BIRKHÄUSER

Heinz Lüneburg

Von Zahlen und Größen

Dritthalbtausend Jahre Theorie und Praxis

Band 2

Birkhäuser
Basel · Boston · Berlin

Autor:

Heinz Lüneburg
Fachbereich Mathematik
Technische Universität Kaiserslautern
Erwin-Schrödinger-Straße
D-67663 Kaiserslautern
e-mail: luene@mathematik.uni-kl.de

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

ISBN 3-7643-8778-5 Birkhäuser Verlag, Basel – Boston – Berlin

Gedruckt auf säurefreiem Papier, hergestellt aus chlorfrei gebleichtem Zellstoff. TCF∞
Printed in Germany

ISBN 978-3-7643-8776-1 Band 1
ISBN 978-3-7643-8778-5 Band 2
ISBN 978-3-7643-8780-8 Set Band 1 und 2

e-ISBN 978-3-7643-8777-8
e-ISBN 978-3-7643-8779-2

9 8 7 6 5 4 3 2 1

www.birkhauser.ch

Inhaltsverzeichnis

Inhaltsverzeichnis von Band I

Vorwort - Der rote Faden

I. Größen. 1. Inkommensurabilität, 2. Dedekindsche Schnitte, 3. Proportionenlehre, 4. Rechnen mit Proportionen, 5. Flächeninhalte, 6. Die vierte Proportionale, 7. Ziffer, das Wort und die Sache, 8. Dezimalbrüche, 9. Nepers Logarithmen, 10. Sinustafeln.

II. Zahlen. 1. Die Lehre vom Geraden und Ungeraden, 2. Teilbarkeit, 3. Rationale Größenbereiche, 4. Geometrische Reihen, 5. Buch IX, 6. Zahlen aus Einheiten, 7. Induktion und Rekursion, 8. Nochmals Peano.

III. Das zehnte Buch. 1. Definitionen und allgemeine Sätze, 2. Die Mediale, 3. Existenzaussagen, 4. Summen von irrationalen Strecken, 5. Lineare Unabhängigkeit, 6. Binomiale, 7. Wurzeln aus Binomialen, 8. Algebra in den Elementen, 9. Fibonaccis kubische Gleichung.

IIII. Gleichungen 2., 3. und 4. Grades. 1. Al-Hwarizmi, 2. Quadratische Gleichungen, 3. Die Berechnung von Wurzeln, 4. Nepers Arithmetica localis, 5. Dramatis personae, 6. Wut über eine verspielte Gelegenheit, 7. Kubische Gleichungen, 8. Biquadratische Gleichungen, 9. Briefverkehr.

V. Negative und komplexe Zahlen, Polynome. 1. Nuñez und Bombelli, 2. Polynome und negative Zahlen, 3. Polynome bei Nuñez, 4. Komplexe Zahlen, 5. Polynome bei Bombelli, 6. Das delische Problem, 7. Negative Zahlen.

VI. Nullstellen von Polynomen. 1. Viète und Descartes, 2. Cauchy, Exercices de mathématiques, 3. Polynomringe, 4. Symmetrische Polynome, 5. Potenzsummen, 6. Angeordnete Körper, 7. Der Fundamentalsatz der Algebra, 8. Gaußens zweiter Beweis, 9. Résumée.

Literaturverzeichnis - Index.

VII.

Resultanten

1. Das gaußsche Lemma. Die Mitte des Buches hat viele Verwandlungen durchgemacht. Das lag vor allem daran, dass die Vorlesungstermine schneller aufeinander folgten, als ich lesen konnte. Meine Hörer haben aber, glaube ich, dennoch eine gehaltvolle Vorlesung bekommen. Es lag aber auch daran, dass ich glaubte, dass ich Lagrangens große Arbeit *Réflexions sur la résolution algébrique des équations* von 1770/71 erst im Zusammenhang mit der galoisschen Theorie behandeln müsse. Die Methoden dieser Arbeit, die auf Cramer, Bézout und Euler zurückzugehen scheinen, waren aber den Mathematikern des ganzen 19. Jahrhunderts geläufig und wurden von ihnen meist stillschweigend benutzt, so dass ich Lagrangens Arbeit jetzt schon, dh. im nächsten Kapitel, behandele, zumal einiges davon auch schon im letzten Kapitel zur Sprache kam.

Um die Arbeit von Lagrange verstehen zu können, benötigen wir den Begriff der Resultanten zweier Polynome, ein Begriff, der am Ende des 20. Jahrhunderts nicht mehr zum Allgemeinwissen der Mathematiker gehörte, der durch die Möglichkeiten, die der Rechner bietet, aber wieder aktuell geworden ist. Vieles, was ich in diesem Kapitel vortragen werde, stammt aus zweiter Hand. Die Bibliotheken Kaiserslauterns sind nicht von der Art, dass man in ihnen Bücher von Cramer und Bézout findet. — Man findet in ihnen auch nicht Bettine von Arnims „Goethes Briefwechsel mit einem Kinde.“ — Wir gehen also wieder einmal nicht historisch vor. Was aber vorgetragen wird, dient dem besseren Verständnis dessen, was folgt.

Um die Resultanten sauber definieren und vor allem dann auch einige ihrer Eigenschaften etablieren zu können, stellen wir erst noch einiges über Polynomringe bereit, mit denen die Mathematiker des 18. Jahrhunderts sehr *non-chalent* umgingen, ehe wir dann im nächsten Abschnitt auf die Resultanten zu sprechen kommen. Was wir nun vortragen werden, geht über das hinaus, was wir für die Resultanten benötigen. Es ist aber zum einen für sich gesehen schon von Interesse und wird uns darüber hinaus auch später noch zu Nutze sein.

Wir beginnen damit, den Beweis für den in dieser Allgemeinheit von Weber stammenden Satz vorzutragen, dass Polynomringe über Körpern stets ZPE-Ringe sind (Weber 1893). Dabei werden wir alles so formulieren, wie es in einer heutigen Vorlesung üblich ist, und darüber hinaus noch etwas allgemeiner sein, indem wir zunächst von ggT-Bereichen statt von ZPE-Bereichen reden werden.

