a). Betreffs der hierdurch nahegelegten Frage, ob die Forderungen (a), (b), (c), (7) in der vorliegenden Gestalt widerspruchsfrei sind, sei bemerkt, daß ein Widerspruch in (a), (b), (c), (7) einen Widerspruch im System der rationalen Zahlen zur Folge hätte, das ja allen jenen Forderungen genügt.

Es sei noch bemerkt, daß die in der Einschränkung $a \neq 0$ in (7) bestehende Unsymmetrie der sonst bezüglich Addition und

Multiplikation symmetrischen Tafel der Forderungen (1) und (2), (3) und (4), (6) und (7) natürlich auf die Unsymmetrie des einzigen beide Operationen verbindenden Gesetzes (5) zurückgehen muß, wie ja auch die obige Begründung jener Einschränkung (Beweis von Satz 2) zeigt.

Definition 2. *Gilt in einem Ringe* B *außer* (a), (b), (c) *auch noch* (7), *so heißt* B *ein* K ö r p e r *bezüglich der Verknüpfungen* (b).

Analog zu Satz 1 gilt in Körpern außerdem:

Satz 3. *In jedem Körper* K *existiert ein eindeutig bestimmtes Element* $e \neq 0$, *das* E i n s e l e m e n t *oder* E i n s *von* K *heißt, mit der Eigenschaft*

$$ae = a \text{ für alle } a \text{ aus } \mathsf{K}.$$

Beweis. Der Beweis wird, zunächst für die wegen (a) sicher vorhandenen $a \neq 0$ aus K, unter Verwendung von (7) statt (6) ganz analog wie bei Satz 1 geführt. Daß ferner $ae = a$ auch für $a = 0$ gilt, ist nach Satz 2 klar. Aus $e = 0$ schließlich würde folgen $a = ae = a0 = 0$ für jedes a aus K, im Widerspruch zu (a).

Außer Ringen und Körpern braucht man in der Algebra noch einen weiteren derartigen Begriff, der logisch zwischen jenen beiden steht, den des *Integritätsbereiches.* Dieser entsteht aus dem Ringbegriff, wenn man nur einen Teil der zum Körperbegriff führenden Zusatzforderung (7) stellt, nämlich aus dieser einerseits die unbeschränkte Existenz des Quotienten wegläßt, also nur die Eindeutigkeit der Division, falls sie überhaupt ausführbar ist, fordert:

(7a) *Aus* $ab = ab'$ *und* $a \neq 0$ *folgt* $b = b'$ (E i n d e u t i g k e i t d e r D i v i s i o n),

andererseits aber doch die Existenz der speziellen Quotienten $\frac{a}{a}, \frac{b}{b}, \ldots$, wo $a, b, \ldots \neq 0$ sind, fordert, was nach dem Vorhergehenden auf die Forderung der Gültigkeit des Analogons zu Satz 3 hinausläuft:

(7b) *Es existiert ein Element e in* B *derart, daß* $ae = a$ *für alle* a *aus* B *ist* (Existenz des Einselementes).

Definition 3. *Gelten in einem Ringe* B *außer* (a), (b), (c) *auch noch* (7a) *und* (7b), *so heißt* B *ein* Integritätsbereich *bezüglich der Verknüpfungen* (b).

Jeder Körper ist ein Integritätsbereich, weil ja (7a) und (7b) aus (7) gefolgert werden können, und jeder Integritätsbereich ist nach Def. 3 ein Ring.

Ringe, Körper, Integritätsbereiche nennen wir auch gemeinsam *Bereiche*[1]) und die in ihnen erklärten Verknüpfungen Addition, Substraktion, Multiplikation, ev. Division die *drei ersten* bzw. *vier elementaren* Rechenoperationen.

In Integritätsbereichen (also speziell in Körpern), die uns im folgenden hauptsächlich interessieren werden, gilt auch die Umkehrung von Satz 2:

Satz 4. *Ist das Produkt zweier Elemente eines Integritätsbereiches Null, so ist mindestens einer der Faktoren Null, d. h. aus* $ab = 0$, $a \neq 0$ *folgt* $b = 0$.

Beweis. Sei $ab = 0$, $a \neq 0$. Da nach Satz 2 $a0 = 0$, also hier $ab = a0$ ist, folgt nach (7a) $b = 0$.

Das Bestehen von Satz 4 ist übrigens nicht nur, wie eben gezeigt, Folge aus (7a), sondern auch umgekehrt. Denn gilt das Analogon zu Satz 4 in einem Ringe und besteht für ein $a \neq 0$ die Gleichung $ab = ab'$, d. h. $a(b - b') = 0$, so folgt $b - b' = 0$, d. h. $b = b'$.

Zusatz zu Definition 3. *Man kann die Forderungen* (7a), (7b) *der Def.* 3 *auch durch die Forderungen ersetzen, daß die Analoga zu Satz* 3 *und Satz* 4 *in* B *gelten sollen.*

Es bedarf wohl nur des Hinweises, daß aus den Gesetzen (a), (b), (c) für Ringe alle allgemeinen Rechenregeln der elementaren Algebra für die Addition, Subtraktion und Multiplikation, insbesondere die sog. Klammerauflösungsformeln, und, wenn man (7) hinzunimmt, auch die allgemeinen Formeln der Bruchrechnung

---

[1]) Bereich bedeutet zwar hiernach dasselbe wie Ring; jedoch ist der neutrale Ausdruck Bereich im angegebenen Sinne geläufiger, während man Ring gewöhnlich nur dort anwendet, wo wirklich kein Integritätsbereich vorliegt.

durch einfache Schlüsse hergeleitet werden können. Die nähere Ausführung darf dem Leser überlassen bleiben.

Man verwendet beim Rechnen in einem Bereich B zweckmäßig folgende abkürzenden Bezeichnungen:

$$-a \text{ für } 0-a,$$

$\ldots, (-2)a, (-1)\,a,\ 0a,\ 1a,\ 2a, \ldots$ für $\ldots -(a+a), -a, 0, a, a+a, \ldots$ (*ganze Vielfache von* a),

$\ldots, a^{-2},\ a^{-1}, a^0, a^1,\ a^2, \ldots$ für $\ldots, \dfrac{e}{aa}, \dfrac{e}{a},\ e,\ a,\ aa, \ldots$

(*ganze Potenzen von* a)

($a^{-1}, a^{-2}, \ldots$ natürlich nur, soweit eindeutig erklärt, also z. B. wenn B ein Körper und $a \neq 0$ ist). Aus (1)—(7) und Satz 1—4 ergeben sich dann mittels der Definition der Rechenoperationen im Bereich der ganzen Zahlen leicht die Tatsachen

$$(m+n)\,a = m\,a + n\,a,\quad a^{m+n} = a^m\,a^n,\ (a^m)^n = a^{mn},$$
$$(m\,n)e = (me)\,(n\,e),\quad e^m = e,\quad m0 = 0,\quad 0^m = 0$$

für ganze Zahlen m, n, soweit die darin vorkommenden Elemente einen eindeutigen Sinn auf Grund des Vorhergehenden haben.

Beispiele

1. Auf Grund der vorstehenden Ausführungen dürfen wir als aus den Elementen bekannt hinstellen:

Satz 5. *Die* $\left\{\begin{array}{l}\textit{ganzen}\\ \textit{rationalen}\end{array}\right\}$ *Zahlen*

bilden einen $\left\{\begin{array}{l}\textit{Integritätsbereich } \Gamma\\ \textit{Körper } \mathsf{P}\end{array}\right\}$, *wenn als Verknüpfungen die gewöhnliche Addition und Multiplikation zugrunde gelegt werden. Die Zahlen* 0 *und* 1 *sind Null- und Einselement von* Γ *und* P.

2. Ferner bilden auch alle reellen, sowie auch alle komplexen Zahlen einen Körper bezüglich der gewöhnlichen Addition und Multiplikation.

3. Die geraden Zahlen bilden einen Ring, aber keinen Integritätsbereich, weil für sie (7b) nicht gilt. Ringe, in denen (7b) gilt, aber (7a) nicht, werden wir in **2**, § 2 kennenlernen. Als Beispiel eines Integritätsbereiches, der kein Körper ist, dient schon Γ.

4. Der folgende Körper mag als Beispiel einerseits für einen solchen genannt werden, dessen Elemente keine Zahlen sind, andererseits für einen mit nur endlich vielen Elementen:

Für zwei Elemente 0 und e werden zwei Verknüpfungsoperationen durch die Festsetzungen

$$\begin{array}{ll} 0+0=0 & 00=0 \\ 0+e=e+0=e & 0e=e0=0 \\ e+e=0 & ee=e \end{array}$$

erklärt. Man bestätigt leicht die Richtigkeit von (1)—(7). Wir haben also einen Körper, der lediglich aus seinem Null- und Einselement besteht. Daß dieser Körper kein uninteressanter Ausnahmefall ist, zeigen die Ergebnisse von **2**, § 20, wonach endliche Körper existieren, deren Elementzahl eine beliebige Primzahlpotenz ist. Siehe auch schon § 2, Beispiel 5 [25].

§ 2. Teilbereiche, Kongruenzrelationen, Isomorphie

In § 1 wird mit der Forderung (a) von einer Menge unterschiedener Elemente, der Grundgegebenheit der *Mengenlehre*, ausgegangen, die dann durch Hinzunahme der Forderungen (b), (c) usw. zu der Grundgegebenheit der *Algebra* d. h. zum *Bereich*, wird. Es ist daher verständlich, daß für das Studium unserer Bereiche u. a. auch Begriffe und Tatsachen heranzuziehen sind, die allein aus (a) folgen, also der Mengenlehre angehören, und von denen dann zu untersuchen ist, wie sie bei Hinzunahme von (b), (c) usw. für das Studium von Bereichen nutzbar gemacht werden können. Wir müssen uns hier darauf beschränken, die heranzuziehenden mengentheoretischen Grundlagen vom sog. naiven Standpunkt aus kurz zusammenzustellen, ohne auf die in neuerer Zeit durch die Paradoxien der Mengenlehre entstandenen begrifflichen Schwierigkeiten einzugehen, die man durch ein entsprechendes axiomatisches Vorgehen beheben kann, wie es in § 1 für Bereiche, gestützt auf den Mengenbegriff, durchgeführt wurde. Wir verzichten also insbesondere auf eine naiv nicht in befriedigender Weise zu gebende Präzisierung des Begriffs der Menge.

1. Teilmengen

Es sei M eine *Menge*, worunter wir stets, wie in § 1, (a), eine Menge unterschiedener Elemente verstehen. Eine Menge M_1 heißt *Teilmenge* von M oder in M *enthalten*, wenn jedes Element von M_1 auch in M vorkommt. Wir rechnen die Menge M selbst, sowie die kein Element enthaltende *leere Menge* (*Nullmenge*) ebenfalls als Teilmengen von M. Alle anderen Teilmengen von M heißen *echt* oder *eigentlich*.

Liegen Teilmengen $M_1, M_2, \ldots$ einer Menge M in irgendeiner endlichen oder unendlichen Anzahl vor, so gibt es dazu zwei bestimmte Teilmengen von M, ihren *Durchschnitt* Δ und ihre *Vereinigungsmenge* E. Der Durchschnitt Δ besteht aus allen und nur den Elementen von M, die sowohl in M_1 als auch in $M_2, \ldots$ enthalten sind. Er kann auch die Nullmenge sein. Die Vereinigungsmenge E besteht aus allen und nur den Elementen von M, die entweder in M_1 oder in $M_2, \ldots$ enthalten sind. E läßt sich auch erklären als Durchschnitt aller $M_1, M_2, \ldots$ enthaltenden Teilmengen von M und ist in diesem Sinne die engste $M_1, M_2, \ldots$ enthaltende Teilmenge von M. Ebenso läßt sich Δ erklären als Vereinigungsmenge aller in $M_1, M_2, \ldots$ enthaltenen Teilmengen von M und ist in diesem Sinne die weiteste in $M_1, M_2, \ldots$ enthaltene Teilmenge von M.

2. Äquivalenzrelationen und Klasseneinteilungen

Für die Algebra von besonderer Wichtigkeit sind Zerlegungen einer Menge M in elementfremde Teilmengen, d. h. Darstellungen von M als Vereinigungsmenge von Teilmengen, von denen je zwei die Nullmenge zum Durchschnitt haben. Solche Zerlegungen von M nennen wir *Klasseneinteilungen von* M und die betr. Teilmengen auch *Klassen*. Liegt eine solche Klasseneinteilung vor, und setzt man zwischen je zwei in bestimmter Reihenfolge gegebene Elemente a, b aus M das Zeichen $\sim$ oder das Zeichen $\nsim$ je nachdem a in derselben Teilmenge wie b vorkommt oder nicht, so bestehen offenbar die Tatsachen:

(α) $a \sim a$ (*Gesetz der* Reflexivität),
(β) *aus* $a \sim b$ *folgt* $b \sim a$ (*Gesetz der* Symmetrie),
(γ) *aus* $a \sim b, b \sim c$ *folgt* $a \sim c$ (*Gesetz der* Transitivität).

