SAMMLUNG GÖSCHEN BAND 930

Elementare und klassische Algebra

vom modernen Standpunkt

Von

Dr. Wolfgang Krull

o. Professor an der Universität Bonn

Zweite, erweiterte Auflage

I

WALTER DE GRUYTER & CO

vormals G J Goschen'sche Verlagshandlung J Guttentag, Verlagsbuchhandlung · Georg Reimer · Karl J Trübner Veit & Comp

Berlin 1952

Archiv-Nr. 11 09 30
Druck von A. W. Hayn's Erben, Berlin SO 36
Printed in Germany

Inhalt.

Literatur.

1. Bieberbach-Bauer, Algebra. Leipzig, Teubner 1928.
2. H. Hasse, Hohere Algebra. I. Lineare Gleichungen. Sammlung Goschen Nr. 931.
3. H. Hasse, Hohere Algebra. II. Gleichungen hoheren Grades. Sammlung Goschen Nr. 932.
4. H. Hasse u. W. Klobe, Aufgabensammlung zur höheren Algebra. Sammlung Goschen Nr. 1082.
5. O. Haupt, Lehrbuch der Algebra. 2 Bde. Leipzig, Akademische Verlagsgesellschaft m. b. H. 2. Aufl. 1952.
6. O. Perron, Algebra. 2 Bde. Berlin, Walter de Gruyter & Co. Goschens Lehrbucherei Bd. 8 u. 9. 3. Aufl. 1951 u. 1952.
7. B. L. van der Waerden, Moderne Algebra I. Grundlehren d Math. Wiss. 33. Berlin, Springer, 3. Aufl. 1950.

Vorbemerkungen.

In dem vorliegenden Buche habe ich mich bemuht, moglichst vollstandig diejenigen Teilgebiete der nichtlinearen Algebra, insbesondere der Gleichungstheorie zu behandeln, die auch dem der Algebra ferner stehenden Mathematiker vertraut sein sollten. Gleichzeitig war es mein Ziel, durch die Form der Darstellung den Leser in die moderne Denkweise einzufuhren und ihn so auf die eigentliche „Hohere Algebra' vorzubereiten Zu den einzelnen Abschnitten sei bemerkt:

Abschnitt I enthalt eine Neubegrundung des bereits auf der Schule geubten Buchstabenrechnens unter Voranstellung des fur die moderne Algebra grundlegenden Korperbegriffs. Der Anfanger moge gerade diesen Abschnitt sorgfaltig durcharbeiten. In Abschnitt II werden die rationalen Beziehungen zwischen den Nullstellen und den Beiwerten (Koeffizienten) algebraischer Gleichungen und die Zerlegung ganzzahliger Polynome behandelt. Auch der Sturmsche Satz hat hier seinen Platz gefunden Die elementare Auflosung der Gleichungen 2. bis 4. Grades durch Wurzelzeichen bringt Abschnitt III. Hohere Gesichtspunkte — eine Einfuhrung in den Gedankenkreis des Bézoutschen Satzes — finden sich dort, wo die homogene Schreibweise benutzt wird, vor allem bei der Losung zweier simultaner quadratischer Gleichungen. — Abschnitt IV behandelt zunachst die Konstruktion algebraischer Oberkorper nach Kronecker und Steinitz, sowie die moderne Gradtheorie. Im ubrigen schließt sich der Abschnitt eng an die geschichtliche Entwicklung an, indem als Vorbereitung fur die Gaußsche Kreisteilungstheorie von Abschnitt V die Untersuchungen von Lagrange besprochen werden, die fur die moderne Gleichungstheorie grundlegend geworden sind. Unmittelbar bis zur allgemeinen Galoisschen Theorie fuhrt Abschnitt VI. Zunachst wird — ohne Gruppentheorie — gezeigt, daß metazyklische Korper und Radikalkorper im wesentlichen gleichwertige Begriffe sind, dann werden fur die „allgemeine Gleichung" die Hauptsatze der Galoisschen Theorie in Lagrangeschem Geiste abgeleitet. So ist abschließend ein Standpunkt erreicht, von dem sich einerseits die Weiterentwicklung leicht uberblicken laßt, und von dem aus andrerseits vor allem der Grundgedanke des Abelschen Beweises fur die Unmoglichkeit der Losung der allgemeinen Gleichung funften Grades durch Radikale vollig durchsichtig wird. — In einem Anhang wird der Gaußsche „Fundamentalsatz der Algebra" vom modernen Standpunkt kurz behandelt.

Abschnitt I. Formales Rechnen.

§ 1. Der Körperbegriff.