Es sei R ein Integritätsbereich. Sind a, b, $d \in R$, so heißt d *größter gemeinsamer Teiler* von a und b, wenn d gemeinsamer Teiler von a und b ist und wenn jeder

gemeinsame Teiler von a und b Teiler von d ist. Haben a und b einen größten gemeinsamen Teiler, so haben sie in aller Regel viele solche, doch unterscheiden sich diese nur um eine Einheit von R, wobei ein Element $a \in R$ *Einheit* heißt, wenn es ein $b \in R$ gibt mit $1 = ab$. Der Integritätsbereich R heißt ggT-*Bereich*, wenn je zwei Elemente von R einen größten gemeinsamen Teiler haben.

Der nächste Satz ist Verallgemeinerung von Dingen, die wir für $\mathbf{N}$ schon in den Elementen bewiesen sahen.

Satz 1. *Ist R ein* ggT-*Bereich, so gilt:*

a) Für alle a, b, $c \in R$ ist $\mathrm{ggT}(ac, bc) = c\,\mathrm{ggT}(a, b)$.

b) Sind a, $b \in R$, ist $(a, b) \neq (0, 0)$ und ist $g := \mathrm{ggT}(a, b)$, so ist

$$\mathrm{ggT}\left(\frac{a}{g}, \frac{b}{g}\right) = 1.$$

c) Sind a, b, $c \in R$ und sind a und b teilerfremd, so ist

$$\mathrm{ggT}(a, bc) = \mathrm{ggT}(a, c).$$

d) Sind a, b, $c \in R$, sind a und b teilerfremd, ist ferner a Teiler von bc, so ist a Teiler von c.

Beweis. a) Das ist sicher richtig für $c = 0$. Es sei also $c \neq 0$. Es ist $c\,\mathrm{ggT}(a, b)$ Teiler von ac wie auch von bc. Also ist $c\,\mathrm{ggT}(a, b)$ Teiler von $g := \mathrm{ggT}(ac, bc)$.

Umgekehrt ist c Teiler von g und $\frac{g}{c}$ ist gemeinsamer Teiler von a und b. Also ist $\frac{g}{c}$ Teiler von $\mathrm{ggT}(a, b)$ und daher g Teiler von $c\,\mathrm{ggT}(a, b)$. Es folgt (bis auf Einheiten) $gc = \mathrm{ggT}(ac, bc)$.

b) Weil a und b nicht beide null sind, ist $g \neq 0$, so dass $\frac{a}{g}$ und $\frac{b}{g}$ eindeutig festliegen. Nach a) ist

$$g\,\mathrm{ggT}\left(\frac{a}{g}, \frac{b}{g}\right) = \mathrm{ggT}(a, b) = g,$$

und folglich, da R ein Integritätsbereich und $g \neq 0$ ist, $\mathrm{ggT}(\frac{a}{g}, \frac{b}{g}) = 1$.

c) Es sei $g := \mathrm{ggT}(a, c)$. Dann ist g gemeinsamer Teiler von a und bc. Es sei t ein weiterer gemeinsamer Teiler von a und bc. Dann ist t auch gemeinsamer Teiler von ac und bc. Nach b) ist

$$\mathrm{ggT}(ac, bc) = c\,\mathrm{ggT}(a, b) = c,$$

so dass t ein gemeinsamer Teiler von a und c und damit von g ist. Folglich ist $\mathrm{ggT}(a, bc) = g = \mathrm{ggT}(a, c)$.

d) Nach c) ist $\mathrm{ggT}(a, bc) = \mathrm{ggT}(a, c)$. Weil a Teiler von bc ist, ist daher

$$a = \mathrm{ggT}(a, bc) = \mathrm{ggT}(a, c),$$

so dass a Teiler von c ist. Damit ist alles bewiesen.

Ist R ein ggT-Bereich, und ist $g = \sum_{i:=0}^{n} a_i x^i \in R[x]$ ein Polynom über R, so nennen wir

$$\mathrm{cont}(g) := \mathrm{ggT}(a_0, \ldots, a_n)$$

Inhalt von g. Das Polynom g heißt *primitiv*, wenn $\mathrm{cont}(g) = 1$ ist.

Satz 2. *Es sei R ein* ggT*-Bereich und $Q(R)$ sei sein Quotientenkörper. Ist $0 \neq f \in Q(R)[x]$, dem Polynomring in der Unbestimmten x über $Q(R)$, so gibt es ein $a \in Q(R)$ und ein primitives $g \in R[x]$ mit $f = ag$. Ist $b \in Q(R)$ und $h \in R[x]$, ist h primitiv und gilt $f = bh$, so gibt es eine Einheit $u \in R$ mit $g = uh$.*

Beweis. Die Existenz der Zerlegung $f = ag$ ist banal. Es sei also $ag = f = bh$ mit primitiven Polynomen g und h und a, $b \in Q(R)$. Es gibt dann α, β, γ, $\delta \in R$ mit $a = \frac{\alpha}{\beta}$ und $b = \frac{\gamma}{\delta}$. Es folgt

$$\alpha\delta g = \beta\delta ag = \beta\delta bh = \beta\gamma h.$$

Weil g und h primitiv sind, folgt mit Satz 1 a)

$$\alpha\delta = \alpha\delta\mathrm{cont}(g) = \mathrm{cont}(\alpha\delta g) = \mathrm{cont}(\beta\gamma h) = \beta\gamma\mathrm{cont}(h) = \beta\gamma v$$

mit einer Einheit v. Letzteres, weil der ggT irgendwelcher Elemente nur bis auf Einheiten bestimmt ist. Hieraus folgt $a = bv$ und mit $u := v^{-1}$ dann

$$ag = f = bh = auh$$

und weiter $g = uh$. Damit ist der Satz bewiesen.

Gauß hat das nach ihm benannte Lemma nur für Polynome über dem Ring der ganzen Zahlen formuliert und bewiesen (Gauß 1801, art. 42. Was seine Formulierung dieses Lemmas anbelangt, siehe die Bemerkung vor Satz 3 weiter unten). Kronecker verallgemeinerte es dann in der Kummerfestschrift auf Polynomringe in mehreren Unbestimmten über Rationalitätsbereichen und Weber schließlich auf Polynomringe über beliebigen Körpern (Weber 1893, S. 532). Wir gehen noch ein Stück weiter und beweisen die folgende Form des gaußschen Lemmas.