Für das Bestehen dieser Tatsachen, gleichgültig welche Bedeutung dabei den Zeichen $\sim$, $\nsim$ zukommt, führen wir eine besondere Ausdrucksweise ein:

(I) *Wenn zwischen je zwei in bestimmter Reihenfolge gegebene Elemente von* M *eines und nur eines von zwei Zeichen* $\sim$, $\nsim$ *in solcher Weise gesetzt ist, daß die Bedingungen* (α), (β), (γ) *bestehen, so sagt man, daß eine* Äquivalenzrelation $\sim$ *in* M *erklärt sei.*

Es gilt dann also:

(A) *Jede Klasseneinteilung von* M *führt zu einer Äquivalenzrelation in* M, *indem zwischen Elemente aus einer Klasse* $\sim$, *zwischen Elemente aus verschiedenen Klassen* $\not\sim$ *gesetzt wird.*

Nicht nur in der Algebra, sondern in fast jeder mathematischen Disziplin hat man außerordentlich häufig die Umkehrung dieser Tatsache zu benutzen, die wir daher hier ausführlich begründen wollen.

(B) *Jede Äquivalenzrelation in* M *entspringt gemäß* (A) *aus einer und nur einer Klasseneinteilung von* M.

Beweis. a) Wenn eine Äquivalenzrelation in M vorliegt, so kann eine Teilmenge M_1 von M die Eigenschaft E haben, daß ein Element c aus M derart existiert, daß M_1 aus allen und nur den Elementen d von M besteht, für die $c \sim d$ ist. Wir nennen dann für den Augenblick M_1 eine E-Teilmenge von M, die durch c erzeugt ist. Jedes Element c aus M erzeugt eine E-Teilmenge, aber natürlich kann dieselbe E-Teilmenge i. a. durch verschiedene Elemente erzeugt sein. Wir betrachten nun die sämtlichen E-Teilmengen von M und zeigen, daß diese die Klassen einer Klasseneinteilung von M sind, aus der die betrachtete Äquivalenzrelation im Sinne von (A) entspringt.

Erstens sind verschiedene E-Teilmengen M_1, M_2 von M elementfremd. Wäre nämlich das Element a in M_1 und M_2 enthalten, und ist M_1 durch c_1, M_2 durch c_2 erzeugt, so wäre $c_1 \sim a$, $c_2 \sim a$, also nach (β), (γ) auch $c_1 \sim c_2$. Ist dann d_1 ein Element aus M_1, d_2 ein Element aus M_2, also $c_1 \sim d_1$, $c_2 \sim d_2$, so folgte wiederum aus (β), (γ) auch $c_1 \sim d_2$, $c_2 \sim d_1$, so daß d_2 auch in M_1, d_1 auch in M_2 enthalten wäre. Es wären also dann gegen die Annahme M_1 und M_2 identisch.

Zweitens ist die Vereinigungsmenge aller E-Teilmengen die Menge M, d. h. jedes Element a aus M kommt wirklich in einer E-Teilmenge vor. Denn nach (α) kommt a in der durch a erzeugten E-Teilmenge vor.

Hiernach sind also die E-Teilmengen von M die Klassen einer Klasseneinteilung von M. Daß die betrachtete Äquivalenzrelation im Sinne von (A) aus ihr entspringt, folgt so:

Erstens steht zwischen zwei Elementen a, b derselben E-Teilmenge M_1 das Zeichen $\sim$. Denn ist M_1 durch c erzeugt, so ist $c \sim a$, $c \sim b$, also nach (β), (γ) auch $a \sim b$.

Zweitens steht zwischen zwei Elementen a, b verschiedener E-Teilmengen M_1, M_2 von M das Zeichen $\not\sim$. Wäre nämlich $a \sim b$, und ist M_1 durch c_1, M_2 durch c_2 erzeugt, so folgte aus $c_1 \sim a$, $c_2 \sim b$ nach (β), (γ) auch $c_1 \sim c_2$ und daraus wie oben ein Widerspruch gegen die Verschiedenheit von M_1 und M_2.

b) Daß eine Äquivalenzrelation nicht aus zwei verschiedenen Klasseneinteilungen von M entspringen kann, folgt daraus, daß die ein Element a enthaltende Klasse notwendig aus allen und nur den b mit $a \sim b$ bestehen muß, also durch die Äquivalenzrelation eindeutig (als die durch a erzeugte E-Teilmenge von M) bestimmt ist.

Liegt eine Klasseneinteilung von M vor, so heißt jede Teilmenge von M, die aus jeder Klasse ein und nur ein Element enthält, ein *vollständiges Repräsentantensystem* für diese Klasseneinteilung.

Die einfachste Äquivalenzrelation ist die logische Identität, d. i. die in § 1 unter (a) durch die Zeichen $=$, $\neq$ definierte Relation. Die zu ihr gehörige Klasseneinteilung ist die Einteilung von M in seine unterschiedenen Elemente selbst.

3. Gleichmächtigkeit und Kardinalzahlen

Man kann aus einer Menge M dadurch eine neue Menge M' herleiten, daß man die Elemente von M irgendwie durch neue Elemente ersetzt, nur so, daß alle Unterschiedenheiten der Elemente von M erhalten bleiben (etwa indem man das Element a durch den „Gedanken an das Element a" ersetzt). Setzt man dann zwischen je zwei Elemente a aus M und a' aus M' das Zeichen $\longleftrightarrow$ oder das Zeichen $\not\longleftrightarrow$, je nachdem a' bei dieser Ersetzung aus a entsteht oder nicht, so bestehen offenbar die Tatsachen:

(δ) *zu jedem a aus M existiert ein a' aus M' mit $a \longleftrightarrow a'$,*

(δ') *zu jedem a' aus M' existiert ein a aus M mit $a \longleftrightarrow a'$,*

(ε) *wenn $a \longleftrightarrow a'$, $b \longleftrightarrow b'$ und $a = b$ gilt, ist $a' = b'$,*

(ε') *wenn $a \longleftrightarrow a'$, $b \longleftrightarrow b'$ und $a' = b'$ gilt, ist $a = b$.*

Für das Bestehen dieser Tatsachen bei zwei vorliegenden Mengen M und M', gleichgültig welche Bedeutung dabei den Zeichen $\longleftrightarrow$, $\not\longleftrightarrow$ zukommt, führen wir eine besondere Ausdrucksweise ein:

(II) *Wenn zwischen je ein Element a einer Menge M und a' einer Menge M' eins und nur eins von zwei Zeichen $\longleftrightarrow$, $\not\longleftrightarrow$ in solcher Weise gesetzt ist, daß die Bedingungen (δ), (δ'), (ε), (ε') bestehen, so sagt man, daß eine* eineindeutige Zuordnung $\longleftrightarrow$ zwischen M und M' *vorliege. Ist eine solche zwischen M und M' möglich, so nennt man M und M'* gleichmächtig.

Die Gleichmächtigkeit ist ersichtlich eine Äquivalenzrelation im Sinne von (I). Für zwei endliche Mengen M und M' ist die Gleichmächtigkeit offenbar mit dem Übereinstimmen der *Anzahlen* der Elemente von M und M' gleichbedeutend. Die durch ein endliches M gemäß (B) erzeugte Klasse gleichmächtiger Mengen ist also die Gesamtheit aller Mengen gleicher Elementanzahl wie M. Diese Klasse kann direkt zur eindeutigen Charakterisierung dieser Anzahl dienen[1]). Daher nennt man nach Cantor allgemein die Klassen, die der Äquivalenzrelation (II) gemäß (B) in der Menge aller Mengen entsprechen, also je die Gesamtheiten aller zu einer Menge gleichmächtigen Mengen *Kardinalzahlen* (*Mächtigkeiten*). Sie geben die Verallgemeinerung des Anzahlbegriffs auf unendliche Mengen. Durch die Zusammenfassung je aller gleichmächtigen Mengen in eine logische Einheit (die Klasse) wird eben von jeder speziellen Bedeutung der Elemente der Einzelmengen abstrahiert und allein die für den Anzahlbegriff charakteristische Gesamtheit [(δ), (δ')] der Elemente nebst ihren Unterschiedenheiten [(ε), (ε')] ins Auge gefaßt.

Als Repräsentant einer endlichen Kardinalzahl n kann etwa die Menge der natürlichen Zahlen $1, 2, \ldots, n$ dienen. Als weitere, für uns wichtige Kardinalzahl nennen wir noch die durch die Menge aller natürlichen Zahlen $1, 2, \ldots$ repräsentierte. Mengen dieser Kardinalzahl, also solche, die mit der Menge der natürlichen Zahlen gleichmächtig sind, deren Elemente also durch Indizierung: $a_1, a_2, \ldots$ den natürlichen Zahlen eindeutig zugeordnet werden können, heißen *abzählbar.*

Die Menge aller reellen Zahlen ist ein Beispiel dafür, daß nicht jede unendliche Menge abzählbar ist[2]).

Wir wenden nunmehr die im vorstehenden auseinandergesetzten Begriffe der Mengenlehre zur Einführung einiger wichtiger entsprechender Begriffe für Bereiche an.

---

[1]) Diesen Gedanken hat R. Dedekind (Was sind und was sollen die Zahlen?, Braunschweig 1887) tatsächlich zur Definition der natürlichen Zahlen als Anzahlen endlicher Mengen benutzt.

[2]) Läge eine Abzählung $a_1, a_2, \ldots$ der als Dezimalbrüche (unter Vermeidung der Periode $00\ldots$) geschriebenen reellen Zahlen vor, so könnte man leicht einen (ebensolchen) Dezimalbruch a bilden, der von $a_1, a_2, \ldots$ verschieden, also doch nicht mit abgezählt wäre. Man wähle nämlich für jedes $n = 1, 2, \ldots$ die n-te Ziffer von a hinter dem Komma verschieden von der n-ten Ziffer von a_n hinter dem Komma (Cantorsches Diagonalverfahren).

1. Teilbereiche

Aus dem Begriff Teilmenge entspringt unmittelbar:

Definition 4. *Bilden die Elemente einer Teilmenge* B_1 *eines Bereiches* B *bezüglich derselben Verknüpfungen, wie sie in* B *zugrunde liegen, einen* 1. *Ring*, 2. *Körper*, 3. *Integritätsbereich, so heißt* B_1 *ein* 1. Teilring, 2. Teilkörper, 3. Teilintegritätsbereich *von* B *und* B *ein* Erweiterungs-Bereich (-Ring, -Körper, -Integritätsbereich) *von* B_1.

Zur Entscheidung darüber, ob eine Teilmenge B_1 eines Integritätsbereiches B Teilring, Teilkörper, Teilintegritätsbereich von B ist, braucht man nicht alle in § 1 aufgeführten Bedingungen zu prüfen, sondern nur die in folgendem Satz genannten:

Satz 6. *Eine aus mindestens zwei Elementen bestehende Teilmenge* B_1 *eines Integritätsbereiches* B *ist dann und nur dann* 1. *Teilring von* B, *wenn die ersten drei elementaren Rechenoperationen, wie sie innerhalb* B *definiert sind, angewandt auf die Elemente von* B_1 *stets wieder Elemente von* B_1 *ergeben*, 2. *Teilkörper von* B, *wenn zudem die vierte Rechenoperation (Division) für Elemente aus* B_1 *(bei von Null verschiedenem Nenner) stets ausführbar ist und immer Elemente von* B_1 *ergibt*, 3. *Teilintegritätsbereich von* B, *wenn* B_1 *Teilring von* B *ist und das Einselement von* B *enthält.*

Beweis. a) Daß diese Bedingungen notwendig sind, ist nach Def. 1—4 klar.

b) Sind diese Bedingungen erfüllt, so stimmen die folgenden Bedingungen des § 1 für B_1: (a), (b), die Existenz in (6), ev. die Existenz in (7) bzw. (7b). Andererseits sind die übrigen nach § 1 erforderlichen Bedingungen, nämlich (1)—(5), die Eindeutigkeit in (6), ev. die Eindeutigkeit in (7), (7a), in B_1 a fortiori erfüllt, weil sie in B gelten.

Das Kriterium von Satz 6 läßt sich natürlich sinngemäß auch auf Ringe B ausdehnen. Wir werden es aber nur für die in Satz 6 genannten Fälle brauchen. Desgleichen werden wir der einfacheren Redeweise halber auch den folgenden Satz 7 sowie Def. 5 nur für Körper formulieren, für die allein sie später zur Anwendung kommen.

Bezüglich des Durchschnittes haben wir für Körper:

Satz 7. *Sind* $K_1, K_2, \ldots$ *irgendwelche [endlich oder unendlich*[1]*) viele] Teilkörper eines Körpers* K, *so ist auch der Durchschnitt der Mengen* $K_1, K_2, \ldots$ *ein Teilkörper von* K; *dieser heißt der* Durchschnittskörper *oder kurz* Durschnitt *der Körper* $K_1, K_2, \ldots$.