Die Algebra wird beherrscht von den vier Grundrechnungsarten Addition, Subtraktion, Multiplikation, Division. Der Leser geht am besten mit diesen Rechnungsarten zunächst so um, wie er es vom elementaren Buchstabenrechnen her gewohnt ist. Eine Zusammenstellung derjenigen formalen Eigenschaften der Addition usw., auf die es in der Algebra allein ankommt, findet sich am Schlusse des Paragraphen.

Ein System $\mathfrak{R}$, für dessen Elemente Addition, Subtraktion und Multiplikation definiert und unbeschrankt ausführbar sind, wird als „Ring" bezeichnet. Ist in $\mathfrak{R}$ außerdem auch die Division durch von 0 verschiedene Elemente unbeschrankt ausfuhrbar, so heißt $\mathfrak{R}$ ein „Körper". — Der Ring $\mathfrak{R}$ ist dann und nur dann ein Körper, wenn $\mathfrak{R}$ gleichzeitig mit einem beliebigen Elemente $a \neq 0$ stets auch das dazu reziproke Element $a^{-1} = \frac{1}{a}$ enthält.

Die Bedeutung des Ring- und Körperbegriffs erkennt man am besten durch die Betrachtung von Beispielen. Beschränkt man sich, wie wir im Folgenden, so weit nichts anderes ausdrücklich angegeben wird, stets tun wollen, auf die Betrachtung von solchen Ringen und Körpern, bei denen das weiter unten erwahnte Element $\overline{0}$ bzw. $\overline{1}$ mit der Zahl 0 bzw. 1 zusammenfallt, so ist der einfachst denkbare Ring das System $\mathfrak{R}_0$ aller positiven und negativen ganzen Zahlen (einschließlich der Null). Das Teilsystem aller positiven ganzen Zahlen bildet fur sich allein keinen Ring, da die Subtraktion innerhalb dieses Teilsystems nicht unbeschrankt ausfuhrbar

ist. Der einfachste Korper $\mathfrak{K}_0$ besteht aus allen rationalen Zahlen, also aus allen Bruchen der Form $\frac{a_0}{b_0}$ (a_0, b_0 in $\mathfrak{R}_0$; $b_0 \neq 0$). Die Menge $\mathfrak{K}_r$ aller reellen Zahlen, also aller endlichen oder unendlichen Dezimalbruche, stellt einen echten Oberkorper von $\mathfrak{K}_0$ dar, also einen Korper, der alle Elemente von $\mathfrak{K}_0$, außerdem aber auch nicht zu $\mathfrak{K}_0$ gehorige Elemente enthalt. Einen echten Oberkorper von $\mathfrak{K}_r$ bildet die Menge $\mathfrak{K}_k$ aller komplexen Zahlen, also aller Zahlen der Form $\alpha = a + bi$ (a und b reell, i imaginare Einheit).

Bei der Betrachtung von $\mathfrak{K}_k$ hat man die Rechenregeln $(a + bi) \pm (c + di) = (a \pm c) + (b \pm d)i$; $(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$, $(a + bi)^{-1} = (a^2 + b^2)^{-1} \cdot (a - bi)$ zu beachten. Aus diesen Regeln folgt nun, daß auch das System $\mathfrak{K}'_k$ aller „rationalen komplexen Zahlen", d. h. aller $\alpha = a + bi$ (a, b in $\mathfrak{K}_0$) einen Korper darstellt. $\mathfrak{K}'_k$ ist ein echter Oberkorper von $\mathfrak{K}_0$ und ein echter Unterkorper von $\mathfrak{K}_k$. Von den Korpern $\mathfrak{K}'_k$, $\mathfrak{K}_r$ ist keiner im anderen enthalten. Der Durchschnitt von $\mathfrak{K}_k$ und $\mathfrak{K}_r$, d. h. die Menge aller gleichzeitig zu $\mathfrak{K}'_k$ und $\mathfrak{K}_r$ gehorigen Elemente ist der Korper $\mathfrak{K}_0$.