Gaußsches Lemma. *Ist R ein* ggT*-Bereich und sind f und g primitive Polynome über R, so ist auch fg primitiv.*

Beweis. Es sei $f = \sum_{i:=0}^{m} f_i x^i$ und $g = \sum_{i:=0}^{n} g_i x^i$. Ferner sei t ein gemeinsamer Teiler der Koeffizienten von fg, der keine Einheit sein möge. Es gibt dann ein $i \in \{0, \ldots, m\}$ mit

$$\mathrm{ggT}(f_0, \ldots, f_{i-1}, t) \neq 1 = \mathrm{ggT}(f_0, \ldots, f_i, t),$$

wobei der ggT links im Falle $i = 0$ als t zu interpretieren ist. Es sei

$$u := \mathrm{ggT}(f_0, \ldots, f_{i-1}, t).$$

Dann ist u keine Einheit. Es gibt daher ein $j \in \{0, \dots, n\}$ mit

$$\mathrm{ggT}(g_0, \dots, g_{j-1}, u) \neq 1 = \mathrm{ggT}(g_0, \dots, g_j, u),$$

wobei der Fall $j = 0$ dem Fall $i = 0$ analog zu interpretieren ist. Es sei

$$v := \mathrm{ggT}(g_0, \dots, g_{j-1}, u).$$

Dann ist auch v keine Einheit. Weil v Teiler von u und u Teiler von t ist, ist v gemeinsamer Teiler der Koeffizienten von fg. Nun ist

$$(fg)_{i+j} = \sum_{k:=0}^{i+j} f_k g_{i+j-k}.$$

Nach Konstruktion ist v Teiler von $f_0, \dots, f_{i-1}, g_{j-1}, \dots, g_0$. Hiermit und mit der vorstehenden Gleichung folgt

$$f_i g_j \equiv (fg)_{i+j} \equiv 0 \bmod v.$$

Also ist v Teiler von $f_i g_j$. Nun ist

$$v = \mathrm{ggT}(g_0, \dots, g_{j-1}, u)$$

und daher

$$1 = \mathrm{ggT}(g_0, \dots, g_j, u) = \mathrm{ggT}(v, g_j).$$

Mit Satz 1 d) folgt daher, dass v Teiler von f_i ist. Daher ist v ein gemeinsamer Teiler von $f_0, \dots, f_{i-1}, f_i, u$ und somit von

$$\mathrm{ggT}(f_0, \dots, f_i, u) = 1.$$

Dies widerspricht aber der Tatsache, dass v keine Einheit ist. Also ist fg doch, wie behauptet, primitiv.

Das gaußsche Lemma ist ein überaus nützliches Werkzeug, wie schon die Beweise der nächsten Sätze zeigen. Satz 3 ist im Übrigen das, was Gauß in den Disquisitiones, art. 42, für den Fall $R = \mathbf{Z}$ zeigt und was er in etwa so formuliert (er schreibt Latein): Sind g und h Polynome mit Leitkoeffizient 1 und sind nicht alle Koeffizienten von g und h ganz, so sind auch nicht alle Koeffizienten von gh ganz. Was wir heute gaußsches Lemma nennen, entstammt der Analyse des gaußschen Beweises des gerade formulierten Satzes.

Satz 3. *Ist R ein* ggT*-Bereich und hat $f \in \mathbf{R}[x]$ den Leitkoeffizienten* 1*, ist ferner $g \in Q(R)[x]$ ein Teiler von f und hat auch g den Leitkoeffizienten* 1*, so ist $g \in R[x]$.*

Beweis. Es sei $f = gh$ mit $h \in Q(R)[x]$. Nach Satz 2 gibt es $a, b \in Q(R)$ und primitive Polynome $G, H \in R[x]$ mit $g = aG$ und $h = bH$. Es folgt $f = gh =$

$abGH$. Nach dem gaußschen Lemma ist GH primitiv. Weil auch f primitiv ist, gibt es nach Satz 2 eine Einheit u in R mit $f = uGH$. Es sei γ der Leitkoeffizient von G und δ der von H. Dann ist $u\gamma\delta$ der von f, so dass $u\gamma\delta = 1$ ist. Folglich sind auch γ und δ Einheiten in R. Nun ist aber $a\gamma$ der Leitkoeffizient von $aG = g$, so dass $a\gamma = 1$ ist, da ja der Leitkoeffizient von g nach Voraussetzung gleich 1 ist. Es folgt $a = \gamma^{-1} \in R$, so dass $g = aG \in R[x]$ ist. Damit ist der Satz bewiesen.

Hier drei Begriffe, die wir im Folgenden brauchen.

Es sei R ein Integritätsbereich. Wir nennen $a \in R$ *reduzibel* oder auch *zerlegbar*, wenn es b, $c \in R$ gibt, wobei weder b noch c Einheit ist, so dass $a = bc$ gilt. Ist a weder Einheit noch reduzibel, so heißt a *irreduzibel* oder auch *unzerlegbar*. Das Element $p \in R$ heißt *Primelement*, falls es keine Einheit ist und falls für alle a, $b \in R$ aus der Eigenschaft, dass p Teiler von ab ist, folgt, dass p Teiler von a oder von b ist. Primelemente sind stets irreduzibel. Die Umkehrung gilt nicht. Ein Integritätsbereich R heißt *ZPE-Bereich*, wenn jedes von null verschiedene Element von R, welches auch keine Einheit ist, Produkt von Primelementen ist. Ist dies der Fall, so ist die Zerlegung auch im Wesentlichen eindeutig, was besagt, dass aus

$$\prod_{i:=1}^{m} p_i = \prod_{j:=1}^{n} q_j$$

mit Primelementen p_i und q_j folgt, dass $m = n$ ist und dass es Einheiten $e_1, \ldots, e_m$ und eine Permutation $\sigma \in S_m$ gibt mit

$$p_i = e_i q_{\sigma(i)}$$

für $i := 1, \ldots, m$. Daher der Name ZPE, das ist, die Zerlegung in Primelemente ist möglich und dann auch eindeutig. Die Eindeutigkeit der Zerlegung zu beweisen, sei dem Leser als Übungsaufgabe überlassen.