Beweis. Daß der Durchschnitt mindestens zwei Elemente enthält, folgt daraus, daß alle $K_1, K_2, \ldots$ die beiden verschiedenen Elemente 0 und e von K gemeinsam enthalten, weil sie Teilkörper von K sind. Dann ergibt sich die Behauptung ohne weiteres aus Satz 6.

Für die Vereinigungsmenge gilt aber ein entsprechender Satz nicht. Denn ist a_1 in K_1, a_2 in K_2, so braucht z. B. $a_1 + a_2$ in keinem der Körper $K_1, K_2, \ldots$ enthalten zu sein. Dagegen läßt sich ein dem Vereinigungsmengenbegriff analoger dadurch einführen, daß wir die auf S. 15 angegebene Zurückführung der Vereinigungsmenge auf einen Durchschnitt für die Verallgemeinerung zugrunde legen.

Definition 5. *Sind* $K_1, K_2, \ldots$ *irgendwelche (endlich oder unendlich viele) Teilkörper eines Körpers* K, *so heißt der Durchschnitt aller* $K_1, K_2, \ldots$ *als Teilkörper enthaltenden Teilkörper von* K *das* Kompositum *von* $K_1, K_2, \ldots$ *oder der aus* $K_1, K_2, \ldots$ komponierte Körper.

Daß dieser Durchschnitt überhaupt gebildet werden kann, folgt daraus, daß zum mindesten ein zu seiner Bildung zugrunde zu legender Körper, nämlich K, existiert.

Das Kompositum von $K_1, K_2, \ldots$ enthält die Vereinigungsmenge der Mengen $K_1, K_2, \ldots$, ist aber i. a. weiter. Es ist der engste $K_1, K_2, \ldots$ als Teilkörper enthaltende Teilkörper von K, ebenso wie der Durchschnitt von $K_1, K_2, \ldots$ der weiteste in $K_1, K_2, \ldots$ als Teilkörper enthaltene Teilkörper von K ist.

2. Kongruenzrelationen und Restklassenringe

Indem wir für den Fall eines Bereiches B zu den Bedingungen (α), (β), (γ) für eine Äquivalenzrelation in der

---

[1]) Die Numerierung soll hier und in der folgenden Def. 5 nicht besagen, daß höchstens abzählbar viele gemeint sind.

Menge B noch zwei in naturgemäßer Weise gebildete Forderungen über das Verhalten der Äquivalenzrelation zu den beiden Verknüpfungen von B hinzufügen, definieren wir:

Definition 6. *Erfüllt eine Äquivalenzrelation* $\equiv$ *in einem Bereiche* B *neben* (α), (β), (γ) noch *die Bedingungen*:

(1) *aus* $a_1 \equiv b_1$, $a_2 \equiv b_2$ *folgt* $a_1 + a_2 \equiv b_1 + b_2$,

(2) *aus* $a_1 \equiv b_1$, $a_2 \equiv b_2$ *folgt* $a_1 a_2 \equiv b_1 b_2$,

so nennen wir sie eine Kongruenzrelation *in* B *und die ihr entsprechenden Klassen die* Restklassen *in* B *nach ihr*[1]).

Wir legen jetzt in § 1, (a) die Menge $\overline{\mathsf{B}}$ der Restklassen nach einer Kongruenzrelation $\equiv$ in B zugrunde. Dazu ist zu fordern, daß mindestens zwei solche Restklassen vorhanden sind, daß also nicht alle Elemente von B einander kongruent sind. Sind dann r und s zwei Restklassen und bildet man alle Summen $a + b$ bzw. Produkte ab von je einem Elemente a aus r und b aus s, so folgt aus (1) und (2), daß diese alle wieder je einer bestimmten Restklasse t bzw. u aus $\overline{\mathsf{B}}$ angehören. Durch die Festsetzungen $r + s = t$ bzw. $rs = u$, die man kurz als elementweise Addition bzw. Multiplikation der Restklassen bezeichnen kann, wird also § 1, (b) realisiert. Wir beweisen nun, daß dann auch § 1, (c) realisiert ist, d. h.:

Satz 8. *Liegt in einem Bereiche* B *eine Kongruenzrelation* $\equiv$ *vor, bei der nicht alle Elemente von* B *einander kongruent sind, und definiert man in der Menge* $\overline{\mathsf{B}}$ *der Restklassen nach ihr zwei Verknüpfungen durch elementweise Addition bzw. Multiplikation, so ist* $\overline{\mathsf{B}}$ *ein Ring bezüglich dieser Verknüpfungen*; $\overline{\mathsf{B}}$ *heißt der* Restklassenring *von* B *nach der Kongruenzrelation* $\equiv$.

Beweis. Das Erfülltsein von § 1, (1)—(5) ist eine unmittelbare Folge des Bestehens dieser Gesetze im Bereiche B. Sind ferner a bzw. c Elemente aus den Restklassen r bzw. t, so

---

[1]) Die Menge M aller $a \equiv 0$ bei einer Kongruenzrelation in B ist genau das, was man unter *Ideal* in B versteht. Dieser Begriff ist für die Teilbarkeitslehre (siehe **2**, § 2) in allgemeinen Bereichen grundlegend (vgl. E. Noether, Idealtheorie in Ringbereichen, Math. Ann. 83 [1921]).

folgt aus § 1, (6) die Existenz eines b, so daß $a + b = c$ ist. Ist dann s die Restklasse, der b angehört, so gilt nach (1) und unserer Additionsfestsetzung $r + s = t$. Diese Restklasse s ist schließlich auch die einzige Lösung von $r + s = t$. Denn ist auch $r + s' = t$ und b' ein Element aus s', so ist $a + b \equiv a + b'$, weil beide Seiten derselben Restklasse t angehören. Daraus und aus der nach (α) sicher richtigen Relation $(-a) \equiv (-a)$ kann aber nach (1) auf $b \equiv b'$, d. h. $s = s'$ geschlossen werden. In $\overline{\mathsf{B}}$ ist also die Subtraktion unbeschränkt und eindeutig ausführbar, d. h. § 1, (6) erfüllt.

Es sei noch bemerkt, daß, wenn B ein Integritätsbereich ist, $\overline{\mathsf{B}}$ nicht notwendig auch Integritätsbereich zu sein braucht, weil zwar § 1, (7b), aber nicht notwendig § 1, (7a) in $\overline{\mathsf{B}}$ erfüllt ist (siehe **2**, Satz 28). Der Fall, daß B sogar ein Körper ist, ist uninteressant, weil es dann nur triviale Restklasseneinteilungen in B gibt (siehe **3**, 1, § 2 Aufg. 10).

3. Isomorphie und Bereichtypen

Wir fügen für den Fall zweier Bereiche B und B' auch den Bedingungen (δ), (δ'), (ε), (ε') für die Gleichmächtigkeit der beiden Mengen B und B' zwei in naturgemäßer Weise gebildete Forderungen über das Verhalten der eineindeutigen Zuordnung zu den beiden Verknüpfungen von B und B' hinzu. In dieser Hinsicht beweisen wir zunächst:

Satz 9. *Die folgende Festsetzung liefert eine Äquivalenzrelation in der Menge aller Bereiche: Es sei* $\mathsf{B} \cong \mathsf{B}'$ *dann und nur dann, wenn erstens* B *und* B' *gleichmächtig sind, und wenn man zweitens die eineindeutige Zuordnung zwischen den Elementen* $a, b, \ldots$ *von* B *und* $a', b', \ldots$ *von* B' *so wählen kann, daß die folgenden Bedingungen bestehen:*

(3) *wenn* $a \longleftrightarrow a', b \longleftrightarrow b'$ *ist, ist* $a + b \longleftrightarrow a' + b'$,

(4) *wenn* $a \longleftrightarrow a', b \longleftrightarrow b'$ *ist, ist* $ab \longleftrightarrow a'b'$.

Beweis. Es ist unmittelbar ersichtlich, daß die für die Gleichmächtigkeit erfüllten Bedingungen (α), (β), (γ) auch bei Hinzunahme der Forderungen (3) und (4) bestehenbleiben.

Ebenso sieht man ohne weiteres:

Zusatz zu Satz 9. *Betrachtet man nur die Erweiterungsbereiche eines festen Bereichs* B_0, *so gilt Entsprechendes zu Satz* 9 *auch dann noch, wenn man den Bedingungen* (3), (4) *die weitere Bedingung hinzufügt, daß die Elemente* a_0 *von* B_0 *bei der eineindeutigen Zuordnung zwischen* B *und* B' *sich selbst entsprechen sollen*:

(5) $a_0 \longleftrightarrow a_0$ *für alle* a_0 *aus* B_0.

Auf Grund von Satz 9 definieren wir nun:

Definition 7. *Eine eineindeutige Zuordnung zwischen zwei Bereichen* B *und* B' *mit den Eigenschaften* (3), (4) *heißt ein* Isomorphismus *zwischen* B *und* B', *und* B *und* B' *selbst heißen dann* isomorph. *Die in Satz* 9 *genannte Äquivalenzrelation* $\mathsf{B} \cong \mathsf{B}'$ *für Bereiche heißt* Isomorphie, *die ihr entsprechenden Klassen die* Typen *der Bereiche.*

Auf Grund des Zusatzes zu Satz 9 definieren wir ferner analog:

Zusatz zu Definition 7. *Ein Isomorphismus zwischen zwei Erweiterungsbereichen* B *und* B' *eines Bereichs* B_0 *mit der Eigenschaft* (5) *heißt ein* Isomorphismus bzgl. B_0, *und* B *und* B' *heißen dann* isomorph. bzgl. B_0. *Die im Zusatz zu Satz* 9 *genannte Äquivalenzrelation für Erweiterungsbereiche von* B_0 *heißt* Isomorphie bzgl. B_0, *die ihr entsprechenden Klassen die* Erweiterungstypen bzgl. B_0.

Die in Satz 9 für die Relation $\mathsf{B} \cong \mathsf{B}'$ geforderten Bedingungen besagen, daß beim Übergang von B zu B' oder von B' zu B durch die betr. Zuordnung erstens nach (δ), (δ') jedem Element von B eines von B' entspricht und umgekeht, oder, kurz gesagt, die *Gesamtheit* der Elemente erhalten bleibt, zweitens nach (ε), (ε') verschiedenen Elementen von B verschiedene von B' entsprechen und umgekehrt, oder, kurz gesagt, die *Unterschiedenheit* der Elemente erhalten bleibt, und drittens nach (3) bzw. (4) jede Additions- bzw. Multiplikationsverknüpfung in B in die für die entsprechenden Elemente aus B' übergeht und umgekehrt, oder, kurz gesagt, die *Verknüpfungen* Addition und Multiplikation erhalten bleiben. Nun sind nach § 1 die vorliegende Gesamtheit B von Elementen inkl. ihrer Unterschiedenheiten [§ 1, (a)] und die Art, wie die Verknüpfungen Addition und Multiplikation für sie erklärt sind [§ 1, (b)], das einzige, was bei Absehen von der Bedeutung der Elemente als charakteristisch für den Bereich B übrigbleibt. Demgemäß ist jede von der Bedeutung der Elemente von B unabhängige Aussage über sie, wie sie ja von dem in der Einleitung formulierten abstrakten Standpunkt aus allein interessiert, lediglich mit den Relationen $=$, $\neq$ und den Verknüpfungen Addition und Multiplikation, auf die ja nach § 1 auch die Subtraktion und Division zurückführbar sind, gebildet und bleibt somit, wenn man durch die betr. Zuordnung von B zu B' übergeht, in obigem Sinne erhalten und ebenso umgekehrt beim Übergang von B' zu B. In dem angegebenen Umfange sind mithin, kurz gesagt, die Bereiche B und B' gar nicht zu unterscheiden. Daher ist es also von unserem Standpunkt aus ganz einerlei, ob man solche Aussagen über B oder B' macht.

Weiter geht für zwei bzgl. B_0 isomorphe Erweiterungsbereiche B und B' von B_0 jede allein auf Gleichheit, Unterschiedenheit und die vier elementaren Rechenoperationen gegründete Aussage, die Elemente von B mit solchen des Teilbereichs B_0 in Beziehung setzt, in eine richtige Aussage über, wenn man die ersteren Elemente durch die ihnen zugeordneten aus B' ersetzt und ebenso umgekehrt bei entsprechendem Übergang von B' zu B. Kurz gesagt sind also die Erweiterungsbereiche B und B' in dem angegebenen Umfange von B_0 aus nicht zu unterscheiden. Daher ist es also wieder einerlei, ob man solche Aussagen über B oder B' macht.