Ein fur die Algebra charakteristischer Vorgang besteht darin, daß man aus einem gegebenen Korper $\mathfrak{K}$ bzw. Ring $\mathfrak{R}$ durch Hinzunahme neuer Elemente einen Oberkorper $\mathfrak{L}$ bzw. Oberring $\mathfrak{Q}$ bildet. Dabei konnen die neuen Elemente „Unbestimmte" sein (vgl. zu diesem Begriff § 3, insbesondere Anm. [1]), es konnen aber auch zwischen ihnen und den Elementen von $\mathfrak{K}$ bzw. $\mathfrak{R}$ algebraische Beziehungen bestehen. Beide Moglichkeiten kommen bereits in der Schulmathematik vor. Das ubliche „Buchstabenrechnen" ist nichts anderes als das Operieren in einem Korper oder Ring, den man aus einem geeigneten Zahlkorper (etwa aus $\mathfrak{K}_0$, $\mathfrak{K}_r$, $\mathfrak{K}_k$) durch Hinzunahme von endlich vielen Unbestimmten gewonnen hat. In diesem Sinne bringen die folgenden Paragraphen (bis § 7 einschließlich) einfach eine Entwicklung der Grundlagen des Buchstabenrechnens „vom hoheren Standpunkt". Aber auch die Bildung von Oberkorpern mit algebraischen Beziehungen

zwischen den neu hinzugenommenen Elementen und denen des Grundkorpers spielt schon in der Schulmathematik eine nicht unbetrachtliche Rolle. Die Bedeutung der ublichen Rechenregeln fur Quadratwurzeln, insbesondere des „Wegschaffens der Quadratwurzeln aus dem Nenner" wird erst vom korpertheoretischen Standpunkt aus voll verstandlich.

Die fur uns allein wichtigen Eigenschaften der Addition und Multiplikation sind bei beliebigen Ringen die folgenden:

a) $(a+b)+c=a+(b+c)$; $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ (assoziatives Gesetz).

b) $a+b=b+a$; $a\cdot b=b\cdot a$ (kommutatives Gesetz).

c) $(a+b)\cdot c=a\cdot c+b\cdot c$ (distributives Gesetz).

d) Es gibt ein „Nullelement" bzw. „Einheitselement" 0 bzw. $\overline{1}$ der Addition bzw. Multiplikation, das fur jedes a der Gleichung $a+\overline{0}=a$ bzw. $a\cdot\overline{1}=a$ genugt.

e) Zu jedem a gibt es ein (eindeutig bestimmtes) Element $-a$, fur das $a+(-a)=\overline{0}$ wird.

In jedem Korper gilt außerdem

f) Es gibt zu jedem Element $a\neq\overline{0}$ ein (eindeutig bestimmtes) Element a^{-1}, fur das $a\cdot a^{-1}=\overline{1}$ wird.

Aus e) folgt sofort die allgemeine eindeutige Ausfuhrbarkeit der Subtraktion, d. h. die Losbarkeit der Gleichung $a+x=b$. Analog ergibt sich aus f) die Moglichkeit der Division durch jedes $a\neq\overline{0}$. Besonders betont sei die Tatsache, daß die Division durch Null grundsatzlich ausgeschlossen ist. Die Gleichung $a\cdot\overline{0}=\overline{0}$ ist eine einfache Folge von c), gilt also in jedem Ring.

Im ubrigen beschranken wir uns auf die Betrachtung von solchen Ringen, in denen keine „Nullteiler" auftreten, d. h. Ringe mit der Eigenschaft:

g) Aus $a\cdot b=\overline{0}$, $a\neq\overline{0}$ folgt $b=\overline{0}$.

Bei einem Korper ist g) selbstverstandlich, denn aus $a \cdot b = \bar{0}$, $a \neq \bar{0}$ ergibt sich durch Multiplikation mit a^{-1} sofort: $\bar{0} = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = \bar{1} \cdot b = b$.

Da sich das Nullelement 0 bzw. das Einselement $\bar{1}$ weitgehend analog den Zahlen 0 und 1 verhalten, lassen wir in Zukunft dort, wo kein Mißverstandnis zu befurchten ist, den Querstrich fort und schreiben einfach 0 und 1.

Dem fur abstrakte Überlegungen interessierten Leser sei empfohlen, uberall dort, wo wir einen gegebenen Korper oder Ring zu einem Oberkorper oder Oberring erweitern, sorgfaltig nachzuprufen, daß die fur den Ausgangsbereich vorausgesetzten Eigenschaften a) bis f) bzw. a) bis e) auch dem Oberbereich zukommen[1]).

§ 2. Quotientenkörperbildung.