Satz 4. *Es sei R ein* ggT*-Bereich. Ist $f \in R[x]$ primitiv, so ist f genau dann in $R[x]$ irreduzibel, wenn f in $Q(R)[x]$ irreduzibel ist.*

Beweis. Ist f in $R[x]$ reduzibel, so auch in $Q(R)[x]$. Es gibt dann nämlich g, $h \in R[x]$, die keine Einheiten sind, mit $f = gh$. Es kann nicht $g \in R$ gelten, da sonst g ein gemeinsamer Teiler der Koeffizienten von f wäre. Weil f primitiv ist, wäre g dann eine Einheit von R, was nicht der Fall ist. Ebenso gilt, dass auch h nicht in R liegt. Also haben g und h positiven Grad, so dass $f = gh$ auch eine nicht triviale Zerlegung von f in $Q(R)[x]$ ist.

Es sei umgekehrt $f = gh$ mit g, $h \in Q(R)[x]$ und g und h mögen positiven Grad haben. Nach Satz 2 gibt es a, $b \in Q(R)$ und primitive G, $H \in R[x]$ mit $g = aG$ und $h = bH$. Es folgt $f = abGH$. Nach dem gaußschen Lemma ist GH primitiv. Weil auch f primitiv ist, folgt mit Satz 2, dass ab eine Einheit in R ist. Also ist $f = (abG)H$ eine Zerlegung von f in $R[x]$, die wegen

$$\mathrm{Grad}(abG) = \mathrm{Grad}(G) = \mathrm{Grad}(g)$$

nicht trivial ist. Damit ist alles bewiesen.

Der gerade bewiesene Satz erhält daher seine Bedeutung, dass arithmetische Eigenschaften von R es immer wieder einmal gestatten zu zeigen, dass ein primitives Polynom in $R[x]$ irreduzibel ist. Dann ist dieses Polynom und alle seine assoziierten in $Q(R)[x]$ irreduzibel. Typisch für diese Situation ist das folgende Irreduzibilitätskriterium, welches Schönemann für den Ring der ganzen Zahlen bewies (Schönemann 1846). Dieses Kriterium wird in der Literatur durchweg „Eisensteinkriterium“ genannt. Es wurde in der Tat von Eisenstein auch für den ZPE-Bereich der ganzen gaußschen Zahlen formuliert und bewiesen (Eisenstein 1850). Eisenstein und die Namengeber haben offensichtlich die schönemannsche Arbeit nicht oder nicht sehr sorgfältig gelesen. Eisenstein jedenfalls sagt, er hätte bislang nur Beweise von Gauß und Kronecker dafür gesehen, dass das p-te Kreisteilungspolynom im Falle, dass p eine Primzahl ist, irreduzibel sei. Doch auch Schönemann benutzt das Kriterium, um die Irreduzibilität des p-ten Kreisteilungspolynoms zu beweisen. Die eisensteinsche Aussage nimmt Schönemann zum Anlass, in Band 40 des Journals für die reine und angewandte Mathematik (1850, S. 188.) darauf hinzuweisen, dass er im Wesentlichen das gleiche Kriterium wie Eisenstein bewiesen und wie jener zum Beweise der Irreduzibilität des p-ten Kreisteilungspolynoms benutzt hätte. Es ist also Schönemann, dem die Priorität gebührt.

Ich glaubte lange Zeit, dass diese Fehlzuordnung im Umkreis von Emmy Noether, Artin, van der Waerden entstanden sei, da ich sie in van der Waerdens „Algebra“ fand. Doch beim Durchblättern von Landaus Werken Bd. I fand ich eine Arbeit (Werke I, S. 360–364), wo Landau das fragliche Kriterium Eisenstein zuschreibt. Die Fehlzuordnung ist also älter. Interessant ist jedoch Folgendes. Bei der Herausgabe der Werke Landaus hat Wefelscheid auch Sonderdrucke aus Landaus Besitz benutzt und handschriftliche Notizen Landaus in ihnen mit in die Werke aufgenommen. Die Randnotiz hier nun lautet: „Schoenemann vor Eisenstein“. Landau hat den Fehler also bemerkt, wenn auch zu spät für die Publikation.

In D. Knuth, The Art of Computer Programming. Vol II, 2. Auflage, Reading/Mass. etc. 1981 findet sich auf S. 438 ebenfalls der Name Eisensteinkriterium. Da Knuth dem Erstentdecker eines Fehlers 2 Dollar versprach, schrieb ich ihm im Jahr 1982 einen Brief des Inhalts, dass Schönemann der Entdecker des Irreduzibilitätskriteriums sei in der Hoffnung, die 2 Dollar kassieren zu können. Ich hörte nichts von ihm und vergaß das Ganze. Im Sommer des Jahres 1996 jedoch bekam ich einen Brief von Knuth. In diesem Brief fand sich neben meinem Brief von 1982 ein Schreiben von Knuth mit dem Warum-so-spät und einen Scheck über 5$ 96c. Die Prämie war von 2 auf 3 Dollar erhöht worden. Hinzu kamen noch Zinsen.

Schönemannsches Irreduzibilitätskriterium. *Es sei R ein* ggT*-Bereich und $f := \sum_{i:=0}^{n} f_i x^i$ sei ein primitives Polynom aus $R[x]$. Ferner gelte*

$$k := \mathrm{ggT}(f_{n-1}, f_{n-2}, \ldots, f_0) \neq 1.$$

Gibt es ein von 0 *verschiedenes* s *in* R*, das auch keine Einheit ist, mit den Eigenschaften:*

a) s *teilt* k*,*

b) Ist t *Teiler von* s *und* t^2 *Teiler von* f_0*, so ist* t *Einheit in* R*,*

dann ist f *irreduzibel in* $R[x]$ *und folglich in* $Q(R)[x]$*.*

Beweis. Es sei $f = gh$ mit $g,\ h \in R[x]$. Ferner sei $g = \sum_{i:=0}^{a} g_i x^i$ und $h = \sum_{i:=0}^{b} h_i x^i$. Ist $\alpha := \mathrm{cont}(g)$ und $\beta := \mathrm{cont}(h)$, so ist $\alpha\beta$ gemeinsamer Teiler aller f_i. Weil f primitiv ist, ist also $\alpha\beta$ eine Einheit, so dass g und h primitiv sind.