Dadurch, daß hiernach die Algebra sich beim Studium von Bereichen schlechthin nur für solche Aussagen interessiert, die allen Bereichen eines Typus gemeinsam sind, und beim Studium der Erweiterungsbereiche eines festen Bereichs B_0 nur für solche Aussagen, die allen Bereichen eines Erweiterungstypus von B_0 gemeinsam sind, rechtfertigen sich die in Def. 7 und Zusatz zu Def. 7 eingeführten Bezeichnungen *Typus* und *Erweiterungstypus* in Hinsicht auf die gewöhnliche Bedeutung des Wortes „Typus“. Von Aussagen der genannten Art sagt man auch, sie betreffen die *Struktur der Bereiche*. Die Gewinnung solcher Aussagen wurde am Schluß der Einleitung als Hauptaufgabe der modernen Algebra hingestellt.

Wenn es nach diesen Ausführungen scheint, als ob in der Algebra ein Unterschied zwischen isomorphen Bereichen überhaupt nicht zu machen sei, so bedarf das einer Einschränkung. Während es zwar gleichgültig ist, ob man die in der Einleitung formulierte Grundaufgabe der Algebra in einem Bereiche B oder in einem zu B isomorphen Bereiche B' behandelt, ist eine Unterscheidung isomorpher Bereiche B und B' natürlich dann geboten, wenn beide Bereiche Teilbereiche eines anderen Bereiches B^* sind, also ihre Elemente auf Grund der Unterschiedenheit der Elemente von B^* (für Betrachtungen innerhalb B^*) zu unterscheiden sind (vgl. die Beispiele auf S. 37 und S. 56).

Es sei noch bemerkt, daß nach den obigen Ausführungen die spezielle Eigenschaft, Körper bzw. Integritätsbereich zu sein, gleichzeitig allen Bereichen eines Typus zukommt, so daß man neben den allgemeinen *Ringtypen* speziell von *Körpertypen* und *Integritätsbereichtypen* reden kann.

Beispiele

1. Jeder Bereich B ist Teil- und Erweiterungsbereich von sich selbst. Jeder andere Teil- bzw. Erweiterungsbereich von B heißt *echt* oder *eigentlich.*

2. Aus den Beispielen 1—3 von § 1 ergeben sich ohne nähere Ausführung verständliche Beispiele für Teil- und Erweiterungsbereiche.

3. Sind $\mathsf{K}_1, \mathsf{K}_2$ Teilkörper von K, so ist dann und nur dann ihr Durchschnitt mit K_1 und ihr Kompositum mit K_2 identisch, wenn K_1 Teilkörper von K_2 ist. Das ist leicht aus Satz 7 und Def. 5 zu entnehmen.

4. Weitere Beispiele für Teil- und Erweiterungsbereiche sowie auch für Isomorphie von Bereichen werden uns in §§ 3, 4 eingehend beschäftigen.

5. Die Einteilung der ganzen Zahlen in gerade und ungerade liefert gemäß (A) eine Äquivalenzrelation, die sich leicht als Kongruenzrelation für den Integritätsbereich Γ (Satz 5 [13]) erweist. Der zugehörige Restklassenring ist isomorph mit dem in § 1, Beispiel 4 genannten Körper, also ein Restklassenkörper.

6. Weitere Beispiele für Kongruenzrelationen und Restklassenringe werden uns in **2**, § 2 eingehend beschäftigen.

§ 3. Der Quotientenkörper eines Integritätsbereiches

Es ist für uns von Wichtigkeit nachzuweisen, daß jeder Integritätsbereich durch Hinzunahme aller aus seinen Elementen zu bildenden „Quotienten" zu einem Körper erweitert werden kann. Wir zeigen nämlich:

Satz 10. *Zu jedem Integritätsbereich* I *existiert ein Erweiterungskörper* K, *dessen sämtliche Elemente sich als Quotienten von Elementen aus* I *darstellen lassen. Der Erweiterungstypus von* K *bzgl.* I *ist durch diese Forderung eindeutig bestimmt.*

Beweis[1]).

a) *Eindeutigkeitsnachweis*

Ist K ein Körper der im Satz genannten Art, so enthält er als Körper auch umgekehrt alle Quotienten $\frac{a}{b}$ von Elementen a, b ($b \neq 0$) aus I, d. h. besteht aus der Gesamtheit aller dieser (natürlich nicht notwendig sämtlich verschiedenen) Quotienten. Nach den Gesetzen § 1, (1)—(7) für Körper bestehen dann die folgenden Tatsachen in K:

(1) $\frac{a}{b} = \frac{a'}{b'}$ dann und nur dann, wenn $ab' = a'b$,

(2) $\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$,

(3) $\frac{a_1}{b_1} \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$,

(4) $\frac{a_1}{b_1} - \frac{a_2}{b_2} = \frac{a_1 b_2 - a_2 b_1}{b_1 b_2}$,

(5) $\frac{a_1}{b_1} \Big/ \frac{a_2}{b_2} = \frac{a_1 b_2}{a_2 b_1}$, wenn $\frac{a_2}{b_2} \neq 0$, d. h. $a_2 \neq 0$ (neben $b_1, b_2 \neq 0$).

Ist nun $\overline{\mathsf{K}}$ ein weiterer Körper der im Satz genannten Art und ordnet man jedem Element α von K auf Grund einer beliebigen seiner Darstellungen als Quotient $\frac{a}{b}$ von Elementen aus I das durch denselben Quotienten dargestellte

[1]) Wir legen hier, wie auch bei dem entsprechenden Beweis zu Satz 11 in § 4 den Nachdruck auf das logische Gerüst des Beweises. Die Bestätigung der bei den einzelnen Schritten angeführten Tatsachen ist auf Grund von §§ 1, 2 stets leicht zu erbringen. Wir begnügen uns fast durchweg mit dem Hinweis auf die heranzuziehenden Stellen aus §§ 1, 2 und überlassen die nähere Ausführung dem Leser.

Element $\bar{\alpha}$ von $\bar{\mathsf{K}}$ zu, so ist das nach dem Bemerkten und (1) eine eineindeutige Zuordnung [§ 2, (δ), (δ'), (ε), (ε')] zwischen den sämtlichen Elementen von K und $\bar{\mathsf{K}}$, die nach (2) und (3) den Bedingungen § 2, (3) und (4) genügt und ferner ersichtlich auch die Bedingung § 2, (5) bzgl. I als Grundbereich erfüllt. Also ist dann $\bar{\mathsf{K}} \cong \mathsf{K}$ bzgl. I. Damit ist der Nachweis für die eindeutige Bestimmtheit des Erweiterungstypus von K bzgl. I erbracht.

b) *Vorbemerkungen zum Existenznachweis*

Der Nachweis der Existenz eines Körpers K der im Satz genannten Art kann prinzipiell nur durch Konstruktion von K, d.h. durch Angabe seiner Elemente und ihrer Verknüpfungen geführt werden. Hierbei dürfen wir natürlich nicht schon mit den Quotienten $\frac{a}{b}$ operieren, da diese erst auf Grund der Existenz von K einen Sinn haben. Wir entziehen daher für die Konstruktion dem Bruchstrich in $\frac{a}{b}$ die Bedeutung eines Divisionszeichens, sehen vielmehr $\frac{a}{b}$ lediglich als geordnetes Elementpaar aus I an und schreiben dafür (a, b), um Verwechslungen mit den ev. schon teilweise in I definierten Quotienten $\frac{a}{b}$ zu vermeiden. Aus (1)—(3) entnehmen wir dann die nötigen Richtlinien für die Angabe der Elemente von K und ihrer Verknüpfungen.

c) *Konstruktion eines zu* K *isomorphen Körpers* K'

In der Menge M aller geordneten Elementpaare (a, b) aus I, bei denen $b \neq 0$ ist, definieren wir eine Äquivalenzrelation durch die Festsetzung:

(1′) $(a, b) \sim (a', b')$ dann und nur dann, wenn $ab' = a'b$.

Man bestätigt leicht das Erfülltsein von § 2, (α), (β), (γ), so daß wirklich eine Äquivalenzrelation im Sinne von § 2, (I) vorliegt.

Auf Grund von (1') zerfällt M in Klassen. Diese Klassen sehen wir als Menge K' unterschiedener Elemente an. Die durch (a, b) erzeugte Klasse werde mit $\{a, b\}$ bezeichnet.

Da nach (1') und dem Analogon zu Satz 3 [11] $\{0, e\} \neq \{e, e\}$ gilt, ist § 1, (a) in K' realisiert.

Wir definieren weiter in K' zwei Verknüpfungen Addition und Multiplikation durch die Festsetzungen:

$$(2')\quad \{a_1, b_1\} + \{a_2, b_2\} = \{a_1 b_2 + a_2 b_1, b_1 b_2\},$$

$$(3')\quad \{a_1, b_1\}\{a_2, b_2\} = \{a_1 a_2, b_1 b_2\}.$$

Da nach Satz 4 [12] mit b_1 und b_2 auch $b_1 b_2 \neq 0$ ist, sind die rechten Seiten in (2') und (3') wirklich bestimmte Klassen aus K'.

Ferner sind diese, zunächst mittels einzelner Repräsentanten (a_1, b_1) und (a_2, b_2) der Klassen links getroffenen Festsetzungen unabhängig von der Auswahl dieser Repräsentanten innerhalb ihrer Klassen. Man bestätigt nämlich leicht, daß sich nur der Repräsentant, nicht die Klasse rechts ändert, wenn man links (a_1, b_1) und (a_2, b_2) durch äquivalente (a_1', b_1') und (a_2', b_2') ersetzt. Somit ist vermöge (2') und (3') auch § 1, (b) in K' realisiert.

Schließlich befriedigen die in (2') und (3') definierten Verknüpfungen die Gesetze § 1, (1)—(7). Für § 1, (1)—(5) folgt das leicht aus dem Erfülltsein jener Gesetze in I, für § 1, (6) und (7) zeigt man ebenso auf Grund der Gültigkeit von § 1, (6) und (7a) in I, daß Differenz und Quotient in K' eindeutig bestimmt und durch

$$(4')\quad \{a_1, b_1\} - \{a_2, b_2\} = \{a_1 b_2 - a_2 b_1, b_1 b_2\},$$

$$(5')\quad \frac{\{a_1, b_1\}}{\{a_2, b_2\}} = \{a_1 b_2, a_2 b_1\}, \text{ wenn } \{a_2, b_2\} \neq 0,$$

stets gegeben sind. Die im Falle (5') zu stellende Bedingung $\{a_2, b_2\} \neq 0$ bedeutet $a_2 \neq 0$, weil nach (2') oder (4') die Klasse $\{0, e\}$ Nullelement von K' ist und nach (1') aus $\{a, b\} = \{0, e\}$ folgt $a = 0$.

Somit ist K' ein Körper bezüglich der Verknüpfungen (2') und (3').

d) *Konstruktion von* K

Der Körper K′ enthält die Teilmenge I′ der speziellen Klassen $\{a, e\}$, die nach (2′)—(4′) und Satz 6 [19] ein Teilintegritätsbereich von K′ und weiter nach (1′)—(3′) und Def. 7 [23] vermöge der Zuordnung $\{a, e\} \longleftrightarrow a$ zu I isomorph ist. Wir können nun aus K′ eine Menge K dadurch bilden, daß wir die zu I′ gehörigen Elemente $\{a, e\}$ von K′ je durch die ihnen zugeordneten Elemente a von I ersetzen, die nicht zu I′ gehörigen Elemente von K′ dagegen beibehalten. Dann wird also K eine K′ eineindeutig zugeordnete Menge unterschiedener Elemente. Weiter können wir in K zwei Verknüpfungen Addition und Multiplikation, die den Gesetzen § 1, (1)—(7) genügen und die für die Teilmenge I mit den in I bereits bestehenden Verknüpfungen identisch sind, dadurch eindeutig erklären, daß wir auf die für die zugeordneten Elemente von K′ definierten Verknüpfungen zurückgehen, m. a. W. die Bedingungen (3) und (4) von Satz 9 [22] zugrunde legen. Dann wird also K ein zu K′ isomorpher Erweiterungskörper von I.

Dieser Körper K hat nun die im Satz genannte Eigenschaft. Da nämlich nach (3′) oder (5′) jedes Element $\{a, b\}$ von K′ eine Darstellung $\{a, b\} = \frac{\{a, e\}}{\{b, e\}}$ als Quotient zweier Elemente von I′ besitzt — (es ist $\{b, e\} \neq 0$ wegen $b \neq 0$) —, folgt für das zugeordnete Element von K die Darstellung $\frac{a}{b}$ als Quotient zweier Elemente von I.

Damit ist Satz 10 bewiesen.