Die folgenden Betrachtungen zeigen an einem einfachen Beispiel den praktischen Wert des allgemeinen Korper- und Ringbegriffs. Bekanntlich ist das Rechnen mit Bruchen, insbesondere die Addition und Division, auch fur viele der Schule entwachsene Gebildete keineswegs eine einfache Sache. Wir behandeln nun die Aufgabe, einen ganz beliebigen, von Nullteilern freien Ring $\mathfrak{R}$ genau so zu einem Korper $\mathfrak{K}$ zu erweitern, wie man es bei dem Ring $\mathfrak{R}_0$ der ganzen Zahlen macht, wenn man durch Einfuhrung der gewohnlichen Bruche zum Korper $\mathfrak{K}_0$ der rationalen Zahlen ubergeht. Dabei wird sich zeigen, daß der allgemeine Fall in gewissem Sinne leichter zu erledigen ist als der von der Schule her bekannte Spezialfall. — Der gesuchte Korper $\mathfrak{K}$ soll offenbar aus allen formalen „Bruchen" $\frac{a}{b}$ (a und b in $\mathfrak{R}$, $b \neq 0$) bestehen („Quotientenkorper"[1]), wobei insbesondere fur beliebige a stets $\frac{a}{1} = a$ zu setzen ist.

[1]) Vgl hierzu Hasse, Hohere Algebra I, Goschen, Nr 931, § 1.

Aus der Tatsache, daß der Bruch $\frac{a}{b}$ eingeführt wird, um eine Lösung der Gleichung $b \cdot x = a$ zu erhalten, ergibt sich sofort zwangslaufig die folgende Gleichheitsdefinition:

$\frac{a_1}{b_1} = \frac{a_2}{b_2}$ in $\mathfrak{R}$ dann und nur dann, wenn $a_1 \cdot b_2 = a_2 \cdot b_1$ in $\mathfrak{R}$.

In der Tat, soll $\frac{a_1}{b_1} = \frac{a_2}{b_2}$ sein, so muß, da ja die Gesetze a) bis f) in $\mathfrak{R}$ gelten sollen, notwendig $a_1 \cdot b_2 = \left(\frac{a_1}{b_1} \cdot b_1\right) \cdot b_2$ $= \frac{a_1}{b_1} \cdot (b_1 \cdot b_2) = \frac{a_2}{b_2} \cdot (b_2 \cdot b_1) = \left(\frac{a_2}{b_2} \cdot b_2\right) \cdot b_1 = a_2 \cdot b_1$ sein. — Haben wir umgekehrt $a_1 \cdot b_2 = a_2 \cdot b_1$, wobei $b_1 \neq 0$, $b_2 \neq 0$ und damit wegen der Nullteilerfreiheit von $\mathfrak{R}$ auch $b_1 \cdot b_2 \neq 0$ ist, so haben wir in anderer Schreibweise $\frac{a_1}{b_1}(b_1 \cdot b_2) = \left(\frac{a_1}{b_1} \cdot b_1\right) b_2$ $= \left(\frac{a_2}{b_2} \cdot b_2\right) \cdot b_1 = \frac{a_2}{b_2} \cdot (b_2 \cdot b_1)$, also $\left(\frac{a_1}{b_1} - \frac{a_2}{b_2}\right) \cdot (b_1 \cdot b_2) = 0$ und daraus muß wegen der Nullteilerfreiheit jedes Körpers $\frac{a_1}{b_1} = \frac{a_2}{b_2}$ folgen.

Unsere Gleichheitsdefinition ist also jedenfalls zwangsläufig festgelegt, es fragt sich nur, ob diese Definition auch immer brauchbar ist[1]). Dazu ist zu zeigen: 1. $\frac{a_1}{b_1} = \frac{a_1}{b_1}$ („Reflexivitat") 2. Aus $\frac{a_1}{b_1} = \frac{a_2}{b_2}$ folgt $\frac{a_2}{b_2} = \frac{a_1}{b_1}$ („Symmetrie") 3. Aus $\frac{a_1}{b_1} = \frac{a_2}{b_2}$, $\frac{a_2}{b_2} = \frac{a_3}{b_3}$ folgt $\frac{a_1}{b_1} = \frac{a_3}{b_3}$ („Transitivitat"). 1. und 2.

[1]) Vgl. hierzu Hasse I a a O. § 2.

sind aber in unserem Fall klar. Ist ferner $a_1 b_2 = a_2 b_1$, $a_2 b_3 = a_3 b_2$ ($b_1 \neq 0$, $b_2 \neq 0$, $b_3 \neq 0$), so haben wir $a_1 \cdot b_2 \cdot b_3 = a_2 \cdot b_1 \cdot b_3 = a_3 \cdot b_1 \cdot b_2$, $(a_1 \cdot b_3 - a_3 \cdot b_1) \cdot b_2 = 0$ und weiter wegen $b_2 \neq 0$ und der Nullteilerfreiheit von $\mathfrak{R}$: $a_1 b_3 = a_3 b_1$, $\frac{a_1}{b_1} = \frac{a_3}{b_3}$.