Nach Voraussetzung teilt s den größten gemeinsamen Teiler k von $f_0, \ldots, f_{n-1}$. Insbesondere ist s also Teiler von $f_0 = g_0 h_0$. Weil s keine Einheit ist, kann nach Satz 1 c) nicht gleichzeitig $\mathrm{ggT}(s, g_0) = 1$ und $\mathrm{ggT}(s, h_0)$ gelten. Wir dürfen annehmen, dass $p := \mathrm{ggT}(s, g_0) \neq 1$ ist. Es sei ferner $t := \mathrm{ggT}(p, h_0)$. Dann ist t Teiler von p und damit von s. Ferner ist t auch Teiler von g_0 und von h_0. Also ist t^2 Teiler von $g_0 h_0 = f_0$. Auf Grund unserer Voraussetzung ist t also Einheit in R. Es gibt nun, da p Teiler von g_0 ist, der keine Einheit ist, und da g außerdem primitiv ist, ein i mit $1 \leq i \leq a$ und

$$q := \mathrm{ggT}(g_0, \ldots, g_{i-1}, p) \neq 1 = \mathrm{ggT}(g_0, \ldots, g_i, p).$$

Dann ist also q keine Einheit und es ist

$$f_i = \sum_{j:=0}^{i} g_j h_{i-j} \equiv g_i h_0 \bmod q.$$

Weil p und h_0 teilerfremd sind, sind auch q und h_0 teilerfremd. Also ist

$$\mathrm{ggT}(g_i h_0, q) = \mathrm{ggT}(g_i, q) = \mathrm{ggT}(g_0, \ldots, g_{i-1}, g_i, p) = 1.$$

Somit ist f_i zu q teilerfremd. Nun ist aber q Teiler von p und p ist Teiler von s und s ist Teiler von k. Daher ist q Teiler von $f_0, \ldots, f_{n-1}$. Weil q keine Einheit ist, ist daher $i = n$, so dass $n \leq a$ gilt. Somit ist $\mathrm{Grad}(f) = \mathrm{Grad}(g)$, so dass f irreduzibel ist. Mit Satz 4 folgt schließlich, dass f auch in $Q(R)$ irreduzibel ist.

Schönemanns Irreduzibilitätskriterium wird üblicherweise in der folgenden, sehr viel handlicheren Fassung formuliert.

Korollar. *Es sei* R *ein* ZPE*-Bereich und* $f := \sum_{i:=0}^{n} f_i x^i$ *sei ein primitives Polynom aus* $R[x]$*. Ist* p *ein Primelement von* R *und gilt* $f_i \equiv 0 \bmod p$ *für* $i := 0, \ldots, n-1$ *und* $f_0 \not\equiv 0 \bmod p^2$*, so ist* f *irreduzibel in* $R[x]$ *und dann auch in* $Q(R)[x]$*.*

Dies folgt sofort mit $s = p$ aus dem schönemannschen Irreduzibilitätskriterium.

Ist p eine Primzahl und a eine ganze Zahl, die nicht durch p teilbar ist, so ist $x^n - pa$ für alle natürlichen Zahlen n irreduzibel über $\mathbf{Q}$. Dies folgt unmittelbar

aus dem Korollar. Damit ist gezeigt, dass es über **Q** irreduzible Polynome jeglichen Grades gibt.

Gauß bewies in seinen Disquisitiones (art. 341), dass das p-te Kreisteilungspolynom Φ_p irreduzibel ist, falls p eine Primzahl ist. Hierzu benötigte er, was er in art. 42 bewiesen hatte, dass eine Zerlegung von Φ_p über **Q** mit Polynomen deren Leitkoeffizient 1 ist, bereits eine Zerlegung über **Z** ist. Dass alle Kreisteilungspolynome irreduzibel sind, ist erst Kronecker gelungen zu zeigen (Kronecker 1854). Ist p eine Primzahl, so ist $f := \sum_{i:=0}^{p-1} x^i$ das p-te Kreisteilungspolynom. Der folgende Beweis für seine Irreduzibilität stammt von Schönemann (1846). Es ist der oben erwähnte.

Es ist $f = \frac{x^p-1}{x-1}$. Ersetzt man hierin x durch $y+1$, so folgt

$$f(y+1) = \frac{1}{y}\left(-1 + \sum_{i:=0}^{p} \binom{p}{i} y^i\right) = \sum_{i:=1}^{p} \binom{p}{i} y^{i-1}.$$

Nun ist $\binom{p}{i}$ für $i := 1, \ldots, p-1$ durch p teilbar, da p eine Primzahl ist. Ferner ist $\binom{p}{p} = 1$, so dass das Polynom $f(y+1)$ primitiv ist. Schließlich ist $\binom{p}{1} = p$ nicht durch p^2 teilbar. Daher ist $f(y+1)$ und damit f irreduzibel.

Der nächste Satz erweitert unseren Vorrat an ggT-Bereichen. Bislang kennen wir ja nur **Z** und die Polynomringe in einer Unbestimmten über einem Körper als solche. Über diese werden wir aber in Satz 7 noch mehr aussagen.

Satz 5. *Ist R ein* ggT*-Bereich, so ist auch der Polynomring $R[x]$ in der Unbestimmten x über R ein* ggT*-Bereich.*

Beweis. Es seien f, $g \in R[x]$ und f und g seien primitiv. Weil $Q(R)[x]$ ein euklidischer Ring ist, haben f und g in $Q(R)[x]$ einen größten gemeinsamen Teiler, den wir μ nennen. Es gibt dann a, $b \in Q(R)[x]$ mit $f = a\mu$ und $g = b\mu$. Es gibt dann weiter α, β, $\gamma \in Q(R)$ und primitive A, B, $M \in R[x]$ mit $a = \alpha A$, $b = \beta B$ und $\mu = \gamma M$. Es folgt $f = \alpha\gamma AM$ und $g = \beta\gamma BM$. Nach dem gaußschen Lemma sind AM und BM primitiv, so dass $\alpha\gamma$ und $\beta\gamma$ nach Satz 2 Einheiten von R sind, da f und g ja primitiv sind. Es folgt, dass M ein gemeinsamer Teiler von f und g in $R[x]$ ist. Es sei d ein gemeinsamer Teiler von f und g in $R[x]$. Dann ist d insbesondere primitiv. Ferner ist d in $Q(R)[x]$ Teiler von μ. Es sei $\mu = d\nu$ mit $\nu \in Q(R)[x]$. Es gibt dann ein $\delta \in Q(R)$ und ein primitives $N \in R[x]$ mit $\nu = \delta N$. Es folgt $\gamma M = \delta dN$. Nach dem gaußschen Lemma ist dN primitiv, so dass es nach Satz 2 eine Einheit u in R gibt mit $M = udN$. Folglich ist d Teiler von M, so dass M größter gemeinsamer Teiler von f und g ist.