Die Eindeutigkeitsaussage von Satz 10 kann noch etwas verschärft werden, nämlich durch den folgenden Zusatz, dessen Existenzaussage nach Satz 6 [19] und (2)—(5) auf der Hand liegt:

Zusatz. *Innerhalb eines beliebigen Erweiterungskörpers* K* *von* I *gibt es einen und nur einen Repräsentanten des in Satz* 10 *genannten Erweiterungstypus, nämlich den Körper* K, *der durch die in* K* *gebildeten Quotienten von Elementen aus* I *gebildet wird.*

Beweis. Wird im vorhergehenden Beweis unter a) die Voraussetzung hinzugefügt, daß K und $\bar{K}$ beide Teilkörper eines und desselben Erweiterungskörpers K^* von I sind, so folgt dort sogar $\bar{\mathsf{K}} = \mathsf{K}$, weil dann die Quotienten $\frac{a}{b}$ in K und $\bar{\mathsf{K}}$ eine und dieselbe, durch K^* festgelegte Bedeutung haben.

Im Hinblick auf die Ausführungen nach Def. 7 [23f.] ist es daher gerechtfertigt, isomorphe Erweiterungskörper von I des in Satz 10 genannten Typus nicht zu unterscheiden und mit dem bestimmten Artikel zu definieren:

Definition 8. *Der in Satz* 10 *genannte Körper* K *heißt* der Quotientenkörper *des Integritätsbereiches* I.

Beispiele

1. Ist I schon selbst ein Körper, so ist sein Quotientenkörper mit I identisch, und umgekehrt.

2. Der Quotientenkörper des in Satz 5 genannten Integritätsbereiches Γ ist der ebendort genannte Körper P. In der Tat geht das unter c) benutzte Konstruktionsverfahren für $\mathsf{I} = \Gamma$ in die bekannte Konstruktion der rationalen Zahlen aus den ganzen Zahlen über.

3. Vgl. § 4, Def. 10 [38].

§ 4. Der Integritätsbereich der ganzen rationalen Funktionen von n Unbestimmten über I und der Körper der rationalen Funktionen von n Unbestimmten über K

Der in der Algebra zu verwendende Begriff der ganzen rationalen und der rationalen Funktion ist von dem in der Analysis üblichen grundsätzlich verschieden.

In der *Analysis* definiert man die Funktionen als Zuordnungen von Funktionswerten zu den Elementen einer Argumentmenge. Dementsprechend würde im Sinne der Analysis (i. S. d. An.) von einer Funktion f von n Veränderlichen über einem Integritätsbereich I zu reden sein, wenn jedem geordneten Elementsystem $x_1, \ldots, x_n$ aus I ein Element $f(x_1, \ldots, x_n)$ aus I zugeordnet ist, und speziell von einer ganzen rationalen Funktion (g. r. Fkt.), wenn jene Zuordnung für alle $x_1, \ldots, x_n$ aus I in ein- und demselben, auf $x_1, \ldots, x_n$ und feste Elemente aus I anzuwendenden Rechenverfahren besteht, das aus endlich vielen Additionen, Subtraktionen und Multiplikationen, wie sie ja in I definiert sind, zusammengesetzt ist. Entsprechend wäre unter Hinzunahme auch der Division eine rationale Funktion (r. Fkt.) i. S. d. An. von n Veränderlichen über einem Körper K zu erklären, wobei allerdings wegen des Nichtdefiniertseins der Division durch 0 bei einem gegebenen Rechenverfahren unter Umständen nicht jedes System $x_1, \ldots, x_n$ aus K als Argumentsystem zulässig ist; das wird nachher noch zu präzisieren sein. Es ist ohne weiteres ersichtlich, daß die g. r. Fkt. bzw. r. Fkt. i. S. d. An. von n Veränderlichen über I bzw. K jedenfalls je einen **Ring** bilden, wenn man die Verknüpfungen durch Addition und Multiplikation je aller (definierten) Funktionswerte erklärt.

In der Algebra kommt man aus einem später (nach Satz 12 [40]) näher auszuführenden Grunde mit diesem Funktionsbegriff, der die *Zuordnung* als das Primäre, die Art der Zuordnung, d. h. im Falle der rationalen Funktionen das *Rechenverfahren* als das Sekundäre hinstellt, nicht aus. Man muß vielmehr umgekehrt für die dort allein zu betrachtenden rationalen Funktionen den Rechenausdruck als das Primäre, die durch ihn gelieferte Zuordnung als das Sekundäre ansehen[1]). Dem letzteren Standpunkte entspricht es, wenn wir im folgenden eine Theorie der in $x_1, \ldots, x_n$ ganzen rationalen bzw. rationalen Rechenausdrücke über I bzw. K entwickeln, die wir dann der formalen Analogie halber, wie üblich, auch g. r. bzw. r. Fkt. von $x_1, \ldots, x_n$ über I bzw. K nennen, und wenn wir dabei, um ein Zurückfallen in den Zuordnungsstandpunkt auszuschließen, den $x_1, \ldots, x_n$ vorläufig die Bedeutung von Veränderlichen in I bzw. K entziehen, sie vielmehr als feste Elemente außerhalb I bzw. K, sog. *Unbestimmte*[2]), einführen.

Zu dem Bereich der ganzen rationalen Funktionen von $x_1, \ldots, x_n$ über einem Integritätsbereich I im Sinne der Algebra gelangen wir durch eine, zu der in § 3 ganz analoge, abstrakte Konstruktion, indem wir beweisen:

Satz 11. *Zu jedem Integritätsbereich I existiert ein Erweiterungsintegritätsbereich I_n mit der Eigenschaft:*

Es existieren n Elemente $x_1, \ldots, x_n$ in I_n derart, daß sich jedes Element von I_n eindeutig in der Form

---

1) Das ist also derjenige, vom Standpunkte der Analysis primitivere Funktionsbegriff, der historisch dem genannten, modernen Funktionsbegriff i. S. d. An. vorausgegangen ist. Unsere nachstehenden Entwicklungen zeigen, daß vom Standpunkte der Algebra umgekehrt jener in der Analysis primitivere Funktionsbegriff der tiefergehende ist.

2) Siehe zu dieser Bezeichnung die Erläuterung hinter Def. 9 [37].

$$\sum_{k_1, \ldots, k_n = 0}^{\infty} a_{k_1, \ldots, k_n} x_1^{k_1} \ldots x_n^{k_n} \text{ [1]}$$

darstellen läßt, wo die $a_{k_1, \ldots, k_n}$ Elemente aus $\mathfrak{l}$ sind, unter denen nur endlich viele von Null verschiedene vorkommen.

Der Erweiterungstypus von $\mathfrak{l}_n$ bzgl. $\mathfrak{l}$ ist durch diese Forderung eindeutig bestimmt.

Beweis [2]. Wir führen den Beweis zunächst für $n = 1$, und zwar in vollständiger Analogie zum Beweis von Satz 10 in § 3.

a) *Eindeutigkeitsnachweis*

Ist $\mathfrak{l}_1$ ein Integritätsbereich der im Satz genannten Art für $n = 1$ und x das im Satz mit x_1 bezeichnete Element aus $\mathfrak{l}_1$, so enthält $\mathfrak{l}_1$ als Integritätsbereich auch umgekehrt alle Ausdrücke $\sum\limits_{k=0}^{\infty} a_k x^k$, wo die a_k Elemente aus $\mathfrak{l}$ sind, von denen nur endlich viele $\neq 0$ sind, d. h. $\mathfrak{l}_1$ besteht aus der Gesamtheit aller dieser Ausdrücke. Wegen der Eindeutigkeitsforderung des Satzes und nach den Gesetzen § 1, (1)—(6) für Ringe bestehen dann folgende Tatsachen in $\mathfrak{l}_1$:

(1) $\sum\limits_{k=0}^{\infty} a_k x^k = \sum\limits_{k=0}^{\infty} a'_k x^k$ dann und nur dann, wenn

$$a_k = a'_k \text{ für alle } k,$$

(2) $$\sum_{k=0}^{\infty} a_k x^k + \sum_{k=0}^{\infty} b_k x^k = \sum_{k=0}^{\infty} (a_k + b_k) x^k ,$$

(3) $$\sum_{k=0}^{\infty} a_k x^k \sum_{k=0}^{\infty} b_k x^k = \sum_{k=0}^{\infty} \Big(\sum_{\substack{\lambda, \mu = 0 \\ \lambda + \mu = k}}^{k} a_\lambda b_\mu\Big) x^k ,$$

---

[1] Die Bedeutung des Summenzeichens Σ mit angefügten Angaben über den Summationsbereich darf als bekannt vorausgesetzt werden. — Daß wir hier für die in Wahrheit endlichen Summen formal unendliche Summen mit nur endlich vielen Summanden $\neq 0$ setzen, wobei natürlich stillschweigend unter einer Summe von unendlich vielen Nullen wieder Null verstanden ist, geschieht lediglich aus bezeichnungstechnischen Gründen. Sonst würden nämlich die Formulierung der Eindeutigkeit unserer Darstellungen, sowie später die Formeln für das Rechnen mit so dargestellten Elementen ziemlich kompliziert.

[2] Vgl. die Anm. 1 [26] zum Beweis von Satz 10.

$$(4) \quad \sum_{k=0}^{\infty} a_k x^k - \sum_{k=0}^{\infty} b_k x^k = \sum_{k=0}^{\infty} (a_k - b_k)\, x^k.$$

Ist nun $\bar{\mathfrak{I}}_1$ ein weiterer Integritätsbereich dieser Art, $\bar{x}$ das im Satz mit x_1 bezeichnete Element für $\bar{\mathfrak{I}}_1$, und ordnet man einem Element $\sum_{k=0}^{\infty} a_k x^k$ von $\mathfrak{I}_1$ immer das Element $\sum_{k=0}^{\infty} a_k \bar{x}^k$ von $\bar{\mathfrak{I}}_1$ zu, so erschließt man aus (1)—(3) ganz entsprechend wie in § 3, a), daß auf Grund dieser Zuordnung $\bar{\mathfrak{I}}_1 \cong \mathfrak{I}_1$ bzgl. $\mathfrak{I}$ ist, also die eindeutige Bestimmtheit des Erweiterungstypus von $\mathfrak{I}_1$ bzgl. $\mathfrak{I}$.

b) *Vorbemerkungen zum Existenznachweis*

Der Nachweis der Existenz eines Integritätsbereiches $\mathfrak{I}_1$ der im Satz genannten Art kann prinzipiell nur durch Konstruktion von $\mathfrak{I}_1$, d. h. durch Angabe seiner Elemente und ihrer Verknüpfungen geführt werden. Hierbei dürfen wir natürlich nicht schon mit dem Element x und den Summendarstellungen $\sum_{k=0}^{\infty} a_k x^k$ operieren, da diese erst auf Grund der Existenz von $\mathfrak{I}_1$ einen Sinn haben. Wir entziehen daher für die Konstruktion dem x die Bedeutung eines Elementes, das mit den Elementen von $\mathfrak{I}$ zusammen den drei ersten elementaren Rechenoperationen unterworfen werden kann, und somit den Ausdrücken $\sum_{k=0}^{\infty} a_k x^k$ die Bedeutung von Rechenausdrücken, sehen diese vielmehr lediglich als geordnete Systeme $(a_0, a_1, \ldots)$ von Elementen aus $\mathfrak{I}$ an. Aus (1)—(3) entnehmen wir dann die nötigen Richtlinien für die Angabe der Elemente von $\mathfrak{I}_1$ und ihrer Verknüpfungen.

c) *Konstruktion eines zu $\mathfrak{I}_1$ isomorphen Integritätsbereiches $\mathfrak{I}_1'$*

Wir sehen die Menge $\mathfrak{I}_1'$ aller geordneten Elementsysteme $(a_0, a_1, \ldots)$ von je abzählbar unendlich vielen Elementen aus $\mathfrak{I}$, wobei aber jedesmal nur endlich viele $a_k \neq 0$ sein sollen, als Menge unterschiedener Elemente an, haben also:

(1′) $(a_0, a_1, \ldots) = (a_0', a_1', \ldots)$ dann und nur dann, wenn $a_k = a_k'$ für alle k.

Wegen $(0, 0, \ldots) \neq (e, 0, \ldots)$ ist dann § 1, (a) in $\mathfrak{I}_1'$ realisiert.

Wir definieren weiter in $\mathfrak{l}_1$ zwei Verknüpfungen Addition und Multiplikation durch die Festsetzungen:

$$(2') \quad (a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots),$$

$$(3') \quad (a_0, a_1, \ldots)(b_0, b_1, \ldots) = (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \ldots).$$

Man überzeugt sich leicht, daß die rechten Seiten in (2′) und (3′) wieder nur endlich viele Glieder $\neq 0$ haben, also zu $\mathfrak{l}_1'$ gehören, so daß § 1, (b) vermöge (2′) und (3′) realisiert ist.

Ferner befriedigen die in (2′) und (3′) definierten Verknüpfungen die Gesetze § 1, (1)—(6). Für § 1, (1)—(5) folgt das leicht aus dem Erfülltsein jener Gesetze in $\mathfrak{l}$, für § 1, (6) zeigt man ebenso auf Grund der Gültigkeit von § 1, (6) in $\mathfrak{l}$, daß die Differenz in $\mathfrak{l}_1$ eindeutig bestimmt und stets durch

$$(4') \quad (a_0, a_1, \ldots) - (b_0, b_1, \ldots) = (a_0 - b_0, a_1 - b_1, \ldots)$$

gegeben ist.