Bedingung 1. 2. und 3. sind also erfullt, unsere Gleichheitsdefinition ist stets brauchbar. Aus ihr ergibt sich sofort die Möglichkeit des Erweiterns und Kurzens, $\frac{a}{b} = \frac{a \cdot c}{b \cdot c}$ ($c \neq 0$), sowie die Tatsache, daß $\frac{a}{b}$ dann und nur dann zu $\mathfrak{R}$ gehort, daß $\frac{a}{b} = \frac{c}{1} = c$ wird, wenn „a in $\mathfrak{R}$ durch b teilbar" ist, d. h. wenn in $\mathfrak{R}$ eine Gleichung $a = b \cdot c$ gilt. — Auch die Definitionen von Addition und Multiplikation ergeben sich sofort zwangslaufig: Offenbar muß $(b_1 \cdot b_2) \cdot \left(\frac{a_1}{b_1} + \frac{a_2}{b_2}\right) = (b_1 \cdot b_2) \cdot \frac{a_1}{b_1} + (b_1 \cdot b_2) \cdot \frac{a_2}{b_2} = b_2 \cdot a_1 + b_1 \cdot a_2$ und $(b_1 \cdot b_2) \cdot \left(\frac{a_1}{b_1} \cdot \frac{a_2}{b_2}\right) = a_1 \cdot a_2$ werden, d. h. man hat zu setzen $\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 \cdot b_2 + a_2 \cdot b_1}{b_1 \cdot b_2}$, $\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 \cdot a_2}{b_1 \cdot b_2}$. Es ist nun noch zu verifizieren, daß bei diesen Definitionen aus $\frac{a_i}{b_i} = \frac{c_i}{d_i}$ ($i = 1, 2$) stets $\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{c_1}{d_1} + \frac{c_2}{d_2}$, $\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{c_1}{d_1} \cdot \frac{c_2}{d_2}$ folgt, und daß die formalen Bedingungen a) bis f) von § 1 fur die Addition und Multiplikation erfullt sind. Aber das sind ganz einfache Überlegungen, deren Durch-

fuhrung dem Leser uberlassen werden kann. (Man muß dabei dauernd die Tatsache ausnutzen, daß der Ring $\mathfrak{R}$ jedenfalls den Forderungen a) bis e) genügt.) Naturlich wird $-\frac{a}{b} = \frac{(-a)}{b}$; $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$ $(a \neq 0)$, das letztere wegen $\frac{a}{b} \cdot \frac{b}{a} = \frac{a \cdot b}{a \cdot b} = 1$. — Damit ist nicht nur die Existenz des Quotientenkorpers $\mathfrak{k}$ gesichert, es ist auch, da wir zwangslaufig auf die Definitionen von Gleichheit, Addition und Multiplikation kamen, nachgewiesen, daß $\mathfrak{k}$ durch den Ausgangsring eindeutig bestimmt ist. Dabei waren die entscheidenden Überlegungen so einfach, daß ihre Rekonstruktion nach einmaliger grundlicher Durchdenkung auch dem Mindergeubten keine Schwierigkeit machen durfte. —

Anders ist es bei der ublichen Einfuhrung der rationalen Bruche in der Schulmathematik. Hier werden einerseits gewohnlich die zwischen den ganzen Zahlen bestehenden, aber fur die Quotientenbildung unwesentlichen Großenbeziehungen zu fruh ins Spiel gebracht. (Einteilung der positiven Bruche in „echte“ (< 1) und unechte (> 1), Darstellung eines Bruches als „gemischte Zahl“, d. h. Herausziehung des großten Ganzen). Andererseits und hauptsachlich wird viel zu großes Gewicht auf die Tatsache gelegt, daß wegen der eindeutigen Primfaktorzerlegung, also einer ganz speziellen und keineswegs selbstverstandlichen Eigenschaft der ganzen Zahlen, jeder rationale Bruch eine „gekurzte“ Normaldarstellung besitzt. Das fuhrt vor allem bei der Bruchaddition zur Vernachlassigung der einfachen und allgemeinen Formel $\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 \cdot b_2}$ und zum ausschließlichen Arbeiten mit dem „Hauptnenner“, dessen Berechnung die Bildung des „kleinsten gemeinschaftlichen Vielfachen“ von b_1 und b_2, d. h. die Losung einer durchaus nicht trivialen zahlentheoretischen Aufgabe erfordert. — Bei einem beliebigen Ausgangsring $\mathfrak{R}$ bleibt die Bestimmung des Hauptnenners erspart, weil ein solcher keineswegs immer existiert. Die Betrachtung des allgemeinen „abstrakten“ Falles fuhrt also hier zwangslaufig zu dem einfachen und gerade auch fur den Ungeubten empfehlenswerten Aufbau der Bruchrechnung.