Es seien nun f, $g \in R[x]$ beliebig. Ist $f = 0$, so ist $\mathrm{ggT}(f, g) = g$. Entsprechend ist $\mathrm{ggT}(f, g) = f$, wenn $g = 0$ ist. Es seien also f und g beide von null verschieden. Ferner sei $\alpha := \mathrm{cont}(f)$ und $\beta := \mathrm{cont}(g)$. Weiter sei $f = \alpha F$ und $g = \beta G$. Dann sind F und G primitive Polynome und haben nach dem schon Bewiesenen einen größten gemeinsamen Teiler D in $R[x]$. Es sei ferner $\delta := \mathrm{ggT}(\alpha, \beta)$. Dann ist δD ein gemeinsamer Teiler von f und g. Wir zeigen, dass δD ein größter gemeinsamer Teiler von f und g ist.

Es sei h ein gemeinsamer Teiler von f und g. Ferner sei $\epsilon := \mathrm{cont}(h)$. Dann ist ϵ gemeinsamer Teiler aller Koeffizienten von f und damit Teiler von α. Entsprechend folgt, dass ϵ Teiler von β ist. Also ist ϵ Teiler von δ. Es sei ferner $f = ah$ und $a = \eta A$. Es folgt $\alpha F = \eta\epsilon AH$. Weil F und AH primitiv sind, gibt es eine Einheit u in R mit $F = uAH$, so dass H Teiler von F ist. Ebensoa folgt, dass H Teiler von G ist. Also ist H Teiler von D. Dann ist aber $h = \epsilon H$ Teiler von δD, so dass δD größter gemeinsamer Teiler von f und g ist. Damit ist $R[x]$ als ggT-Bereich erkannt.

Wir haben mehr bewiesen als in Satz 5 formuliert. Da dieses Mehr für die Rechenpraxis von Bedeutung ist, formulieren wir es als eigenen Satz.

Satz 6. *Es sei R ein* ggT*-Bereich. Ferner seien f, $g \in R[x]$ und es gelte f, $g \neq 0$. Ist $\alpha := \mathrm{cont}(f)$ und $\beta := \mathrm{cont}(g)$, ist ferner $f = \alpha F$ und $g = \beta G$, so ist*

$$\mathrm{ggT}(f, g) = \mathrm{ggT}(\alpha, \beta)\mathrm{ggT}(F, G).$$

Überdies ist $\mathrm{ggT}(F, G)$ *primitiv.*

Man kann noch mehr in dieser Richtung beweisen. Nämlich

Satz 7. *Ist R ein* ZPE*-Bereich, so ist auch der Polynomring $R[x]$ in der Unbestimmten x über R ein* ZPE*-Bereich.*

Beweis. Es sei p ein Primelement von R. Ferner seien f, $g \in R[x]$ und p teile fg. Dann teilt p alle Koeffizienten von fg. Wir müssen zeigen, dass p Teiler von f oder Teiler von g ist. Es sei p kein Teiler von f. Es gibt dann ein i, so dass die Koeffizienten $f_0, \ldots, f_{i-1}$ von f durch p teilbar sind, f_i aber nicht. Dann ist

$$f_i g_0 \equiv \sum_{j:=0}^{i} f_j g_{i-j} = (fg)_i \equiv 0 \bmod p.$$

Es folgt, dass p Teiler von g_0 ist. Es sei $k > 0$ und p teile $g_0, \ldots, g_{k-1}$. Dann ist

$$f_i g_k \equiv \sum_{j:=0}^{i+k} f_j g_{i+k-j} = (fg)_{i+k} \equiv 0 \bmod p.$$

Es folgt $g_k \equiv 0 \bmod p$, so dass g durch p teilbar ist. Somit ist p auch Primelement in $R[x]$.

Es sei nun $f \in R[x]$ beliebig. Dann ist $f = \mathrm{cont}(f)F$ mit einem primitiven Polynom F. Weil R ein ZPE-Bereich ist, ist $\mathrm{cont}(f)$ Produkt von Primelementen in R und damit von Primelementen in $R[x]$, weil die Primelemente von R in $R[x]$ ja prim bleiben, wie gerade gesehen. Das primitive Polynom F ist Produkt von endlich vielen in $R[x]$ irreduziblen Polynomen, da der Grad eines echten Faktors eines primitiven Polynoms ja kleiner ist, als der Grad des gegebenen Polynoms. Es ist also nur noch zu zeigen, dass ein irreduzibles Polynom prim ist. Dazu beachte man zunächst, dass $R[x]$ nach Satz 6 ein ggT-Bereich ist. Es sei f ein irreduzibles

Polynom und dieses Polynom teile das Produkt gh. Ist f kein Teiler von g, so ist $\mathrm{ggT}(f,g)=1$. Dann teilt f aber nach Satz 1 d) das Polynom h. Folglich ist f ein Primpolynom. Damit ist der Satz bewiesen.

Der Nachweis innerhalb des Beweises von Satz 7, dass irreduzible Polynome aus $R[x]$ prim sind, wenn R ein ggT-Bereich ist, liefert auch noch das allgemeinere

Korollar 0. *Ist R ein* ggT*-Bereich und ist $u \in R$ irreduzibel, so ist u ein Primelement von R.*

Das folgende Korollar 1 steht für endliches X, wie schon erwähnt, bei Weber 1893.