Näherer Ausführung bedarf jedoch der Nachweis, daß das Gesetz § 1, (7a) in $\mathfrak{l}_1'$ gilt, an dessen Stelle nach dem Zusatz zu Def. 3 [12] auch der Nachweis treten darf, daß das Analogon zu Satz 4 [12] in $\mathfrak{l}_1'$ richtig ist. Da sich als Nullelement von $\mathfrak{l}_1'$ aus (2′) oder (4′) das Element $(0, 0, \ldots)$ ergibt, bedeutet die Voraussetzung

$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = 0,$$

daß alle Glieder dieses nach (3′) zu bildenden Produktsystems Null sind. Wäre nun $(a_0, a_1, \ldots) \neq 0$, $(b_0, b_1, \ldots) \neq 0$, so daß also ein letztes $a_\nu \neq 0$ und ein letztes $b_\mu \neq 0$ existierte, so folgte für das $(\nu + \mu)$-te Glied

$$a_0 b_{\mu+\nu} + \cdots + a_{\nu-1} b_{\mu+1} + a_\nu b_\mu + a_{\nu+1} b_{\mu-1} + \cdots + a_{\nu+\mu} b_0$$

des Produktsystems nach Wahl von a_ν und b_μ, daß es gleich $a_\nu b_\mu$, also wegen der Gültigkeit von Satz 4 in $\mathfrak{l}$ von Null verschieden wäre, im Widerspruch zu der Voraussetzung. Somit gilt das Analogon zu Satz 4 in $\mathfrak{l}_1'$.

Schließlich gilt auch § 1, (7b), d. h. das Analogon zu Satz 3 [11] in $\mathfrak{l}_1'$, weil nach (3′) das Element $(e, 0, 0, \ldots)$ Einselement von $\mathfrak{l}_1'$ ist.

Somit ist $\mathfrak{l}_1'$ ein Integritätsbereich bezüglich der Verknüpfungen (2′) und (3′).

d) *Konstruktion von* $\mathfrak{I}_1$

Der Integritätsbereich $\mathfrak{I}_1'$ enthält die Teilmenge $\mathfrak{I}'$ der speziellen Elemente $(a, 0, 0, \ldots)$, die nach (2′)—(4′) und Satz 6 [19] ein Teilintegritätsbereich von $\mathfrak{I}_1'$ und weiter nach nach (1′)—(3′) und Def. 7 [23] vermöge der Zuordnung $(a, 0, 0, \ldots) \longleftrightarrow a$ zu $\mathfrak{I}$ isomorph ist. Ganz entsprechend wie in § 3, d) kann man dann einen zu $\mathfrak{I}_1'$ isomorphen Erweiterungsintegritätsbereich $\mathfrak{I}_1$ von $\mathfrak{I}$ herleiten, indem man die Elemente von $\mathfrak{I}'$ durch die ihnen zugeordneten von $\mathfrak{I}$ ersetzt.

Dieser Integritätsbereich $\mathfrak{I}_1$ hat nun die im Satz genannte Eigenschaft. Bezeichnet nämlich x das spezielle Element $(0, e, 0, 0, \ldots)$ von $\mathfrak{I}_1'$, so daß also nach (3′) gilt

$$x^0 = e = (e, 0, 0, \ldots), x^1 = x = (0, e, 0, 0, \ldots),$$
$$x^2 = (0, 0, e, 0, 0, \ldots), \ldots,$$

und ist $(a_0, a_1, \ldots)$ irgendein Element von $\mathfrak{I}_1'$, so ist nach (2′) und (3′)

$$(a_0, a_1, \ldots) = (a_0, 0, 0, \ldots)\, x^0 + (a_1, 0, 0, \ldots)\, x^1 + \cdots.$$

Da x nicht zum Teilbereich $\mathfrak{I}'$ von $\mathfrak{I}_1'$ gehört, bleibt es beim Übergang zu $\mathfrak{I}_1$ erhalten, und es besteht demnach für das zugeordnete Element von $\mathfrak{I}_1$ die Darstellung $\sum\limits_{k=0}^{\infty} a_k x^k$.

Diese Darstellung ist schließlich eindeutig. Denn aus $\sum\limits_{k=0}^{\infty} a_k x^k = \sum\limits_{k=0}^{\infty} a_k' x^k$ folgt durch Übergang zum isomorphen $\mathfrak{I}_1'$ zunächst $(a_0, a_1, \ldots) = (a_0', a_1', \ldots)$ und daraus nach (1′) $a_k = a_k'$ für alle k.

Damit ist Satz 11 für $n = 1$ bewiesen. Zum Beweise für beliebiges n stehen folgende zwei Wege zur Verfügung:

Entweder kann man den gesuchten Integritätsbereich $\mathfrak{I}_n$ sukzessive konstruieren. Bezeichnet man dazu den zu irgendeinem Integritätsbereich $\mathfrak{I}$ nach dem schon bewiesenen Teil des Satzes vorhandenen Integritätsbereich $\mathfrak{I}_1$ mit $\mathfrak{I}[x]$, so bilde man sukzessive

$$\mathfrak{I}_1 = \mathfrak{I}[x_1], \mathfrak{I}_2 = \mathfrak{I}_1[x_2], \ldots, \mathfrak{I}_n = \mathfrak{I}_{n-1}[x_n].$$

Dann lassen sich die Behauptungen des Satzes für I_n sämtlich durch vollständige Induktion bezüglich n beweisen.

Oder man übertrage die Entwicklungen des vorstehenden Beweises für $n = 1$ sinngemäß auf beliebiges n, was ohne weiteres möglich ist. An Stelle von (1)—(3) tritt dabei:

$$(1\,\mathrm{a})\quad \sum_{k_1,\ldots,k_n=0}^{\infty} a_{k_1,\ldots,k_n} x_1^{k_1} \ldots x_n^{k_n} = \sum_{k_1,\ldots,k_n=0}^{\infty} a'_{k_1,\ldots,k_n} x_1^{k_1} \ldots x_n^{k_n}$$

dann und nur dann, wenn $a_{k_1,\ldots,k_n} = a'_{k_1,\ldots,k_n}$ für alle Systeme $(k_1, \ldots, k_n)$,

$$(2\,\mathrm{a})\quad \sum_{k_1,\ldots,k_n=0}^{\infty} a_{k_1,\ldots,k_n} x_1^{k_1} \ldots x_n^{k_n} + \sum_{k_1,\ldots,k_n=0}^{\infty} b_{k_1,\ldots,k_n} x_1^{k_1} \ldots x_n^{k_n} = \sum_{k_1,\ldots,k_n=0}^{\infty} (a_{k_1,\ldots,k_n} + b_{k_1,\ldots,k_n})\, x_1^{k_1} \ldots x_n^{k_n},$$

$$(3\,\mathrm{a})\quad \sum_{k_1,\ldots,k_n=0}^{\infty} a_{k_1,\ldots,k_n} x_1^{k_1} \ldots x_n^{k_n} \cdot \sum_{k_1,\ldots,k_n=0}^{\infty} b_{k_1,\ldots,k_n} x_1^{k_1} \ldots x_n^{k_n}$$
$$= \sum_{k_1,\ldots,k_n=0}^{\infty} \Big(\sum_{\substack{\lambda_1,\mu_1=0\\ \lambda_1+\mu_1=k_1}}^{\infty} \cdots \sum_{\substack{\lambda_n,\mu_n=0\\ \lambda_n+\mu_n=k_n}}^{\infty} a_{\lambda_1,\ldots,\lambda_n} b_{\mu_1,\ldots,\mu_n} \Big) x_1^{k_1} \ldots x_n^{k_n},$$

und daraus ist die zu treffende Wahl der Elemente von I_n [nämlich alle in ein n-dimensionales Schema geordneten Systeme $a_{k_1,\ldots,k_n}$ $(k_1, \ldots, k_n = 0, 1, \ldots)$ von Elementen aus I mit nur endlich vielen $\neq 0$] und der Verknüpfungen für sie ohne weiteres ersichtlich.

Die nähere Ausführung darf auf Grund dieser Hinweise für beide Wege dem Leser überlassen bleiben.

Während der erste Weg neben dem Vorzug des Auskommens mit den rechnerisch einfachen Entwicklungen des ausgeführten

Beweises für $n = 1$ insofern auch theoretisch von Bedeutung ist, als manche Sätze über I_n nur durch vollständige Induktion bezüglich n, also durch Zurückgehen auf die angegebene rekursive Konstruktion von I_n beweisbar sind (vgl. z. B. **2**, Satz 49 [41]), ist der zweite Weg deshalb befriedigender, weil er einmal die besondere Behandlung des Falles $n = 1$ entbehrlich macht, dann aber auch im Gegensatz zum ersten einer wichtigen Eigenschaft von I_n gerecht wird, nämlich der Symmetrie in $x_1, \ldots, x_n$, d. h. der aus Satz 11 ohne weiteres ersichtlichen Tatsache, daß I_n in sich übergeht, wenn die Rollen der Elemente $x_1, \ldots, x_n$ irgendwie vertauscht werden.

Anders als in §3, Satz 10, Zusatz [29] können hier zwar innerhalb eines beliebigen Erweiterungsintegritätsbereiches I^* mehrere verschiedene Repräsentanten des in Satz 11 genannten Erweiterungstypus vorhanden sein (z. B. wenn $I^* = I[x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m}]$ ist, alle $I[x_{i_1}, \ldots, x_{i_n}]$, wo $i_1, \ldots, i_n$ irgendwelche n verschiedenen Ziffern aus der Reihe $1, \ldots, n + m$ sind); aber offenbar ist jeder solche Repräsentant innerhalb I^* durch die Angabe derjenigen Elemente aus I^*, die die Rolle von $x_1, \ldots, x_n$ haben, eindeutig bestimmt, nämlich als die Gesamtheit der Ausdrücke der in Satz 11 genannten Form in diesen Elementen.

Im Hinblick auf die Ausführungen nach Def. 7 ist es daher wieder gerechtfertigt, mit dem bestimmten Artikel zu definieren:

Definition 9. *Der in Satz* 11 *genannte Integritätsbereich* I_n *heißt* der Integritätsbereich der ganzen rationalen Funktionen der n Unbestimmten $x_1, \ldots, x_n$ *über* I. *Er werde mit* $I[x_1, \ldots, x_n]$, *seine Elemente auch kurz mit* $f(x_1, \ldots, x_n), \ldots$ *oder noch kürzer mit* $f, \ldots$ *bezeichnet.*

Die eindeutigen Darstellungen dieser Elemente in der Form von Satz 11 *nennen wir ihre* Normaldarstellungen *und die darin auftretenden Elemente* $a_{k_1, \ldots, k_n}$ *aus* I *die* Koeffizienten *dieser Darstellungen.*

Die Bezeichnung *Unbestimmte* für die x_i erläutern wir dahin, daß jedes einzelne der x_i von I aus keiner anderen Bestimmung fähig ist, als der negativen, daß keine Gleichung $\sum_{k=0}^{\infty} a_k x_i^k = 0$ (mit nur endlich vielen Koeffizienten $a_k \neq 0$) besteht, außer der trivialen, wo alle $a_k = 0$ sind. Die x_i sind also weder Elemente von I, noch genügen sie algebraischen Gleichungen in I (siehe § 5 [47] und **2**, Def. 21 [54]). Steinitz (Lit.-Verz. 21) nennt sie daher bzgl. I *transzendente* Elemente. Übrigens sind die x_i wegen (1a) auch nicht untereinander durch positive Bestimmungen (algebraische Gleichungen) verknüpft. Steinitz nennt sie daher genauer ein System bzgl. I *algebraisch unabhängiger* Elemente.

I $[x_1, \ldots, x_n]$ ist stets ein echter Erweiterungsbereich von I, da infolge der Eindeutigkeit der Normaldarstellungen z. B. die Elemente $x_1, \ldots, x_n$ nicht zu I gehören.