§ 3. Polynome in einer Unbestimmten.

Es sei $\mathfrak{K}$ ein beliebiger Korper, x eine Unbestimmte[1]), $\mathfrak{P} = \mathfrak{K}[x]$ bedeute den „Polynomring in x uber $\mathfrak{K}$". d. h. die Menge aller „Polynome"

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \; (n \geqq 0)^2)$$

bei denen die „Beiwerte" (Koeffizienten) a_i dem Korper $\mathfrak{K}$ angehören. Addition, Subtraktion und Multiplikation erfolgen in $\mathfrak{P}$ nach bekanntem Schema:

$$(a_0 + a_1 x + a_2 x^2 + \cdots) \pm (b_0 + b_1 x + b_2 x^2 + \cdots)$$
$$= (a_0 \pm b_0) + (a_1 \pm b_1) x + (a_2 \pm b_2) x^2 + \cdots;$$
$$(a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n) \cdot (b_0 + b_1 x + b_2 x^2 + \cdots$$
$$+ b_m x^m) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0)\, x^2$$
$$+ \cdots + a_n b_m x^{m+n}.$$

Daß $\mathfrak{P}$ ein Ring ist, ist selbstverstandlich; daß $\mathfrak{P}$ keinen Korper darstellt, folgt z. B. aus der Tatsache, daß $x^{-1} = \frac{1}{x}$ nicht zu $\mathfrak{P}$ gehort. Unter dem „Grad" des Polynoms $p(x)$ versteht man den Exponenten der hochsten Potenz von x, die in $p(x)$ „wirklich", d. h. mit einem von 0 verschiedenen

---

[1]) Eine „Unbestimmte" x im Sinne des Textes ist einfach eine Rechenmarke Wesentlich ist, daß x mit den Elementen des Ausgangskorpers $\mathfrak{K}$ durch keine algebraische Beziehung verknupft ist, daß also keine Gleichung $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ mit Beiwerten a_i aus $\mathfrak{K}$ gilt In diesem Sinn sind z B die Zahlen e und π Unbestimmte über dem Körper $\mathfrak{K}_0$ der rationalen Zahlen, — (aber nicht uber dem Korper $\mathfrak{K}_r$ der reellen Zahlen, der ja selbst e und π als Elemente enthalt). Andererseits braucht bei Anwendungen eine Unbestimmte x keineswegs immer als Zahl gedeutet zu werden Sehr haufig wird z B über dem Korper aller reellen oder aller komplexen Zahlen unter x irgend eine Funktion, — etwa $w = \frac{1}{z}$, $w = \sin z$ usw —, zu verstehen sein, und zwar die Funktion im ganzen, nicht der Funktionswert an einer einzelnen Stelle Im ubrigen ist die Moglichkeit derartiger anschaulicher Deutungen von x fur unsere algebraischen Betrachtungen nebensachlich — Man unterscheide scharf zwischen dem Begriff der „Unbestimmten" und dem der (in irgend einer Gleichung auftretenden) „Unbekannten".

[2]) Potenzen mit ganzzahligem Exponenten können in jedem Ring in der aus der Elementarmathematik bekannten Weise gebildet werden. Insonderheit wird stets $a^0 = 1$ gesetzt, auch für $a = 0$.

Beiwert auftritt. Aus dem Multiplikationsschema der Polynome folgt sofort der

Gradsatz. Der Grad des Produktes zweier Polynome ist gleich der Summe der Grade der Faktoren.

Der Gradsatz zeigt insbesondere, daß das Produkt zweier von Null verschiedener Polynome stets selbst von Null verschieden ist. Aus $a(x) \cdot b(x) = a(x) \cdot c(x)$, $a(x) \neq 0$ folgt daher (wegen $a(x) \cdot (b(x) - c(x)) = 0$) stets $b(x) = c(x)$.