Korollar 1. *Ist K ein kommutativer Körper, so ist der Polynomring $K[X]$ in den Unbestimmten aus X ein* ZPE*-Bereich.*

Beweis. Für endliche X folgt dies mittels Induktion aus Satz 7. Es sei also X beliebig. Sind f, $g \in K[x]$, so kommen in f und g nur endlich viele x_1, …, $x_n \in X$ vor. In $K[x_1,\dots,x_n]$ haben f und g einen größten gemeinsamen Teiler d. Es sei u ein gemeinsamer Teiler von f und g in $K[X]$. Weil K als Körper nullteilerfrei ist, kann kein $y \in X - \{x_1,\dots,x_n\}$ in u vorkommen, es sei denn, f und g sind beide null. Dann ist aber auch $d=0$ und u Teiler von d. Im anderen Falle ist also $u \in K[x_1,\dots,x_n]$ und folglich auch hier Teiler von d. Also ist d größter gemeinsamer Teiler von f und g in $K[X]$, so dass $K[X]$ ein ggT-Bereich ist. Der gleiche Schluss, der zeigte, dass $d \in K[x_1,\dots,x_n]$ ist, zeigt, dass jeder Teiler eines von null verschiedenen Polynoms in $K[x_1,\dots,x_n]$ liegt, wenn x_1, …, x_n die Unbestimmten sind, die in dem gegebenen Polynom vorkommen. Also ist jedes Polynom in $K[X]$ Produkt von irreduziblen Polynomen. Da $K[X]$ ein ggT-Bereich ist, sind diese aber allesamt Primpolynome nach Korollar 0. Damit ist Korollar 1 bewiesen.

Ebenso folgt (Kronecker?)

Korollar 2. *Der Polynomring $\mathbf{Z}[x_1,\dots,x_n]$ in den Unbestimmten x_1, …, x_n über $\mathbf{Z}$ ist ein* ZPE*-Bereich.*

Die Aussagen über ggT-Bereiche gehören wohl, so denke ich, zur mathematischen Folklore. Ich habe mir keine Mühe gegeben, sie in der Literatur aufzuspüren. Die Aussage des Korollars 0 fiel mir im April 1997 auf, als ich nach einem Beweis für Satz 7 suchte, der ihn auf Satz 5 zurückführt, aber nicht vom Auswahlaxiom Gebrauch macht, das ich bei früherer Gelegenheit an dieser Stelle benutzte. Nichts von dem, was wir bislang in diesem Buche machten, benötigt das Auswahlaxiom.

2. Resultanten. Über die Ursprünge der Resultanten habe ich nur Vermutungen. Sie haben zu tun mit der Elimination einer Unbestimmten aus zwei algebraischen Gleichungen und drängen sich daher auf im Zusammenhang mit Bézouts Satz, dass zwei ebene algebraische Kurven der Grade m und n höchstens mn Schnittpunkte haben. Geschrieben hätten über dieses Thema G. Cramer in seinem Buch *Introduction à l'analyse des lignes courbes*, Bézout in den *Mémoires de l'Académie des*

Sciences de Paris vom Jahre 1764 und auch Euler in den *Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin* der Jahre 1748 und 1764, so Lagrange in Lagrange 1771, S. 141, wo er selbst auch über diesen Gegenstand schreibt. Die beiden eulerschen Arbeiten fand ich in Eulers „Gesammelten Werken", die beiden anderen habe ich nicht in der Hand gehabt.

Den ersten Satz entnehme ich van der Waerden 1955, S. 94. Bei ihm hat Euler Pate gestanden, wie aus van der Waerdens Text (S. 95) hervorgeht. Ein Zitat gibt er nicht. Es muss die Arbeit Euler 1764 gewesen sein, die ihn inspirierte. Darauf werden wir gleich zurückkommen. Dieser Satz und der Hinweis auf Euler findet sich auch schon in van der Waerden 1931, S. 2 und 1937, S. 88.

Satz 1. *Es sei R ein* ggT*-Bereich und f und g seien zwei von* 0 *verschiedene Polynome in der Unbestimmten x über R. Genau dann haben f und g einen gemeinsamen Faktor positiven Grades, wenn es von null verschiedene Polynome γ, $\varphi \in R[x]$ gibt mit* $\operatorname{Grad}(\varphi) < \operatorname{Grad}(f)$ *und* $\operatorname{Grad}(\gamma) < \operatorname{Grad}(g)$*, so dass $\gamma f = \varphi g$ gilt.*

Beweis. Es sei δ ein gemeinsamer Faktor positiven Grades. Es gibt dann φ, $\gamma \in R[x]$ mit $f = \delta\varphi$ und $g = \delta\gamma$. Es folgt $\gamma f = \gamma\delta\varphi = \varphi\delta\gamma = \varphi g$. Weil δ positiven Grad hat, ist der Grad von φ kleiner als der Grad von f und der Grad von γ ist kleiner als der Grad von g.

Es gelte umgekehrt die Gleichung $\gamma f = \varphi g$ mit den entsprechenden Nebenbedingungen. Weil R ein ggT-Bereich ist, ist dies auch $R[x]$ nach Satz 5 von Abschnitt 1. Es folgt

$$\gamma \frac{f}{\operatorname{ggT}(f,\varphi)} = \frac{\varphi}{\operatorname{ggT}(f,\varphi)} g.$$

Weil $\frac{f}{\operatorname{ggT}(f,\varphi)}$ und $\frac{\varphi}{\operatorname{ggT}(f,\varphi)}$ nach Satz 1 b) von Abschnitt 1 teilerfremd sind, folgt mit Satz 1 d) von Abschnitt 1, dass $\frac{f}{\operatorname{ggT}(f,\varphi)}$ Teiler von g ist. Weil der Grad von φ kleiner als der Grad von f ist, ist $\frac{f}{\operatorname{ggT}(f,\varphi)}$ ein Polynom positiven Grades. Damit ist alles bewiesen.

Euler nimmt bei seinen Untersuchungen an, dass f und g eine gemeinsame Nullstelle haben. Dann haben f und g einen gemeinsamen Linearfaktor, mit dem er dann weiter schließt, wobei die Linearität keine wesentliche Rolle spielt.