I $[x_1, \ldots, x_n]$ ist in keinem Falle ein Körper (auch nicht, wenn I ein Körper ist). Auf Grund der obigen sukzessiven Konstruktion genügt es, das für I $[x]$ zu beweisen. In I $[x]$ existiert aber sicher nicht der Quotient $\frac{e}{x}$, weil für jedes $f(x) = \sum_{k=0}^{\infty} a_k x^k$ aus I $[x]$ gilt

$$x f(x) = \sum_{k=0}^{\infty} a_k x^{k+1}$$

$$= 0 + a_0 x + a_1 x^2 + \ldots \neq e + 0x + 0x^2 + \ldots = e.$$

Um auch die zu Beginn dieses Paragraphen schon genannten *rationalen* Rechenausdrücke in $x_1, \ldots, x_n$ einzubeziehen, erweitern wir I $[x_1, \ldots, x_n]$ zum Quotientenkörper. Da hierbei insbesondere der Teilbereich I zum Quotientenkörper erweitert wird, genügt es, von vornherein von einem Körper K und dem zugeordneten Integritätsbereich K $[x_1, \ldots, x_n]$ auszugehen:

Definition 10. *Ist* K *ein Körper, so heißt der Quotientenkörper des Integritätsbereiches* K $[x_1, \ldots, x_n]$ der Körper der rationalen Funktionen der n Unbestimmten $x_1, \ldots, x_n$ *über* K. *Er werde mit* K $(x_1, \ldots, x_n)$, *seine Elemente auch kurz mit* $\varphi(x_1, \ldots, x_n), \ldots$ *oder noch kürzer mit* $\varphi, \ldots$ *bezeichnet.*

Aus den im vorstehenden vom algebraischen Standpunkt aus definierten ganzen rationalen bzw. rationalen Funktionen über I bzw. K lassen sich nun die ganzen rationalen bzw. rationalen Funktionen i. S. d. An. über I bzw. K dadurch herleiten, daß man den bisherigen *Unbestimmten* $x_1, \ldots, x_n$ die Bedeutung von *Elementen aus* I *bzw.* K beilegt. Wir definieren zunächst für I $[x_1, \ldots, x_n]$:

Definition 11. *Unter der einem Element* f *von* I $[x_1, \ldots, x_n]$ zugeordneten ganzen rationalen Funktion i. S. d. An.

verstehen wir diejenige Funktion i. S. d. An. über I, *die entsteht, wenn man jedem Elementsystem* $x_1, \ldots, x_n$ *aus* I *das durch die Normaldarstellung von* f *gelieferte Element von* I *als Funktionswert zuordnet.*

Wir bezeichnen für den Augenblick den zu Beginn dieses Paragraphen erwähnten Ring der ganzen rationalen Funktionen i. S. d. An. von $x_1, \ldots, x_n$ über I mit $\overline{\mathsf{I}\,[x_1, \ldots, x_n]}$ und beweisen die folgende, für den Übergang von $\mathsf{I}\,[x_1, \ldots, x_n]$ zu $\overline{\mathsf{I}\,[x_1, \ldots, x_n]}$ grundlegende Tatsache, die wir **Einsetzungsprinzip** nennen:

Satz 12. *Beim Übergang von* $\mathsf{B} = \mathsf{I}\,[x_1, \ldots, x_n]$ *zu* $\mathsf{B}' = \overline{\mathsf{I}\,[x_1, \ldots, x_n]}$ *durch die in Def.* 11 *erklärte Zuordnung sind die Bedingungen* § 2, (δ), (δ'), (ε), (3), (4), (5) *erfüllt, dagegen nicht immer* (ε'). *Jener Übergang liefert also die Gesamtheit der Elemente von* $\overline{\mathsf{I}\,[x_1, \ldots, x_n]}$ *aus der Gesamtheit derjenigen von* $\mathsf{I}\,[x_1, \ldots, x_n]$, *und es bleiben bei ihm die Gleichheit und alle Verknüpfungsbeziehungen, dagegen nicht immer die Unterschiedenheit der Elemente von* $\mathsf{I}\,[x_1, \ldots, x_n]$ *erhalten. Dann und nur dann, wenn auch* § 2, (ε') *erfüllt ist, gilt auf Grund jener Zuordnung* $\mathsf{I}\,[x_1, \ldots, x_n] \cong \overline{\mathsf{I}\,[x_1, \ldots, x_n]}$.

Beweis. a) Das Erfülltsein von § 2, (δ), (ε) liegt natürlich in der eindeutigen und für jedes Element aus $\mathsf{I}\,[x_1, \ldots, x_n]$ anwendbaren Zuordnungsvorschrift von Def. 11.

b) Das Erfülltsein von § 2, (3), (4), (5) ist leicht aus den obigen Formeln (2a), (3a) zu entnehmen, die die Normaldarstellung der Summe und des Produkts zweier Elemente von $\mathsf{I}\,[x_1, \ldots, x_n]$ aus denen der Summanden bzw. Faktoren unter alleiniger Anwendung der in $\mathsf{I}\,[x_1, \ldots, x_n]$ gültigen Gesetze § 1, (1)—(5) berechnen. Denn weil diese Gesetze auch in I gültig sind, dürfen jene Umformungen auch vorgenommen werden, wenn $x_1, \ldots, x_n$ Elemente aus I sind.

c) Um das Erfülltsein von § 2, (δ') einzusehen, ist zu zeigen, daß auch umgekehrt jede ganze rationale Funktion i. S. d. An. von $x_1, \ldots, x_n$ über I einem Element f von $\mathsf{I}\,[x_1, \ldots, x_n]$ gemäß Def. 11 zugeordnet ist. Nun liefert jedes auf $x_1, \ldots, x_n$ und feste Elemente aus $\mathfrak{I}$ anzuwendende, aus endlich vielen Additionen, Subtraktionen und Multiplikationen bestehende Rechenverfahren, wenn man zunächst $x_1, \ldots, x_n$ als Unbestimmte, also als Elemente aus $\mathfrak{I}[x_1 \ldots, x_n]$ auffaßt, ein Element f aus $\mathfrak{I}[x_1, \ldots, x_n]$, einfach weil im Integritätsbereich $\mathfrak{I}[x_1, \ldots, x_n]$ jene Operation unbeschränkt ausführbar sind. Nach dem unter b) schon Bewiesenen bleiben ferner beim Übergang von $\mathfrak{I}[x_1, \ldots, x_n]$ zu $\overline{\mathfrak{I}[x_1, \ldots, x_n]}$ durch unsere Zuordnung alle Verknüpfungsbeziehungen erhalten. Wendet man das auf diejenige Verknüpfungsbeziehung an, die das Element f durch die Elemente $x_1, \ldots, x_n$ und die festen Elemente aus $\mathfrak{I}$ ausdrückt, so folgt, daß die durch jenes Rechenverfahren gelieferten Funktionswerte dieselben sind, wie die durch die Normaldarstellung von f gelieferten, daß also die betr. ganze rationale Funktion i. S. d. An. mit der f zugeordneten identisch ist.

d) § 2, (ε') ist z. B. nicht erfüllt, wenn für $\mathfrak{I}$ der nur aus 0 und e bestehende Körper K (§ 1, Beispiel 4) gewählt wird. Denn dann ist den beiden verschiedenen Elementen $x + x^2$ und 0 von $\mathsf{K}[x]$ dieselbe Funktion 0 i.S.d.An. zugeordnet, weil ja auch $x + x^2$ für alle x aus K (d.h. für $x = 0$ und $x = e$) Null ist.

Wir werden im übrigen in **2**, Satz 49 [41] und **3**, 1, § 4, Aufg. 7, 8 sowie § 1, Aufg. 9 sehen, daß § 2, (ε') dann und nur dann erfüllt ist, wenn $\mathfrak{I}$ unendlich viele Elemente besitzt, daß also für unendliches $\mathfrak{I}$ gilt $\overline{\mathfrak{I}[x_1, \ldots, x_n]} \cong \mathfrak{I}[x_1, \ldots, x_n]$ bzgl. $\mathfrak{I}$, für endliches $\mathfrak{I}$ aber nicht.

In der nach d) vorhandenen Möglichkeit liegt der Grund, weswegen man in der Algebra mit dem auf Zuordnung gestützten und demgemäß die Funktionen nach ihren Funktionswerten unterscheidenden Funktionsbegriff nicht auskommt, sondern den auseinandergesetzten formalen Funktionsbegriff braucht, der eine feinere Unterscheidung der Funktionen vermöge ihrer Rechenausdrücke liefert. Wenn auch diese Notwendigkeit nach dem unter d) Bemerkten tatsächlich nur für endliche Integritätsbereiche vorliegt, so sprechen natürlich weiterhin methodische Gesichtspunkte dafür, von den in § 1 gegebenen Grundlagen ausgehend den Rechenausdruck als den durch ihn gelieferten Funktionswerten übergeordnet anzusehen.

Wir haben im vorhergehenden absichtlich nicht in der Bezeichnung, sondern nur im Text unterschieden, ob $x_1, \ldots, x_n$ als Unbestimmte oder als Elemente aus I gemeint sind, um den im folgenden oft auszuführenden Übergang von der ersten zur zweiten Bedeutung der $x_1, \ldots, x_n$ nicht immer mit einem Bezeichnungswechsel verbinden zu müssen. Auf Grund von Satz 12 ist es weiterhin hinsichtlich der Verknüpfungen angängig, auch die Bezeichnung $f(x_1, \ldots, x_n)$ der Elemente von $\mathsf{I}[x_1, \ldots, x_n]$ unverändert für die zugeordneten Funktionswerte zu verwenden. Wir wollen daher fortan $f(x_1, \ldots, x_n)$ auch zur Bezeichnung des f zugeordneten Funktionswertes für das Elementsystem $x_1, \ldots, x_n$ aus I gebrauchen und einen solchen Funktionswert dann der kürzeren Ausdrucksweise halber auch einfach eine ganze rationale Funktion von $x_1, \ldots, x_n$ über I nennen; dagegen soll die Bezeichnung f (ohne Argumente) für das Element von $\mathsf{I}[x_1, \ldots, x_n]$ vorbehalten bleiben. [$f(x_1, \ldots, x_n)$ ist hiernach nicht auch Zeichen für die f zugeordnete Funktion i. S. d. An., sondern nur für einen einzelnen Wert dieser Funktion, die selbst erst durch die Gesamtheit aller Funktionswerte $f(x_1, \ldots, x_n)$ gebildet wird.] Wir müssen dann nur irgendwie einen Bezeichungsunterschied für die folgenden beiden ganz verschiedenartigen Gleichheitsaussagen einführen:

$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ als Elemente von $\mathsf{I}[x_1, \ldots, x_n]$,
$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ als Funktionswert für das Elementsystem $x_1, \ldots, x_n$ aus I.

Daher setzen wir weiter fest, daß fortan zur Bezeichnung der ersteren dieser beiden Aussagen das Zeichen $\equiv$ (Gegenteil $\not\equiv$) verwendet werden soll[1]). Auf Grund obiger Verabredung können und wollen wir aber die Schreibweise $f = g$ gleichbedeutend mit $f(x_1, \ldots, x_n) \equiv g(x_1, \ldots, x_n)$ verwenden.

[1]) Die Relation $f(x_1, \ldots, x_n) \equiv g(x_1, \ldots, x_n)$ hat dann zwar die Relation:
$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ für alle $x_1, \ldots, x_n$ aus I
zur Folge, aber nach obigem nicht notwendig umgekehrt. Das Zeichen $\equiv$ hat also i. a. eine weitergehende Bedeutung, als die häufig darunter verstandene: gleich für alle $x_1, \ldots, x_n$. — Eine Verwechslung der hier gemeinten Relation $\equiv$ mit einer Kongruenzrelation im Sinne von Def. 6 [21] wird durch den Zusammenhang ausgeschlossen.

Nach diesen Festsetzungen geht aus der gewählten Bezeichnung stets unzweideutig hervor, welche der beiden möglichen Auffassungen der $x_1, \ldots, x_n$ in einer Gleichheits- oder Ungleichheitsrelation vorliegt.