Das Polynom $p(x)$ heißt „teilbar" durch das Polynom $q(x)$, wenn der Quotient $\frac{p(x)}{q(x)}$ zu $\mathfrak{P}$ gehört, wenn also eine Gleichung $p(x) = q(x) \cdot r(x)$ gilt. Ist $p(x)$ durch $q(x)$ teilbar, so kann wegen des Gradsatzes der Grad von $p(x)$ nicht kleiner sein als der von $q(x)$; haben $p(x)$ und $q(x)$ den gleichen Grad, so unterscheiden sie sich nur um einen Faktor a aus dem Beiwertkörper $\mathfrak{R}$, und es ist nicht nur $p(x)$ durch $q(x)$, sondern auch $q(x)$ durch $p(x)$ teilbar: $p(x) = a \cdot q(x)$, $q(x) = a^{-1} \cdot p(x)$. Zwei wechselseitig durcheinander teilbare Polynome werden im Folgenden als *„nicht wesentlich verschieden"* angesehen. In jeder Schar wechselseitig durcheinander teilbarer Polynome gibt es ein einziges „normiertes" Polynom, das dadurch ausgezeichnet ist, daß bei ihm die höchste wirklich auftretende x-Potenz den Beiwert 1 besitzt. Gleichzeitig mit $b(x)$ und $c(x)$ ist stets auch $b(x) \cdot c(x)$ normiert. Ist umgekehrt $a(x) = b(x) \cdot c(x)$ eine beliebige Faktorzerlegung des normierten Polynoms $a(x)$, und bedeutet β bzw. γ den Beiwert der höchsten in $b(x)$ bzw. $c(x)$ wirklich auftretenden x-Potenz, so ist $\gamma = \beta^{-1}$, und es wird $a(x) = (\beta^{-1} \cdot b(x)) \cdot (\beta \cdot c(x))$ eine Zerlegung von $a(x)$, bei der die von $b(x)$ bzw. $c(x)$ nicht wesentlich verschiedenen Faktoren $\beta^{-1} \cdot b(x)$ bzw. $\beta \cdot c(x)$ beide normiert sind. Bei einem normierten Polynom braucht man daher nur Zerlegungen in normierte Faktoren zu betrachten. — Die Grundlage für die Teilbarkeitstheorie der Polynome bildet der

Ausdivisionssatz. Zu zwei Polynomen $p(x)$ und $q(x)$ von den Graden m und n ($n \leqq m$) gibt es stets ein eindeutig bestimmtes drittes Polynom $s(x)$, derart, daß der „Rest“ $p(x) - q(x) \cdot s(x) = r(x)$ ein Polynom hochstens $(n-1)$-ten Grades wird.

Die Bestimmung von $s(x)$ (und damit auch von $r(x)$) erfolgt nach dem von der elementaren Buchstabenrechnung her bekannten Divisionsverfahren. Zunachst wahlt man c_0 so, daß in $p(x) - c_0 x^{m-n} \cdot q(x)$ der Beiwert von x^m gleich 0 wird, dann macht man (fur $m - 1 \geqq n$) durch geeignete Wahl von c_1 den Beiwert von x^{m-1} in $(p(x) - c_0 x^{m-n} \cdot q(x)) - c_1 x^{m-n-1} \cdot q(x) = p(x) - (c_0 x^{m-n} + c_1 x^{m-n-1}) \cdot q(x)$ zu Null usw. — Hat ferner sowohl $r_1(x) = p(x) - q(x) \cdot s_1(x)$ als auch $r_2(x) = p(x) - q(x) \cdot s_2(x)$ einen kleineren Grad als n, so ist auch der Grad von $r_1(x) - r_2(x) = q(x)\,(s_2(x) - s_1(x))$ kleiner als der Grad n von $q(x)$, und daraus folgt sofort $r_1(x) - r_2(x) = 0$, $s_1(x) - s_2(x) = 0$.

Offenbar ist $p(x)$ dann und nur dann durch $q(x)$ teilbar, wenn der Rest $r(x)$ gleich Null wird. — Ist aber in der Gleichung $p(x) = q(x) \cdot s(x) + r(x)$ der Rest $r(x)$ von 0 verschieden, und etwa vom Grade $n_1 < n$, so dividiere man $q(x)$ durch $r(x)$ aus, $q(x) = r(x) \cdot s_1(x) + r_1(x)$. Ist ferner $r_1(x)$ von 0 verschieden und vom Grade $n_2 < n_1$, so bilde man zu $r(x)$ und $r_1(x)$ den zugehorigen Rest: $r(x) = r_1(x) \cdot s_2(x) + r_2(x)$. Fur $r_2(x) \neq 0$ bilde man zu $r_1(x)$ und $r_2(x)$ den Rest $r_3(x)$ usw.