Es sei

$$f = \sum_{i:=0}^{m} a_i x^{m-i}, \quad g = \sum_{i:=0}^{n} b_i x^{n-i}, \quad \varphi = \sum_{i:=0}^{m-1} c_i x^{m-1-i}, \quad -\gamma = \sum_{i:=0}^{n-1} d_i x^{n-1-i}.$$

Gesucht sind nun notwendige und hinreichende Bedingungen an die Koeffizienten von f und g, so dass man c und d so finden kann, dass $\gamma f + \varphi g = 0$ ist. Die Polynome γf und φg haben jeweils $m + n - 1 + 1 = m + n$ Koeffizienten. Ausmultiplizieren der Polynome führt daher auf das folgende System von $m + n$ homogenen linearen

Gleichungen für die $m+n$ Koeffizienten der gesuchten Polynome.

$$\begin{array}{lllllll}
0 = d_0a_0 & & & + c_0b_0 & & & \\
0 = d_0a_1 + d_1a_0 & & & + c_0b_1 + c_1b_0 & & & \\
0 = d_0a_2 + d_1a_1 & + d_2a_0 & & + c_0b_2 + c_1b_1 & + c_2b_0 & & \\
 & \vdots & & \vdots & & & \\
0 = & d_{n-2}a_m + d_{n-1}a_{m-1} + & & & c_{m-2}b_n + c_{m-1}b_{n-1} & & \\
0 = & d_{n-1}a_m + & & & c_{m-1}b_n & &
\end{array}$$

Es gibt also genau dann zwei Polynome γ und φ der verlangten Art, wenn dieses Gleichungssystem eine nicht triviale Lösung hat, also genau dann, wenn die Determinante des Gleichungssystems 0 ist.

Die folgende $((m+n)\times(m+n))$-Matrix

$$\begin{pmatrix}
a_0 & a_1 & \dots & \dots & \dots & a_m & & \\
 & a_0 & a_1 & \dots & \dots & \dots & & \\
 & & \dots & \dots & \dots & \dots & \dots & \\
 & & & a_0 & a_1 & \dots & \dots & a_m \\
b_0 & b_1 & \dots & \dots & b_n & & & \\
 & b_0 & b_1 & \dots & \dots & \dots & & \\
 & & \dots & \dots & \dots & \dots & \dots & \\
 & & & b_0 & b_1 & \dots & \dots & b_n
\end{pmatrix}$$

ist die Transponierte der Koeffizientenmatrix dieses Gleichungssystems. Die erste Zeile dieser Matrix besteht aus den Koeffizienten des Polynomes f gefolgt von $n-1$ Nullen. Die nächsten $n-1$ Zeilen der Matrix entstehen aus der ersten durch zyklische Vertauschung der Koeffizienten der ersten Zeile. Die $(n+1)$-ste Zeile besteht aus den Koeffizienten des Polynoms g gefolgt von $m-1$ Nullen. Die restlichen $m-1$ Zeilen entstehen durch zyklische Vertauschung der Koeffizienten der $(n+1)$-sten Zeile. Diese Matrix wird *Sylvestermatrix* genannt. Sie findet sich, wohl zum ersten Male, in Sylvester 1840. Ihre Determinante heißt *Resultante* der Polynome f und g. Wir bezeichnen sie mit $\mathrm{Res}(f,g)$. Da das Vertauschen zweier Zeilen einer Matrix das Vorzeichen ihrer Determinante ändert, gilt

$$\mathrm{Res}(g,f) = (-1)^{mn}\mathrm{Res}(f,g).$$

Da die Determinante sich beim Transponieren nicht ändert, gilt, wie gesehen, der folgende Satz.

Satz 2. *Es sei R ein* ggT*-Bereich und $f = \sum_{i:=0}^{m} a_i x^{m-i}$ und $g = \sum_{i:=0}^{n} b_i x^{n-i}$ seien zwei Polynome vom Grade m bzw. n über R. Genau dann haben f und g einen nicht trivialen Faktor, wenn* $\mathrm{Res}(f,g) = 0$ *ist.*

Wie sehr Matrizen- und Determinantentheorie noch in den Kinderschuhen steckte, als Sylvester seine Arbeit schrieb, zeigt das folgende Zitat (Sylvester 1840). Die

Koeffizienten der beiden Polynome heißen auch bei Sylvester a und b. Die Rollen von m und n sind aber vertauscht.

A Rule for absolutely eliminating x.

Form out of the (a) progression of coefficients m lines, and in like manner out of the (b) progression of coefficients form n lines in the following manner:

1. (a) Attach $(m-1)$ zeros all to the *right* of the terms in the (a) progression; next attach $(m-2)$ zeros to the right and carry over 1 to the left; next attach $(m-3)$ zeros to the right and carry over 2 to the left. Proceed in like manner until all the $(m-1)$ zeros are carried over to the left and none remain on the right.

The m lines thus formed are to be written under one another.

1. (b) Proceed in like manner to form n lines out of the (b) progression by scattering $(n-1)$ zeros between right and left.

2. If we write these n lines under the m lines last obtained, we shall have a solid square $(m+n)$ terms *deep* and $(m+n)$ terms *broad*.

3. Denote the lines of this square by arbitrary characters, which write down in vertical order and permute in every possible way, but separate the permutations that can be derived from one another by an even number of interchanges (effected between *contiguous* terms) from the rest; there will thus be half of one kind and half of another.

4. Now arrange the $(m+n)$ lines accordingly, so as to obtain

$$\tfrac{1}{2}\big\{(m+n)(m+n-1)\ldots 2.1\big\}$$

squares of one kind which shall be called positive squares, and an equal number of opposite kind which shall be called negative.

Draw diagonals in the same direction in all the squares; multiply the coefficients that stand in any diagonal line together; take the sum of the diagonal products of the *positive* squares, and the sum of the diagonal products of the *negative* squares; the difference between these two sums is the prime derivative of the zero degree, that is, the result of elimination between the two given equations reduced to its ultimate state of simplicity, there will be no irrelevant factors to reject, and no terms which mutually destroy.

Bemerkenswert finde ich auch, dass Sylvester die Zeilen seines Quadrates mit „irgendwelchen Charakteren“ indiziert, bemerkenswert deshalb, weil so mancher Autor darauf besteht, dass die Zeilen und Spalten einer Matrix mit $1, \ldots, m$, bzw., $1, \ldots, n$ zu nummerieren seien, was er dann sofort vergisst, wenn er Untermatrizen einer Matrix betrachtet. Für eine der Sache angemessene Indizierung einer gewissen $(n^2 \times n!)$-Matrix siehe der Leser Lüneburg 1989, S. 292 ff.

Wir wollen nun für zwei spezielle Polynome die Resultante auf eine andere Weise berechnen, nämlich für die Polynome

$$f := a_0 \prod_{i:=1}^{m} (x - u_i)$$