Wir vollziehen nun schließlich den Übergang von den Elementen von $\mathsf{K}(x_1, \ldots, x_n)$ zu den rationalen Funktionen i. S. d. An. durch folgende Definition:

Definition 12. *Unter der einem Element φ von $\mathsf{K}(x_1, \ldots, x_n)$* zugeordneten rationalen Funktion i. S. d. An. *verstehen wir diejenige Funktion i. S. d. An. über* K, *die entsteht, wenn jedem Elementsystem $x_1, \ldots, x_n$ aus* K, *für das mindestens eine Darstellung $\frac{f}{g}$ von φ als Quotient zweier Elemente aus* $\mathsf{K}[x_1, \ldots, x_n]$ *mit $g(x_1, \ldots, x_n) \neq 0$ existiert, als Funktionswert der Quotient $\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}$ der Funktionswerte von f und g zugeordnet wird.*

Analog zu Satz 12 gilt dann hier das **Einsetzungsprinzip:**

Satz 13. *Für den Körper $\mathsf{K}(x_1, \ldots, x_n)$ und den Ring $\overline{\mathsf{K}(x_1, \ldots, x_n)}$ der rationalen Funktionen i. S. d. An. von $x_1, \ldots, x_n$ über* K *gilt vermöge der in Def.* 12 *erklärten Zuordnung entsprechendes wie in Satz* 12, *nur daß hier die ev. Nichtgültigkeit von* § 2, (ε') *stets auch die Nichtgültigkeit von* § 2, (δ) *zur Folge hat.*

Beweis. a) Um das Erfülltsein von § 2, (ε) zu beweisen, ist zu zeigen, daß die einem Element φ von $\mathsf{K}(x_1, \ldots, x_n)$ nach Def. 12 zugeordnete Funktion i. S. d. An. unabhängig von der speziellen Wahl der (der Bedingung von Def. 12 genügenden) Quotientendarstellung $\frac{f}{g}$ allein durch φ bestimmt ist. Sind nun $\frac{f}{g}$ und $\frac{f'}{g'}$ zwei (dieser Bedingung genügende) Quotientendarstellungen von φ, so folgt aus der dann nach § 3, (1) bestehenden Relation $fg' = f'g$ nach Satz 12, daß auch

$$f(x_1, \ldots, x_n)\, g'(x_1, \ldots, x_n) = f'(x_1, \ldots, x_n)\, g(x_1, \ldots, x_n)$$

ist, woraus sich unter der Annahme von Def. 12 über g und g' weiter $\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} = \frac{f'(x_1, \ldots, x_n)}{g'(x_1, \ldots, x_n)}$ ergibt.

b) Durch Zurückgehen auf die Formeln § 3, (2) und (3) und Anwendung von Satz 12 ergibt sich ebenso das Erfülltsein von § 2, (3), (4), (5).

c) Das Erfülltsein von § 2, (δ') folgt dann entsprechend wie im Beweis zu Satz 12 unter c); siehe dazu die Präzisierung und Anleitung in **3**, 1, § 5, Aufg. 1.

d) Daß § 2, (ε') nicht notwendig erfüllt ist, zeigt dasselbe Beispiel wie oben. Es tritt das offenbar dann und nur dann ein, wenn mindestens ein Element g in $K[x_1, \ldots, x_n]$ derart existiert, daß zwar $g \neq 0$, aber doch $g(x_1, \ldots, x_n) = 0$ für alle $x_1, \ldots, x_n$ aus K ist. Ist nun einerseits dies der Fall, so hat das Element $\frac{e}{g}$ aus $K(x_1, \ldots, x_n)$ die Eigenschaft, daß zu ihm für kein Elementsystem $x_1, \ldots, x_n$ aus K eine Quotientendarstellung existiert, deren Nenner einen von Null verschiedenen Funktionswert hat; denn nach § 3, (1) ist $\frac{f}{gf}$ seine allgemeinste Quotientendarstellung, wo f ein beliebiges Element aus $K[x_1, \ldots, x_n]$ ist. Also existiert dann zu $\frac{e}{g}$ keine zugeordnete Funktion i. S. d. An., indem die Def. 12 des Funktionswertes für jedes $x_1, \ldots, x_n$ aus K versagt. Existiert andererseits kein g der angegebenen Art in $K[x_1, \ldots, x_n]$, so läßt sich dem Quotienten $\frac{f}{g}$ mindestens für ein Elementsystem $x_1, \ldots, x_n$ aus K ein Funktionswert gemäß Def. 12 zuordnen.

Auf Grund von Satz 13 übertragen sich die im Anschluß an Satz 12 gemachten Bemerkungen über $I[x_1, \ldots, x_n]$ sinngemäß auch auf $K(x_1, \ldots, x_n)$. Es sollen daher unsere Bezeichnungsfestsetzungen auch für die Elemente von $K(x_1, \ldots, x_n)$ Gültigkeit haben.

§ 5. Ausführliche Formulierung der Grundaufgabe der Algebra

Mittels der im vorhergehenden auseinandergesetzten Begriffe wollen wir jetzt eine genaue Formulierung der in der Einleitung genannten Grundaufgabe der Algebra geben.

Eine mittels der vier elementaren Rechenoperationen gebildete „*Gleichung*“ zwischen bekannten und unbekannten Elementen eines Körpers K, wie sie in der Formulierung der Einleitung gemeint ist, entsteht, wenn zwei auf die Unbekannten $x_1, \ldots, x_n$ und vorgegebene (bekannte) Elemente von K anzuwendende Rechenverfahren vorliegen und gefragt wird, für welche Elementsysteme $x_1, \ldots, x_n$ aus K beide Verfahren dasselbe Ergebnis liefern. Hierbei haben also die Unbekannten $x_1, \ldots, x_n$ zunächst den Charakter von Unbestimmten, und die vorliegenden Rechenverfahren sind zwei Elemente φ und φ' von $\mathsf{K}(x_1, \ldots, x_n)$. Die in der „Gleichung“ liegende Frage bezieht sich dann, in gewisser Analogie zu den letzten Entwicklungen von § 4, auf die Ersetzung der Unbestimmten $x_1, \ldots, x_n$ durch Elementsysteme $x_1, \ldots, x_n$ aus K und geht dahin, für welche solchen Elementsysteme die Gleichung $\varphi(x_1, \ldots, x_n) = \varphi'(x_1, \ldots, x_n)$ besteht.

Da das Hinschreiben einer solchen „Gleichung“ als F o r d e r u n g oder F r a g e logisch einen ganz anderen Sinn hat als die gewöhnlich ebenso bezeichnete T a t s a c h e des Bestehens der Gleichung, wollen wir für die Forderungsgleichheit ein besonderes Zeichen $\doteq$ (Gegenteil $\not\doteq$) einführen, also die eben genannte Frage mit

$$\varphi(x_1, \ldots, x_n) \doteq \varphi'(x_1, \ldots, x_n)$$

bezeichnen.

Die Gleichung $\varphi(x_1, \ldots, x_n) \doteq \varphi'(x_1, \ldots, x_n)$ ist nun zunächst nach dem Einsetzungsprinzip, angewandt auf die Verknüpfungsbeziehung $\varphi - \varphi' = \psi$, gleichbedeutend mit einer Gleichung der Form $\psi(x_1, \ldots, x_n) \doteq 0$, wo ψ wieder ein Element von $\mathsf{K}(x_1, \ldots, x_n)$ ist.

Ehe wir diese Gleichung weiter reduzieren, müssen wir uns mit dem folgenden Umstand auseinandersetzen: Einerseits besteht das zu ψ führende Rechenverfahren im Sinne der gestellten Aufgabe (das gemäß $\psi = \varphi - \varphi'$ aus den beiden ursprünglich gegebenen, zu φ und φ' führenden zusammengesetzt ist) genauer betrachtet in einer Kette von Einzeloperationen, deren jede eine Addition, Substraktion, Multiplikation oder Division von je zwei Elementen ist, deren jedes entweder ein Element aus K oder eines der $x_1, \ldots, x_n$ oder ein Resultat einer der vorhergehenden Operationen ist. Andererseits läßt sich ψ als Element von $\mathsf{K}(x_1, \ldots, x_n)$ in der einfachen Form eines Quotienten $\frac{f}{g}$ zweier Elemente aus $\mathsf{K}[x_1, \ldots, x_n]$ in Normaldarstellung darstellen. Nach dem Einsetzungsprinzip hat es dabei auf das Resultat der Einsetzung eines Elementsystems $x_1, \ldots, x_n$ aus K keinen Einfluß, ob man diese Einsetzung *vor* der Ausführung des Verfahrens stattfinden läßt (ob man also, wie es dem Sinn der Aufgabe entspricht, von vornherein mit den $x_1, \ldots, x_n$ als Elementen aus K losrechnet), oder ob man erst *nach* der Ausführung des Verfahrens, in eine Quotientendarstellung $\frac{f}{g}$ einsetzt, *solange man nur solche Einsetzungen betrachtet, für die weder der Nenner g noch einer der sukzessive bei dem Rechenverfahren auftretenden Nenner Null wird.* Es ist nun keineswegs von vornherein sicher, daß der Nenner g genau für diejenigen Elementsysteme aus K nicht Null wird, für die keiner der sukzessiven Nenner des Verfahrens Null wird, *die also im Sinne der gestellten Aufgabe zulässig sind.* Doch läßt sich zeigen, daß es unter allen Quotientendarstellungen von ψ (mindestens) eine mit dieser Eigenschaft gibt (siehe dafür **3**, 1, § 5, Aufg. 1). Eine solche, der Aufgabe naturgemäß angepaßte Quotientendarstellung $\psi = \frac{f}{g}$ sei im folgenden zugrunde gelegt.

Vermöge einer Quotientendarstellung $\psi = \frac{f}{g}$ (der eben näher charakterisierten Art) reduziert sich nun nach § 3 und dem Einsetzungsprinzip die Lösung der Gleichung $\psi(x_1, \ldots, x_n) \doteq 0$ weiter darauf, alle diejenigen Lösungen von $f(x_1, \ldots, x_n) \doteq 0$ zu bestimmen, die zudem Lösungen von $g(x_1, \ldots, x_n) \not\doteq 0$ sind. Da man nun die Lösungen der letzteren Ungleichung kennt, wenn man die der Gleichung

$g(x_1, \ldots, x_n) \doteq 0$ kennt, reduziert sich die Aufgabe auf die Behandlung von Gleichungen der Form

$$f(x_1, \ldots, x_n) \doteq 0,$$

wo f ein Element aus $\mathsf{K}[x_1, \ldots, x_n]$ ist.

Obwohl man nun im Prinzip die gemeinsamen Lösungen einer Anzahl von Gleichungen beherrscht, wenn man die Lösungen jeder Einzelgleichung kennt, ist es doch sowohl von theoretischen als auch von praktischen Gesichtspunkten aus zweckmäßig, solche *Gleichungssysteme* als Ganzes zu behandeln. Somit formulieren wir als die uns zum Leitfaden dienende **Aufgabe der Algebra:**

Es seien K ein Körper und $f_1, \ldots, f_m$ Elemente aus $\mathsf{K}[x_1, \ldots, x_n]$. Es sollen Methoden zur Gewinnung aller Lösungen des Gleichungssystems

$$f_i(x_1, \ldots, x_n) \doteq 0 \quad (i = 1, \ldots, m)$$

entwickelt werden[1]).

Eine systematisch vollendete Theorie zur Lösung dieser Aufgabe in ihrer vollen Allgemeinheit würde den Rahmen dieser Darstellung übersteigen. Daher sollen uns hier nur die beiden nachstehenden, für den allgemeinen Fall grundlegenden Spezialfälle beschäftigen:

1) Die Elemente $f_1, \ldots, f_m$ sind linear, d. h. in ihrer Normaldarstellung (Def. 9 [38]) sind höchstens die $n+1$ Koeffizienten

$$a_{0,\ldots,0}, \; a_{1,0,\ldots,0}, \ldots, a_{0,\ldots,0,1}$$

von Null verschieden. Dann handelt es sich also um ein Gleichungssystem, das in der Form

$$(1) \qquad \sum_{k=1}^{n} a_{ik} x_k \doteq a_i \quad (i = 1, \ldots, m)$$

[1]) Es sei auf die beiden folgenden, naheliegenden Verallgemeinerungen dieser Aufgabe hingewiesen:
1. die Anzahl der Gleichungen und Unbekannten wird auch als abzählbar unendlich zugelassen,
2. an Stelle des Körpers K wird ein Integritätsbereich (oder auch nur ein Ring) zugrunde gelegt,

mit denen man sich in neuerer Zeit ebenfalls beschäftigt hat.

geschrieben werden kann, wo die a_{ik} und a_i Elemente aus K sind. Ein Gleichungssystem der Form (1) heißt ein *lineares Gleichungssystem* in K.

2) Es ist $m = n = 1$. Dann handelt es sich also um eine einzelne Gleichung der Form

$$\sum_{k=0}^{\infty} a_k x^k \doteq 0\,,$$

wo die a_k Elemente aus K sind, von denen nur endlich viele $\neq 0$ sind. Von dem trivialen Falle, wo alle $a_k = 0$ sind und somit jedes x aus K Lösung der Gleichung ist, darf abgesehen werden. Dann existiert also ein letztes $a_r \neq 0$. Der so bestimmte Index r heißt der Grad des links stehenden Elementes aus $\mathsf{K}[x]$. Der Fall $r = 0$ ist ebenfalls trivial, weil dann wegen der Annahme $a_0 \neq 0$ kein x aus K Lösung der Gleichung ist. Somit ist eine Gleichung der Form

$$(2) \qquad \sum_{k=0}^{r} a_k x^k \doteq 0 \qquad (a_r \neq 0, \quad r \geqq 1)$$

zu behandeln. Eine Gleichung der Form (2) heißt eine *algebraische Gleichung r-ten Grades* in K.

In **1**, III und IV werden wir die Teilaufgabe 1), in **2** die Teilaufgabe 2) behandeln.

II. Gruppen

§ 6. Definition der Gruppen

Man redet von einer Gruppe, wenn folgender Tatbestand realisiert ist:

(a) *Es liegt eine* Menge $\mathfrak{G}$ von unterschiedenen Elementen *in irgendeiner endlichen oder unendlichen Anzahl vor.*

Vgl. die Bemerkungen zu § 1, (a). Anders als dort wird hier nicht gefordert, daß $\mathfrak{G}$ mindestens zwei verschiedene Elemente besitzt. Wir bezeichnen Gruppen mit großen deutschen, Elemente aus Gruppen mit großen lateinischen Buchstaben.