Wegen der dauernd abnehmenden Gradzahlen muß die Folge $q(x)$, $r(x)$, $r_1(x)$, $r_2(x)$, ... schließlich abbrechen, d. h. es muß schließlich $r_\sigma(x) = r_{\sigma-2}(x) - r_{\sigma-1}(x) \cdot s_\sigma(x) \neq 0$, $r_{\sigma+1}(x) = r_{\sigma-1}(x) - r_\sigma(x) \cdot s_{\sigma+1}(x) = 0$ werden. Wir behaupten nun: $r_\sigma(x)$ ist ein „größter gemeinschaftlicher Teiler“ (abgekurzt „gr. g. T.“) von $p(x)$ und $q(x)$, d. h.: a) $r_\sigma(x)$ teilt sowohl $p(x)$ als auch $q(x)$, und b) jeder gemeinsame Teiler von $p(x)$ und $q(x)$ teilt $r_\sigma(x)$.

In der Tat, aus $r_\sigma(x) \cdot s_{\sigma+1}(x) = r_{\sigma-1}(x)$ folgt $r_{\sigma-2}(x) = r_{\sigma-1}(x) \cdot s_\sigma(x) + r_\sigma(x) = r_\sigma(x) \cdot (1 + s_\sigma(x) \cdot s_{\sigma+1}(x)) = r_\sigma(x) \cdot a_1(x)$, $r_{\sigma-3}(x) = r_{\sigma-2}(x) \cdot s_{\sigma-1}(x) + r_{\sigma-1}(x) = r_\sigma(x) \cdot (s_{\sigma+1}(x) + s_{\sigma-1}(x) \cdot a_1(x)) = r_\sigma(x) \cdot a_2(x)$ usw.; es ergibt sich also schrittweise die Teilbarkeit von $r_{\sigma-2}(x)$, $r_{\sigma-3}(x), \ldots r_1(x), r(x), q(x), p(x)$ durch $r_\sigma(x)$. — Ist andererseits $p(x) = t(x) \cdot a_1(x)$, $q(x) = t(x) \cdot a_2(x)$, so wird

$$r(x) = t(x) \cdot (a_1(x) - s(x) \cdot a_2(x)) = t(x) \cdot a_3(x),$$
$$r_1(x) = t(x) \cdot (a_2(x) - s_1(x) \cdot a_3(x)) = t(x) \cdot a_4(x), \ldots,$$
$$r_\sigma(x) = t(x) \cdot a_{\sigma+3}(x).$$

$r_\sigma(x)$ besitzt also wirklich die Eigenschaften a) und b). Das Gleichungssystem, das uns zur Konstruktion von $r_\sigma(x)$ diente, zeigt aber noch mehr. Man erhalt der Reihe nach:

$$r(x) = p(x) - q(x) \cdot s(x) = b_0(x) \cdot p(x) + c_0(x) \cdot q(x);$$
$$r_1(x) = q(x) - (b_0(x) \cdot p(x) + c_0(x) \cdot q(x)) \cdot s_1(x)$$
$$= b_1(x) \cdot p(x) + c_1(x) \cdot q(x);\ r_2(x) =$$
$$(b_0(x) \cdot p(x) + c_0(x) \cdot q(x)) - (b_1(x) \cdot p(x) + c_1(x) \cdot q(x)) \cdot s_2(x)$$
$$= b_2(x) \cdot p(x) + c_2(x) \cdot q(x);\ \ldots;\ r_\sigma(x) = b_\sigma(x) \cdot p(x)$$
$$+ c_\sigma(x) \cdot q(x).$$ — Das Endergebnis lautet also:

Zwei beliebige Polynome $p(x)$ und $q(x)$ besitzen stets einen gr. g. T. $R(x)$. Es gilt eine Polynomgleichung $R(x) = B(x) \cdot p(x) + C(x) \cdot q(x)$.

Was die Eindeutigkeitsfrage angeht, so ist klar, daß zwei gr. g. T. $R_1(x)$, $R_2(x)$ von $p(x)$ und $q(x)$ wechselseitig durcheinander teilbar, also nicht wesentlich verschieden sind. In der Gleichung $R(x) = B(x) \cdot p(x) + C(x) \cdot q(x)$ konnen $B(x)$ und $C(x)$ im wesentlichen eindeutig festgelegt werden durch die Forderung, daß der Grad von $B(x)$ bzw. $C(x)$ kleiner sein soll als der Grad von $q(x)$ bzw. $p(x)$; doch gehen wir auf diesen Punkt nicht naher ein. — Zwei Polynome heißen „teilerfremd", wenn ihr gr. g. T. den Grad 0 besitzt, also bei geeigneter Normierung gleich 1 wird. Nach dem Hauptsatz uber den gr. g. T. sind $p(x)$ und $q(x)$ dann und